CST804: ETHICAL HACKING AND PENETRATION TESTING

AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

NATIONAL OPEN UNIVERSITY OF NIGERIA

Course Guide for CST804

Introduction

CST804 – Ethical Hacking and Penetration Testing is a 3-credit unit. The course is a core course in second semester. It will take you 15 weeks to complete the course. You are to spend 91 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination. The credit earned in this course is part of the requirement for graduation.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

Course Competencies

By the end of this course, you will gain competency in:

- Protecting Data at Rest and During Transmission
- Protecting System and Network Infrastructure
- Assessing Software Development Vulnerabilities

Course Objectives

The course objectives are to:

- Provide practical knowledge and skills for vulnerability assessment and penetration testing in order to discover weaknesses in applications and infrastructure
- Provide a solid knowledge of the main issues related to security in modern networked computer systems and IT infrastructure

Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study the intended learning outcome(s) before going to the main content and at the end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

Module 1: Overview of Hacking
Unit 1: Footprinting
Unit 2: Target Scanning
Unit 3: Covering of Tracks

Module 2: Targetted Attacks
Unit 1: Windows System
Unit 2: Linux System
Unit 3: Web Server and Web Applications

Module 3: Types of attacks
Unit 1: Trojans and Viruses
Unit 2: Social Engineering & Distributed Denial of Service
Unit 3: Spyware

Module 4: Penetration Testing
Unit 1: Security Audit
Unit 2: Vulnerability Assessment
Unit 3: Penetration testing roadmap
Unit 4: Penetration test plan

There are thirteen units in this course. Each unit represent a week of study.

Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

Table I: Weekly Activities

Week	**Activity**
1	Orientation and course guide
2	Module 1 Unit 1
3	Module 1 Unit 2
4	Module 1 Unit 3
5	Module 2 Unit 1
6	Module 2 Unit 2
7	Module 2 Unit 2
8	Module 3 Unit 1
9	Module 3 Unit 2
10	Module 3 Unit 3
11	Module 4 Unit 1
12	Module 4 Unit 2
13	Module 4 Units 3 and 4
14	Revision and response to questionnaire
15	Examination

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

Table 2: Required Minimum Hours of Study

S/N	Activity	Hour per Week	Hour per Semester
1	Synchronous Facilitation (Video Conferencing)	2	26
2	Asynchronous Facilitation (Read and respond to posts including facilitator's comment, self-study)	4	52
3	Assignments, mini-project, laboratory practical and portfolios	1	13
	Total	7	91

Assessment

Table 3 presents the mode you will be assessed.

Table 3: Assessment

S/N	**Method of Assessment**	**Score (%)**
1	Portfolios	10
2	Mini Projects with presentation	20
3	Laboratory Practical	20
4	Assignments	10
5	Final Examination	40
Total		100

Portfolio

A portfolio has been created for you tagged “**My Portfolio**”. With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

Application of Knowledge Gained

Module	Topic	Knowledge Gained	Application of Knowledge Gained

You may be required to present your portfolio to a constituted panel.

Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

Laboratory Practical

The laboratory practical may be virtual or face-to-face or both depending on the nature of the activity. You will receive further guidance from your facilitator.

Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be two hours of online real time contact per week making a total of 26 hours for thirteen weeks of study time.
- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

Course Information

Course Code:	CST 804
Course Title:	Ethical Hacking and Penetration Testing
Credit Unit:	3
Course Status:	
Course Blurb:	Focuses on penetration testing and vulnerability analysis. Introduces methodologies, techniques and tools to analyse and identify vulnerabilities in stand-alone and networked applications. An in-depth understanding of penetration (pen) testing and "ethical hacking", including requirements and reporting. Students will examine the business impact of testing. They will conduct security testing (including network and web application penetration testing) in the lab environment that includes: intelligence gathering, identifying and exploiting vulnerabilities, conducting post-exploitation exercises, and reporting results. Students will be required to create a comprehensive report summarising the findings, including recommendations to mitigate the risks identified. Topics will include social engineering, web application testing, managing a security test, and tools of attack.
Semester:	Second
Course Duration:	13 weeks
Required Hours for Study:	91

Course Team

Course Developer:	ACETEL
Course Writers:	Dr Abayomu Joshua Jegede and Dr Muhammed Aminu Ahmed
Content Editor:	Dr Ismaila Idris
Instructional Designers:	Inegbedion, Juliet O. (PhD) and Dr Lukuman Bello
Learning Technologists:	Dr Adewale Adesina and Mr Miracle David
Graphic Artist:	Mr Henry Udeh
Proofreader:	Mr Awe Olaniyan Joseph

Module 1: Overview of Hacking

Module Introduction

This module presents an overview of hacking and the techniques used by hackers. The module discusses how hacking activities such as footprinting, target scanning and covering of track on systems and networks. Also discussed are the techniques tools used to carry out these activities and ways by which you can protect your network against intrusions. The module consists of the following units.

Unit 1: Footprinting
Unit 2: Target Scanning
Unit 3: Covering of Tracks

Unit 1: Footprinting

Contents

1.0 Introduction

In this unit, you will acquire skills for gathering useful information about a target to be hacked. To achieve this, you will learn about the techniques and tools used to obtain information that will simplify the task of breaking into a target system or network.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe hacking and hackers
- highlight different types of hackers
- identify the phases in hacking
- describe and perform footprinting
- search for information.

3.0 Main Content

3.1 Introduction to Hacking

Hacking is the process by which a person attempts to gain unauthorised access into a computer or network. It involves the use of specialised tools and techniques to modify the computer to disclose information which would otherwise be accessible to only legitimate users. The tools and techniques used by hackers leverage the vulnerabilities inherent in computer hardware and software. The main goal of hacking is to violate the confidentiality, integrity and availability of computer and network resources. Hacking may result in unauthorised access, disclosure, disruption, modification, or destruction of these resources. Some of these resources include database, programs, memory, etc. Hacking may also be used to impersonate a legitimate user, say a bank's customer service executive and gain sensitive information such as bank account details and associated password or PIN from a customer.

You have heard about hacking since the beginning of this module. From what you have learnt about hacking, is it legal or illegal?

A hacker is someone who manipulates the computer or network to achieve unauthorised access, modification or destruction of data and information. Some of the factors that motivate hackers include. Hackers are motivated by factors such as profit, protest, enjoyment or the need to identify systems vulnerabilities. The success of the hacker or hacking depends largely on three major factors, namely

- the vulnerabilities (or weaknesses) in the target system or network
- the availability of hardware and software tools to exploit the vulnerabilities
- the knowledge or skills of the attacker.

3.1.1 Types of Hackers

Hackers are classified in terms of the actors and their motivation. There are seven main types of hackers as illustrated by By McAfee on Mar 16, 2011. Click on this link or here to read it.

- **White Hat Hackers:** These are the computer security experts who use penetration testing techniques to verify the security of an organisations systems and network. They use a wide array of tools, techniques and methodologies to combat the activities of malicious hackers.
- **Black Hat Hackers:** These are malicious hackers who attempt to secure unauthorised access to networks or computers or create computer viruses, worms or any other malicious codes. Black hat hackers leverage technologies and human to find the path of least resistance in a system or network. Black hat hackers are often referred to as "crackers", and their motivation is to achieve financial gain.
- **Script Kiddies:** These are black hat hackers who use downloaded programs known as scripts to attack networks. They usually engage in website defacement, and their motivation is to have fun.
- **Hacktivists:** This category of hackers are motivated by politics, religion, human right or the desire for revenge.
- **State-Sponsored Hackers:** Governments of different nations attempt to control cyberspace to achieve specific military and defence objectives. Governments fund state-sponsored hackers, and they have immense time, skills and resources to attack civilian, corporate, and governments systems.
- **Spy Hackers:** They are hired by corporations to infiltrate the networks of competitors and steal valuable information such as customer data, product design, and steal trade secrets. Spy hacking may occur in the form of internal or external attack.
- **Cyber Terrorists:** These groups are usually motivated by religious or political beliefs. They attack critical infrastructures such as nuclear system, transportation network and electricity distribution systems. They are the most dangerous, and their ultimate goal is to fear, chaos and commit murder.

3.1.2 Phases in Hacking

Hacking is usually not a one-step activity. But a process consisting of several phases. There are five phases in hacking.

- **Phase 1: Reconnaissance**

Reconnaissance or footprinting involves gathering preliminary data or intelligence on the target organization to enable a hacker plan for the attack.

- **Phase 2: Scanning**

The phase uses technical tools to gather more detailed intelligence on the systems and applications on the target organisation’s network. An example is the use of a vulnerability scanner to collect information on the weaknesses inherent in the target network.

- **Phase 3: Gaining Access**

In this phase, an attacker gains control of one or more network devices which he uses to obtain data from the target system or network. He may also use the device he controls to launch further attacks on other systems and networks.

- **Phase 4: Maintaining Access**

An attacker uses this phase to maintain his presence on the target network to gather as much information as possible. The attacker must remain stealthy to avoid detection.

- **Phase 5: Covering Tracks**

The final phase requires the attacker to take the necessary steps to remove all traces of his activities. The attacker uses this phase to return the system to its previous state to avoid detection by the administrators of the host network.

Figure 1 illustrates the phases of hacking (Canavan, 2001). The only thing omitted in the diagram is covering of tracks. It was assumed that it forms part of the access maintenance phase because a hacker must continue to remain unnoticed to maintain continuous access to the network.

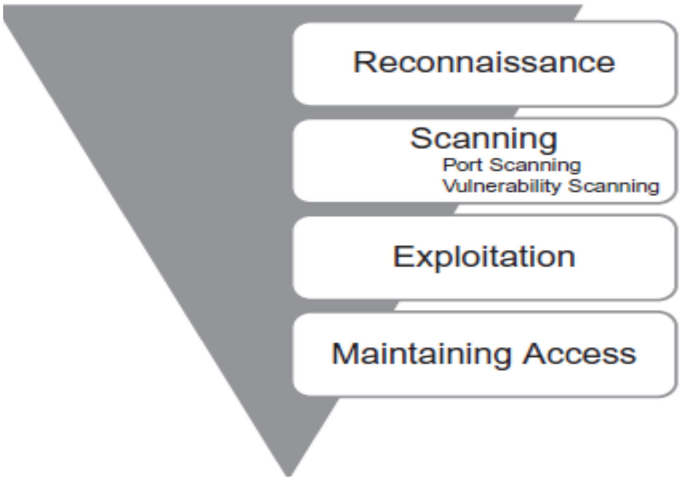

Fig. 1: Phases of Hacking

You will observe that the upper part of the inverted triangle is wider than the lower part. This shows that the phases proceed from the general to the specific. The earlier phases involve carrying out a wide array of activities on many targets and produces a large amount of information. The lower phases are more specific and focus on a few targets.

How do hackers obtain information about target organisations, systems and networks?

3.2 Footprinting

This is the process used to gather information about the target network in order to find the weaknesses that may be used to exploit the system (Engebretson, 2013). Footprinting involves profiling an organisation to collect information about the systems, network and people associated with to the organisation. An ethical hacker spends a lot of time gathering information about the target organisation’s computer systems and uses this information to penetrate the network. Footprinting enables an ethical hacker to know as much as possible about a system, its ports and services, security capabilities and whether it supports remote access. Businesses carry out footprinting to identify vulnerabilities so they can address them and make changes to the business policy.

Footprinting enables an ethical hacker to achieve the following purposes:

Know Security Posture: Hackers use data gathered during footprinting to know the security posture of the company such as the presence of a firewall, IDS/IPS, security configurations of applications etc.

Reduce Attack Surface: This enables hackers to identify and focus on a specific range of systems. This will significantly reduce the time and effort required for penetration testing.

Identify vulnerabilities: Footprinting enables hackers and security professionals to gain additional knowledge about the vulnerabilities and threats in the target network and the kinds of exploits that may be launched against it.

Draw Network map: It helps to map the networks in the target environment, including the topology, trusted routers, firewalls, and servers.

Hackers use footprinting to obtain information such as:

- Details about an organisation, employees and email addresses
- Relationship with other companies.

- Projects involving other companies.
- Legal documents of the company.
- News relating company website.
- Patents and Trademarks.
- Important dates about new projects

There are two jot categories of information gathering techniques:

1. Active information gathering
2. Passive information gathering

Active information gathering, a form of active attack (Stallings, 2011) occurs when a hacker directly engages a target by gathering information about open ports on a machine, the services that run on such ports and what operating systems they are using. Active information gathering techniques are not stealthy, as the victim easily detects them. These techniques are detected by the intrusion detection system (IDS), intrusion prevention system (IPS) and firewalls, which generate a log of their activities. Active information techniques are not recommended when an attacker wants to gather information covertly from systems and networks that are highly monitored.

Passive footprinting is a way of collecting information about a system remotely. This involves a situation where an attacker does not engage a target computer on the network directly. Instead, the attacker uses search engines, social media, and other websites to gather information about the target system or network. The method is suitable for covert information gathering as it does not generate logs of the activities of the hacker. An example is the use of Facebook, Twitter, LinkedIn, and other social networks to gather information about employees, their activities and interests. This is useful for carrying out keylogging, browser exploitation, phishing and other client-side attacks on employees.

3.2.1 Sources of Information Gathering

Hackers obtain relevant information about the target organisation from sources such as:

Social Media: Many people post personal information online. Some of this information is sensitive, and hackers can use it to launch attacks against unsuspecting social media users online. For example, hackers may create a fake account using stolen details of genuine individuals. These accounts may be used to defraud or obtain personal information from other social media users.

Job Websites: Job postings give details of available positions as well as personal and technical requirements. The technical requirements may contain information about the operating systems, network devices and hardware the organisation uses. It may also give a hacker an idea of the systems and network configuration of the organisation. Hackers can use this information to determine the vulnerabilities in the hardware and software which the organisation uses. They can also create a list of possible attacks that may be used to take advantage of the vulnerabilities.

Search Engines: Hackers use search engines such as Google to carry out detailed searches on an individual or devices. An attacker can use the right keywords on Google search to find relevant personal information such as an address, phone number, net worth, etc. about a target. A hacker can also use an approach known as Google hacking to combine basic search techniques with advanced operators such as "inurl:","allinurl:","filetype:", etc. to carry out devastating attacks. This method can be used to find internet enabled devices By typing a search string such as inurl:"ViewerFrame?Mode=" will help an attacker find public web cameras. "The "link:" search operator in Google can be used to obtain results only from specified sites. Google's advanced search features enable a hacker to find websites that are affiliated to the target. Affiliate websites belong to vendors, suppliers and clients and contain back-links to the victim's website.

It is possible to use switches to carry out a more in-depth search and gain access to files belonging to an organisation. To discover a specific file or word on the website of company XYZ, type the following line into Google

site www.xyz.com keyword
site www.xyz.com filename

It is also possible to download Flash .swf files that can be decompiled to obtain data belonging to company XYZ. PDF files containing sensitive data are also accessible using this technique.

File: swf XYZ
Filetype: pdf XYZ confidential

Google Groups
Google Groups contain a wide array of publicly available personal information, such as domain names, IP addresses and usernames. Members share a lot of information on Google Groups, and some of this information may relate to a system and network security.

Social Engineering: This approach uses various forms of human interaction to obtain information from targets of attack. Examples of social engineering techniques are:

- **Eavesdropping:** An attacker uses this to record a personal conversation between the target victim and other people, usually over communication mediums like telephone.
- **Shoulder Surfing:** In this case, an attacker looks over the victim's shoulder while he (the victim) is typing sensitive personal information such as Email address, password, ATM PIN, etc.
- **Phishing:** Attackers create fake websites or webpages similar to genuine ones. They use this method to obtain personal information by tricking unsuspecting victims to create accounts and log onto malicious sites. This method is used to obtain personal data such as email-id and passwords of social media accounts.

Organisation's Website: Organisations use their websites to share information with clients, customers, or the general public. This is the best place to begin for an attacker who wants to gain access to know about products and service offerings as well as personal details of names, ranks, email addresses and telephone numbers of key personnel.

Older versions of websites are available in an archival form and are stored in a website known as archive.org. The archived versions are snapshots of all websites that are collected at regular intervals. Archived.com provides hackers with access to website information and features that might have changed over time.

Web Crawling

Web crawling involves mirroring a website and downloading all the publicly accessible files from the website. This allows a hacker to scan the target website offline. An attacker can use the saved website to uncover information about the configuration and layout of the website, files and directories, the source code for the web pages, names and addresses of IT employees and comments about the workings of code.

Using NeoTrace: NeoTrace is a powerful tool that provides path information between a source and a remote site. The tool can produce a graphical display of the route between an attacker and the remote site. The tool also uses a GUI to display information on all intermediate nodes, including IP address, contact information, and location

Who is: Hackers use the Whois website to obtain information about the domain name, email-id and domain owner. It is a tool for Website Footprinting; that is, it enables a hacker to trace a website.

Does footprinting have any benefit? If so, what are the benefits?

3.2.2 Advantages of Footprinting

- Hackers use footprinting to know the basic security configurations of a target machine or network. It also provides information about network route and data flow.
- It simplifies the hacking process. A hacker who finds vulnerabilities can focus on specific attacks that can be launched against the target machine.
- It reduces the attacks surface. It allows the hacker to identify which machines are most vulnerable and can be attacked easily.

How can you protect your network infrastructure from footprinting?

3.2.3 Countermeasures against Footprinting

- Do not post sensitive personal data on social media websites.
- Be careful when accepting friend requests on social media platforms.
- Provide internet users with security education on various tricks used by hackers.
- Use footprinting techniques to identify and remove sensitive information from social media platforms.
- Ensure proper configuration of webservers to prevent the loss of configuration data.

Can you summarise what you have learned so far?

Discussion

Social media sites like Facebook, Twitter, Instagram and LinkedIn contain photographs, names, sex, dates of birth and phone numbers and other personal details of people. Click on the profiles of your friends and other people. Which personal information can you find about them? In which ways do you think hackers can use this information to attack social media users?

Case Studies

Real-life Scenario

Stuxnet Attack on Iranian Nuclear Systems

Stuxnet was believed to have gained access to the Natanz nuclear plant via an infected memory device (USB stick). It was highly probable that an individual would have inserted the USB into one of the computers on the nuclear plant's network. The worm then became automatically installed on infected computer system.

Stuxnet spread through the plant's network quickly, looking for computers that control centrifuges. Once it infected the computer system, it searched for software that controlled the centrifuges. Centrifuges are machines which separates nuclear materials into different components by spinning them at high speeds. The operators in Natanz plant used the centrifuges to separate different types of uranium and isolate the component (called 'enriched uranium') that is used as the raw material for both nuclear power and nuclear weapons.

The attack reprogrammed hundreds of centrifuges and caused them to spin out of control. This was achieved when the Stuxnet worm identified and penetrated the controlling software. The exploit was carried out in two separate ways. First, it increased the speed at which the centrifuges operate to an extremely high and dangerous levels for about 15 minutes, and then returned to normal speed. The speed of operation was reduced to about 50 minutes about a month later. This sequence of manipulated operations was repeated for several months.

The severity of the attack created the need for the replacement of about 1,000 fuel enrichment centrifuges. The extremely high speeds of operation led to the disintegration of the infected machines. Overall, about 20 per cent of the centrifuges was decommissioned as a result of this exploit.

Can you identify the methods used to perform footprinting?

Can a system or network not connected to the Internet suffer malware attack?

4.0 Self-Assessment Exercise(s)

1. Which of the following describes hacking? Choose all that apply
   A. A process by which a legitimate user accesses the system.
   B. A process by which an intruder gains unauthorized access to a system or network.
   C. The use of specialized tools and techniques to compromise hardware and software.
   D. The act of breaking a bank's strong room to steal money.
   Correct Answer: B, C
2. Hackers who attempt to gain unauthorized access in order to achieve financial gain are referred to as:
   A. White hat hackers
   B. Black hat hackers

C. Hacktivists

D. Script kiddies

Correct Answer: B

3. Which of the following represents the correct sequence of a hacking process?

A. Reconnaissance -> Gaining Access -> Maintaining Access -> Scanning -> Covering Tracks

B. Scanning -> Gaining Access -> Reconnaissance -> Maintaining Access -> Covering Tracks

C. Reconnaissance -> Scanning -> Gaining Access -> Covering Tracks -> Maintaining Access

D. Reconnaissance -> Scanning -> Gaining Access -> Maintaining Access -> Covering Tracks

Correct Answer: D

4. Footprinting enables a hacker to achieve the following purposes except

A. Determine the presence of firewall, IDS/IPS and security configurations of applications.

B. Identify and focus on a specific range of systems.

C. Know the actual amount of time and resources required for hacking

D. Identify the weaknesses and threats in systems, networks and applications

Correct Answer: C

5. Which footprinting technique would you use to identify open ports and services on a network?

A. Passive footprinting

B. Ping

C. Active fooprinting

D. Social media exploitation

E. Covering Tracks

Correct Answer: C

6. Which of the following are countermeasures against footprinting? Choose all that apply

A. Do not post sensitive personal data on social media websites.

B. Be careful when accepting friend requests on social media platforms.

C. Provide internet users with security education on various tricks used by hackers.

D. Do not connect your computer to the Internet.

Correct Answer: A,B,C

Mini project

A hacker can do people search on websites containing information about organisations and their employees. Search the following websites and discuss your findings.

1. yahoo finance (click here to access the website)
2. Nigeria securities and exchange commission (click here to access the website)
3. The United States patent and trademark office (click here to access the website)
4. LexisNexis Risk Solutions (click here to access the website)

Enter the names and addresses of some people and organisations you know. Record as many as possible personal and corporate information you can gather on the people and organisations. You can screenshot your findings then submit to your tutor.

5.0 Conclusion

A hacker needs to obtain relevant information about a target organisation in order to penetrate the system. The information is used to determine the range of systems in the organisation’s network, the security infrastructures, architecture and configuration of the organisation, and the vulnerabilities inherent in the devices and application on the network.

6.0 Summary

In this unit, you have learnt about footprinting, the purpose of footprinting, sources of information, and types of information gathering techniques. You have also learned the advantages of footprinting and ways to prevent footprinting.

7.0 References/Further Reading

Seven Types of Hacker Motivations. Available here

Ryan (n.d.). *Summarising The Five Phases of Penetration Testing.* Available here

Canavan, J.E. (2001) *Fundamentals of Network Security*. London: Artech House.

What is Footprinting? Available here

Stallings, W. (2011) Cryptography and Network Security Principles and Practice. New York: Prentice-Hall.

Helba, S. (2010). Ethical Hacking and Countermeasures: Threats and Defence Mechanisms. New York: Cengage Learning.

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing*. 2nd ed.)., Elsevier.

Hall, G. & Watson, E. (2016). Hacking, Computer Security Testing, Penetration Testing and Basic Security.

Forouzan, B.A. & Fegan, S.C. (2007). Data Communications and Networking. McGraw-Hill

Unit 2: Target Scanning

Contents

1.0 Introduction

In this unit, you will acquire the skills for identifying vulnerabilities and threats in the target network. To achieve this, you will learn about the tools and techniques for discovering active hosts, ports, and services, as well as operating system and architecture of the target environment.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define scanning
- perform various types of scanning
- identify and use the scanning tools
- discuss the phases of scanning.

3.0 Main Content

3.1 Scanning: Definition and Purpose

Scanning refers to the use of complex and aggressive reconnaissance techniques to identify live hosts, ports, and services, as well as operating system and architecture of a target system (Helba, 2010). This enables the hacker to know the vulnerabilities and threats inherent in the network.

This methodology involves two main activities:

- **Check for Live Systems:** This is achieved by using ping scan to send ICMP echo request packets to discover systems that are active on the network. Any active system responds with ICMP echo reply packet containing details such as packet size, Time-to-Live (TTL), packet size etc.

- **Check for Open Ports:** This helps the hacker to discover open ports, services running on them, their versions etc. NetScan Tools Pro and Nmap are powerful tools used mainly for this purpose. An ethical hacker uses a network analyzer, such as Wireshark to monitor network traffic on open ports.

There are three major types of scanning used in ethical hacking (Hall and Watson, 2016):

- Port scanning
- Network scanning
- Vulnerability scanning

3.1.1 Phases in Scanning

The phases an ethical hacker goes thorough in carrying out scanning on a network are presented as follows:

Detect Live Systems -> Look for Open Ports -> Find out the running services -> Identify the Operating System (OS Footprinting) -> Scan Vulnerabilities -> Document details and draw Network diagram -> Prepare Proxies to avoid being caught -> Proceed with Exploitation.

How does a pair of computers or devices establish communication?

3.1.2 TCP/IP Handshake

A knowledge of 3-way TCP/IP is a prerequisite to understanding the way scanning works. Handshaking is the automated process used to set up the parameters which manage the channel of communication between two entities, based on some communication protocols (Forouzan and Fegan, 2007). A client and a server use Transmission Control Protocol (TCP) and Internet Protocol (IP) for handshaking. The client sends an SYN (synchronisation) packet to indicate that it wishes to establish a connection. If the server is available, it responds with an SYN/ACK packet to the client. The client sends an ACK packet to the server to indicate the receipt of the message from the server. An SYN (denotes synchronise) is used to initialise connections between the client and the server. ACK (denotes acknowledgement) is used to establish a connection between two hosts.

In Figure 2, Computer A, sends an SYN packet, to indicate that it wishes to connect with Computer B. The Computer B confirms its readiness for communication by sending an SYN+ACK. Finally, Computer A sends an ACK packet to acknowledge B’s reply, and thus the connection is established.

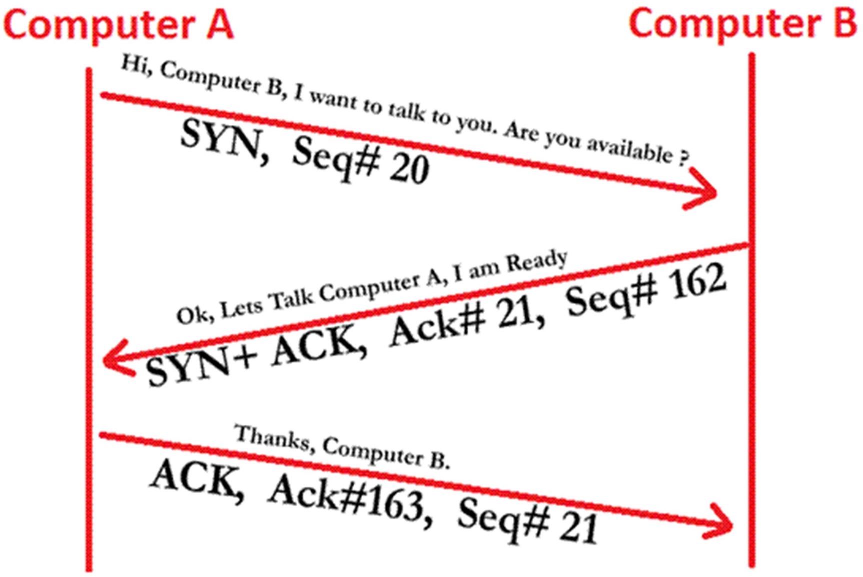
Computer A
Computer B
Hi, Computer B, I want to talk to you. Are you available ?
SYN, Seq# 20
Ok, Lets Talk Computer A, I am Ready
SYN+ ACK, Ack# 21, Seq# 162
Thanks, Computer B.
ACK, Ack#163, Seq# 21

Fig. 2: TCP/IP Handshake

These handshaking processes are crucial to the establishment of a remote connection between a hacker’s computer and victims’ machines. Watch this video on TCP/IP handshake for a better understanding of the steps and processes that a pair of devices used to establish a connection before communicating with each other.

3.2 Port Scanning

Port Scanning is used to discover open ports on the network and the services that run on such ports. This process involves sending client requests to the range of ports on the target network and saving the details about the ports that respond to the requests. The ports are assigned values, and each value references a specific port. There are three types of ports:

1. Well known Ports: assigned numbers ranging from 0 to 1023
2. Registered ports: assigned numbers ranging from 1024 to 49151
3. Dynamic Ports: assigned numbers ranging from 49152 to 65535

You can use the following path: C:\Windows\System32\Drivers\etc\services to access common or well-known ports in a Windows system.

Table 1 contains a list of some common port numbers:

Table1: Common Port Numbers

Port Number	**Service**
20 and 21	FTP
23	Telnet
25	SMTP
80	HTTP
443	HTTPS
110	POP3
500	IPSec;
53	DNS

3.2.1 Types of Port Scan

There are various types of port scan:

- Connect scan**:** Establishes a TCP handshake with the target to identify open ports. Fig 3 depicts how to connect scan occurs between two computers.

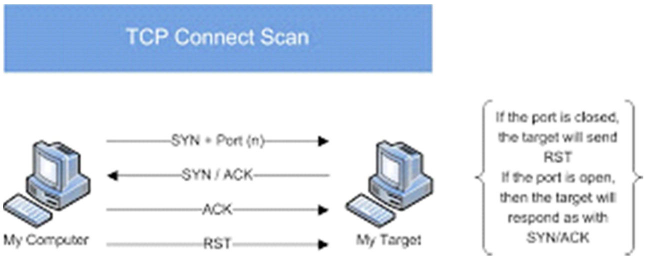
TCP Connect Scan
SYN + Port (n)
SYN / ACK
ACK
RST
My Computer
My Target
If the port is closed, the target will send RST
If the port is open, then the target will respond as with SYN/ACK

Fig. 3: Connect Scan

- **Half-open scan:** Performs a stealthy scan on a target by setting up an incomplete TCP handshake. This results in an abrupt reset of the communication. Figure 4 illustrates how a half-open scan occurs between two parties.

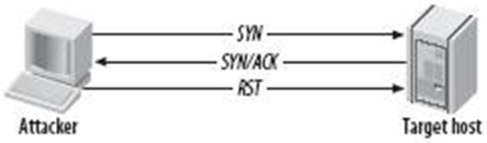

Fig. 4: Half-Open Scan

- **XMAS scan:** Known as inverse TCP scanning. It sends packets set with PSH, URG, FIN flags. Machines with open ports do not respond to XMAS scan. However, a reset (RST) response is sent if ports are closed. Figure 5 depicts the operation of Xmas scan.

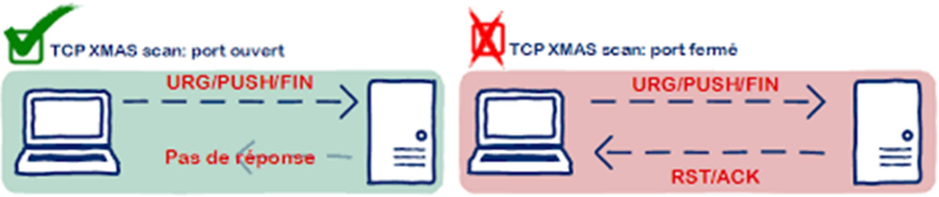

Fig. 5: XMAS Scan

- **FIN scan:** Works by setting the FIN flag in the TCP packets sent to the target. The FIN flag indicates an end to data communication and terminates a TCP/IP connection. Open ports on a target who receives a FIN scan on do not send a response, while closed ports responds with a reset. Figure 6 illustrates the fin scan.

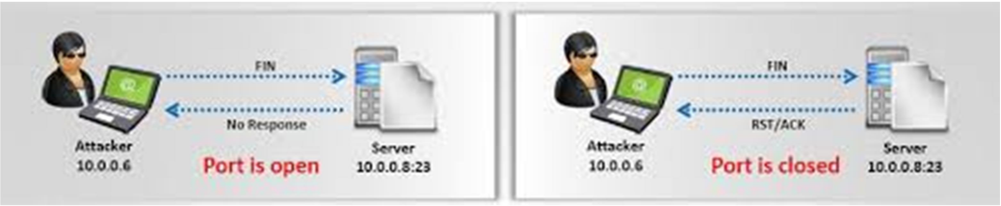

Fig. 6: FIN Scan

ACK scan: Here, the attacker first sets the ACK flag in the TCP header and then uses window size and TTL value of RESET packets to obtain the status of the ports on the target machine. Ack scan mode of operation is presented in Figure 7 below

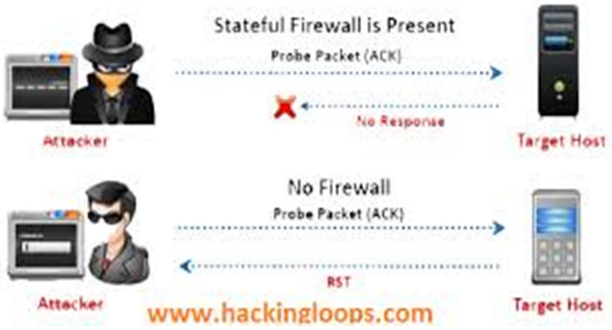

Fig. 7: ACK Scan

Null Scan: Here, an attacker sends TCP packets with no flags set to the target. No response is received from open ports, while closed ports respond with a RESET packet.

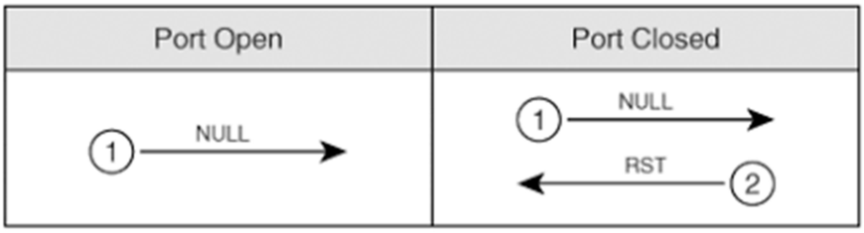

Fig. 8: Null Scan

Idle Scan: Attacker uses this technique to mask his identity on an idle machine to probe the status details of target ports.

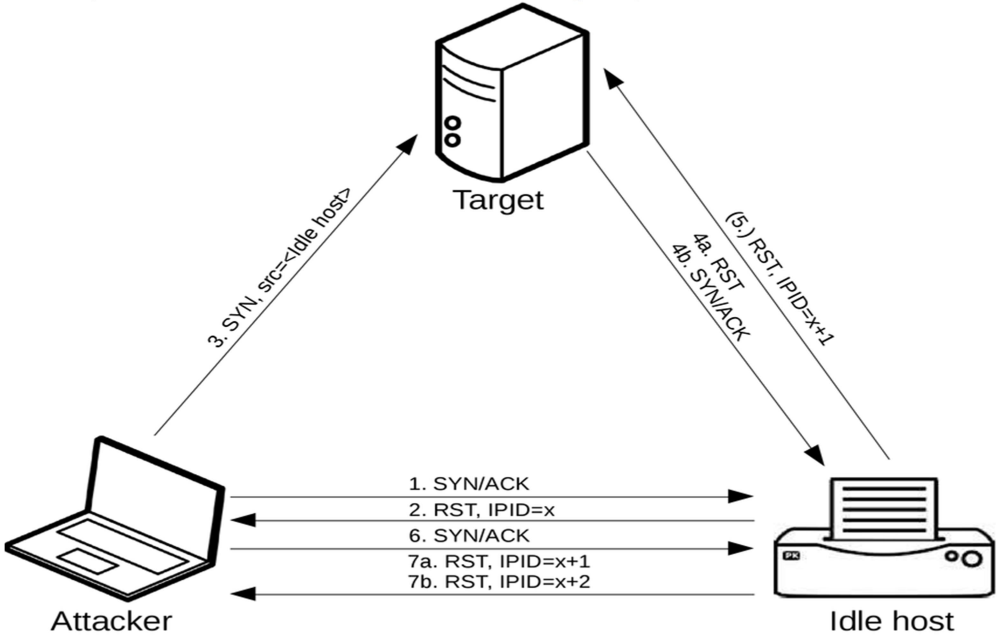

Fig. 9: Idle Scan

3.2.2 Tools for Scanning

A set of tools are used to carry out port scanning. One of such is NMAP. NMAP is a very popular tool used for port scanning. It is available for Windows command-line interface (CLI) as Nmap, and for the graphical user interface as (GUI) as Zenmap.

Click this link for a video on practical demonstration of scan types and options using Nmap.

Other tools for port scanning are:

- MegaPing, CurrPorts, Advanced Port Scanner, SoftPerfect Network Scanner, Net Tools, PRTG Network Monitor, Network Inventory Explorer, etc. These are famous for PCs
- Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Panm IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc – Commonly used in mobile device.
- Various scanners freely available and inbuilt in Kali Linux OS.

After download, you can easily install Nmap. This screen will appear once the installation is complete. You need to specify the target IP address or a range of IP addresses, and the type of scan you want to perform under "Profile".

Zenmap provides you with a GUI where you can enter details such as the target IP address or a range of IP addresses, and the type of scan you want to perform. It also provides command-line equivalent as you can directly copy the syntax or command from the GUI and run it on CLI.

Table 2 lists common port scans and their Nmap syntax

Table 2: Common Port Scans and Nmap Syntax

Scan Type	**Nmap command**
Connect scan	nmap -sT -v -p- <TargetIP>
Half open scan	nmap -sS -v <TargetIp>
FIN Scan	nmap -SF <targetIp>
ACK Scan	nmap -SA -v <targetip>
Null Scan	nmap -sN -p- <targetIP>
Idle scan	nmap -Pn -sI ZombieIp TargetIp
Intense scan	nmap -T4 -A -v <targetIP>
Intense scan, all TCP Ports	nmap -p 1-65535 -T4 -A -v <targetIP>

An intense scan is a very detailed, comprehensive scan and takes much longer time than other types of scan. For example, intense scan on all TCP ports of a machine with IP address 192.168.12.131 can be done using the following Nmap command.

```
nmap -p 1-65535 -T4 -A -v 192.168.12.131
```

To scan a selected port, use the command

```
nmap -T4 -A -v 192.168.12.131
```

To find the operating system of a host, use the ‘O’ switch, as shown in the following command.

```
nmap -O 192.168.12.131
```

To Scan multiple IP addresses or subnet (IPv4)

```
nmap 192.168.1.1/24
```

To scan a range of IP address:

```
nmap 192.168.1.1-20
```

It is also possible for nmap to read IP addresses from a file. The -iL option is used to achieve this. This is illustrated using the following example:

Create a file using the following command:

```
cat > /temp/test_ips.txt
```

Sample outputs:

```
server1.domain1.com
192.168.1.0/24
192.168.1.1/24
```

Use the following syntax to run the:

```
nmap -iL /temp/test_ips.txt
```

You may exclude some hosts from a scan if you do not want to access the full network. Use the following syntax:

```
nmap 192.168.2.0/24 –exclude 192.168.2.10
nmap 192.168.2.0/24 –exclude 192.168.2.10,192.168.2.234
```

To find if a machine or network is protected by a firewall:

```
nmap -sA 192.168.2.25
nmap -sA server1.domain1.com
```

To scan a device even if it is protected by the firewall

```
nmap -PN 192.168.2.25
nmap -PN server1.domain1.com
```

The option -6 is used if you want to scan IPv6 addresses.

```
nmap -6 server1.domain1.com
nmap -6 2302:f0e0:1001:41::3
```

Use the following syntax if you want to access only open ports

```
nmap –open 192.168.1.5
nmap –open server1.domain1.com
```

To see the target interfaces and routes

```
nmap –iflist < IP Address of target>
nmap –iflist 192.168.12.131
```

The MAC addresses and interface routes are hidden for security purposes, but you can see all the details if you perform the scan in a secure environment such as a lab.

To scan for specific ports

```
nmap -p [port] Target name or IP address
```

For example, nmap -p 80 192.168.12.131. This GUI shows that the machine runs HTTP service on port 80.

3.2.3 Banner Grabbing

Banner grabbing is a technique used to collect information about the operating system, running services and version numbers details, etc. There are two main types of banner grabbing:

- Active Banner Grabbing: Here, an attacker sends packets to the target to retrieve information about OS. Such information may be its name, version, running services, etc.

- Passive Banner Grabbing: Operating systems related errors can reveal the type of OS running on the machine. For example, If you get some error related to Internet Information Server (IIS), you will know that the Windows web server is running the IIS OS.

Ports 80, 21, and 25 are examples of service ports used for banner grabbing. Services running on ports 80, 21, and 25 are those used by HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol) respectively. Netcat is the most commonly used tool for banner grabbing. Other suitable tools for banner grabbing are Telnet, Nmap and ZMap. Netcat uses TCP or UDP protocol to read and write data to and from various sources and destinations on the network. Netcat can also be used for creating a backdoor, chat, and port scanning. Netcat is available for Windows and Linux operating systems.

Netcat command: nc [options] [Target IP] [Port (s)

For example, you can could use Netcat to establish a connection to a victim's web server whose URL is www.victimhost.com, and then send an HTTP request. You will obtain a response from the server with details of the service running on the host:

```
[root@prober]# nc www.victimhost.com 80

HEAD / HTTP/1.1
HTTP/1.1 200 OK
Date: Mon, 10 Aug 2019 22:10:40 EST
Server: Apache/2.0.46 (Unix)  (Red Hat/Linux)
Last-Modified: Thu, 16 Jul 2019 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

An attacker can also use this information to get a narrow view of possible exploits he can launch against the target. It is also possible to use Netcat for banner grabbing attacks against web servers by connecting to port 80 and then sending a **HEAD / HTTP/1.0** or **HEAD / HTTP/1.1** request depending on the protocol which runs on the servers.

The following steps can be used to protect against banner grabbing attacks.

- Use false banners to confuse the attacker
- Disable unnecessary services
- Used IIS Lockdown Tool or Server Mask if you are using IIS.

When you come across the word "network scanning", what comes to your mind?

3.3 Network Scanning

Network scanning is one of the methods of intelligence gathering. It is a mechanism for information retrieval used by an attacker to identify active hosts, ports and the services used by the target application on a network (Hutchens, 2014). This technique is mainly used to find an IP address in the network of the target. An ethical hacker uses this approach to identify the vulnerabilities in the system before a malicious hacker can use the same weaknesses to exploit the network. This can be done using tools or scripts to probe all IP addresses on the network and obtain a list of the active nodes and their IP addresses.

What seems to be the reason why hackers perform network scanning?

Objectives of Network Scanning

- To detect active hosts/computer, IP address and open ports.
- To detect services that are running on a device.
- To identify the operating system and architecture of the target system or network.
- To identify and address vulnerabilities in active hosts.

3.3.1. Nmap for Network Scanning

Nmap is a free and open-source tool for network scanning.You can download Nmap here. You can scan a network with Nmap either by using the IP address of the target:

```
$ nmap 172.16.254.1
```

Or using the hostname

```
$ nmap www.example.com
```

It is illegal to scan the network without authorisation by the owner of the network. However, you can use the Nmap Organisation Website to practice scanning using Nmap.

You can use Nmap to display open ports on the network. The option '**v**' is used to obtain a verbose (detailed) output and option '**A**' is to identify the operating system. You can use many options to make Nmap tool produce different kinds of results. The Nmap tutorial provides further information on the usage and options of Nmap. See the video of network scanning using Nmap. It shows the procedures and commands for carrying out network scanning using Nmap.

3.3.2 Nikto for Network Scanning

Nikto is a tool primarily developed for scanning web server as quickly as possible. The purpose of the scan is to detect dangerous files and outdated service software. An attacker can use this information to launch exploits against a network. To use Nikto, open the terminal and run the following command:

```
$ nikito -host scanme.nmap.org
```

The result of the scan reveals the vulnerabilities in the network or application being scanned. You can choose relevant exploits once you know the weaknesses of the network.

3.3.3 Nessus for Network Scanning

Nessus is one of the most potent tools for vulnerability scannin. You can install it using the following steps.

Open a browser to download Nessus. Click on "**Get Activation Code**". You will have the option to choose between the two versions of Nessus: Nessus Home (a free version) and a paid version. Choose the free version, and click on the "**Register Now**" button under "**Nessus Home**".

Enter your first name, last name, and email address. You will receive a link via your address. A click on the link will redirect you to the download page. You can download a suitable file, such as **.deb** file for **AMD64**, which is compatible with the Kali Linux operating system. At the end of the download, install Nesses using the following command:

```
$ cd Downloads
$ dpkg -I Nessus-8.3.0-ubuntu910_amd64.deb
```

Nessus will be installed, and now you will have to start the Nessus service to use it. Use the following command to start the Nessus application:

```
$ /etc.init.d/nessusd start
```

Once the service starts, open a web browser, go to //kali:8834/ and create an account.

Enter a username and a password. Enter the activation code (that was sent to your Email Id) in the next page. Nessus will download the necessary plugins after successful activation.

To scan a network, click on "**New Scan**" on the top right corner. This will show you different types of scans that Nessus provides. Enter the name for your scan, description, folder, and the target and click on "**Save**". At the end of the scan, you can view the vulnerability report under the "**Vulnerabilities**" tab.

Click on this link for a video of a simulation of scanning using nessus. The video provides a practical demonstration of the use of Nessus to detect open ports on the network.

3.4 Vulnerability Scanning

Vulnerability scanning is the proactive and automated identification of vulnerabilities in a system or network. Pen-testers use this technique to detect the likelihood of network security attacks. Vulnerability scanning identifies weaknesses due to application programming errors or network misconfiguration. The can technique to detect weaknesses such as unnecessary services, missing updates, weak authentication or weak encryption algorithm. You should compile a list of vulnerabilities found during scanning. Note that vulnerability scanning requires an internet connection and the use of automated tools.

What are the tools for vulnerability scanning?
How can you use these tools?

3.4.1 Tools and Steps Used for Vulnerability Scanning

You can perform manual ICMP (Internet Control Message Protocol) scanning by following the following steps:

- Open Windows OS
- Press Win+R (Run) buttons in combination
- In the Run, type- cmd
- Type the command: ping IP Address or type: ping DomainName

Ping

Ping works by sending an ICMP echo request to the target's domain name or IP address. The target will respond with an ICMP Reply if it is active. This will also help a hacker to know if ICMP request can bypass a firewall. Most organisations block ICMP requests to prevent attacks. See Figure 9 for an illustration of the ICMP probe.

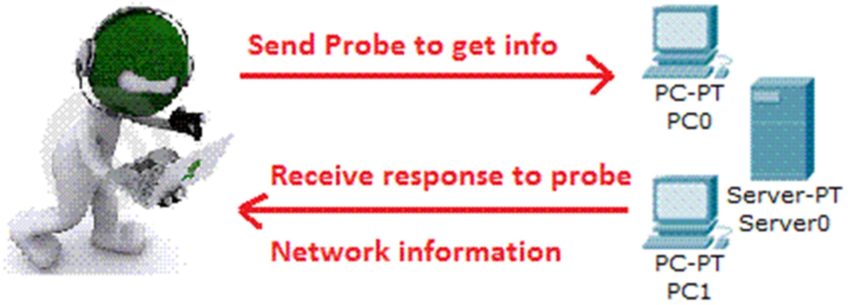

Fig. 10: ICMP Probe

There is a popular tool used to perform ping scanning, can you identify this tool?

Nessus is a popular tool for ping scanning. It is also a powerful tool which can identify many gives vulnerabilities on the target. The tool helps in data collection, identification of live hosts, port scanning and preparation of vulnerability of report.

Nessus can detect vulnerabilities in databases and provides a brief description of each vulnerability. It can also reveal the risk level or severity of the vulnerabilities. Click on this link for a video of a simulation of vulnerability scanning using Nessus. The video provides a practical demonstration of the use of Nessus to detect weaknesses that a hacker can use to exploit a network.

Another important tool for vulnerability scanning is GFI LAN guard. The tool is used for network inventory and vulnerabilities on the nodes or servers.

Nmap also provides a large number of scripts for vulnerability scanning (Hutchens, 2014). This video (here) shows network scanning of a vulnerable test server using Nmap. Other popular tools for network vulnerability scanning are Retina CS, Qualys Guard, Nexpose, Open VAS etc.

3.4.2 Countermeasures against Vulnerability Scanning

- Configure firewalls and IDS to detect and block intrusions.
- Disable ICMP based scanning at the firewall
- Do not keep unnecessary ports open
- Use custom rules to secure the network and disable unnecessary ports.
- Run port scanning tools to determine whether the firewall accurately detects the port scanning activities.
- Configure anti-scanners and anti-spoofing rules properly.
- Use necessary firewall rules to control access to ports.
- Avoid using public servers to store sensitive data
- Update IDS, routers, and firewall firmware with the latest patches.

What have you learned so far in this unit?

Discussion

Many authors have claimed that TCP/IP handshaking is crucial to target scanning. Do you agree with this?

Hackers place a lot of emphasis on knowing the operating system, running services and version numbers details when attempting to conduct target scanning on an organisation. In which ways can this information be useful for hacking?

Kali Linux virtual machine provides the environment and resources for practising target scanning. Nmap is one of the major tools used for port scanning.

Download and install Kali Linux OS virtual machine on your computer.
Download and install Nmap.

Run the various Nmap commands on the Nmap website. What are your findings?

Case Studies

Netsparker: A vulnerability scanner used by ISACA

The security team at the Information Systems Audit and Control Association (ISACA) security team chose Netsparker Web Application Security Scanner after testing many tools. Netsparker scanner was used to support the information security efforts and assisted in meeting web security requirements.

The team chose Netsparker because of the following reasons:

- It provides a clear definition and explanation of impending vulnerabilities;
- It helps to assess vulnerability at different phase of application development.
- It provides a means for customization, scanning and automation of activities;
- It is easy to use.

Feedback from the senior management of the ISACA security team demonstrated that: "Netsparker was able to further define and explain the specific issues at hand. It was also able to assist in the proof of concept for vulnerability assessments during development."

"It is very easy to use, thus allowed everyone in our team to cooperate. Of course, the ability to customise, scan, and automate the tasks was a big plus. Netsparker helped us identify the areas to remediate before we migrated new code into the production environment."

“Netsparker has been an integral part of ISACA's development life cycle and has been used to scan website changes and new web applications, both on their staging server and development environment.”

Chris Evans, Security and Compliance Manager at ISACA wrote:
“As we are faced with perpetual evolving security threats and vulnerabilities, Netsparker brings a level of assurance to our business as it is included as part of our development lifecycle to help identify and mitigate such threats before deployment. With Netsparker, being able to provide zero false positives, it ensures that time is not wasted deciphering whether a vulnerability is legitimate or not."

Identify the tools and techniques used for vulnerability scanning.

Why is it necessary for security professionals to perform regular vulnerability assessment on their systems and networks?

4.0 Self-Assessment Exercise(s)

1. ---------- refers to the use of complex and aggressive reconnaissance techniques to identify live hosts, ports, and services, as well as operating system and architecture of a target system.
   A. Service detection
   B. Scanning
   C. Open port checking
   D. Active system detection
   Correct Answer: B
2. The following are major types of scanning used in ethical hacking except
   A. Port scanning
   B. Network scanning
   C. Vulnerability scanning
   D. System scanning
   Correct Answer: D
3. Which of the following techniques performs a stealthy scan on a target by setting up an incomplete TCP handshake?
   A. XMAS scan
   B. FIN scan
   C. Half open scan
   D. TCP scan
   Correct Answer: C
4. Which of the following Nmap command is used for Connect Scan?
   A. nmap -sT -v -p- <TargetIP>
   B. nmap -sS -v <TargetIP>
   C. nmap -SF <targetIP>
   D. nmap -SA -v <targetIP>
   Correct Answer: A
5. ------------ is a technique used to collect information about the operating system, running services and version numbers details
   A. Operating system detection
   B. System parameter verification
   C. Banner grabbing
   D. Operating system analysis
   Correct Answer: C
6. The following are objectives of network scanning except:
   A. To detect active hosts/computer, IP address and open ports.
   B. To detect services that are running on a device.
   C. To identify the registered users on the network.
   D. To identify and address vulnerabilities in active hosts
   Correct Answer: C

7. Which of the following tools is suitable for both network scanning and vulnerability scanning? Choose all that apply
   A. Nessus
   B. Nikkito
   C. Nmap
   D. Ping

   Correct Answer: A,B,D

Portfolio
Kali Linux virtual machine provides the environment and resources for practising target scanning. Nmap is one of the major tools used for port scanning. Perform the following tasks to demonstrate the Nmap scan:

1. Download and install Kali Linux OS virtual machine on your computer.
2. Download and install Nmap (though Nmap is pre-installed on Linux OS).
3. Run the various Nmap commands on the Nmap website.
4. Document your findings and submit it to your tutor.

5.0 Conclusion

Hackers and security professionals use target scanning to access the security of systems, networks and application. They use complex and powerful tools and techniques to discover active hosts, ports, and services, as well as operating system and architecture of the target environment. This enables them to identify the vulnerabilities, threats as well as a variety of attacks that can be used to exploit devices in the target environment.

6.0 Summary

In this unit, you have learned the procedures, tools and techniques for discovering active hosts, ports, and services, as well as operating system and architecture of a target environment. This knowledge will enable you to identify vulnerabilities and threats in a target network. You will also be able to determine the range of attacks you can launch against the systems and applications in the target environment.

7.0 References/Further Reading

Allen, L., Heriyanto, T. & Ali, S. (2014). *Kali Linux – Assuring Security by Penetration Testing*. UK: Packt Publishing Ltd.

Canavan, J.E. (2001) *Fundamentals of Network Security.* London: Artech House.

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing*. (2nd ed.) Elsevier.

Hall, G. & Watson, E. (2016). *Hacking, Computer Security Testing, Penetration Testing and Basic Security*. Available here

Helba, S. (2010)*. Ethical Hacking and Countermeasures: Threats and Defence Mechanisms.* New York: Cengage Learning.

Hutchens, J. (2014). *Kali Linux Network Scanning Cookbook*. UK: Packt Publishing Ltd.,.

Ryan (n.d.). *Summarising The Five Phases of Penetration Testing*. Available here

Stallings, W. (2011). Cryptography and Network Security Principles and Practice. New York: Prentice Hall.

Unit 3: Covering of Tracks

Contents

1.0 Introduction

In this unit, you will acquire the skills required to avoid detection after carrying out penetration testing activities. To achieve this, you will learn the methods, tools and techniques hackers and penetration testers use to eliminate traces of their activities on systems, networks and applications.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain covering tracks
- disable auditing
- clear logs
- modify logs and registry files
- cover track on the network.

3.0 Main Content

How do hackers evade detection after pen-testing activities?

Covering tracks is the final stage of a hacking process. Its goal is to erase electronic traces of the activities of the hacker on the targeted computer system or network. The process consists of a set of anti-incident response measures (that is, activities for the prevention of real-time detection) and anti-forensics measures (for the prevention of digital evidence collection) during a post-incident investigation. At the end of the hacking process, the attacker will want to erase digital footprints that may be used to trace his activities on the network. A hacker carries out the following activities to prevent investigators from tracing him:

- Disable auditing.
- Clearing logs.
- Modify logs and registry files.
- Remove all files and folders created.

3.1 Disable Auditing

A computer security audit is an assessment of the security of a system or application. It may be carried out manually or may involve a systematic and measurable technical assessment of security. Manual assessments can be carried out by interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analysing physical access to the systems. The main reason why attackers disable audit is to disrupt or prevent incident response activities. This also enables a hacker to gain long-term access to the compromised network even after he has been detected. The following are the steps taken by hackers to disable auditing:

- Secret deployment of backdoors
- Set up an agile lateral movement infrastructure
- Reduce the number of compromised hosts as much as possible during each round of attack
- Use different types of malware to attack the network
- Work as fast as possible to prevent incident responders or investigators from keeping track of their activities.
- Use busy servers to prevent detection of internal hop-points
- Use busy file servers for data staging areas
- Establish a VPN for C2 communication to bypass some network monitoring activities.
- Disguise the origin of malware files.

These activities prevent discovery of an ongoing, and even persistent security violations.

Anti-forensics measures prevent investigators from finding enough digital evidence to prosecute an attacker in a court of law. Criminals or pen testers usually attempt to damage the evidence and cause digital investigation procedure to become almost impossible. Hence, hackers place a lot of emphasis and urgency on anti-incident response activities because they carry out most of their actions on live systems in real-time.

Incident response activities are more urgent and more time-constrained than those by investigators.

3.2 Clearing Logs

Log files contain a record of events that take place during the execution of the operating system or other software. Logs also consist of a record of messages between different users of communication software. System and network administrators use logging to track activities on their systems and networks. Log files also show records of malicious activities. They also provide an indication of the actual state and health of the system and issues related to the availability or characteristics that may draw unwanted attention—log files record all unsuccessful login, successful login, and security event. Hackers and pen testers delete or corrupt log files and prevent the success of the digital investigation. Log clearing is an anti-forensics activity that makes it difficult or almost impossible to find enough digital evidence to prosecute a hacker.

Identify a few tools used for clearing logs.

3.2.1 Tools for Clearing Logs

The following are some of the tools and procedures for clearing log files on computer systems.

Clearing event logs with the meterpreter

Event logs can be cleared on a Windows system using a meterpreter script called Clearev. It also removes connections and/or attempted connections from the log files. Metasploit is used as follows:

First, run Metasploit on the system and launch the meterpreter command prompt. The type:

meterpreter > clearev

click here to view the steps in clearing logs.
This will clear all application, system, and security event logs on the victim system.

Clearing event logs on Windows machines

You can also clear the log files on Windows systems by using the clearlogs.exe file. You can download it here.

An attacker needs to have physical access to the system to be able to install and then run clearlogs. However, an attacker can install clearlogs remotely by uploading it to the system with TFTP (Trivial File Transfer Protocol) and then run it on the system. An attacker may choose to clear the security, application, or security logs. For example, to clear the security logs, type:

```
        clearlogs.exe -sec
```

You can confirm whether all security events have been cleared by clicking on the Event Viewer and then clicking on Security events.

Ensure that you remove clearlogs.exe after pen testing as its mere presence of the clearlogs file can indicate that an intruder has compromised the system.

Clearing event logs on Linux computers
Linux systems store log files in the **/var/log** directory. This plain text file contains log messages. The file can be opened with any text editor. You can type

kwrite /var/log/messages

to view log messages in BackTrack.

An attacker may open this file in a text editor and simply delete all the entries before leaving the compromised system. Alternatively, He may carefully go through and delete any entries related specifically to his activities if he has the luxury of time.

Erasing the command history
This is the last phase of attack against a compromised Linux system. A system administrator can use the command history to track all of the commands a hacker enters on the system. This will show the record of the hacker's activities as well as potential evidence of the attack.

Use the **more** command to view the command history:

```
        more ~/.bash_history
```

The environment variable **HISTSIZE** determines size of the history file. Type:

```
        echo $HISTSIZE
```

to check the size of the HISTSIZE variable

And then type :

```
        export HISTSIZE=0
```

to set it to zero.

This will delete the entire information in the Linux shell. A hacker can set export HISTSIZE to zero before beginning the hack to prevent the system from storing any of his commands. Alternatively, erase command history by logging out and logging back in to after setting the HISTSIZE to zero in case he has already written some commands

Shredding the History File
A hacker who has a limited time may not be able to delete the history file or change the HISTSIZE variable. He can simply shred the history file by typing:

```
shred -zu root/.bash_history
```

The **shred** command with the **-zu** switch overwrites the history with zeros and deletes the file.

To check whether a history has been deleted, type:

```
more /root/.bashhistory
```

Click this link for a video on how to clear tracks logs on Linux. The video provides a detailed understanding of the procedures and commands that a hacker can use to clear his tracks after compromising a Linux system or network.

3.3 Modifying Logs and Registry File

A hacker may decide to modify log files instead of outrightly deleting them in order not to raise suspicion about his activities. A pen tester must have root (administrator) privileges in order to tamper with information in log files. A pen tester who has escalated privileges can manipulate the record of his activities stored in the log file. This will prevent any investigation by the system administrator from revealing suspicious activities.

Windows-based computer systems stores all log files in the event viewer. You can find the events via the “Search” bar. Linux and UNIX operating systems store log files in the /var/log directory. Administrators examine the log files to check for malicious activities in the system they monitor. Log files may be system generated or application generated. An attacker can manipulate log files either by deleting an entire log or altering its content. Any of these options prevents an administrator from detecting evidence of the attack.

Log tampering can be prevented by configuring the system to transfer all logs to a remote dedicated log server. This leaves hacker with either of two options: prevent the transfer of logs to the dedicated server or attempt to compromise the log server

3.4 Removing Files and Folders Created

An attacker can also evade detection by deleting files, changing file locations, changing extensions or renaming files and folders. Similarly, he can also use some programs to split files into small parts and append each part at the end of other files. It is also possible for a pen tester to transfer data into file slack (unused storage locations in the computer). A pen tester can use packers (a kind of program) to hide executable (.exe) files in other types of files. Specialized tools called binders can be used to bcombine multiple executable files or hide an executable file in another file. Some tools can be used to change file headers and make the computer see a file as a different type of file. For example, a hacker can rename an mp3 file so that it will appear as a .gif file.

Data (or file) carving is a technique used to conduct an exact sequential scan of media for different sets of artefacts. This technique can extract low-level data directly from the media instead of reading them using only the file names and locations. For example, the actual data in the files stored in a zip archive will be used to identify the archive, instead of using the file names. Hackers can also encrypt important evidence and render the data unreadable during an investigation.

3.5 Covering Tracks on Network

This section discusses how attackers cover their tracks on the network. Some methods that can be used include (Helba, 2010):

- **Using Reverse Http Shells:**
  Thisbattack is carried out by installing reverse HTTP shell on the victim computer. The reverse HTTP shell receives external commands at regular intervals. This service runs on port 80, which makes network perimeter security devices as firewall sees it as a normal traffic.

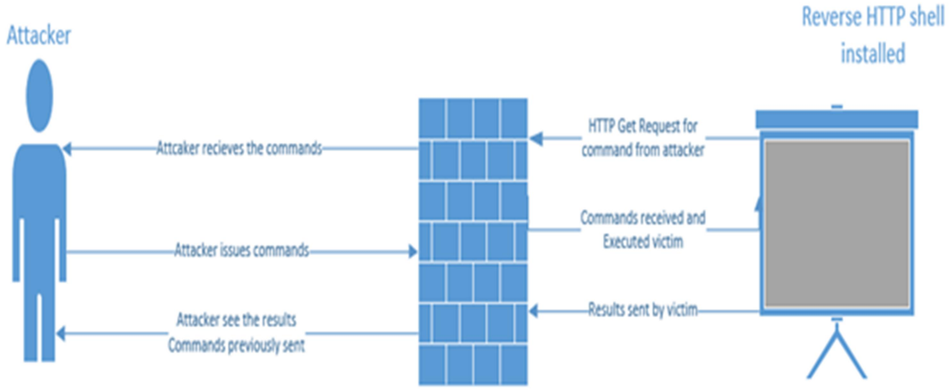
Attacker
Reverse HTTP shell installed
HTTP Get Request for command from attacker
Attcaker recieves the commands
Commands received and Executed victim
Attacker issues commands
Results sent by victim
Attacker see the results Commands previously sent

Fig. 11: Reverse HTTP

An attacker's machine issues command to be executed on the victim's computer in response to the request from the reverse HTTP shell. Network devices see all these communications as normal HTTP request /response. The results of the execution of the commands are sent out in the next web request. You can also program HTTP reverse shells to bypass any static authentication requirements of perimeter devices such as a firewall.

- **Using ICMP Tunnels**
  ICMP tunnelling is used to transmit traffic covertly using ICMP packets. This is possible because most organisations block only incoming ICMP traffic and ignore outgoing ones. This configuration allows an attacker to to transfer TCP payloads using ICMP packets.

ICMP tunnelling is illustrated in Figure 12.

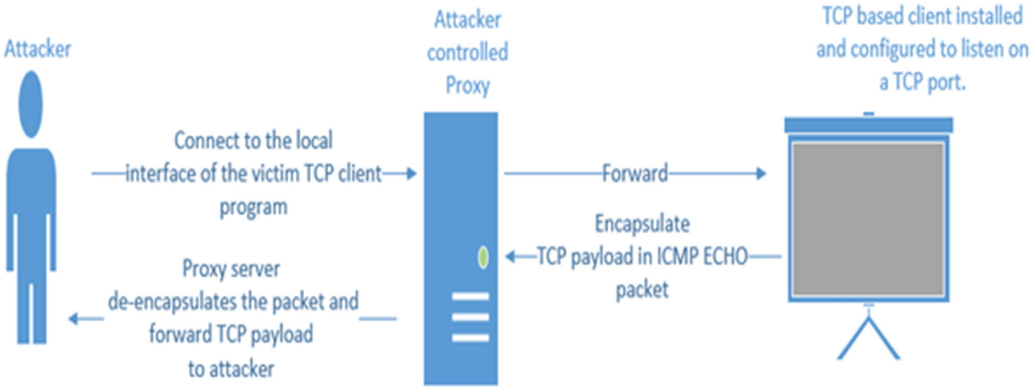
Attacker
Attacker controlled Proxy
TCP based client installed and configured to listen on a TCP port.
Connect to the local interface of the victim TCP client program
Forward
Encapsulate TCP payload in ICMP ECHO packet
Proxy server de-encapsulates the packet and forward TCP payload to attacker

Fig. 12: ICMP Tunnelling

The attacker first sets up a connection between his computer and the victim's machine. The victim uses an ICMP packet to encapsulate the TCP traffic before sending it to the proxy server.

  The proxy server, in turn, de-encapsulates the ICMP packet, extracts the TCP payload and sends it to the attacker. This looks like normal traffic to network security devices.
  Examples of tools for tunnelling include:
  - Loki
  - PingChat
  - Ptunnel
  - ICMPShell
  - ICMPCmd

- **Using TCP Parameters**
  An attacker can bypass IDS/IPS by embedding the exploit’s payload in a normal TCP packet instead of encapsulating a TCP protocol. The attacker can use the parameters which are not set in the TCP packet to distribute the payload. Attack payload may be sent using the following TCP packet fields:
  - IP Identification: A simple attack which requires an established session between the hacker and the victim. The IPID field is used to transfer the bits of the attack payload.
  - TCP initial acknowledgement sequence number: A tricky method which uses a bounce server to receive the packet from the client and send it to the attacker’s machine. This method uses the following steps:
    - The client spoofs the source address of the receiving server and the destination address of the bounce server and uses information to generate a TCP SYN packet. Assume the initial sequence number is ISNA, which contains the character to be transmitted.

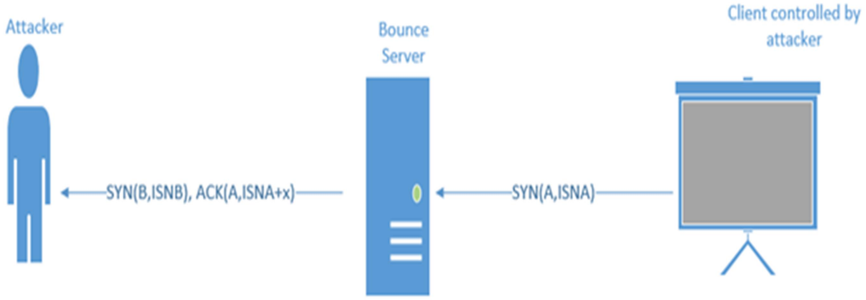

Fig. 13: Covering Tracks Using TCP Parameters

    - Bounce server receives the packet and sends an SYN-ACK or RESET, depending on whether the port is closed or not. It sends the reply to the receiving server using a spoofed source address. It replies with an SYNB, ACK(ISNA+1).

- Receiving server receives this information and retrieves the character from sequence number field.
- TCP initial sequence number: This method does not even require an established connection as is required in the IP identification method. An SYN packet is sent with an ISNa (initial sequence number) containing the payload (bit). Even though if it gets a RESET in reply, the content is already extracted by the other side.

Discussion

Hackers and pen testers usually attempt to cover their tracks after hacking activities. Why do you think this is necessary?

Case Studies

Examples of log attacks:

- A group of sophisticated hackers compromised the systems of Bangladesh's central bank and made awayh with stole $101 million. The outcome of forensic investigation revealed thet the attackers attempted to evade detection by deleting computer logs after carrying out the attack.

  1. Can a cleared log be recovered as in this case by investigators?
  2. Why is it necessary for hackers to cover their tracks after hacking?

A hacker used a phishing attack to in compromise the systems at JP Morgan Chase. Robert Capps, a cybersecurity expert at RedSeal, commented that "Getting access to bank records is uncommon but not unheard for hackers, who often change computer logs to cover their tracks but can't always get to more sensitive data." Investigations by the FBI revealed that the hackers used sophisticated and previously unknown malware to delete and manipulate records.

1. Can FBI recover this logs?
2. What are the possible tools that this hacker used to carry out this attack?

4.0 Self-Assessment Exercise(s)

1. Which of these steps do hackers take to prevent the auditing team from tracing their activities?
   a) Disable firewall
   b) Disconnect network access
   c) Modifying logs and registry files
   d) Removing all application software

Answer: C

2. Listed below are the techniques used by attackers to prevent detection of their activities on a network except.

   a) Reverse Http Shells
   b) UDP Tunnel
   c) ICMP Tunnel
   d) TCP Parameters

Answer: B

3. Hackers erase the record of their activities because of the following reasons. Choose all correct answers.
   A. To prevent real-time detection of their activities
   B. To remove the usernames and passwords of legitimate users
   C. To prevent digital evidence collection during a post-incident investigation.
   D. To remove the tools used for hacking
   Answer: A,C

4. You can use the following steps to disable auditing except:
   A. Secret deployment of backdoors
   B. Set up an agile lateral movement infrastructure
   C. Reduce the number of compromised hosts as much as possible during each round of attack
   D. Work as slowly and as patiently as possible to disable all record logging applications on the network.
   Answer: D

5. Log tampering can be prevented by
   A. Configuring the system to transfer all logs to a remote dedicated log server
   B. Saving all logs on a local network
   C. Disable all log activities
   D. Use flash memory devices to store all logs
   Answer: A

6. Which of the following is not a suitable technique for evading detection after a hacking activity?
A. Using reverse HTTP shells
B. Using direct HTTP shells
C. Using ICMP tunnels
D. Using TCP parameters
Answer: B

7. ---------- is a utility for clearing all application, system, and security event logs on the victim system
A. Meterpreter
B. Clearev
C. echo $HISTSIZE
D. Shred -zu
Answer: B

5.0 Conclusion

Hackers and pen testers must avoid detection as much as possible. Hence, they must disable auditing, clearing logs, modifying logs and registry files and remove all files and folders created. These tasks require knowledge of procedures, tools and techniques for covering tracks and erase evidence of their activities on the systems and applications in the target environment.

6.0 Summary

In this unit, you have learned the skills required to avoid detection after carrying out penetration testing activities. You have also learned the methods, tools and techniques hackers and penetration testers use to eliminate traces of their activities on systems, networks and applications.

7.0 REFERENCES/Further Reading

Allen, L., Heriyanto, T. & Ali, S. (2014). *Kali Linux – Assuring Security by Penetration Testing*. UK: Packt Publishing Ltd.

Bosworth, S., Kabay, M.E. & Whyne, E. (Eds.).(2014). *Computer Security Handbook.* (6th ed.). Vol. 1, Wiley & Sons, Inc.

Canavan, J.E. (2001). *Fundamentals of Network Security*. London: Artech House.

Hall, G. & Watson, E. (2016). *Hacking, Computer Security Testing, Penetration Testing and Basic Security*. Available here

Helba, S. (Ed.). (2010). *Ethical Hacking and Countermeasures: Threats and Defence Mechanisms*. New York: Cengage Learning.

Hutchens, J. (2014)*. Kali Linux Network Scanning Cookbook*. UK: Packt Publishing Ltd.

Ryan (n.d.). *Summarising The Five Phases of Penetration Testing.* Available here

Stallings, W. (2011). Cryptography and Network Security Principles and Practice. New York: Prentice-Hall.

Module 2: Targetted Attacks

Module Introduction

Operating systems and application vulnerabilities provide gateways for attackers to compromise the security of systems and networks. This module focuses on the methodologies, tools and techniques for evaluating the security of two popular operating systems (Windows and Linux) as well as web applications. These approaches enable hackers and pen testers to identify vulnerabilities which may be used to exploit the system. Ethical hackers use these methods to detect holes in their systems and applications, and quickly fix known weaknesses or vulnerabilities that may be used to compromise their systems.

Unit 1: Windows System
Unit 2: Linux System
Unit 3: Web Server and Web Applications

Unit 1: Windows System

Contents

1.0 Introduction

In this unit, you will acquire the skills for evaluating the security of the Windows operating system. To achieve this, you will learn the vulnerabilities inherent in Windows OS and the attacks that can be used to exploit these vulnerabilities. You will also learn the methods, tools and techniques hackers and penetration testers use to exploit systems and networks that run on Windows.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define ARP spoofing
- describe and analyse malware attacks
- perform password-based Attacks
- discuss TCP-SYN flood
- explain war dialling.

3.0 Main Content

Have you observed that most personal computers run on the Windows operating system?

Do you think this may attract hackers to Windows-based computers more than computers running on other platforms?

What should administrators and users of Windows OS do to protect their systems and applications?

Hackers exploit flaws in operating system and application to compromise the security of systems and networks. A system flaw is any flaw that makes a program to (1) exhibit improper behaviour (under normal or extreme conditions) and (2) allow hackers to take advantage of weaknesses (or improper operation) to crash or gain unauthorized access or control of a system (Anonymous, 2001). A primary flaw is a weakness in the security structure of the operating system, which allows a hacker to gain one-step, unauthorised access to the system or datase. A secondary flaw is any weaknesses in a program that may not be related to security, but causes a security issue in other parts of the system. An example of a secondary security flaw is the requirement of root or superuser privileges to complete a task in a program.

i. *Do you remember Address Resolution Protocol (ARP) and its purpose?*
ii. *How do you know that hackers can use the vulnerability in ARP to attack your network?*

3.1 ARP Spoofing

Local area network (LAN) devices use physical hardware addresses to communicate on IPv4 networks. Individual hardware manufacturers design these Media Access Control (MAC) addresses and the MAC address for each computer is distinct from that of any other computer anywhere in the world. The MAC address is used to identify each device in the LAN via its network interface card. On the other hand, devices on different LANs use IP addresses to communicate. If Computer A wants to communicate Computer B within the same network, it must first use address resolution protocol to associate the appropriate MAC address with its IP address. Computer A sends an ARP request (a broadcast request) containing its pair of MAC address and IP address to all devices on the network. The request will also contain the IP address of Computer B. The MAC address and IP address pair sent by A is stored in the local table or ARP cache of each computer on the network. The table is temporary storage for all known MAC addresses and their corresponding IP addresses. This process ensures that only Computer B responds to the ARP request even though all devices on the LAN receive the request. Computer A uses the information contained in reply to send data packets to Computer B.

What happens if the reply does not come from Computer B, but from another device controlled by an attacker? This is what leads to ARP spoofing.

3.1.1 Attack Method

ARP spoofing (ARP cache poisoning, or ARP poison routing) is a technique used by an attacker to send spoofed ARP messages to a LAN. The attacker aims to link his MAC address with the IP address of another computer, such as the default gateway. This is called ARP poisoning. Click the link for a video on ARP poisoning. This makes any traffic meant for the legitimate host to be redirected to the attacker. Attackers use ARP spoofing to capture data frames, modify traffic, or interrupt all network traffic. It may also be a precursor to other attacks, such as a denial of service, man in the middle (See the video on simulation man in the middle attack using ARP spoofing), and session hijacking. The attack can only be launched against networks running the ARP and requires a hacker to have direct access to the target network segment. Click this link for a simulation of ARP spoofing.

3.1.2 Legitimate Usage of ARP Spoofing

ARP spoofing techniques can also be used to enhance network availability by implementing redundancy of network services. For instance, some network applications allow a backup server to issue a redundant ARP request to handle take over of the responsibility of a failed server. Developers also use ARP spoofing to debug IP traffic between two hosts on a switched network. Normally, a monitoring host M cannot access the traffic between two computers, say A and B, connected by an Ethernet switch. The administrator can configure A to have M's MAC address for B, and B to have M's MAC address for A; and also configures M to forward packets. M can now monitor the traffic between A and B, in a way that is analogous to a man-in-the-middle attack.

3.1.3 Detection and Prevention

Detection tools usually certify or cross-check ARP responses in order to detect ARP spoofing. This technique ensures the blockage of uncertified ARP responses. AntiARP is a tool which prevents ARP spoofing in Windows-based OS at the kernel level. Virtual machines such as Kali VM have security measures for preventing MAC spoofing between guests running on the same physical hardware. Some ethernet adapters also have features which prevent MAC and VLAN spoofing.

3.2 Malware Attacks

A malware (or malicious software) is a software that is purposely designed to damage a computer, server, client, or computer network. Malware may be used to steal, encrypt/delete sensitive data. They may also alter/control core computing functions and perform unauthorised tracking of users on the network. Examples of malware are a worm, virus, ransomware, Trojan horse, spyware and adware.

Attackers use physical (such as an infected USB drive) and virtual means (via the internet) to infect devices and networks with malware. The drive-by-download attack automatically downloads malware to systems without the user's permission or knowledge. Hackers also spread malware through phishing attacks, where emails containing malicious links or attachments are sent to unsuspecting users. In sophisticated malware attacks, a hacker sets up a command-and-control server which enables him to connect to infected systems. This allows the attacker to steal sensitive data and even control the compromised system or server from a remote location. Emerging strains of malware use evasion and obfuscation techniques to prevent security administrators and anti-malware products from detecting them.

What is the common malware which targets Windows systems?

Can you describe the mode of operation of different types of malware?
Which countermeasures should security administrators use against malware?

3.2.1 Virus

A computer virus is a malicious program that replicates by attaching itself to another program. A virus usually spreads when an unsuspecting user runs an infected program or downloads an infected file, usually in the form of an email attachment. Computer viruses perform two main functions, namely propagation and destruction (Stewart, 2015). Hackers infect vulnerable systems with viruses to gain administrative control and steal sensitive data.

Virus scanning programs identify the "signature' of known viruses and use it to build a database of known signatures. The database is compared to scanning results, and a match indicates the presence of a virus. The database requires regular updates to ensure that the virus scanner does not become outdated quickly. Windows OS is vulnerable to virus codes such as Melissa, Sasser, Zeus, Conficker, Stuxnet and Mydoom (Hall and Watson, 2016). Common antivirus software for Windows systems include Windows Defender, Norton, Kaspersky, Panda, Bit defender, and Trend micro

3.2.2 Worm

A worm is a self-contained (or independent program) that is usually designed to propagate without human intervention (Stewart, 2015). A worm replicates itself on infected systems and uses available network connections to infect other systems. The main difference between a worm and a virus is the mode of propagation. A worm propagates without attaching itself to an executable file, but a virus requires an attachment to an executable file to propagate itself.

Windows OS is vulnerable to worm infection. The replication of worms consumes computer processing time and network bandwidth, which would have been used by legitimate programs. They also carry destructive payloads as they propagate. Worms may delete files on an infected system (for example, the ExploreZip worm), encrypt files (in a ransomware attack), or disclose sensitive data (e.g. sensitive files or passwords). The most common form of worm attack is to install a backdoor, which allows an attacker to control the infected computer remotely. A worm attack may also involve networks of computers (often referred to as botnets) which are commonly used for malicious purposes, such as spam and DoS attacks. Common defences against worms involve the use of antivirus and anti-spyware software. These must be updated regularly to ensure detection of new strains of worms which surface almost every day. A firewall also offers protection against worm attack.

3.2.3 Trojan Horse

A Trojan horse is a malicious program or code fragment that usually performs a disguised function. This trojan horse program is usually hidden within another program, where it covertly performs malicious functions. It may also disguise itself as a legitimate program while carrying out destructive activities secretly. Such destructive activities may involve the modification of an existing program or replacement of the existing program with a new one. Other malicious functions include copying and sending sensitive information or opening a trap door to allows unauthorized, privileged access to a system or process. Examples of Trojan horse are password grabber, Exploit, Rootkit, Trojan-Banker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper and Trojan-GameThief (Engebretson, 2013; Helba, 2010). You can protect your systems against Trojan attacks by using updated antivirus or antimalware software, which scan links for malicious data and remove Trojans.

This video shows the differences between Viruses, Worms and Trojans.

3.2.4 Ransomware

Hackers use ransomware attack to hold a computer or its resources hostage until the legitimate owner pays a ransom (money), usually in bitcoin. The malicious code identifies the drives on an infected system or network, encrypts the files in each drive and prevents legitimate users from gaining access to the files. One of the indicators of a ransomware attack is the addition of an extension to the encrypted file. Popular extensions use by ransomware include .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault, or .petya. Each extension is used to identify the type of ransomware that has attacked the file. The attacker also creates and displays a file (or files) containing instructions on how to pay the ransom. The attacker provides a cryptographic key to unlock the files once the victim pays the ransom.

Ransomware spreads through malicious email attachments or when an unsuspecting user visits an infected website. The second method downloads and installs the malware without the user's knowledge. Popular ransomware includes Cryptolocker, Locker, Bad Rabbit, Goldeneye, Zcryptor, Jigsaw, LeChiffre, and Petya. For the protection of your files and applications against ransomware attacks, you can use Comodo Advanced Endpoint Protection.

How to protect data and networks against a ransomware attack?

- Back up your computer: Perform regular backups of your system and other important files. Also, ensure that you verify your backups regularly. Backup copies provide a means for restoring the system to its previous state in the event of a ransomware attack.
- Store your backups separately: Storing your backups on a separate device such as an external hard drive makes them inaccessible from a network. This also minimises the possibility of deliberate or accidental corruption or destruction of backup files.
- Education and training: Organisations should educate their personnel about current cybersecurity threats and modes of attack through regular cybersecurity awareness training. Organisations can assess security awareness by carrying out simulated phishing and social engineering attacks against their personnel.

Countermeasures against ransomware infections

- Regular installation of updates and patches – eliminates vulnerabilities in applications and operating systems, which are the target of most ransomware attacks.
- Do not click on links or open emails whose source you are not sure of. Verify website addresses by contacting your organisation's helpdesk, searching the internet for the sender organisation’s website or the topic mentioned in the email.
- Be careful when opening email attachments, even from known senders, particularly when they contain attachments in the form of compressed (or ZIP) files.
- Keep your personal information safe: Provide your personal information only on websites which offers encryption before data transmission.
- Update yourself about recent cybersecurity threats and current ransomware techniques.
- Use and maintain preventative software programs. Install updated versions of antivirus software, firewalls, and email filters.

3.2.5 Spyware and Adware

Spyware is a malicious software which steals sensitive information from infected computers. Spyware steals personal information such as internet usage data, credit card details, bank account information, personal identity, and sends them to advertisers, data firms, or external users. Hackers also use spyware to monitor track users’ login and password information and other internet activities. Some spyware can perform unauthorized software installation and change the settings on an infected device.

Adware monitors browser history and downloads, to predict the products or services which the user is interested in. Adware is used for marketing purposes and can reduce the performance of the computer. Protection against spyware and adware infection includes the use of secure passwords and regular update of applications on computers.

Spyware infects computers through the following ways:

- Clicking a prompt or pop-up without first reading.
- Downloading software from an unreliable source
- Accessing email attachments from unknown senders
- Pirated media such as music, movies or games

Windows operating systems may be more susceptible to spyware attacks than PCs, Macs, and iOS or Android devices. This is because Windows is the most commonly used OS in personal computers and are thus the main target of attacks by hackers.

3.3 Password Attacks

Password attacks focus on recovering passwords from data that are stored in or transmitted by computer systems. Examples of password attacks include password guessing, dictionary attack, password resetting, brute-force attack, password cracking, password sniffing, password capturing, and rainbow table attack. Password guessing is the most common password attack. This involves the use of a manual or automated approach to guess passwords on a local or remote machine. Password guessing is usually successful against networks that do not use long and complex words. Moreover, some authentication protocols do not provide effective protection against guessing attacks.

Dictionary attacks assume that most passwords are formed using words, dates, or numbers that are found in a dictionary. Tools used for this attack require a dictionary input list consisting of words and vocabularies. Databases used as input list for dictionary attack can be downloaded from the internet. Sometimes, attackers prefer to reset passwords, rather than guessing them. This prevents a legitimate user from using his password to access the infected system or application. Popular tools for password reset attack include Petter Nordahl-Hagen program and Winternals ERD Commander 2005. Password cracking is the recovery of a plaintext password from a compromised password hash (or some other scrambled or protected form of the plaintext password or challenge-response packets). Hackers crack passwords by using tools such as extractors for hash guessing; rainbow tables for looking up plaintext passwords; and password sniffers to capture authentication data. Pwdump suite is a popular Windows password hash extractor that can retrieve plaintext passwords from LM (LAN Manager) password hash. Other password crackers for Windows OS are John the Ripper and Cain & Abel.

A brute force (or exhaustive search) attack uses all possible combinations of input to guess the correct password. The longer or complex the password, the more combinations that will need to be tested, and the more time consuming will be the attack. This means cracking a weak password could merely take a few seconds and minimal effort. Strong passwords created using sophisticated methods such as data obfuscation are very difficult and sometimes almost impossible to crack. Hence, organiSations should enforce a strong password policy across all systems and networks. Password cracking may also involve sniffing authentication traffic between a client and a server and extracting password hashes or any other authentication information to crack the password. Examples of sniffing password crackers are Cain & Abel, ScoopLM and KerbCrack. A similar attack known as password capturing occurs when a hacker installs a keyboard-sniffing Trojan horse or any other physical keyboard-logging on the target system. Physical keyboard logging devices are small in size (not up to an inch long) and can easily be installed (by inserting it between the keyboard cable and the computer's keyboard port) on the victim’s computer. It is also easy to sniff passwords from wireless keyboards by installing wireless sniffers a few metres away from the target. See video for simulation of brute force password cracking using Medusa password cracking tool here.

A rainbow table is a lookup table containing all possible combinations of passwords and their hashes. An attacker who obtains a password hash from a compromised system can easily look up the plaintext password from the rainbow table. Cracking tools (and Web sites) can use rainbow tables to crack any LM hashes within a very short period of time.

Password strength measures the robustness of a password against guessing or brute-force attacks. In its usual form, it is an estimate of the average number of attempts (and consequently the amount of time) required by an attacker to guess the password correctly. Password strength depends on length, complexity, and unpredictability. Automated password cracking (using software crackers) depends on the number of possible passwords that can be compromised within a second

3.3.1 Password Cracking Tools

- John the Ripper: A free and one of the most popular password crackers available. It is a preferred password cracking suite for ethical hackers because of its ability to detect password hash types automatically. A professional version of the tool is more effective and has better features.

Supported platforms: Windows, Linux, DOS, and OS X. You can use this link to download John the Ripper.

- Aircrack-ng: one of the most suitable tools used to crack Wi-Fi (WPA and WEP) passwords. Aircrack uses its cracking algorithm to retrieve plaintext passwords from encrypted password packets.

  Supported platforms: Windows, Linux, OpenBSD, FreeBSD, Android. Use this link to download Aircrack-ng. Click the link for a simulation of password cracking with aircrack.

- RainbowCrack uses rainbow tables to crack password hashes. It performs an advance cracking time computation using a large-scale time-memory trade-off, It has both command line and graphical interface versions.

After the pre-computation stage, RainbowCrack will crack passwords about hundred time faster than a brute force attack. The tool also has free rainbow tables for different hashing techniques such as LM, NTLM, MD5 and SHA1.

Supported platforms: Windows and Linux. See the download link for RainbowCrack here.

- Cain and Abel is a multipurpose cracking tool used to retrieve different types of passwords. Cain and Able can use dictionary, brute-force, and cryptoanalysis attacks to crack encrypted passwords. It also can sniff network packets, record VoIP conversations, retrieve
- network keys, decode scrambled passwords, and analyze routing protocols.

Cain and Abel has two components: a frontend and a backend. Cain is the frontend application used to recover passwords and perform sniffing, while Abel is the backend Windows NT service that performs traffic scrambling.
Supported Platforms: Windows

- THC Hydra - performs hacking using different network protocols, such as HTTP-Proxy, FTP, MYSQL, XMPP, Asterisk and Telnet. THC Hydra uses these protocols to perform brute-force and dictionary attacks quickly against a login page. It is a free tool which helps pen testers to assess the vulnerability of a system to remote attacks.

Supported Platforms: Windows, Linux, Solaris, FreeBSD, OS X
See the download link for THC Hydra here.

- OphCrack is a free tool which uses rainbow tables to crack password hashes of Windows log-in passwords. OphCrack can retrieve the passwords of a Windows computer within a short period of time because it imports and uses multiple format hashes from different sources.

Supported Platforms: Windows OS
Click this link to download OphCrack

- L0phtCrack – a tool that uses a wide variety of attacks (such as a dictionary, hybrid, brute force, and rainbow tables) to sniff password hashes. It is very effective for cracking passwords in Windows desktops, network servers,

Supported Platforms: Windows
You can use this link to download L0phtCrack

Can a hacker obtain confidential information from a computer without compromising the algorithms used to secure data?
If yes, how can you protect yourself against such attacks?

3.4 Side-Channel Attacks

A side-channel attack is a passive, noninvasive attack that seeks to extract information from the implementation and operation of a computer system, rather than weaknesses in the implementation of an algorithm (Stewart, 2015). This involves a situation whereby an attacker monitors electronic emissions resulting from the operation of the victim's computer. A hacker uses side-channel attacks to exploit the way the operating system interacts with the hardware, rather than targeting a vulnerability resulting from coding or configuration errors. Any system or network is susceptible to side-channel attacks irrespective of the operating system running or it. Common examples of side-channel attacks are timing attack, power analysis attack and optical side-channel attack.

3.4.1 Timing Attack

Hackers use a timing attack to monitor data transmission between the CPU and memory on the hardware running the cryptographic algorithm. An attacker can determine the secret key by observing variations in the amount of time taken to perform cryptographic operations. This involves a statistical analysis of timing measurements across the system and network (Brumley and Tuveri, 2011).

3.4.2 Power Analysis Attack

A power analysis attack is based on an observation of the power rates of a hardware device such as a CPU or cryptographic circuit. It consists of two main types, namely simple power analysis (SPA) and differential power analysis (DPA). A power analysis attack also occurs when fluctuations in current generate radio waves. Attackers can extract valuable information by using statistical techniques to analyze the measurements of such electromagnetic emissions.

3.4.3 Optical Side-Channel Attack

Optical side-channel attacks use audio/visual recorder (such as a video camera) to gather information about the activity of a hard disk. This involves extracting information about the activities of the hard disk or reading a few number of photons emitted by transistors as they change state (Ferrigno and Hlaváč, 2008).

3.4.4 Other Forms of Side-Channel Attacks

- Exploits based on how and when a physical system accesses a cache
- Differential fault analysis attacks – use errors in computations to obtain information from a system
- Thermal-imaging attacks – extracts executed code by using infrared images to scan the surface of a CPU chip.

3.4.5 Countermeasures Against Side-Channel Attacks

The following are the options for preventing side-channel attacks:

- Reduce the release of electromagnetic information that could be used to launch an attack or
- Make it impossible for an attacker to link the activity of the CPU with specific compute operations. For example, you may use randomization to change the order of operations on data in the system.
- Increase the noise in a channel to minimise the amount of useful data an attacker can extract from electromagnetic leaks.

What are flooding attacks?
Which effects do such attacks have against Windows systems?

3.5 TCP-SYN Flood

SYN flood is a distributed denial of service (DDoS) attack that exploits part of the normal TCP three-way handshake used for communication between two devices on a TCP/IP network. In this attack, a hacker causes network saturation by sending TCP connection requests at faster rates than the targeted machine can process them. The goal is to exhaust the resources (memory, transmission channel) on the targeted server and prevent it from responding to legitimate client requests.

3.5.1 Attack Description

In an SYN flood attack (see Figure 13), the attacker uses falsified IP address to repeatedly send multiple SYN packets to every port on the targeted server. The server treats the malicious packets as legitimate connection requests and responds to each attempt with an SYN-ACK packet from each open port. The malicious client either does not send the expected ACK or—if the IP address is spoofed—never receives the SYN-ACK in the first place. This makes the target server to experience significant delays while waiting for acknowledgement of its SYN-ACK packet.

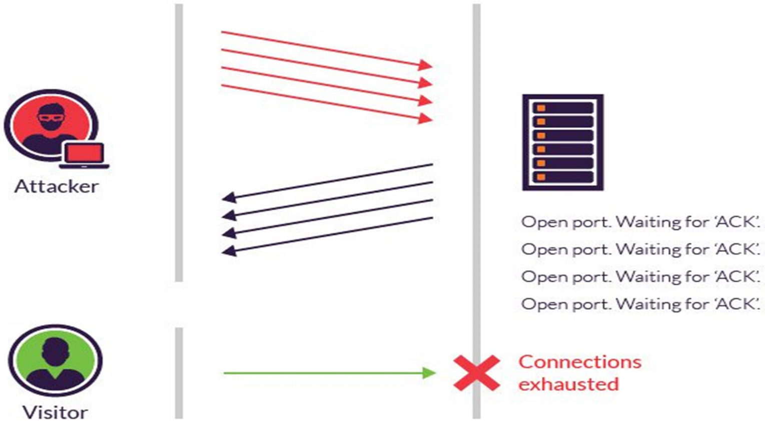
Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

Fig. 14: SYN Flood Attack

This video (here) provides further explanation and simulation of an SYN flood attack. The connections remain open during the attack because the server cannot use the RST packets to close them. The increasingly large number of open connections deny legitimate clients from connecting to and accessing resources from the server.

3.5.2 Methods of Mitigation

Common techniques to mitigate SYN flood attacks include:

- Micro blocks: instead of allocating a complete connection object, administrators may allocate a micro-record (as few as 16 bytes) in the server memory to handle each incoming SYN request.

- SYN cookies: The server derives a sequence number from the client IP address, port number, and other unique information and uses cryptographic hashing to send its SYN-ACK response. The hash is included in the ACK packet from the client. The server only allocates memory for the connection after verifying the ACK.

- RST cookies: Here, the server intentionally sends an invalid SYN-ACK reply to the first connection request from a client. Normally, the client generates an RST packet in response to the invalid SYN-ACK received from the server. Once the server receives the RST packet, it confirms the legitimacy of the request, logs the client, and accepts subsequent incoming connections from it.

- Stack tweaking - administrators can alter TCP by reducing the timeout until a stack relinquishes memory allocated to a traffic, or selectively dropping incoming traffics.

What does war dialling entails and how sophisticated can this attack be?

3.6 War Dialing

Hackers use war dialling to search for modems, computers, bulletin board systems (servers) and fax machines. It is a technique used to search for live devices by (automatically) scanning a list of telephone numbers and dialling every number in a local area code. Malicious hackers use this method for guessing user accounts (by capturing voicemail greetings) or identifying modems that may provide an attack route to a computer or other network devices. Ethical hackers perform war dialling to detect unauthorised devices (such as modems or faxes) on an organisations telephone network.

3.6.1 Attack Description

A common technique is to use a telephone number of a target organization and then war dial the entire prefix which the number belongs to. For example, an attacker who targets the Chinese embassy in Washington, D.C., would dial every number starting with (202)328.

War dialling one telephone number takes approximately 35 seconds. This means that war dialling a prefix of ten thousand numbers will take about four days. You can do war dialling by hand if the numbers are few. However, dialling several thousand telephone numbers by hand is extremely strenuous and time-consuming, hence the need for
a war dialling program (also called a war dialer or a demon dialer).

3.6.2 War Dialing Tools

War dialer is the most important tool for detecting modems. A war dialer is a software used to identify the phone numbers that can be used to connect to a modem. The program automatically identifies numbers that successfully connect to the modem from a range of phone numbers. A war dialer software can also identify the actual operating system running on the system and may also conduct automated penetration testing. War dialers for Windows OS include ToneLoc, ModemScan and TeleSweep.

Can you discuss different attacks that can be used to exploit Windows systems?

Which methods, tools and techniques would you use to evaluate the security of your Windows platform?
Can you identify practical cases of attacks against Windows OS?

Discussion

Passwords are not stored in the server in plaintext format. They are usually protected by encrypting them using appropriate cryptographic algorithms. However, hackers use password crackers to reveal encrypted (protected) passwords.
Why do you think it is necessary to protect passwords?
In which ways can hackers take advantage of compromised passwords?

4.0 Self-Assessment Exercise(s)

1. ---------- is attack method used by a hacker to link his MAC address with the IP address of another computer.
   A. Ping of death
   B. Smurf
   C. ARP spoofing
   D. Ransomware
   Answer: C

2. Which of the following malware can infect a computer without human intervention?
   A. Worm
   B. Virus
   C. Trojan horse
   D. Ransomware
   Answer: A

3. --------- is the currency in which ransomware victim pay attackers.
   A. United States dollars
   B. Pound sterling
   C. Bitcoin
   D. Deutschemark
   Answer: C

4. Which of the following is not a characteristic of Trojan horse?

   A. Trojan horse is a malicious program
   B. Trojan horse program is usually hidden within another program,
   C. It can modify an existing program or replace an existing program with a new one.
   D. It can propagate without human intervention.

   Answer: D

5. --------- is a malicious program used to track users' login and password information and other internet activities.

   A. Ransomware
   B. Spyware
   C. Adware
   D. Virus

   Answer: B

6. --------- attack uses all possible combinations of input to guess the correct password.

   A. Dictionary
   B. Guessing
   C. Rainbow table
   D. Brute force

   Answer: D

7. Which of the following is a side-channeling attack? Choose all that apply.

   A. Timing attack
   B. Power analysis attack
   C. Optical side attack
   D. Exhaustive search attack

   Answer: A,B,C

Assignment
Identify various kinds of password cracking tools.
Use one of the tools to crack passwords.
Post your findings, including screenshots to your course tutor.

5.0 Conclusion

Windows OS is the most commonly used operating system for workstations and servers. This makes it a great target for many attackers. Numerous exploits have been developed to compromise the security of Windows OS and to gain unauthorized access to stored information. Ethical hackers should have a mastery of the common vulnerabilities and exploits used to attack Windows OS. Security professionals must have expertise in methodologies, tools and techniques for cracking Windows OS. This will enable them (system administrators) detect loopholes in their systems before attackers can use such weakness to compromise the security of their systems.

6.0 Summary

In this unit, you have acquired the skills for evaluating the security of Windows-based systems and networks. The chapter introduced you the vulnerabilities in Windows OS and the attacks that can be used to exploit these vulnerabilities. You have also learned the methodologies, tools and techniques used by hackers and pen testers to compromise the security of Linux OS. In the next unit, you will learn about the vulnerabilities and exploits that target Linux systems and networks.

7.0 References/Further Reading

Anonymous (2001). *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis, United States: Sams Publishing.

Bosworth, S., Kabay, M.E. & Whyne, E. (Eds.).(2014). *Computer Security Handbook*. (6th ed.). Vol. 1, Wiley & Sons, Inc.

Brumley, B.B. & Tuveri, N. (2011). "Remote Timing Attacks are Still Practical." Proceedings of the 16th European conference on Research in computer security, Pp. 355-371, Leuven, Belgium, Sept. 12-14, 2011. Springer-Verlag Berlin, Heidelberg.

Canavan, J.E. (2001). *Fundamentals of Network Security*. London: Artech House.

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing*. (2nd ed.). Elsevier.

Ferrigno, J. & Hlaváč, M. (2008). *When AES Blinks: Introducing Optical Side Channel, IET Information Security*, 2 (3): 94–98, doi:10.1049/iet-ifs:20080038

Helba, S. (2010). *Ethical Hacking and Countermeasures: Threats and Defence Mechanisms*. New York: Cengage Learning.

Stewart, J.M., Chapple, M. & Gibson, D. (2015) *CISSP Certified Information Systems Security Professional Study Guide*. (7th ed.). John Wiley & Sons, Inc

Unit 2: Linux System

Contents

1.0 Introduction

In this unit, you will acquire the skills for evaluating the security of the Linux operating system. To achieve this, you will learn the vulnerabilities inherent in Linux OS and the attacks that can be used to exploit these vulnerabilities. You will also learn the methods, tools and techniques hackers and penetration testers use to exploit systems and networks that run on Linux.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- define spoof attacks
- explain the concept of scanning
- demonstrate a denial of service attacks
- describe malware attacks
- discuss wiretapping.

3.0 Main Content

Have you observed that Linux is less popular than Windows among users of personal computers?

Have you heard Linux users brag about the security of their systems?

Do you agree that Linux OS is very secure or even foolproof?
Which methods can hackers use to compromise Linux systems?

3.1 Spoofing Attacks

Occurs when an attacker uses falsified IP address to impersonate an authorised system. The attacker pretends to be a legitimate host by using the IP addresses in network packets. A well-known exploit of the BSD (Berkeley Software Distribution) Linux login service can guess the TCP sequence numbers and mimic a TCP connection from another host. Common protocols such as ARP (Address Resolution Protocol), IP Address, DNS (Domain Name System) and MAC (Message Authentication Code) are vulnerable to spoofing attacks. You can prevent spoofing attacks in the following ways:

- always confirm the authenticity of datagrams and commands;
- do not allow invalid source addresses to perform datagram routing;
- use unpredictable parametrs to control data transmission. Examples of such parameters are TCP sequence numbers and dynamic port addresses.

3.1.1 ARP Spoofing

ARP Spoofing also known as ARP (Address Resolution Protocol) poisoning occurs when a hacker modifies the MAC (Media Access Control) address in the ARP cache of the target computer. In other words, the hacker compromises an Ethernet LAN by inserting forged ARP request and reply packets in the target computer's ARP cache.

This video (here) describes the simulation of ARP spoofing. In Kali Linux 2016, ARP poisoning or spoofing requires the following steps:

1. Identify the IP address of the target host.
   ```
   #ifconfig
   ```
2. Then look for the router's mac address in the arp table.
   ```
   #arp
   ```
3. Ping the target host and confirm if its mac address in now in the arp table.
   ```
   #ping Victim-IP
   #arp
   ```
4. Set up IP forwarding using the following command.
   ```
   #echo 1 > /proc/sys/net/ipv4/ip_forward
   ```
5. Check your default gateway.
   ```
   #ip route
   ```
6. Identify the network interface.
   ```
   #ifconfig
   ```
7. You can now begin the arp poisoning/spoofing using the following commands.
   ```
   #arpspoof -i eth0 -t victimIP -r DefaultGateway
   ```
   -i is for the interface.

-t is for the target.
-r is for the default gateway.

3.1.2 DNS Spoofing

DNS spoofing is an attack in which legitimate domains names are resolved into fake IP addresses. This method is used to divert traffic meant for the victim's system to the attacker's system. Detection of DNS spoofing is difficult because it evades a firewall or an antivirus. For example, a hacker can launch DNS spoofing on a victim's system and divert the IP of facebook.com to his (attacker's) IP address. When the victim opens the Facebook website, the DNS will open the attacker's IP (instead of facebook.com). The attacker can use this method to steal data or cookies from the victim's system.

Click this link for a video on simulation of a DNS spoofing attack. A tool known as dnsspoof (a member of the Dsniff suite) is used to forge DNS response for a DNS server on the local network. The dnsspoof tool forges a response and diverts the request to the attacker's system before the legitimate DNS server responds. For example, consider 192.168.1.5 as the DNS server and 192.168.1.245 as the victim. Assume we run the following commands,

```
# echo 1 > /proc/sys/net/ipv4/ip_forward enable port forwarding)
# arpspoof -t 192.168.1.245 192.168.1.5 &;
# arpspoof -t 192.168.1.5 192.168.1.245 &;
# dnsspoof -f  spoofhosts.txt host  192.168.1.245  and  udp  port 53
```

The attacker uses the first three commands to fool a victim (whose IP address is 192.168.1.245) to believe that the attacker's system is the gateway (router). The final command listens for DNS traffic involving 192.168.1.245, and any queries for hosts beginning with www or mail will be answered with an IP address of 192.168.1.100. If 192.168.1.245 attempts to open his web browser to yahoo website, the connection will be diverted to the webserver running on 192.168.1.100, which is the attacker's machine.

3.1.3 MAC Spoofing

MAC spoofing attacks occur when an attacker sends a message on the network with a victim's MAC address instead of his (attacker's) address. Watch a demo on MAC spoofing attack. The attacker changes the MAC address of his computer to a MAC address of the victim's machine.

MAC spoofing can be carried out in the following ways:

A. modify of MAC address
B. generate a random MAC address
C. configure a MAC address of another manufacturer

D. configure a MAC address without modifying the manufacturer and then activate the new MAC address automatically.

You can prevent MAC spoofing using both protection and active detection (network monitoring and analysis). These include:

- Enforce strict access controls to prevent unauthorized access to the company's network. This includes restricted access to the network connection by visitors.
- Ensure you do not allow unauthorized persons in the company's premises and that visitors are well monitored. This will prevent unauthorized connection or manipulation of the internal network via direct connection to the ethernet using a cable, thus bypassing the Wi-Fi protection.
- prevent eavesdropping of existing MAC addresses by implementing IPsec technologies and encryption of trasmissions.

3.2 Scanning

Port scanning is a process used to detect open ports of a workstation or a server. Gamers and hackers use this method to identify the available ports and to fingerprint services running on them.

3.2.1 TCP Scanning

To scan for a TCP open port, a hacker sends an SYN packet to the server. The port is open if the server responds with an SYN-ACK. The port is closed if the server replies with an RST and fails to complete the handshake.

3.2.2 UDP Scanning

Unlike TCP, UDP is a connectionless protocol and does not require a three-way handshake. In UDP scanning, the port scanner sends a UDP packet to the port. Click the link for a simulation of UDP scanning attack. The port is closed if the destination machine replies with an ICMP packet; otherwise, the port is open. UDP port scanning is often unreliable because firewalls block ICMP packets leading to the generation of false positives.

3.2.3 Port Scanners

Some of the port scanners used for Windows OS are also applicable to Linux OS. We shall discuss scanners like Nmap, Zenmap and Netcat which we explored in unit 1.

- **Nmap:** It is the most general-purpose and detailed port scanner available. It can handle a variety of tasks such as port scanning, OS fingerprinting and vulnerability scanning. Nmap provides a variety of options for quick and effective scans. Run the following commands to install Nmap in Linux.

```
sudo apt-get
update
sudo apt-get
upgrade -y
sudo apt-get install nmap -y
```

To use Nmap to identify open ports and running services on a server such as the hackme server, simply type nmap and the server address. That is

```
nmap hackme.org
```

To scan UDP ports, include -sU option sudo command because the scan requires root privileges.

```
sudo nmap -sU hackme.org
```

Other options available in nmap are:
-p- :   Scan for all 65535 ports
-sT :   TCP connect scan
-O :   Scans for the installed operating system
-v :   Verbose or detailed scan
-A :   Aggressive scan, scans for everything
-T[1-5] : To set the scanning speed
-Pn :   used in case the server blocks ping

- **Zenmap:** is a GUI interface of Nmap, which eliminates the need to remember a lot of commands. To install it, type

```
sudo apt-get install -y zenmap
```

To scan a server, enter its address and select any of available scan options.

- **Netcat:** Netcat is a raw TCP (and UDP) port writer and port scanner. It is not as fast as Network Mapper because it uses connect scan. To install it, type

  ```
  ubuntu@ubuntu:~$ sudo apt install netcat-traditional -y
  ```

  To check for an open port, write

  ```
  ubuntu@ubuntu:~$ nc -z -v hackme.org 80
  ```

  An output such as

  ```
  hackme.org [217.78.1.155] 80 (http) open
  ```

Indicates that port 80 on the hackme server is open. An open port means the server can communicate with other devices via the port.

To scan for a range of ports, type

```
ubuntu@ubuntu:~$ nc -z -nv 127.0.0.1 20-80
```

The following outputs

```
(UNKNOWN) [127.0.0.1] 80 (http) open
(UNKNOWN) [127.0.0.1] 22 (ssh) open
```

shows that port 80 on hackme server uses the http (hypertext transfer protocol), while port 22 runs on ssh (secure shell protocol). Both ports are also open.

- **Unicornscan -** is a detailed and efficient port scanner used mainly for vulnerability research. It has some features which Nmap does not possess. Some of these features include:
  - ✓ Asynchronous stateless TCP banner grabbing
  - ✓ Asynchronous protocol-specific UDP Scanning (sending enough of a signature to elicit a response)
  - ✓ Active and passive remote OS, application, and component identification by analysing responses.
  - ✓ PCAP file logging and filtering
  - ✓ Relational database output
  - ✓ Custom module support
  - ✓ Customised data-set views

To install Unicornscan, type

```
ubuntu@ubuntu:~$ sudo apt-get install unicornscan -y
```

3.3 Denial of Service Attacks

Attackers use denial of service to prevent legitimate users from accessing specific computer systems, devices, services or other resources. This is accomplished by flooding the target system, network or application with enormous traffic, or sending it malicious packets that make the system crash. This is a demo on how to perform ping of death DoS attack. The goal of DoS is not to steal information or cause a security breach. Dos attacks lead to loss of reputation, which may result in loss of time and money. Fig 15 illustrates a typical DOS attack

There are two main categories of Dos attacks, namely;

- DoS: a single host performs this.
- Distributed DoS: a type of DoS attack performed by a group of compromised hosts that attack the same target.

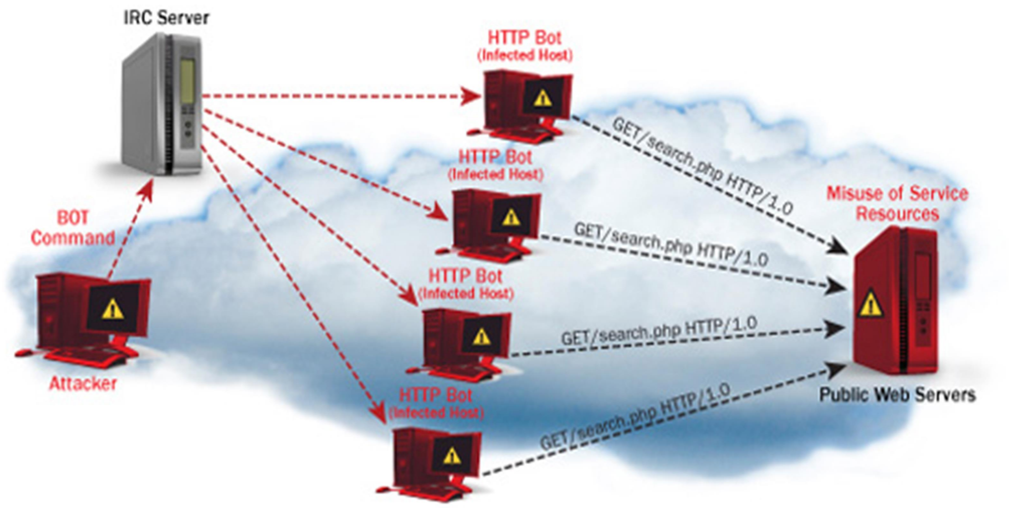

Fig. 15 How DoS Attacks Work

Identify common types of DoS attacks in Linux?

3.3.1 Ping of Death

The ping command tests network availability by sending small data packets to a host or server. The ping of death exploits this feature by sending ICMP packets that are greater than 65,536 bytes, which is the maximum limit that TCP/IP allows. See video on the ping of death attack (here). TCP/IP fragmentation breaks the packets into small chunks that are sent to the server. This causes the server to freeze reboot, or crash because the server receives more data packages than it can handle.

3.3.2 Smurf

This involves sending a large number of Internet Control Message Protocol (ICMP) packet to an Internet Broadcast Address. The attacker replaces the reply IP address with that of the intended victim. Hosts on the Internet broadcast Address send all their replies to the victim instead of the IP used for the pings. A smurf attack rebroadcasts a single ping 255 times because a single Internet Broadcast Address can support a maximum of 255 hosts. This loads the network with overwhelming traffic and slows down its performance. In the worst-case scenario, it renders the network unusable by legitimate users.

3.3.3 Buffer Overflow

Computer's RAM uses a temporary storage known as a buffer to store data. This is to enable the CPU process the data before writing the result to the disk. Buffer overflow (or buffer overrun) attack loads the fixed-sized buffer with more data than it can hold. This leads to an overflow of buffer and corruption of stored data. For example, buffer overflow occurs when you send emails containing 256 character file names.

3.3.4 Teardrop

This type of attack sends large data packets, which are broken down by TCP/IP into small fragments before they are transmitted to the destination. The fragmented packets are reassembled on the receiving host. The packets are sett in such a way that they overlap each other. This causes the victim host to crash while re-assembling the packets.

3.3.5 SYN Attack

SYN attack exploits the three-way handshake, which TCP uses to establish communication. SYN attack floods the target with incomplete SYN messages. This makes the target to allocate memory resources that are never used and prevents legitimate users from accessing the system.

3.3.6 DoS Attack Tools

Tools used to carry out DoS attacks include:

- Nemesy: used to generate random packets on windows systems. Click link to download Nemesy.
- Land and LaTierra: used to spoof IP addresses and establish TCP connections.
- Blast: download from this link
- Panther: used to flood a victim's network with UDP packets.
- Botnets: a large number of compromised computers used to perform a distributed denial-of-service attack.

3.3.7 Protection against DoS Attacks

An organisation can use the following policy to prevent DoS attacks.

- Install security patches to minimize SYN flooding, which exploits bugs in the operating system.
- Use intrusion detection systems to identify and prevent illegitimate activities.
- Use firewalls to prevent DoS attacks by identifying a malicous IP and blocking all traffic originating from it.
- Use the Access Control List to configure routers to mimimize access to the network and block unauthorized traffic.

3.4 Malware Attacks

Malware is a “code used to perform malicious actions” (SANS Technology Institute, 2015). Malware infects a target by exploiting vulnerabilities in host machines. This may involve tricking the victim into executing a file which results in the automated exploitations of specific Linux OS vulnerabilities. Malware consists of many parts such as exploit code, payload, propagation mechanism and command and control functions (Amine, Mohamed,&Benatallah,2014)

Linux, like any OS, has design flaws and security vulnerabilities, which makes it possible for hackers to craft exploits that attack the Linux platform.

Three factors, however, make the Linux platform less susceptible to virus attacks than Windows or Mac operating system.

1. Faults get fixed quickly due to the large community and Linux's open-source nature. Anyone with the time and knowledge can sit and fix an error.
2. It is not targeted by virus developers as much as other platforms
3. It has a more secure design than Windows, making the development and spread of viruses more difficult

3.4.1 Worms and Targeted Attacks

Virus and worms exploit vulnerabilities network services, such as secure shell (SSH) and web servers to attack workstations and servers running Unix-like applications. These attacks are not widespread as Linux platforms provide patches as soon as a vulnerability is found. However, hackers can compromise the security of a network installation using an attack that exploits a vulnerability that is not publicly known. Even in the absence of such vulnerabilities, servers that are protected with weak passwords can be attacked.

3.4.2 Web Scripts

Malware can use Linux servers to attack clients without carrying out any attack against the server itself. Such attacks occur in situations where the server does not restrict or check web content and scripts sufficiently. Hackers also use complex or advanced malware to attack Linux servers. When the malware gains full root access, hackers can attack the system by modifying information like replacing binaries or injecting modules. This may redirect users to different content on the web. For example, a common graphical interface (CGI) script used for comments, can accidentally allow hackers to include code for exploiting vulnerabilities in the web browser.

3.4.3 Cross-Platform Viruses

Cross-platform viruses leverage on the widespread use of cross-platform applications. These viruses became popular after the discovery of a type of an OpenOffice.org virus called Badbunny. It is important to consider cross-platform viruses because malware that can survive on different platforms and application environments are pushed out regularly via Web sites. Attackers can attack a web server with a JavaScript infector regardless of platform.

3.4.4 Malware and Rootkits Detection on Linux Servers

Linux servers suffer attacks and port scans regularly. You can secure your systems by configuring your firewall properly and carrying out regular security system updates. This also helps to protect your server from any program that can disrupt its normal operation.

The following malware scanning tools can identify a virus, malware, rootkits and malicious behaviours.

- Lynis: a free, and widely used tool used to scan and audit Unix/Linux operating systems. It scans systems to uncover security information and issues related to file integrity, configuration errors; performs firewall auditing, checks installed software, file/directory permissions, and so much more.

- Chkrootkit: this is a free and open-source tools that detects rootkit on Unix-like systems. It alos detect unknown security weaknesses on local machines. The chkrootkit application is made up of (1) a shell script that examines whether a rootkit has modified system binaries; and (2) other programs that detects various security concerns.

- Rootkit Hunter (RKH): Is a free, efficient and easy to use tool for scanning backdoors, rootkits and local exploits on POSIX compliant systems such as Linux. It monitors, analyzes and inspects a system to detect unknown vulnerabilities.

- ClamAV: is a well-known, open-source standard and general purpose cross-platform antivirus for detecting viruses, trojans and other malicious programs on a Linux systems. It is commonly used for mail gateway scanning.

3.5 Wiretapping

Wiretapping is used to listen to traffic on the network. The attack uses tools such as tcpdump or Wireshark to place the network interfaces into a promiscuous mode. For example, you can use wireshark packet sniffer to obtain usernames, passwords, and web pages. This redirects all packets from the switch to the tcpdump application, instead of the port.

Normally, network interfaces drop packets sent to them by network devices when the destination IP addresses are not configured on the host. Communication protocols and mechanisms such as ethernet, wifi, USB and cellular networks are susceptible to wiretapping.

Discussion

Form a study group comprising of Windows users, Linux users and those who currently use both operating systems simultaneously. Share your experience with these operating systems, particularly in the area of security. Discuss issues like susceptibility to and robustness against various security attacks.

Case Studies

Ransomware attack against Linux servers

The new strain of ransomware called Linux.Encoder.1 created by Russian antivirus firm, Dr. Web attacks website via the vulnerabilities in website plugins or third-party software. It encrypts MySQL, Apache, and home/root folders on Linux websites and servers. It also encrypts backup directories and the system folders related to Website files, pages, images, code libraries and scripts. Attackers usually demand for a ransom of 1 Bitcoin (~ *$300*) to decrypt the files.

Using malware to steal information

Symantec reported that 82 per cent of the popular malware compromise confidential information such as passwords. A keyboard keystroke logger is relatively cheap (~ $99) and can be used to capture more than 2 million keystrokes. Small sized physical keyboard logging devices can easily be inserted between the keyboard's cord and the port connecting the keyboard to the computer. It is also easy to capture passwords from a wireless keyboard even from a distance several meters away from where the device is located.

Buffer overflow in Linux

Older versions of Linux OS relatively susceptible to buffer overflow attacks because of the limited protecteion offerd by the kernel. An attacker can use the access rights of a compromised application to execute arbitrary code. The attack is more suitable for applications that gain root privileges even when executed by ordinary users via the setuid bit. However, Linux kernels developed from 2009 upwards include address space layout randomisation (ASLR), enhanced memory protection and other features which makes such attacks difficult to carry out.

Identify ways by which hackers use ransomware to exploit users? How do victims of ransomware exploits pay ransom to attackers?
What are the implications of a successful buffer overflow attack against Linus operating system?

4.0 Self-Assessment Exercise(s)

1. ---------- is an attack in which legitimate domains names are resolved into fake IP addresses.
   A. ARP spoofing
   B. DNS spoofing
   C. IP redirection
   D. SYN attack
   Answer: B

2. A hacker who attempts to scan for a TCP open port sends a sends a SYN packet to the server. The port is open if the server responds with a --------
   packet.
   A. ACK
   B. RST
   C. SYN-ACK
   D. ACK-SYN
   Answer: C

3. Which of the following is not a characteristic of DoS attacks?
   A. It prevents legitimate users from accessing specific computer systems, and services
   B. It floods the victim system, network or application with enormous traffic, that make the it crash.
   C. The goal of DoS is to steal information or cause a security breach
   D. It can lead to loss of reputation or time.
   Answer: C

4. --------- attack exploits this feature by sending ICMP packets that are greater than 65,536 bytes.
   A. ping of death
   B. Smurf
   C. Buffer overflow
   D. SYN flood
   Answer: A

5. Which of the following does not protect against denial of service attacks?
   A. Install security patches to minimize SYN flooding, which exploits bugs in the operating system.
   B. Use intrusion detection systems to identify and prevent illegitimate activities.
   C. Use firewalls to prevent identify a malicious IP and block all traffic originating from it.
   D. Install the latest antivirus
   Answer: D

6. The following are reasons why Linux are less susceptible to virus attacks than Windows or Mac operating system except:
   A. There is no virus that can compromise Linux systems
   B. Bugs get fixed quickly due to the large community and Linux's open-source nature.
   C. It is not targeted by virus developers as much as other platforms
   D. It has a more secure design than Windows or MAC
   Answer: C

7. -------- is a tool that can be used to sniff usernames, passwords, and web pages.
   A. ClamAV
   B. Lynis
   C. Wireshark
   D. Rootkit hunter
   Answer: C

5.0 Conclusion

Linux is an open-source platform which enables a large community of developers to identify and fix vulnerabilities as quickly as possible. This makes it more secure and stable than proprietary operating systems such as Windows and Mac. However, hackers are usually one step ahead of security professionals and still find some vulnerabilities which they use to exploit Linux systems. Knowledge of common vulnerabilities and exploits will help Linux administrators evaluate the security of their systems and networks. A mastery of the tools and techniques for cracking Linux OS will enable system administrators to detect loopholes in their systems before attackers can use the same loophole to compromise security.

6.0 Summary

In this unit, you have acquired the skills for evaluating the security of Linux-based systems and networks. The chapter introduced you the vulnerabilities in Linux operating systems and the attacks that can be used to exploit these vulnerabilities. You have also learned the methodologies, tools and techniques used by hackers and pen testers to compromise the security of Linux OS. In the next chapter, you will learn about the vulnerabilities and exploits that target web servers and web applications

7.0 References/Further Reading

Amine, A., Mohamed, O.A. & Benatallah, B. (eds.).(2014). Network Security Technologies: Design and Applications: Design and Applications. IGI Global.

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing*. (2nd ed.). Elsevier.

Distler, D. (2008). *Malware Analysis: An Introduction.* SANS Institute. Available here

Hall, G. & Watson, E. (2016). *Hacking, Computer Security Testing, Penetration Testing and Basic Security*. Available here

Helba, S. (2010). *Ethical Hacking and Countermeasures: Threats and Defence Mechanisms*. New York: Cengage Learning.

SANS Institute (2015). *Malware Analysis Fundamentals.* Available here
Smith, R.W., (2009). CompTIA Linux+ Study Guide. Wiley Publishing, Inc.

Unit 3: Web Servers and Web Applications

Contents

1.0 Introduction

In this unit, you will acquire the skills for evaluating the security of web server and web applications. To achieve this, you will learn the vulnerabilities inherent in web servers and web applications and the attacks that can be used to exploit these vulnerabilities.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe webserver attacks
- explain the types of attacks against web applications
- evaluate vulnerabilities of web servers and web application.

3.0 Main Content

3.1 Web Server Attacks

Organisations make information resources and services available to users by hosting their websites on web servers. The servers are computers running an operating system; and are connected to the back-end database, where they run various applications. Attackers can use vulnerabilities in the applications, database, operating system or in the network configuration to attack the webserver. The vulnerability stack of a web server is illustrated in Figure 16.

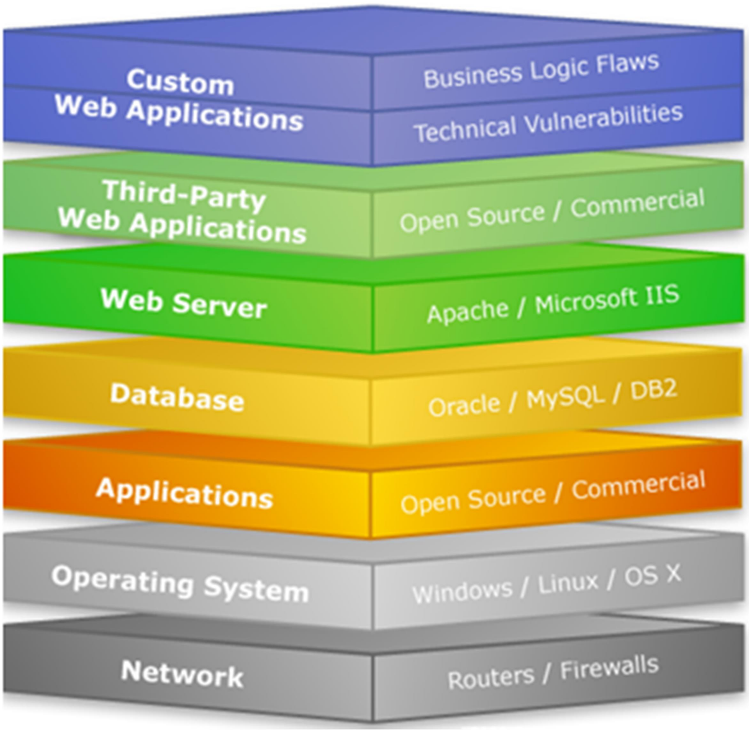

Fig. 16: Vulnerability Stack of the Webserver

Examples of web servers are Internet Information Service (IIS) and Apache webserver.

3.1.1 Denial of Service Attack

Hackers cause a denial of service (DoS) attack by sending many packets to the server at the same time. This overwhelms the capability of the web server and prevents the server from responding to legitimate clients' requests. Another alternative is for the attacker to take advantage of a programming error in the application to cause an attack.

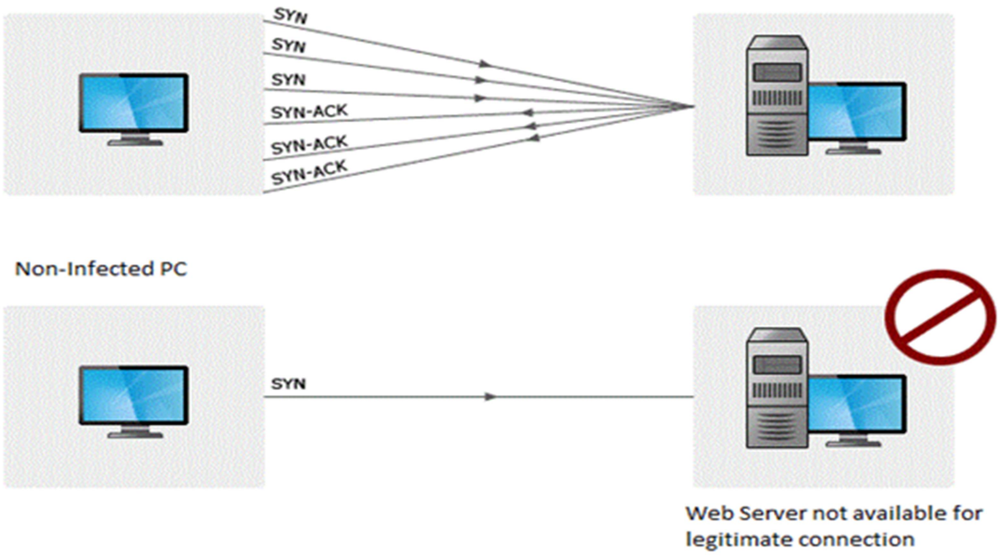

Fig. 17: Web-based DoS Attack

Security administrators use network flow analyser to detect web-based DoS attacks.

3.1.2 URL Interpretation Attack

URL interpretation attack (also called URL poisoning) occurs when an attacker manipulates the URL by changing its meaning and without altering the structure. The attacker changes the parameters of the URL so that he can obtain additional information from the web server. The attack is very common with CGI-based websites. URL interpretation attack can be prevented by regular installation of patches and updates and through in-depth checking and verification of the web server configuration.

3.1.3 Impersonation Attack

Impersonation attack (also called IP spoofing) is a situation whereby a hacker uses the IP address of a legitimate user to access the webserver. The attacker uses specialized programs to falsify IP addresses and use fake addresses to gain unauthorized access to the webserver. Impersonation attacks leverage on the weaknesses in the authentication protocols to gain unauthorized access to the web servers and the databases. You can prevent such attacks by using a strong authentication algorithm and verifying all the traffic going to the server. Other countermeasures include locking down of web configurations and using a firewall to track machines sending IP requests to the webserver. You can also disable cookies to prevent hackers from using them for impersonation attacks.

3.1.4 Directory Traversal

This allows a hacker to gain privileged access via the application. The attacker uses the application to get beyond the webroot directory and execute OS commands as well as obtain sensitive information or access restricted directories.

3.1.5 Misconfiguration Attack

This attack occurs due to wrong or insecure configuration of the server. A hacker can launch various exploits such as password cracking, phishing, error-based SQL injection and command injection if an administrator enables unnecessary services, uses default configuration files are used, or fails to mask verbose/error information.

3.2 Web Application Attacks

These attacks target applications which run on web servers. These applications are designed to provide services to multiple users who connect to servers using their client systems. Users interact with server-based applications with the aid of client-side applications on their devices.

3.2.1 Cross-Site Scripting

These attacks occur in web applications which contain reflected input. For example, if a web application requests a user to enter his name in a text box. On clicking Submit, the web application displays a new page containing the string:
"Hello, *name*."

A hacker can use such application to decieve an innocent victim. Remember, you can use HTML tags <SCRIPT> to embed scripts in web pages as shown below
</SCRIPT>.

Assume you enter the following text in the Name field, in the Name field,
Mike<SCRIPT>alert('hello')</SCRIPT>
instead of entering *Mike*
The browser displays execute the script and displays the text whenever the web application "reflects" input on a web page. This makes the script to opens a pop-up window containing "hello".

See a demo on cross-site scripting (reflected XSS). A hacker could use a more advanced script to obtain the user's a password and transmit it to another attacker. A hacker can use the link "Check your account at First Bank" to create a web page and encode a form input. A user who clicks the link will see a web page which looks like a genuine First Bank website with a valid SSL certificate. Such a website executes malicious script embedded in the input and included as part of the valid web page.

3.2.2 Website Defacement

An attacker can use SQL strings to construct a query once he discovers that a website does not sanitise the input field properly. The web browser executes the malicious query and this results in website defacement. The hacker may also fill the backend database with malicious/unrelated data. The website becomes defaced and displays irrelevant data when it is launched.

3.2.3 SQL Injection

SQL injection attack modifies a backend database or extracts information from it. This occurs in a situation where the server executes SOL query without validating the input data. See this link for more explanation and demonstration on SQL Injection attack. Attackers use this attack to gain unauthorized access to the underlying database (Stewart et al., 2015). The attack is common in e-commerce websites which uses a large database to store user's information.

Fixing SQL injection vulnerability requires a thorough source code review, using least privilege access control model for database applications and removing redundant (and unnecessary) database users and procedures.

3.2.4 Buffer Overflow

Buffer overflow attack is the intentional overflowing of the buffer memory allocated for the user's input (Stewart et al., 2015). An application allocates a stack with a memory location an input data is stored. A hacker fills the allocated space with arbitrary data leaving no room for the storage of user input data. This video (here) will show you how to exploit a buffer overflow vulnerability.

The best way to address buffer overflow attack is to install vendor-supplied patches and software updates. A good mitigation strategy is to check the bounds within the application. Oher effective countermeasures are buffer overflow testing and source code review.

3.2.5 Source Code Disclosure

Hackers use source code disclosure attack to retrieve the application files without performing any parsing. The attacker recovers the application's source code and analyzes it to find vulnerabilities that can be used to exploit the web servers. It is usually caused by configuration errors or poor design of the application. This attack enables the hacker to access the source code of the server application. These codes should not normally be accessible to anyone apart from the authorised programmers. Source code disclosure attack can be prevented by a proper check of the configuration of web server proxy, and exercising due diligence while creating URL mappings to the internal servers.

Discussion

Several web server and web application attacks have been discussed in this unit. Some practical demos and simulations of such attacks were also presented. Which of them:

- ✓ Are easier or difficult to perform?
- ✓ Have the most and least devastating effects?
- ✓ Can be fixed more easily than the others?

What would you recommend as solutions to these attacks?

Case Studies

Theft of more than one billion passwords via SQL injection attack

In August 2014, Hold Security (an IT Security company) revealed that a Russian hacking syndicate known as "CyberVor", stole **1.2 billion logins and passwords on 420,000 websites** worldwide. The report also mentioned that the attack might have compromised about 500 million email accounts. The hackers used botnets perform to carry out SQL injection attacks and gain access to databases. It was a large scale attack without any major consequence. Investigations by the FBI revealed that the information obtained by the attackers were only used to launch massive spamming attacks against social networks. The FBI was unable to uncover the real intention of the hackers.

Alteryx data leak exposes 123 million households due to server misconfiguration

Erros in server misconfiguration compromised an online database owned by Alteryx (a marketing analytics company), and exposed sensitive personal information of about 123 million households in the United States on a publicly accessible AWS S3 storage cache. This information included addresses, income, ethnicity and personal interests. Other details revelaed are phone numbers, email addresses, mortgage ownership, financial histories and whether dog lovers or cat lovers live in a household. The only exception was the Names of the people.

Identify the web application attacks you know.

In which ways can an organisation suffer losses as a result of web application attacks?

4.0 Self-Assessment Exercise(s)

1. A web server is vulnerable to which of the following DoS attacks?

   A. buffer overflow
   B. ping of death
   C. HTTP gets Request Flooding
   D. All of the above
   Answer: D

2. Which of the following best describes a URL interpretation attack?

   A. occurs when an attacker manipulates the URL by changing its meaning and without altering the structure.
   B. occurs when an attacker manipulates the URL by changing its meaning and altering the structure.
   C. occurs when an attacker manipulates the URL without changing its meaning or altering the structure.
   D. occurs when an attacker manipulates the URL by altering the structure and without changing its meaning.
   Answer: A

3. ----------- attack modifies a backend database or extracts information from it.

   A. SQL injection
   B. Source code disclosure
   C. Cross-site scripting
   D. Web defacement
   Answer: A

4. A wrong or insecure configuration of the server can result in which of the following attacks?

   A. password cracking
   B. phishing
   C. command injection
   D. All of the above
   Answer: D

5. A hacker cannot achieve one of the following goals by carrying out directory traversal attack.

   A. gain privileged access via the application.
   B. execute OS commands
   C. obtain sensitive information or access restricted directories.
   D. Install virus and worm
   Answer: D

6. What is the key advantage of Session Hijacking?

A. It can be easily done and does not require sophisticated skills.
B. You can take advantage of an authenticated connection.
C. You can successfully predict the sequence number generation.
D. You cannot be traced in case the hijack is detected.

Answer: B

7. What is Hunt used for?
A. Hunt is used to footprint networks
B. Hunt is used for sniffing traffic
C. Hunt is used for hacking web servers
D. Hunt is used for intercepting traffic, i.e. man-in-the-middle traffic
E. Hunt is used for password cracking

Answer: D

5.0 Conclusion

Web servers and web applications provide how users access resources held in computer systems and networks. Unauthorised access, disclosure, modification or deletion of these resources can cause catastrophic damages to individuals and organisations. Hence the need to protect the servers and applications. A mastery of the methodologies, tools and techniques used by hackers to compromise the security of web servers and applications will provide penetration testers will the requisite skills and competencies to verify the security of their web platforms. Such regular assessments will also enable them to fix security holes that may exist in servers and applications before attackers can use the same vulnerabilities to exploit their systems

6.0 Summary

In this unit, you have acquired the skills for evaluating the security of web servers and web applications. The unit introduced you to the vulnerabilities inherent in web servers and web applications, as well as the attacks that can be used to exploit these vulnerabilities. You have also learned the methodologies, tools and techniques used by hackers and pen testers to compromise the security of web servers and web applications. In the next module, you will learn about the vulnerabilities and exploits that target web servers and web applications

7.0 References/Further Reading

Bosworth, S., Kabay, M.E. & Whyne, E. (Eds.).(2014). *Computer Security Handbook*. (6th ed.). Vol. 1, Wiley & Sons, Inc,.

Brumley, B.B. & Tuveri, N. (2011). “Remote Timing Attacks are Still Practical.” Proceedings of the 16th European conference on Research in computer security, Pp. 355-371, Leuven, Belgium, Sept. 12-14, 2011. Springer-Verlag Berlin, Heidelberg.

Canavan, J.E. (2001). *Fundamentals of Network Security*. London: Artech House.

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing*. (2nd ed.). Elsevier.

Ferrigno, J. & Hlaváč, M. (2008), *When AES Blinks: Introducing Optical Side Channel, IET Information Security,* 2 (3): 94–98, doi:10.1049/iet-ifs:20080038

Hall, G. & Watson, E. (2016). *Hacking, Computer Security Testing, Penetration Testing and Basic Security*. Available: https://www.pdfdrive.com/hacking-computer-hacking-security-testingpenetration-testing-and-basic-security-e178134258.html

Helba, S. (2010). *Ethical Hacking and Countermeasures: Threats and Defence Mechanisms*. New York: Cengage Learning.

Stewart, J.M., Chapple, M. & Gibson, D. (2015). *CISSP Certified Information Systems Security Professional Study Guide.* (7th ed.). John Wiley & Sons, Inc

Module 3: Types of Attacks

Module Introduction

There is a substantial increase in the number of cyber-attacks coordinated using malware. These attacks undoubtedly target government, military, public and private sectors to extract valuable information and achieve other goals. Therefore, you need the knowledge, skills, and tools required to understand malware. This is to enable you to detect, investigate and defend against malware attacks. In module 2, you learned how hackers use vulnerabilities to carry out targeted attacks on Microsoft Windows systems, Linux systems, Web Servers and Web applications. In this module, I will take you through the use of malware such as viruses, worms, Trojans and spyware to launch malicious activities on victims. I will also take you through the techniques used by hackers to entice users into revealing sensitive information or installing malicious software on victims' computer systems. Moreover, I will explain how massive coordinated attacks are conducted using denial of service attack. Finally, I will take you through how spyware is used to steal information and monitor user activity.

This module is classified into the following three units:

Unit 1: Trojans and Viruses
Unit 2: Social Engineering and Distributed Denial of Service
Unit 3: Spyware

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1: Trojans and Viruses

Contents

1.0 Introduction

Malicious software (malware) such as viruses, worms and Trojans are used by hackers to launch attacks on computer systems. Each type of malware uses a unique approach of attacking a computer system. In this unit, I will take you through how viruses, worms and Trojan horses work. Therefore, you will understand the infection behaviour of each malware to defend a computer system. In the self-assessment exercise at the end of the unit, you will have the opportunity to check or gauge your understanding of viruses, worms and Trojan horses and provide preventive methods against the different categories of malware.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe viruses, worms and Trojans, and how they can be used to infect systems
- highlight the tools and techniques use in developing viruses, worms and Trojans
- discuss how to defend against viruses, worms and Trojan horses.

3.0 Main Content

3.1 Viruses

A virus is a parasitic program that spreads from one computer system to another by attaching itself to other files. When the file is accessed, the virus is activated. Once activated, the code carries out whatever attack or action the hacker wishes to execute. The main and most common actions of a virus are corrupting or destroying data and disrupting computer operations.

3.1.1 Types of Viruses

There exist different types of viruses. In this section, I will briefly take you through some of the major virus types. Viruses can be classified by either their propagation methods or their activities on the target computer systems. Understanding each type of virus can give you a better idea of how to thwart them and address the threats they pose.

1. **Macro Virus**: Macro viruses infect macros in office documents. Macros are mini-programs designed in office products, such as Microsoft Office, to replace repetitive series of actions. These actions include searching Microsoft Outlook address book, deleting or sending out emails. Therefore, hackers leverage this to develop a macro virus that can compose an email using Microsoft Outlook. The virus then attaches a malicious script to the email and spread it to the email addresses found in the address book of the victim computer.
2. **Multi-partite Virus**: Multi-partite viruses are used by hackers to attack a computer in multiple ways. The attack is conducted by infecting the boot sector of the hard disk and one or more files. Therefore, if the copy of the virus that infects the boot sector is removed, the copy of the virus that infects the file(s) will re-infect the computer and vice versa.
3. **Armoured Virus**: An armoured virus is designed with a technique that makes it hard to analyse. The technique used to shield the virus is code confusion. In this type of virus, hackers designed the code such that if the virus is disassembled, the code will be difficult the read and understand.
4. **Sparse Infector Virus**: A sparse infector virus hide from antivirus software by performing its malicious activities sporadically. The malicious activities of this virus occur at irregular interval and place; that is, the user will see symptoms for a short period, then no symptoms for a time. For example, the virus can infect a program, but it will only execute after the program is executed five times.

Polymorphic Virus: A polymorphic virus changes its contents periodically to avoid detection by antivirus software. The virus changes itself by rewrite or changing the code after every execution. The virus can also change itself completely. Polymorphic viruses uses several techniques that include:

a. **Polymorphic Engines**: They are designed to change the design of the virus design while keeping the payload intact. The payload is the part that does the infection.

b. **Encryption**: This is used to scramble or hide the payload so that antivirus engines cannot detect the virus.

3.1.2 How Viruses Infect Systems

A virus spreads initially by sending a copy of itself to email addresses. The delivery of the virus to an email address is achieved using the email addresses found in the email address book of a victim's computer, such as Microsoft Outlook. In this case, the virus searches the address book and email itself to the email addresses found as an attachment or a link. Another method of initial infection is to design an internal email engine for the virus and a number of the target email address, to begin with. In this case, the virus uses its independent email engine to send a copy of itself to several targets.

The method of delivering a virus to a target computer relies on user activity. The hacker will entice users in the email address to perform specific actions to get the virus installed on their computers. These actions include visiting a website through a link or downloading and opening a malicious file. Regardless of the way a virus arrives at a computer system, it will attempt to

1. Spread by emailing itself to email addresses found in the victim's computer.
2. Cause some harm to the computer system such as deleting files and changing system settings.
3. Attach itself to files and programs found on the computer.
4. Cause malicious activities.

The activities of a virus on arriving at the target computer depends on the type of virus and the goal of the hacker. Apart from using email addresses, an infected file in a victim computer can be passed to another computer by sharing the file through a network or external media such as removal drives.

Thus, a virus generally spreads from one computer to another through human actions such as sending emails with the virus as attachments, visiting website or link to download the virus or sharing a virus-infected file through a network or removable drive.

What is the difference between a virus and a worm?

3.1.3 Defensive Techniques

Several techniques and tools can be used to deal with the threat of viruses.

1. **Email Attachment**: This is the most common way for a virus to spread. Here are some rules that reduce the odds of virus infection.
    a. Use scanners to verify an attachment.
    b. Do not open suspicious attachment.
    c. Use a code word to share attachment.

    d. Do not use “security alerts” that are delivered through email attachments.
2. **Education**: This is to inform users on how to safeguard the spread of the virus to their computer systems. These include:
    a. Do not allow employees to bring media from home.
    b. Instruct users not to download files except known and trusted sources.
    c. Do not allow workers to install software without permission from the IT department of the company.
    d. Inform IT or security of strange system behaviours or virus notifications.
    e. Ban flash drives and portable hard drives.
    f. Limit the use of administrative accounts.
3. **Antivirus**: Antiviruses are software designed to run in the background on a system, staying vigilant for the activity that suggests viruses and stopping or shutting it down. Antiviruses are effective tools, but they can be so only if they are kept up-to-date.
4. **Applying Updates**: The are patches released by vendors of operating systems and other application software to close holes and address vulnerabilities on systems that viruses could exploit. Missing a patch or update can make a computer system open to virus attack.

3.2 Worms

A worm is a self-propagating virus that uses network awareness to spread. Worms require no action from a user to execute or move from one computer system to another.

What is the difference between a virus and a worm?

A worm is a self-propagating malware that exploits vulnerabilities and spread across networks by transferring a copy of itself. Unlike a virus, worms do not require a host program to propagate; that is, they self-contained. Worms can also cause substantially more harm than a virus because it can search for computer systems across networks and spread its infection. Generally,

1. A worm can be considered as a virus that can replicate and consume memory, but not attach to other programs; that is, they do not need a host program to function.
2. A worm spreads through networks automatically.

3.2.1 How Worms Infect Systems

The infection of a worm occurs by exploiting network services or weaknesses and flaws in software design available on a computer system. Worm infection often begins with a single host, which then targets a set of Internet Protocol (IP) addresses on the Internet, searching for more vulnerable computers. If the worm successfully hits a vulnerable computer, it then transfers over a copy of itself to the new computer, which begins executing the worm code.

A worm spreads a copy of itself after discovering a vulnerable host. The distribution of the worm is classified as

1. **Self-carried propagation**: The worm is carried along during target discovery; in other words, the worm propagates by attaching a copy of itself in the payload of the initial packet sent for discovering a vulnerable host.
2. **Second-channel propagation**: The worm uses a secondary contact to transmit the worm after successfully contacting a vulnerable host.
3. **Embedded propagation**: The worm is distributed in a normal communication channel.

The propagation of worms uses either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Worms are usually intended to cause denial-of-service (DoS) attacks, collect personal or confidential information from an infected host and perform other malicious activities. These are deleting files and, in some cases, creating a backdoor on the infected host, which allows the attacker to control the host remotely.

3.2.2 Worm Defensive Techniques

1. **Antivirus**: One of the primary lines of defence against worms is reputable antivirus and anti-spyware applications. Having an antivirus application on a system helps prevent a worm infection, but only if it is kept up-to-date. Modern and up-to-date antivirus applications can easily stop most worms when they appear.
2. **Firewall**: Another way to stop worms is the firewall. A firewall is a valuable tool as it can block the scans to and from a system that worms use both to spread the infection and to deliver it from an infected system to other systems. Most modern operating systems include this feature as part of the core system.

3.3 Trojan Horses

A Trojan horse (or Trojan) is a program that carries something of hidden malicious intent. This hidden characteristic of Trojans enables the malware to hide from detection. A program is said to be "Trojaned," if it has been infected or embedded with some functions that are malicious in purpose. A variety of legitimate software packages can be used to hide Trojans. These packages include games, chat software, email, flash movies and other interesting software packages.

A successfully planted Trojan on a system usually opens what is known as a **backdoor**. These openings enable an attacker to bypass normal security measures on a system and gain acces to the system remotely without detectection. Therefore, the attacker can steal information, or use the system launch an attack.

Trojans use overt and covert channels to transfer information between systems and processes in ways that are supported and unsupported, respectively. Overt channels represent the path that data and other information are supposed to travel. As such, the paths can be properly monitored and controlled. Covert channels are said to be in effect whenever data and other information are transferred over mechanisms not specifically designed to carry the desired information.

How do hackers develop and use a Trojan for attack?

Attaching a Trojan to a legitimate program can be achieved using wrappers. Wrappers enable a hacker to merge a malicious program with a harmless and legitimate program to produce a single executable from both programs. The new executable is then shared to users for download. Wrapper programs include:

1. **EliteWrap**: EliteWrap is a wrapping tools that provides rich feature set such as the ability to perform redundancy checks on merged files and the ability to check if the software will install as expected. Furthermore, EliteWrap can be configured to allow an attacker choose an installation directory for the payload. Finally, EliteWrap enables installing software secretly without any user interaction.
2. **Saran Wrap**: A wrapper program specifically designed to work with and hide Trojans. It can bundle Back Orifice with an existing program into what appears to be a standard "Install Shield" installed program.
3. **Trojan Man**: This wrapper merges programs and can encrypt the new package in order to bypass antivirus programs.
4. **Teflon Oil Patch**: Another program designed to bind Trojans to a specified file in order to defeat Trojan detection applications
5. **Restorator**: An example of an application designed originally with the best of intentions but now used for less than honourable purposes. Restorator has the ability to add a payload to a package, such as a screen saver before it is forwarded to the victim.
6. **Firekiller 2000**: A tool designed to be used with other applications when wrapped. This application is designed to disable firewall and antivirus software.

3.3.1 Types of Trojans

There are many different types of Trojans. These include:

1. **Remote Access Trojan**: Remote access Trojans (RAT) are designed to allow attackers have control over a target system.
2. **Data Sending Trojan**: Trojans of this type are designed to capture and redirect data to a hacker. The types of data these Trojans can capture vary but can include anything from keystrokes and passwords to any other type of information that may be generated or reside on the system. This information can be redirected to a hidden file or even e-mail if there is a predefined e-mail account.
3. **Destructive Trojan**: Trojans of this type are designed to do one thing only: destroy data and kill a system.
4. **Denial of service (DoS) Trojans**: DoS Trojans are designed to target a specific service or system, overwhelm it and shut it down.
5. **Proxy Trojans**: These Trojans allow attackers to use a victim's computer system to perform their own activities. Using a victim's system to carry out a crime makes locating the actual perpetrator much more difficult.
6. **FTP Trojans**: These Trojans are designed to set up the infected system as an FTP server. An infected system will become a server hosting all sorts of data including illegal software, pirated movies and music or pornography.
7. **Security Software Disablers**: These Trojans are designed to specifically target the defensive mechanisms present on a system and shut them down. Therefore, if a system has antivirus or firewall installed, the application will be disabled. Trojans often use this strategy first to infect a system and then perform activities from one of the other categories, such as setting up a proxy server or FTP site.

3.3.2 How Trojans Infect Systems

Trojans are designed to target an individual or a group of people. For example, if a hacker wishes to spy on a target, the hacker could craft a program specifically to attract the attention of the individual or group of persons. Once the Trojan is successfully installed, it downloads and installs a monitoring software unknown to the user or group of users. The software can then be used to spy the activities of the user(s) or perform other malicious activities.

Hackers have a range of options for getting Trojans onto a target computer. Here are the common methods for installing a Trojan:

1. **Peer-To-Peer Networks (P2P)**: This mechanism is common due to the increased number of individuals using P2P networks to obtain the software free of charge. A hacker can easily grab a legitimate piece of software, embed a Trojan in it and post it on file sharing and wait for victims to download it.

2. **Instant Messaging (IM)**: Delivering malicious software via IM has been very common as it is easy.
3. **Internet Relay Chat (IRC)**: IRC is a mechanism commonly used to deliver messages and software due to its widespread use and its ability to entice new users to download software.
4. **E-mail Attachments**: With the rise of e-mail as a communication medium, the practice of using it to distribute Trojans also rose. Trojans have been distributed in this medium as attachments and as clickable links.
5. **Physical Access**: Once an attacker gains physical access, it becomes relatively easy to install the Trojan and compromise the system.
6. **Browser Defects**: With many users forgetting to or choosing not to update their browsers as soon as updates are released, the distribution of Trojans becomes easier. Since Web browsers are designed by their very nature to treat content that they are sent as trusted, this allows malicious programs to run unabated.
7. **Freeware**: Downloading free software from unknown or untrusted sources can mean downloading a malicious software such as a Trojan.

The activities performed by attackers using a Trojan on a compromised include:

1. Data theft
2. Installation of software
3. Downloading or uploading of files
4. Modification of files
5. Viewing the system user's screen
6. Consuming computer storage space
7. Crashing the victim's system

Trojans require instructions from the hacker to fully realize their purpose after distribution. Once attackers release their code into the world, they switch their involvement from the distribution to the listening phase, where Trojans will call home, indicating they have infected a system and may be awaiting instructions.

3.3.3 Targets of Trojans

Here are some of the targets that tempt hackers to launch a Trojan attack:

1. **Credit Card Data**: Hackers tend to steal credit card data and personal information for shopping.
2. **Passwords**: Hackers tend to obtain user passwords in order to attack the victim’s computer, internet and backing information because most users reuse passwords.
3. **Insider Information**: Hackers tend to steal confidential or insider information of an organization that is not made public.

4. **Data Storage**: Hackers use data storage to host illegal music or movies and pirated software.
5. **Random Acts of Mischief**: In some cases, the hacker intends to irritate or annoy the system owner.

3.3.4 Symptoms of Trojan Infection

Some symptoms indicate the presence of a Trojan on a computer system. These includes:

1. Opening and closure of CD drawer.
2. Flipping of computer screen.
3. Screen settings change by themselves.
4. Redirection of web browser to an unknown webpage.
5. Windows colour settings change.
6. Screen saver settings change.
7. Right and left mouse buttons reverse their functions.
8. The mouse pointer disappears.
9. The start button disappears.
10. Chat boxes appear on the infected system.
11. The system shuts down by itself.
12. The taskbar disappears.
13. The account passwords are changed.
14. Legitimate accounts are accessed without authorization.
15. Modems dial and connect to the Internet by themselves.
16. CTRI+AIT+DEL stops working.
17. Apperance of a message that states there are other users still connected while restaring the computer.

3.3.5 Trojans Defensive Techniques

Applications that can be used to protect systems against Trojans are:

1. **Antivirus**: Having software in place that actively looks for infection and eradicates them is paramount.
2. **Anti-spyware**: This software works in concert with other forms of protection, looking for suspicious behaviour.
3. **Firewalls**: Stopping communications between software such as clients and servers can block Trojan attacks.
4. **Updates**: Updating software and systems is a key defensive strategy that can address defects in software such as browsers that can be exploited by hackers.
5. **Education**: Educating users on proper procedures and how to prevent Trojan infections.

Other tools can be used to determine Trojan infection. These include:

1. **Taskmanager**: It is provided with Windows and used to display detailed information about running processes.
2. **Ps**: The command equivalent to task manager, which is used to display the currently running processes on UNIX/Linux systems.

3. **Netstat**: Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics and more.
4. **Tlist**: A Windows-based tool used to list currently running processes on local or remote machines.
5. **TCPView**: A GUI tool by Winternals used to display running processes
6. **Process viewer**: A Windows Graphical User Interface (GUI) utility that displays data about running processes
7. **Inzider**: Lists processes on a Windows system and the ports each one is listening on. Inzider is useful in locating Trojans that have injected themselves into other processes.

Scenario

Mr Stark downloaded an unsigned free software online, immediately after installation, his computer hanged and he has to reboot. After the reboot, he couldn't find some of his files. He informed cybersecurity analyst about this, and after a thorough investigation, he was told that this event was triggered by malware embedded in the software he installed. What type of malware possess these characteristics that attack Mr Stark?

4.0 Self-Assessment Exercise(s)

1. One of the following is a technique that can be used to mitigate Trojans
   A. Antivirus
   B. Anti-forensics
   C. Firewall
   D. Update
   Answer: B

2. ____________ virus changes its form from time to time to avoid detection by antivirus software
   A. Macro Virus
   B. Multi-partite Virus
   C. Armoured Virus
   D. Polymorphic virus
   Answer: **D**

5.0 Conclusion

In this unit, you have learned how viruses, worms and Trojan horses work. Each malware has a unique pattern of infection. Viruses are mainly used to corrupt or destroy programs and files on a victim's computer because they are attached to a program or file in the system. However, for a more virulent attack and coverage, worms are more effective than viruses. This is due to their capability to search for vulnerable computer systems across networks and self-propagate their infections. This makes a worm a more suitable option for a massive attack on computer systems across networks hosts compared to viruses. Trojans are mainly used for espionage and stealthy malicious activities. Trojans are particularly more dangerous than viruses because tools are available for novice programmers and software developers to easily create and transmit Trojans. Generally, the three types of malware can be detected and prevented using good antivirus software, anti-spyware, firewall, intrusion detection/prevention systems and other monitoring tools, applying updates and user awareness.

6.0 Summary

In this unit, I discussed how computer systems and networks are attacked using viruses, worms and Trojan horses. Each type of attack comes in many distinct variations. It is obvious to you now that securing systems and networks from malware is critical. However, malware attacks are preventable. In most cases, prompt and regular patching of the system, use of antivirus tools, and blocking unneeded ports through firewall would prevent malware attack.

7.0 References/Further Reading

Ahmad, M. A. (2018). "The SAGE Encyclopaedia of the Internet Worm." In: *The SAGE Encyclopaedia of the Internet.* SAGE Publications Inc.

Chuck, E. (2016). *Computer Security Fundamentals* (3rd ed.), Pearson Education, Inc.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Oriano, S. & Solomon, M. G., (2011). *Hacker Techniques, Tools, and Incident Handling,* Jones & Bartlett learning

Unit 2: Social Engineering and Distributed Denial of Service

Contents

1.0 Introduction

In this unit, I will take you through the social engineering techniques used by hackers to make users fall into their trap of malicious activity. Having understood how malware such as virus, worm and Trojans work from Unit 1, this unit explores how hackers use social engineering to entice victims to reveal personal or organisational sensitive information or get the victim to have malware delivered and installed onto a computer system. I will also take you through a particular type of attack that is prevalent and dangerous – it is known as denial-of-service (DoS) attacks. I will finally take you through how a particular type of malware, known as a botnet, is used in denial of service attacks.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain social engineering attacks and their countermeasures
- discuss distributed denial of service (DDoS) attacks
- describe the tools and techniques used in launching DDoS) attacks
- describe how botnets are used to launch a coordinated DDoS attack.

3.0 Main Content

3.1 Social Engineering

Social engineering is when a hacker pretends to be a different person in order to acquire information that would be difficult to get by other means. The information acquired from the victim can then be used to steal files, destroy resources, commit fraud or spy on an organisation. Social engineering is distinct from physical security hack attempts, but they usually are carried out together. In social engineering, hackers exploit user negligence, not computer systems. Once the hackers gain the trust of the users, they exploit them and get information that helps conduct an attack. To carry out a social engineering attack, a hacker can pose as:

1. **Support Personnel**: Hackers claim that they require a user to install a software patch or update. They convince the victim to download the software, which enables the hacker to access the victim's system remotely.
2. **Product Vendors**: Hackers claims to be vendors of a particular product that an organization relies on. They claim they need to update the existing systems and request administrator passwords.
3. **Employees**: Hacker pretends to be an employee that misplaced their access badges for accessing the organisation's data centre. They inform the security department, who hand them keys, only for them to gain unauthorised entry to digital and physical records.

In-Text Question(s): What are the ways of conducting a social engineering attack remotely?

Email is the common vector used for social-engineering attacks. This happens in the form of phishing attack by posing as a trusted person via email or other electronic means and attempting to trick a user into giving up sensitive information. Phishing emails can be used to attract a victim to a malicious site or download malicious attachments that enables the hacker to gain control of the system. Another method of social engineering attack is to send a patch or software update to a victim in the form of a Trojan via email, claiming to be from a verified software manufacturer. Once installed, the hacker will have unrestricted access into a computer or network.

3.2 Performing Social Engineering Hacks

Hackers use a variety of methods to gain the trust of their target. This can be face to face or via electronic means, with the strategy being to use whatever mode of communication that the potential target is most comfortable with. Here are some strategies hackers use during social engineering:

3.2.1 Building Trust Via Words and Actions

Hackers try to establish trust with a victim. However, there few signs of a social engineering attack. These include:

1. Being too friendly or enthusiastic about meeting a person.
2. Talking about high profile people in the organisation
3. Bragging that they have authority in the organisation
4. Being nervous when asked questions
5. Over-elaborating about things that do not require such
6. Speaking like an insider, yet they are an outsider.
7. Knowledge of issues that outsiders should not
8. Appearing to be in a hurry
9. Asking weird questions

These are all signs that a person has malicious intentions. However, a good hacker will be very skilled at hiding these signs. Another strategy that hackers use is to find a way of assisting a victim and then asking for a favour. This is one of the most common and effective tricks in the social engineering attack. Conversely, hackers also use reverse social engineering technique. In this case, a hacker causes a specific problem to occur, and when the intended victim needs help, the hacker swoops in and solve the problem. Afterwards, the hacker will request for a favour.

A hacker may also falsify a work badge and get a fake uniform of an organisation just to blend in with the real employees. The employees in the organisation will assume that since the hacker dresses like them, he is an employee that can be trusted with information.

3.2.2 Phishing for Information

Hackers use technology to achieve social engineering attack goals. In most cases, they send a text message or email to a victim. The message will appear to originate from a source that the victim trusts. However, the email address or IP address that is displayed could simply have been spoofed. The email normally contains a link that the victim is asked to click. The link will take the victim to a website that appears legitimate and known to the victim. The aim is to steal confidential information by encouraging the victim to update their user IDs, social security number, and passwords.

3.3 Social Engineering Defensive Techniques

Hackers should never be underestimated. They can manipulate naive and untrained people to allow them access into a computer system. However, there are few countermeasures for social engineering attacks. Some of these measures apply mainly to organisations. There are also measures that individuals can take to protect themselves. For organisations, there are stringent organisational policies and user awareness and training.

3.3.1 Stringent Organisational Policies

1. Classifying information such that employees only have access to information relevant to their duties, not all levels of information.
2. Establish an identity system for all employees, independent contractors, and consultants.
3. Ensure that all employees, contractors, and consultants who do not work for the organisation any more return their user IDs.
4. Change user passwords regularly.
5. Take immediate action of suspicious behaviour and security breaches.
6. Take good care of private and proprietary information.
7. Make sure that all guests into the premises have an official escort.

If these countermeasures are to be as effective as possible, it is important to inform the people involved and enforce them across the board.

3.3.2 User Awareness and Training

If the employees of an organisation are to be effective in defending themselves against social engineering attacks, they will have to be trained in how to detect and respond to such threats. In establishing a long-term solution, the following must be kept in mind:

1. An organisation should continuously provide security awareness and training.
2. An organisation should set out security for personal and professional information as part of their job description.
3. An organisation should ensure that the content shared with people is tailored and controlled.
4. An organisation should give people incentives to report and prevent security incidents.

3.3.2 Individual countermeasure

1. Avoid giving out personal or confidential information to people unless you verify who is requesting it and why they need it.
2. Do not click on any unsolicited email links that lead to web pages that request for personal information to be updated.

3. Do not hover your mouse over any email links. This may seem harmless, but this may trigger malware to be downloaded onto your computer. If you have anti-malware installed, it will be able to protect against such vulnerabilities.
4. Do not share private information with people on social media. Hackers will try to approach unsuspecting victims with friend and connection requests.
5. Do not tell people your passwords.
6. Do not open email attachments that come from strange addresses.
7. Do not allow strangers to connect to your wireless network or network jacks.

3.4 Denial of Service (DOS)

Denial of Service (DoS) is an attack which makes information or data unavailable to its intended hosts. The concept of a DoS attack is to do whatever it takes to make a service unavailable to users. DoS attack does not attempt to intrude on a system or to obtain sensitive information, it rather prevents legitimate users from accessing the system. The most commonly used method is to flood the target in order to exhaust its resources such as memory, CPU and buffer. The exact resource being flooded depends on the target.

Another form of DoS attack is to send packets that are confusing to the target system. Once the computer or network device tries to process the packets, it will crash. To summarize, a DoS attack denies the use of a system or service through the systematic overloading of its resources. A hacker wants the system to become unstable, substantially slower or overwhelmed to the point it cannot process any more requests.

3.4.1 Categories of DoS Attacks

There are different categories of DoS attacks. They can be broken down into three broad categories: consumption of bandwidth, consumption of resources and exploitation of programming defects.

Consumption of Bandwidth
This type of DoS attack is when the network bandwidth flowing to and from a computer system or network is consumed to the point of exhaustion. A hacker must not completely exhaust the bandwidth to and from a system to achieve a DoS attack. Rather, using up so much of the bandwidth to the point that performance becomes unacceptable to users suffices. So the attacker's goal is to consume enough bandwidth to make the service unusable. Some well-known forms of attacks that consume bandwidth include:

1. **Smurf**: Smurf attack exploit the Internet Control Message Protocol (ICMP). This involves sending ICMP packets to the broadcast of a network by spoofing the IP address of the victim. The large number

of reply packets generated will consume the bandwidth of the victim.

2. **Fraggle**: This type of attack is similar to the smurf attack, but instead of using ICMP, the hacker uses User Datagram Protocol (UDP) packets. This occurs by sending UDP traffic the broadcast address of the network.

Consumption of Resources

This type of DoS attack is when the resources of the target system are exhausted. When an attack of this nature is carried out, a service or an entire system may become overloaded to the point where it slows, locks or crashes. The common form of this type of DoS attack includes:

1. **SYN Flood**: This type of DoS attack involves sending forged Transmission Control Protocol (TCP) packets with the SYN flag set to the target. When the victim receives multiple but forged TCP SYN packets, the connection resources will be consumed to the point where no resources are available for legitimate connections.
2. **ICMP Flood**: This type of DoS attack comes in two variants: smurf attack and ping flood.
    a. Smurf attack: This is carried out when a large amount of traffic is directed to the broadcast address of a network instead of a specific system.
    b. Ping flood: This is carried out by sending a large number of ping packets to the victim with the intent of overwhelming the victim. The command to pull off such an attack, depending on whether it is a Windows or Linux operating system, would be:

       ping -t/-I <victim I P address>
3. **Teardrop Attack**: In this type of DoS attack, the hacker manipulates IP packet fragments in such a way that when reassembled by the victim, a crash occurs. This process involves having fragments reassembled in illegal ways or having fragments reassembled into larger packets than the victim can process.
4. **Reflected Attack**: This type of DoS attack is carried out by spoofing or forging the source address of packets or requests and sending them to numerous systems, which in turn respond to the request. This type of attack is a scaled-up version of what happens in the ping flood attack.

The exploitation of Programming Defects

This category of DoS attack involves exploiting known weaknesses or vulnerability in the system. Some of the common methods of exploiting programming defects include:

1. **Ping of Death (PoD)**: This type of DoS attack leverages the inability of some systems to handle oversized packets. In the attack, a hacker sends fragments of packets to the victim. When the victim receives the fragments and reassembles them, the 65,536

bytes allowed by the IP protocol is reached or exceeded. This will cause the system to crash.

2. **Teardrop**: This type of DoS attack exploits a weakness in the way packets are processed by a system. In this type of attack, the packets are sent in a malformed state, that is, their offset values will be adjusted to overlap, which is illegal. When a system that does not know how to deal with this issue receives the packet, it crashes or locks.
3. **Land**: This involves sending a packet to a victim system with the same source and destination IP addresses and ports. The result of this action is system crash or lockup because the system does not know how to process the packet.

3.5 Distributed Denial of Service (DDOS)

DDoS consists of many systems that work together to launch a much powerful attack. In DDoS attacks, the hacker comprises many computers to create "zombie" machines that perform the actual DoS attack. A DoS attack program is installed on the zombie machines. The machines will then be used by the hacker to launch a massive DoS attack. This makes DDoS to be the most common DoS attack today.

Can malware be used to conduct a DDoS attack? How?

A typical way of conducting a DDoS attack is to deliver a Trojan horse to vulnerable computer systems (Zombies) that will be used to attack a specified target at a particular date and time. In this form of DDoS, the attacker does not have direct control of the various machines used in the attack. The comprmised computer systems are merely used to participate in the attack on a particular date and time. To effectively control the attack, attackers use botnets.

Botnets are networks of compromised computers that provides an attacker with full control of the infected systems. This is often accomplished via delivery of a Trojan horse. However, unlike the previous DDoS scenario, the attacker will have direct control of the attacking machines in the botnet.

3.5.1 Characteristics of DDoS Attacks

Here are some characteristics of a DDoS attack:

1. Attacks of this type are characterised by being very large, using hundreds or thousands of systems to conduct the attack.
2. DDoS has two types of victims: primary and secondary. The primary victim is the recipient of the actual DDoS attack, while the secondary victim is the system used to launch the DDoS attack.
3. The attack can be very difficult if not impossible, to track back to its true source because of the sheer number of systems involved.

4. The defence is extremely difficult due to the number of attackers. Configuring a router or firewall to block a small number of single IP addresses is easy. Larger numbers of attackers are nearly impossible to block.
5. The impact of this attack is increased over standard DoS. This is because many hosts are involved in the attack, multiplying the strength and power of the attack.

3.5.2 Tools for DDoS

Several tools are available to initiate a DDoS attack. The tool(s) used in a DDoS attack depends on the preferences of the hacker.

1. **Tribal Flood Network (TFN)**: TFN can be used to launch ICMP, Smurf, UDP and SYN flood attacks against a target at will. TFN has the distinction of being the first publicly available DDoS tool.
2. **Trinoo**: Trinoo can command and control many systems to launch an attack.
3. **Stacheldraht**: This offers features that are seen both in Trinoo and TFN. Stacheldraht uses TCP and ICMP to send commands and control its agents to attack.
4. **TFN2K**: An upgrade to TPN, it provides some more advanced features including spoofing of packets and port configuration options. TFN2K also includes encryption features, but not as strong as those of Stacheldraht.
5. **WinTrinoo**: This software is a Windows port of Trinoo and has the ability to use Windows clients as drones.
6. **Shaft**: This is similar to Trinoo, but includes the ability for the client to configure the size of the flooding packets and the duration of the attack.
7. **MStream**: This utilises spoofed TCP packets to attack a designated victim.
8. **Trinity**: This performs several DDoS functions, including SYN, RST, ACK and others.

3.6 Botnets

A botnet is a network of computers that are controlled by a single machine called a botmaster (hacker). This makes botnets an extremely effective tool for performing attacks such as distributed-denial-of-service (DDoS) attacks. A typical bot can be created and preserved in four phases as shown in Figure 18.

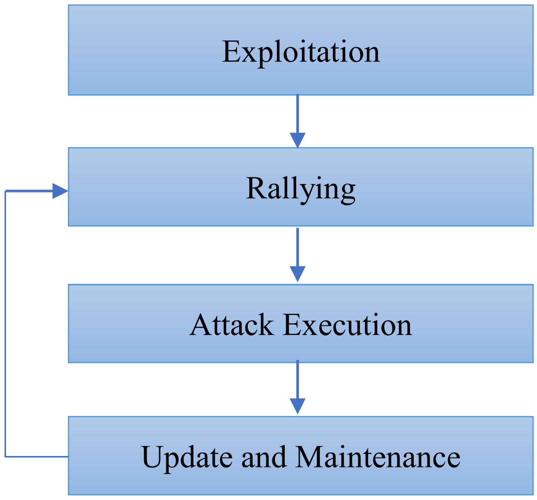

Fig. 18: Life Cycle of a Botnet

Exploitation Phase

This is the first step of a botnet. The hacker makes a remote infection by exploiting a vulnerability on the target systems. The hacker uses social engineering techniques to get the victim to execute the malware on the system, such as opening an e-mail attachment. Once installed, the bots will connect to a remote server controlled by the hacker to download the bot.

Rallying Phase

In this phase, the bots connect back to the hacker through a Command and Control (C&C) server. At this stage, the hacker ensures that the activities of the bots are stealthy. This is achieved by equipping the bots with a DNS lookup functionality in order to locate the command and control (C&C) server. Therefore, they will rally to connect back to the C&C server.

Attack Execution Phase

In this phase, the group of bots performs malicious activities on target machines as instructed by the hacker. The hacker sends the needed commands to the C&C servers. Bots will then grab the command from the C&C server to start the malicious activities. For instance, the group of bots may receive commands from the C&C server to launch a DDoS attack on a target.

Update and Maintenance Phase

The last phase of the botnet life cycle is updating and maintaining the botnets. In this phase, the hacker keeps the bots up to date through instructing the bots to update their binaries from time to time for better coordination and patching. Additionally, the hacker may migrate the C&C server to a different location to evade detection.

4.0 Self-Assessment Exercise(s)

1. What is the most effective way of conducting a denial of service attack on a target across the internet using hundreds of online computer systems?

Answer
The most effective way of conducting a DDoS attack on a large number of computers is to use a botnet. Botnet enables a hacker to compromised other computers and uses then to launch a DDoS attack.

2. Social Engineering can be defended using the following techniques except

   A. Stringent organisational policies
   B. User awareness and training
   C. Individual countermeasure
   D. Policy review

Answer: D

5.0 Conclusion

Social Engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the hacker. Social engineering also involves getting a user to download a malicious email attachment or click a link that leads to the victim to install malware or reveal sensitive information to the hacker. Hackers used denial-of-service (DoS) attack to sends a large number of connection or information requests to a target. These will crash the target system or simply become unable to perform ordinary functions. A distributed denial of service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which thousands of systems are compromised. The compromised machines are turned into zombies, machines that are controlled remotely by the hacker to participate in the attack. Botnets are one of the most effective techniques that hackers used to control zombies and launch DDoS attacks.

6.0 Summary

In this you, I discussed how hackers use social engineering attack to compromise systems and user accounts by enticing victims to reveal sensitive information or install malware. Social engineering attack can be conducted physically or via communication (web, email or phone). It is apparently important for users to be aware of the social engineering tricks and techniques used by hackers in order to thwart their malicious activities. Furthermore, I explored DDoS attacks in this unit and how hackers use malware and other denial-of-service attacks tools to launch malicious activities. There exist different ways for a hacker to launch a DDoS attack on a target, e.g. the use of a botnet. Botnets enable hackers to launch coordinates and controlled DDoS attack on a target using multiple hosts across the internet.

7.0 Further Readings

Alieyan, K., ALmomani, A., Manasrah, A., & Kadhum, M. M. (2017). "A Survey of Botnet Detection Based on DNS." *Neural Computing and Applications*, 28(7), 1541-1558.

Chuck, E. (2016). *Computer Security Fundamentals (3rd ed.),* Pearson Education, Inc.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016) *HACKING: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Oriano, S & Solomon, M. G., (2011). Hacker Techniques, Tools, and Incident Handling, Jones & Bartlett Learning.

Unit 3: Spyware

Contents

1.0 Introduction

In this unit, I will take you through how spyware works and the techniques used by hackers to deliver spyware to a target system. Hackers used spyware to collect information without the consent of the user from a computer system or user accounts.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the concept of spyware
- describe how hackers use malware for malicious activities
- discuss the methods of delivering spyware to a target.

3.0 Main Content

3.1 Spyware

Spyware is a software that is designed to collect and report information on user activities without the user's knowledge or consent. Spyware can collect any type of information about the user that the author wishes to gather, such as browsing habits, keystrokes, software usage and general computer usage. Additionally, spyware can be a precursor to further attacks or infection. It can be used to download and install other malicious software.

Spyware can be as simple as a cookie used by a website to record a few brief facts about a visit to the website. Spyware can also be a program designed to capture usernames and passwords and every document you type. This data can be stored in a small file hidden on the target system. The information can later be extracted or sent out to the hacker. The spyware can be set to wait until after hours before uploading the data to some server or use your email software to send the data to an anonymous email address. Regardless of the specific mode of operation, spyware is a software that literally spies on user activities on a particular computer.

What are the common ways of using spyware?

Hackers use backdoors and key loggers to steal information from a target system. Many hackers use backdoors to steal information from a target system. The owner of a compromised system will not know that someone else is even using the system. Typically, a backdoor, when implemented, will achieve one or more of three key goals:

1. Provide the ability to access a system regardless of security measures that an administrator may take to prevent such access
2. Provide the ability to gain access to a system while keeping a low profile. This would allow an attacker to access a system and circumvent logging and other detective methods.
3. Provide the ability to access a system with minimal effort in the minimum amount of time. Under the right conditions, a backdoor will allow the attacker to gain unrestricted access to a system.

Here are some common backdoors used on a system.

1. **Password-cracking backdoor**: This backdoor is used by hackers to uncover and exploit weak passwords that have been configured by the system owner. System owners who fail to follow accepted guidelines for strong passwords become vulnerable to attacks of this type.
2. **Rootkits**: This is a backdoor used by hackers to replace existing files on a target system with their versions. This technique enables a hacker to replace key system files on a computer and therefore alter the behaviour of a system at a fundamental level.
3. **Services Backdoor:** Network services are another target for attack and modification with a backdoor. When a network service runs, a port such as 80 or 666 is used for communication. Therefore, if a network service is answering on a port, a hacker can use the port to issue commands to the service to compromise the target system.
4. **Process hiding backdoors**: This is a backdoor used by hackers to stay undetected for as long as possible by hiding the software in the target system. This is achieved by renaming a malicious program to the name of a legitimate program or altering other files on a system to prevent them from being detected and running.

Similarly, information can be extracted from a comprominsed using a **keylogger**. This malware is designed to capture and report activity, particularly keyboard usage on a target system. Key loggers enable hackers to monitor all activity on a system and have it reported back to the hacker. Key logger can be used to capture passwords, confidential information and sensitive data.

Typically, key loggers are implemented as a small piece of code that resides in the interface between the operating system and keyboard. The software is installed the same way any other Trojan would be bundled with a legitimate application. Once a key logger is installed on a target system, the malware can send all the needed information to a hacker.

3.1 Methods of Delivery and Infection

Spyware can be placed on a system using a number of different methods, each of which is effective in its own way. When the software is installed, it typically remains hidden and proceeds to carry out its task. Do you remember how Trojans are delivered to the target computer system in Unit 1. Hacker used the same methods to delivery spyware which include:

1. **Peer-To-Peer Networks (P2P)**: This is most commonly used medium to deliver spyware because of the increased number of individuals using these type of networks to obtain free software.
2. **Instant messaging (IM)**: Hackers use IM to delivering spyware in the form of free software.
3. **Internet Relay Chat (IRC)**: IRC is used to deliver messages and software because of its widespread use and the ability to entice new users to download software.
4. **E-mail Attachments**: Hackers use email attachment to distribute spyware using social engineering techniques.
5. **Physical Access**: Gaining physical access to a system make it relatively easy for a hacker to install spyware and compromise the system.

4.0 Self-Assessment Exercise(s)

1. One of the common backdoors that are placed on a system is
    a. Worm
    b. Trojan
    c. Rootkit
    d. Keylogger

   Answer: C

2. Methods through which Spyware can be placed on a system include
    a. Instant messaging
    b. Internet Relay Chat
    c. Media Access Control
    d. Rootkits

   Answer: A and B

5.0 Conclusion

Spyware programs can track all activities on a computer, and retrieve information via several different methods. The most common method is a Trojan horse. It is also possible that when a user visits certain websites, spyware may download in the background while the user is simply perusing the website.

6.0 Summary

In this unit, you have learned what spyware is and how the software can be delivered to a target system. Spyware is used by hackers to gather or steal sensitive information from a target remotely. Thus, this class of malware is suitable for espionage and stealthy malicious activities.

7.0 References/Further Reading

Chuck, E. (2016). *Computer Security Fundamentals (3rd ed.).* Pearson Education, Inc.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Hall, G. & Watson, E. (2016). *Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Oriano, S & Solomon, M. G., (2011). Hacker Techniques, Tools, and Incident Handling, Jones & Bartlett Learning.

Module 4: Penetration Testing

Module Introduction

Penetration testing is used by organisations to evaluate the security level of computer and network systems to identify a weakness that can be exploited by hackers. This is to determine effective security measures needs to be placed to protect computers and network infrastructure from attack.

In module 2, you learnt how hackers use the vulnerability to carry out targeted attacks on Microsoft Windows systems, Linux systems, Web servers and Web applications. Also, you learned how hackers use malware to launch secret and destructive attacks in module 3. In this module, I will take you through how to conduct a security audit of an organisation to determine compliance with security policies, procedures and standard and ascertain protection. You will also learn how to assess vulnerabilities in systems, services, applications and infrastructure that enable hackers to launch targeted and malware attacks and identify ways to mitigate the risk of attacks. Finally, I will take you through penetration testing roadmap and plans in order to identify vulnerabilities.
This module is classified into the following four units:

Unit 1: Security Audit
Unit 2: Vulnerability Assessment
Unit 3: Penetration Testing Roadmap
Unit 4: Penetration Test Plan

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I will highlight resources for further reading at the end of each unit.

Unit 1: Security Audit

Contents

1.0 Introduction

In this unit, you will learn how to measure the compliance of user and computer systems implementation with standard security policies and procedures of an organisation. This is to identify and analyse security risks in terms of human behaviour and systems set up that enables activities such as targeted attacks, social engineering attacks, malware attacks and other unauthorised activities in an organisation. You will also learn the tools used to audit the security of an organisation.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe how security audit is conducted
- explain security audit tools
- highlight how to audit the security of an organisation.

3.0 Main Content

3.1 Security Audit

A security audit is a periodic assessment of the level of compliance of users and systems with the security policy and standards of an organisation. This is to determine the state of protection and effective implementation of security measures. Security audit ensures that the minimum set of controls required for reducing risk to an acceptable level is maintained and vulnerabilities at a particular point in time are revealed.

To perform a security audit, you need security policy and standards, audit checklists and an inventory list, which may cover different areas such as web application, network architecture and wireless communication. The auditing process also involves the use of different auditing tools and different review techniques to reveal the security non-compliance and loopholes. After the audit process, an audit report is prepared to highlight the compliance and gaps that existed between the current protection and the requirements specified in the security policies and standards. This determines the strength and potential weaknesses of the security of an organisation.

The major objectives of a security audit are to:

1. Ensure compliance with and effectiveness of the security policy, standards, guidelines and procedures.
2. Identify and review vulnerabilities, regulatory and contractual requirements.
3. Review existing security controls on operational, administrative and managerial issues, ensure effective implementation of security measures and compliance to minimum security standards.
4. Recommend actions for improvements.

Several scenarios exist on when a security audit should be performed depending the system requirements and resources.

1. New installation/enhancement audits: before the implementation of major enhancements, to ensure compliance with existing policies and guidelines and meet the configuration standard.
2. Regular audits: conduct annual audits using security-related tools to ensure the minimum set of controls are implemented to detect and handle security loopholes or vulnerabilities.
3. Random audits: This is to perform random checks in order to reflect the actual practice.
4. Nightly or non-office hour audits: This is to reduce the auditing risks by performing audit during non-office hours or at night.

3.2 Risk Analysis

Security audit requires the need to **risk analysis** and **risk management,** that is, assessing the risks of loss, compromise or damage to information. Risk analysis is the process of identifying and assessing the risk of something happening. The principles of risk analysis are summarised as:

1. The establishment of mechanisms to keep risks under review and to ensure they are being addressed.
2. A means of identifying the potential risks to the business.
3. An assessment of the likelihood of each risk materialising.
4. An assessment of the probable impact of each risk.
5. The formulation of measures to avoid each risk occurring.
6. The development and deployment of fall-back measures to mitigate the risks if avoidance actions fail.
7. The determination of the imminence of the risk and of taking appropriate countermeasures.

Generally, risk analysis and management is necessary before commencing security audit.

3.3 Security Audit Tools

Several security audit tools are available to aid security auditors to find vulnerabilities in systems and services. These tools run on Windows and Unix-based operating systems. The choice of security audit tools depends on the security assessment needed, that is, whether the vulnerability check is on a network or specific hosts. Table 1 shows some security audit tools.

Table 1: Security Audit Tools

Security Audit Tool	**Platform**	**Type**
COPS/Tiger	Linux and Unix	Intrusion detection
Crack	Linux, Unix and Windows	Password cracking
Nmap	Linux, Unix and Windows	Port scanner
tcpdump	Linux, Unix and Windows	Network monitoring
snifit	Linux, Unix and Windows	Network monitoring
CyberCop	Linux and Windows	Password cracking, port scanning and network monitoring
Nessus	Linux, Unix and Windows	Exploit tester
Metasploit	Linux, Unix and Windows	Exploit tester
TripWire	Linux, Unix and Windows	Intrusion detection

3.4 Security Audit Stages

A security audit comprises several stages, as shown in Figure 19.

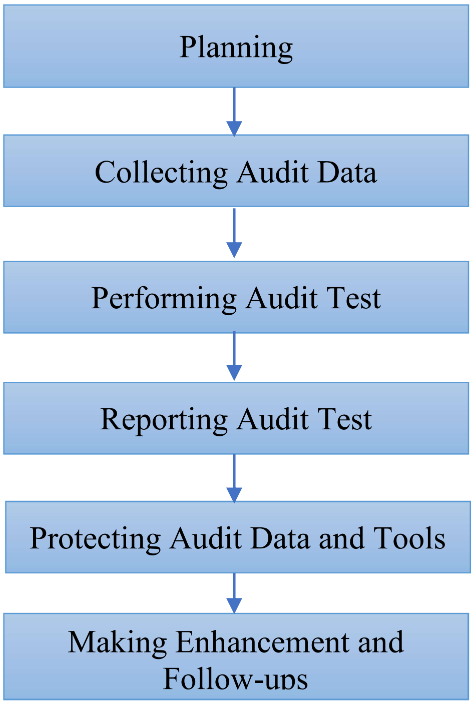

Fig. 19: Security Audit Stages

Planning
This is the process of selecting the effective and efficient methods of performing security audit and obtaining all necessary information. The required time for planning depends on the nature, extent and complexity of the audit. In this stage, the security audit scopes are clearly defined and established. Examples of security audit scopes include:

1. General security of an internal network and hosts
2. Security of the Internet and network servers
3. Security of mission-critical systems and other services
4. Security of network components and devices such as firewalls, routers, directory services and mailing services
5. Security of a computer room

Collecting audit data
This stage determines the amount and type of information to capture, and how to filter, store, access and review the audit information and logs. Audit data can be collected and stored in different ways such as log files, reports and storage media. Apart from electronic data collection, some physical events should also be recorded and collected. These includes:

1. Computer equipment repair and maintenance activities such as date, time, supporting vendor information and the activity's description.

2. Change control and administration events such as configuration changes, installation of new software, data conversion or patches updating.
3. Physical site visit by external parties such as security auditors or guests.
4. Procedure and policy changes.
5. Operation logs.
6. Security incident records.

Performing audit tests

This stage involves technical investigation using different automated security audit tools for diagnostic review and penetration tests. The security audit tools are useful in gathering information because they require little user intervention, which saves time. It is important to check systems against know vulnerability advisories from groups such as Computer Emergency Readiness Team (CERT), Common Vulnerabilities and Exposures (CVE), bugtraq and National Vulnerability Database (NVD).

Reporting Audit Results

This stage involves writing a comprehensible security audit report after completion of the audit work. Security auditors should analyse the auditing results and provide a report, which reflects the current security status. The report should be presented in a way that explains your findings clearly to your intended audience. The audience may comprise executive members of an organisation, information technology managers and staff. It is essential to present the report in a clear and non-technical language.

Protecting audit data and tools

This stage involves safeguarding the audit data and tools. Audit data and other related documents shall also be classified and protected appropriately. The auditing tools should be properly maintained, controlled and monitored to avoid misuse. The security auditors should only use such tools in a controlled manner, and then be removed immediately after use unless proper control has been made to protect them from unauthorized access. Security auditors shall also return all audit information.

Making enhancements and follow-up

This stage involves discussing the action that should be taken based on the results of the security audit. If corrective actions are required, resources should be allocated to ensure that the enhancements could be performed at the earliest opportunity.

4.0 Self-Assessment Exercise(s)

1. One of the following is not included in the activities you need to perform in conducting a security audit for an organisation?
    A. Performing Audit Tests
    B. Modifying Audit Results
    C. Protecting Audit Data and Tools
    D. Planning

    Answer: B

2. Security audit is conducted__________?
    A. Annually
    B. Daily
    C. Periodically
    D. Monthly

    Answer: C

5.0 Conclusion

In this unit, you have learned the stage and processes of measuring the compliance of organisation security with standard security policies and procedures. Several security audit tools are available. However, the use of an audit tool depends on the type of security audit you will conduct and the platform used by the organisation.

6.0 Summary

In this unit, I discussed the security audit and the activities performed at each stage of the audit process. A security audit is conducted to identify the strength and weakness of an organisation regarding compliance with security policies. I also highlight some security audit tools used to facilitate conducting a security audit for an organisation.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

IGeorgia, W. G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Kapp, J. (2000). "How to Conduct a Security Audit. PC Network Advisor." (120), 3-8.

SPG-SM01 (2017). Practice Guide for Security Risk Assessment and Audit

Unit 2: Vulnerability Assessment

Contents

1.0 Introduction

In this unit, I will explain how the assessment vulnerabilities in applications, systems, services and network infrastructure. In Unit 1, you learned how to perform a security audit to determine compliance with security policy. In this unit, I will take you through how to find a weakness, not in compliance with security policy as in security audit, but in the design of systems and network infrastructure. I will also take you through the activities performed at the stages of vulnerability assessment and approached used in assessing vulnerabilities.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain vulnerability assessment
- discuss the types of vulnerability assessments
- describe approaches to vulnerability assessment.

3.0 Main Content

3.1 Vulnerability Assessment

Vulnerability is a weakness in software design, network services, operations, control and procedure that could be exploited to gain unauthorised access or compromise a system. This includes anything from a weak password on a router to an unpatched programming flaw in an exposed network service. Vulnerability assessments are the process of locating and reporting vulnerabilities. The assessment is used to detect and resolve security problems before being exploited by a hacker. Once vulnerabilities are identified, the affected systems and services can be fixed by patching the vulnerabilities. Then, the assessment can be repeated to verify the effectiveness of the fixes. This is the standard method for many organisations to manage their security issues.

3.2 Types of Vulnerability Assessment

There are two types of vulnerability assessment; host vulnerability assessment and network vulnerability assessment.

3.2.1 Host Vulnerability Assessments

In a host vulnerability assessment, you analyse the security of a single system. The assessment is conducted on the systems using specialised tools and an administrative user account. The host vulnerability assessment tools are installed on the system(s) you want to assess or linked to a central system on the network. A host vulnerability assessment identifies vulnerabilities at system level such as insecure file permissions, missing software patches, noncompliant security policies, and malware installations.

Host vulnerability assessment provides an in-depth test of the host, which is good for monitoring the security of critical systems. However, host vulnerability assessment requires administrative access and specialised tools for the operating system and software packages installed on the system under test. Thus, host assessments are often reserved for a few critical systems.

3.2.2 Network Vulnerability Assessments

In a network vulnerability assessment, you used to test an entire network of systems at once. A network vulnerability assessment identifies all live systems on a network, determines what network services are running on the systems, and then analyses the services for potential vulnerabilities.

Network vulnerability assessment differs from host vulnerability assessment because it does not require any configuration changes on the systems being assessed. Network vulnerability assessments provide the feasible of testing the security of large, complex networks of heterogeneous systems. The strength of network vulnerability assessment is its effectiveness in identifying vulnerabilities in a large number of systems at a time. However, network vulnerability assessment has limitations that include:

- Inability to detect certain types of backdoors
- Complications with the firewall.
- Disruption of normal operations
- Interference with many devices such as printers
- Network bandwidth consumption.

3.3 Network Vulnerability Assessment Process

There are a set of activities that you conduct when assessing network vulnerabilities. The activities are as shown in Figure 20.

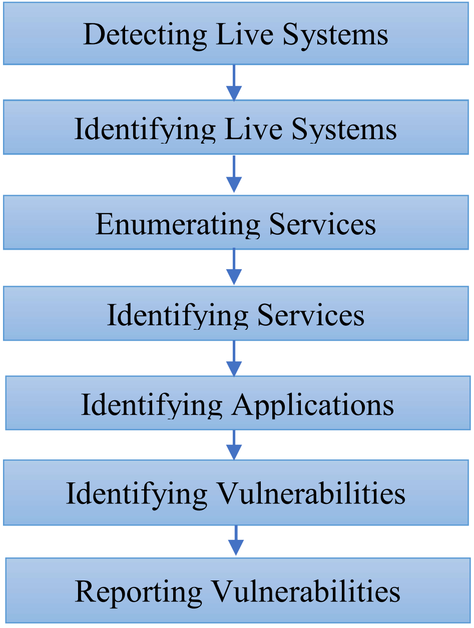

Fig. 20: Vulnerability Assessment Process

Detecting live systems

This is to identify the systems being assessed using Internet Protocol (IP) addresses to determine whether the systems are accessible. Several probes are sent to the systems for responses. If a response is received, the system is considered reachable and valid.

Identifying live systems

In this stage, the systems being assessed are probed to identify their types and platforms used by the systems. Do you remember fingerprinting in Unit 2 of Module 1? Fingerprinting techniques are used here to detect system type and platform. The fingerprinting techniques used from Simple Network Management Protocol (SNMP) queries to complex TCP/IP stack-based operating system identification.

Enumerating services
Once a system is detected and identified, the activity that follows is an enumeration, that is, port scan. A port scan is a process of determining what TCP and UDP services are open on the system being assessed. Do you remember port scanning in Unit 2 of Module 1? TCP and UDP port scanning are used to send connection requests to the systems. There are 65,536 available TCP ports; however, limiting the scan to a subset of the available ports reduces the amount of time it takes to perform the assessment and substantially decreases the bandwidth required.

Identifying services
After enumerating services on network systems, the next activity is to identify the services that are in use on each open port. This process starts with sending some common application requests, such as HyperText Transfer Protocol (HTTP) on port 80, and analysing the responses against a set of signatures. When a signature matches a known application, this information is stored for the later use and the next service is tested.

Identifying applications
The next step after service detection is to determine the application used for each detected service. This is to identify the vendor, type, and version of every service detected in the previous stage.

Identifying vulnerabilities
After identifying systems and applications, the systems are now ready to begin testing for vulnerabilities. This process begins with information gathering techniques, then active configuration probes, and finally attacks that can identify the existence of vulnerabilities on the tested system.

Reporting vulnerabilities
After the analysis is finished, the final stage of the assessment process is reporting. The assessment report lists the systems discovered during the assessment and any vulnerabilities that were identified on them.

3.4 Vulnerability Assessment Approaches

When performing a vulnerability assessment, the actual perspective of the test can have a huge impact on the depth and quality of the results. Essentially, there are three different approaches to vulnerability testing: administrative, outsider and hybrid.

3.4.1 Administrative Approach

The administrative approach uses a normal, authenticated system administrator or user to perform the assessment. The credential provided can be used to detect missing patches, insecure configuration settings, and potentially vulnerable client-side software. This is useful when trying to detect and resolve client-side vulnerabilities on a network of computer systems.

3.4.2 The Outsider Approach

The outsider approach uses unauthenticated malicious intruder access trying to break into the network. The assessment process can make decisions about the security of a system only through a combination of application fingerprinting, version identification, and actual exploitation attempts. Assessment tools built on this approach have the capabilities of detecting vulnerabilities across a wider range of operating systems and devices than the administrative approach.

3.4.3 The Hybrid Approach

In this approach, the assessment tools use administrative credentials when possible but fall back to remote fingerprinting techniques if an account is either not available or not accepted on the tested system. The hybrid approach provides results that are often better than those using administrative or outsider approach.

4.0 Self-Assessment Exercise(s)

1. What are the strengths of using the hybrid approach of vulnerability assessment compared to a single approach?
2. Identify the limitations of network vulnerability assessment
   a. Ability to detect certain types of backdoors
   b. Complications with antivirus
   c. Disruption of normal operations
   d. Interference with many devices, such as printers.

5.0 Conclusion

In this unit, you have learnt how to assess vulnerabilities in applications, systems, services and network infrastructure. To assess vulnerabilities, you need to determine the systems to be assessed in order to apply the relevant type and approach of vulnerability assessment.

6.0 Summary

In this unit, I have discussed vulnerability assessment and the activities performed at each stage of the assessment process. I also explored the types and approaches used by security administrators to assess vulnerabilities in systems, applications, services, and network infrastructure.

7.0 References/Further Reading

Beale, J., Meer, H., van der Walt, C., & Deraison, R. (2004). Nessus Network Auditing: Jay Beale Open-Source Security Series. Elsevier.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia Weidman G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

ISPG-SM01 (2017). Practice Guide for Security Risk Assessment and Audit.

Unit 3: Penetration Testing Roadmap

Contents

1.0 Introduction

In Unit 2, you learned vulnerability assessment. Unlike vulnerability assessment that focuses on identifying vulnerabilities on a network, a penetration test focuses on gaining unauthorised access to the tested systems by exploiting the vulnerabilities identified during assessment. In this unit, I will discuss the roadmap for conducting a penetration test.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the rules for a successful penetration test
- discuss how to develop penetration testing plan.

3.0 Main Content

3.1 Penetration Testing Roadmap

Penetration testing is an authorised attempt to locate and successfully exploit vulnerabilities in computer systems to make the systems more secure. Penetration testing provides proof of concept attacks to demonstrate the vulnerabilities in computer systems.

What is the difference between vulnerability assessment and penetration testing?

A vulnerability assessment reviews services and systems for potential security issues, whereas a penetration test performs exploitation and proof of concept attacks to prove that a security issue exists. Penetration tests go a step beyond vulnerability assessments by simulating the hacker activity and delivering live payloads.

3.2 Penetration Testing Rules

Before conducting a penetration test, there are certain rules you need to know. These are:

1. **Set a goal**: If you have planned to evaluate the security of an online system or network, you must first try to answer three questions:
    a. What information does a hacker see when they look at the target network?
    b. Can the hacker misuse that information?
    c. Is the target aware of any attempts to penetrate their system?
2. **Plan ahead**: A penetration testing plan must be defined. The plan should include:
    - Identifying the networks to be tested
    - Determining the intervals of the tests
    - Clearly defining the testing procedure
    - Creating a plan that you can share with stakeholders
    - Getting the plan approved.
3. **Get authorisation**: Before conducting a penetration test, you must obtain the necessary authorisation from the organisation. An authorisation document must be issued by the organisation showing that you have the approval to test the system according to an approved plan and that the organisation will support you in case of any legal charges.
4. **Be ethical**: Before conducting a penetration test, you must bound by the code of professionalism, confidentiality and conscience. Make sure that you always stick to the plan that was previously approved and avoid adding any new details to it down the road. You are not to release or share the results of your security test with unauthorised persons both within and outside the organisation. Any information you discover should be treated as sensitive. It is also important to be aware of any local laws or governance regulations within the organisation that relate to hacking.
5. **Maintain good records**: Some basic rules should be followed when it comes to record-keeping:
    - Note down every task performed.
    - Log every piece of information directly.
    - Always have a backup copy of the log.
    - Note down every test performed, including the dates.

6. **Protect confidential information**: You are likely to come across a lot of personal and private information during your penetration testing. You must respect people's privacy and treat every piece of information with confidentiality. Passwords, encryption keys, and other sensitive information must not be abused. Always treat other people’s personal or confidential information with the same respect you would want others to treat your own.
7. **Do not cause harm**: There are times when you may get excited about the job and the positive test results you are receiving, so you keep plugging away. However, you may accidentally cause some kind of outage or even interfere with another's rights. This is why you should always have a plan and then commit to sticking to it. Be knowledgeable about the tools you are using, especially their implications. Choose your tools wisely and always read the documentation.
8. **Always be empirical**: If you want your test results to be accepted, you need to use a scientific process that is characterised by these features:
   a. Quantifiable goals: Set a goal that you will be able to quantify. You can set task goals or time-related goals.
   b. Consistency and repeatability: Every test that you perform must produce the same results. If they do not, then your results are inconsistent and probably invalid. If you repeat a test over and over, you should get the same results every time. Consistency and repeatability of tests are critical features of an empirical process.
   c. The permanence of results: The client that you work for will look forward to your test results if you focus on fixing persistent problems for good, instead of solving temporary ones that may recur later on.
9. **Do not use any random tool**: There are a lot of hacking tools in the market today. It is easy to be tempted to try them all out, probably since most of them are free. However, it is advisable to just focus on a few tools that you know are effective, and you are familiar with.
10. **Report all your findings**: If you are hired for penetration systems, and the process takes longer than a week, you need to give your clients weekly status updates. If you discover any high-risk weaknesses and vulnerabilities in the system during your tests, you need to report them to those concerned. The reports that you issued is what the client will use to determine how thorough and sincere you are in your work. A report will also help during the analysis and critique of your results.

3.3 Penetration Testing Plan

Having learned the rules for conducting a penetration test, it is important to take you through the steps that guide you through planning the penetration testing process. The penetration testing plan steps include:

i. Determine the most critical and vulnerable systems to be tested first. These can include server passwords or email phishing. Once the core areas have been tested, you can then cascade down to all the other systems.

ii. Assess the risks involved. It is important to always have a contingency plan in case the penetration testing process goes wrong. Determine how people and systems will be affected beforehand.

iii. Determine testing schedule. It could be during regular business hours, early mornings, or maybe late at night. The best way to test the system would be to launch any type of test at any time of day. The only exceptions would typically be full DoS attacks, physical security and social engineering tests.

iv. Have a basic understanding of the system being tested. You may need to get more details of the systems to be tested.

v. Define the actions to be taken in case major vulnerabilities are found. If you discover a couple of security weaknesses, let the key players know about it immediately. Keep testing the system until you find it impenetrable.

vi. Determine the deliverables. These include detailed scanning reports containing information about vulnerabilities and recommendations on how to fix them.

vii. Determine the specific set of tools that you will need for your task. Always ensure that you are using the appropriate tool for the right task.

4.0 Self-Assessment Exercise(s)

What is the major difference between internal penetration testing and external penetration test?

Answer:
the major difference between internal and external penetration testing is that with internal penetration testing, it is assumed the attacker already has access. In contrast, external penetration testing is the ability of a remote attacker to get to the internal network.

5.0 Conclusion

In this unit, I explored the concept of a penetration test, rules and steps that you need to follow to achieve a successful penetration test. A penetration test is a great way to determine how well the security measures of an organisation respond to a real-life attack.

6.0 Summary

In this unit, you learnt the concept of exploiting the weaknesses identified during vulnerability assessment to gain unauthorised access to systems. It is important to note that you need to properly plan and follow the rules of a penetration test to achieve successful results.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *HACKING: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Unit 4: Penetration Test Plan

Contents

1.0 Introduction

In Unit 2, you learnt the roadmap to carry out a penetration test. In this unit, I will take you through the main steps of the penetration test plan from information gathering to the actual test.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- perform reconnaissance
- conduct penetration testing
- evaluate system vulnerabilities.

3.0 Main Content

3.1 Penetration Test Plan

A penetration test plan is an essential step-by-step procedure used to prepare for a penetration test. Penetration test exploits every potential entry point into the network, such as customer networks, wireless networks, or mobile devices. Testing everything is important because hackers use people, physical components, or computer systems to launch an attack. The primary aim is to figure out how hackers can exploit the vulnerabilities in the systems and other network components. You can decide to simulate a restricted attack on a single computer or comprehensively attack the whole system.

There are two ways to test a system; a covert test and an over test. The overt test is where you have some inside knowledge of the system you intend to test. In the covert test, you do not know much information apart from the name of the organisation. In the covert test, you have to search for information on your own, the same way a hacker will do. This enables you to see what a hacker would see when they try to gain access. However, a covert test takes more time, and there is a higher chance of overlooking certain vulnerabilities.

There are three main steps for conducting a penetration test. These are reconnaissance/information gathering, evaluating system vulnerability and penetration test.

3.2 Reconnaissance/Information Gathering

This is the process of collecting information about the person or organisation that you want to test. It is a passive approach that mainly involves using publicly available resources to find information about something. There are some techniques that you can use to gather information. These include:

Web Searches
These involve using the target's website and browse around as you try to collect as much useful information as possible. If you are using Google, you can use keywords to get the most relevant information.

Web Crawling
A **Web crawler** sometimes called a **spider** or **spiderbot** and often shortened to **crawler**, is an Internet bot that systematically browses the World Wide Web, typically for Web indexing (*web spidering*).

Web search engines and some other sites use Web crawling or spidering software to update their web content or indices of other sites' web content. Web crawlers copy pages for processing by a search engine which indexes the downloaded pages so users can search more efficiently. Certain web crawling tools can mirror a website and download all the publicly accessible files from the target website. This then allows you to scan the copy offline.

Websites
There are certain websites that contain information about different organisations and their employees. You can even do a people search if you just know which websites to use.

Network mapping
This is the process of searching public databases to discover the information available about a particular network such as Whois. Whois

enables you to obtain information that will help you scan a network or prepare a social engineering attack. You will be able to get the names, phone numbers, and addresses linked to a specific Internet domain registration.

System scanning
The information gathered from external sources can provide you with a map of the entire network, revealing how the systems are interconnected. You should be able to see the hostnames, IP addresses, open ports, running protocols and applications.

Hosts
Scan and record those hosts that can be accessed externally via the Internet and internally by an insider. Begin by pinging the IP addresses or the hostnames. You can use either the standard ping tool that comes with operating systems or a 3rd party tool such as SuperScan or fping.

Open ports
Several networking tools can be used to scan for open ports. These include OmniPeek, Wireshark, SuperScan, among others. It is easier to perform a scan internally than externally. To scan internally, connect your computer to the local network and run the software. To scan externally, just assign the computer you are using a public IP address and connect it to a hub that is not within the firewall.

3.3 Evaluating System Vulnerabilities

After discovering a potential vulnerability, it is time to start testing. However, you should confirm if the vulnerability is real. There are several websites and hacker message boards that you can manually search to determine whether what you have discovered is on the list of classified vulnerabilities. These websites include www.sans.org, nvd.nist.gov, and cve.mitre.org/cve.

The next step is to start testing right away. You can either perform a manual evaluation or an automated evaluation. In manual evaluation, the potential vulnerabilities are assessed by linking to the ports that can be exploited by hackers. Automated evaluations involve the use of tools that test for weaknesses on a platform or network. Though these tools make work easier and much faster, most of them only can test for specific and individual system vulnerabilities.

3.4 Penetration Testing

Once you have discovered the major security vulnerabilities, the next step is to penetrate the vulnerable system using the available tools or a tool you develop for a penetration test. After penetrating the system, you should carry out the following:

1. Gather more information from the host system
2. Access other interconnected systems in the network
3. Start and stop specific services
4. Get a remote command prompt
5. Launch a denial of service attack
6. Gain access to confidential files
7. Disable inbuilt logging security checks
8. Perform SQL injection attacks
9. Take screenshots
10. Send emails to people as the administrator
11. Upload a file.

Generally, your job is to expose the presence of system vulnerabilities, so there is no need actually to exploit them and mess around with people. Unless for some reason, it is necessary to show the management just how serious system flaws are.

4.0 Self-Assessment Exercise(s)

1. ____________ is an Internet bot that systematically browses the World Wide Web, typically for Web indexing.

A. Zombie
B. Botnet
C. Spider
D. Hosting

2. Which of the following statements is true about a penetration testing plan?
   A. It is an essential plan used to conduct a vulnerability assessment.
   B. It is an essential step-by-step procedure used to prepare for a penetration test.
   C. It is the plan for gathering information from external sources, revealing how the systems are interconnected.

   Answer: B

3. There are four main steps for conducting a penetration test, true or false?

   Answer: True

Mini-project

A Nigerian bank has been using online banking for ten years now. They have their web servers at the head office in Abuja. The bank wishes to understand their current level of risk. They contact you with an offer to carry out a penetration test. They provide you with the IP address of their web servers. Develop a penetration testing plan to assess the security risk of their web servers.

5.0 Conclusion

In this unit, you learnt how to develop a penetration test plan to assess the security risk of an organisation.

6.0 Summary

In this unit, I explored the necessary step needed by a security expert to develop a plan for a penetration test.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *HACKING: Computer Hacking, Security Testing, Penetration Testing and Basic Security*

Unit 3: Spyware

Contents

1.0 Introduction

In this unit, I will take you through how spyware works and the techniques used by hackers to deliver spyware to a target system. Hackers used spyware to collect information without the consent of the user from a computer system or user accounts.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain the concept of spyware
- describe how hackers use malware for malicious activities
- discuss the methods of delivering spyware to a target.

3.0 Main Content

3.1 Spyware

Spyware is a software that is designed to collect and report information on user activities without the user's knowledge or consent. Spyware can collect any type of information about the user that the author wishes to gather, such as browsing habits, keystrokes, software usage and general computer usage. Additionally, spyware can be a precursor to further attacks or infection. It can be used to download and install other malicious software.

Spyware can be as simple as a cookie used by a website to record a few brief facts about a visit to the website. Spyware can also be a program designed to capture usernames and passwords and every document you type. This data can be stored in a small file hidden on the target system. The information can later be extracted or sent out to the hacker. The spyware can be set to wait until after hours before uploading the data to some server or use your email software to send the data to an anonymous email address. Regardless of the specific mode of operation, spyware is a software that literally spies on user activities on a particular computer.

What are the common ways of using spyware?

Hackers use backdoors and key loggers to steal information from a target system. Many hackers use backdoors to steal information from a target system. The owner of a compromised system will not know that someone else is even using the system. Typically, a backdoor, when implemented, will achieve one or more of three key goals:

1. Provide the ability to access a system regardless of security measures that an administrator may take to prevent such access
2. Provide the ability to gain access to a system while keeping a low profile. This would allow an attacker to access a system and circumvent logging and other detective methods.
3. Provide the ability to access a system with minimal effort in the minimum amount of time. Under the right conditions, a backdoor will allow the attacker to gain unrestricted access to a system.

Some common backdoors that are placed on a system are of the following types and purposes:

1. **Password-cracking backdoor**: This backdoor is used by hackers to uncover and exploit weak passwords that have been configured by the system owner. System owners who fail to follow accepted guidelines for strong passwords become vulnerable to attacks of this type.
2. **Rootkits**: This is a backdoor used by hackers to replace existing files on a target system with their versions. This technique enables a hacker to replace key system files on a computer and therefore alter the behaviour of a system at a fundamental level.
3. **Services Backdoor:** Network services are another target for attack and modification with a backdoor. When a network service runs, a port such as 80 or 666 is used for communication. Therefore, if a network service is answering on a port, a hacker can use the port to issue commands to the service to compromise the target system.
4. **Process hiding backdoors**: This is a backdoor used by hackers to stay undetected for as long as possible by hiding the software in the target system. This is achieved by renaming a malicious program to the name of a legitimate program or altering other files on a system to prevent them from being detected and running.

Another powerful way of extracting information from a victim's system is to use a piece of technology known as a **keylogger**. This malware is designed to capture and report activity, particularly keyboard usage on a target system. Key loggers enable hackers to monitor all activity on a system and have it reported back to the hacker. Key logger can be used to capture passwords, confidential information and sensitive data.

Typically, key loggers are implemented as a small piece of code that resides in the interface between the operating system and keyboard. The software is installed the same way any other Trojan would be bundled with a legitimate application. Once a key logger is installed on a target system, the malware can send all the needed information to a hacker.

3.1 Methods of Delivery and Infection

Spyware can be placed on a system using a number of different methods, each of which is effective in its own way. When the software is installed, it typically remains hidden and proceeds to carry out its task. Do you remember how Trojans are delivered to the target computer system in Unit 1? Hacker used the same methods to delivery spyware which include:

1. **Peer-To-Peer Networks (P2P)**: This delivery mechanism has become very popular because of the increased number of individuals using these networks to obtain free software.
2. **Instant messaging (IM)**: Hackers use IM to delivering spyware in the form of free software.
3. **Internet Relay Chat (IRC)**: IRC is a commonly used mechanism to deliver messages and software because of its widespread use and the ability to entice new users to download software.
4. **E-mail Attachments**: Hackers use email attachment to distribute spyware using social engineering techniques.
5. **Physical Access**: Gaining physical access to a system make it relatively easy for a hacker to install spyware and compromise the system.

4.0 Self-Assessment Exercise(s)

1. One of the common backdoors that are placed on a system is

    e. Worm
    f. Trojan
    g. Rootkit
    h. Keylogger

    Answer: C

2. Methods through which Spyware can be placed on a system include

e. Instant messaging
f. Internet Relay Chat
g. Media Access Control
h. Rootkits

Answer: A and B

5.0 Conclusion

Spyware programs can track all activities on a computer, and another party can retrieve information via several different methods. The most common method is a Trojan horse. It is also possible that when a user visits certain websites, spyware may download in the background while the user is simply perusing the website.

6.0 Summary

In this unit, you have learned what spyware is and how the software can be delivered to a target system. Spyware is used by hackers to gather or steal sensitive information from a target remotely. Thus, this class of malware is suitable for espionage and stealthy malicious activities.

7.0 References/Further Reading

Chuck, E. (2016). *Computer Security Fundamentals (3rd ed.).* Pearson Education, Inc.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Hall, G. & Watson, E. (2016). *Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Oriano, S & Solomon, M. G., (2011). Hacker Techniques, Tools, and Incident Handling, Jones & Bartlett Learning.

Module 4: Penetration Testing

Module Introduction

Penetration testing is used by organisations to evaluate the security level of computer and network systems to identify a weakness that can be exploited by hackers. This is to determine effective security measures needs to be placed to protect computers and network infrastructure from attack.

In module 2, you learnt how hackers use the vulnerability to carry out targeted attacks on Microsoft Windows systems, Linux systems, Web servers and Web applications. Also, you learned how hackers use malware to launch secret and destructive attacks in module 3. In this module, I will take you through how to conduct a security audit of an organisation to determine compliance with security policies, procedures and standard and ascertain protection. You will also learn how to assess vulnerabilities in systems, services, applications and infrastructure that enable hackers to launch targeted and malware attacks and identify ways to mitigate the risk of attacks. Finally, I will take you through penetration testing roadmap and plans in order to identify vulnerabilities.

This module is classified into the following four units:

Unit 1: Security Audit
Unit 2: Vulnerability Assessment
Unit 3: Penetration Testing Roadmap
Unit 4: Penetration Test Plan

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I will highlight resources for further reading at the end of each unit.

Unit 1: Security Audit

Contents

1.0 Introduction

In this unit, you will learn how to measure the compliance of user and computer systems implementation with standard security policies and procedures of an organisation. This is to identify and analyse security risks in terms of human behaviour and systems set up that enables activities such as targeted attacks, social engineering attacks, malware attacks and other unauthorised activities in an organisation. You will also learn the tools used to audit the security of an organisation.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe how security audit is conducted
- explain security audit tools
- highlight how to audit the security of an organisation.

3.0 Main Content

3.1 Security Audit

A security audit is an assessment of the level of compliance of users and systems with the security policy and standards of an organisation to determine the state of protection. A security audit is conducted periodically to ensure the compliance of the security policies and effective implementation of security measures. The audit also determines the minimum set of controls required for reducing risk to an acceptable level. It should be noted that a security audit only gives a snapshot of the vulnerabilities revealed at a particular point in time.

To perform a security audit, you need security policy and standards, audit checklists and an inventory list, which may cover different areas such as web application, network architecture and wireless communication. The auditing process also involves the use of different auditing tools and different review techniques to reveal the security non-compliance and loopholes. After the audit process, an audit report is prepared to highlight the compliance and gaps that existed between the current protection and the requirements specified in the security policies and standards. This determines the strength and potential weaknesses of the security of an organisation.

The major objectives of a security audit are to:

1. Check for compliance with existing security policy, standards, guidelines and procedures.
2. Identify the inadequacies and examine the effectiveness of the existing policy, standards, guidelines and procedures.
3. Identify and review relevant statutory, regulatory and contractual requirements.
4. Identify and understand the existing vulnerabilities.
5. Review existing security controls on operational, administrative and managerial issues, ensure effective implementation of security measures and compliance to minimum security standards.
6. Provide recommendations and corrective actions for improvements.

There are different scenarios when a security audit should be performed. The exact timing depends on your system requirements and resources.

1. New installation/enhancement audits: before the implementation of major enhancements, to ensure compliance with existing policies and guidelines and meet the configuration standard.
2. Regular audits: conduct audits periodically, e.g. once a year, either manually or automatically using security-related tools to assure the minimum set of controls are implemented to detect and handle security loopholes or vulnerabilities.
3. Random audits: This is to perform random checks in order to reflect the actual practice.
4. Nightly or non-office hour audits: to reduce the auditing risks by performing during non-office hours or at night.

3.2 Risk Analysis

During the audit, you will need to understand a little about **risk analysis** and **risk management** - a security audit is all about assessing the risks of loss, compromise or damage to information. Risk analysis is the process of identifying and assessing the risk of something happening. Space does not allow us to cover risk management and analysis in detail, but its principles are summarised here:

1. The establishment of mechanisms to keep risks under review and to make sure they are being addressed
2. A means of identifying the potential risks to the business
3. An assessment of the likelihood of each risk materialising
4. An assessment of the probable impact of each risk
5. The formulation of measures to avoid each risk occurring
6. The development and deployment of fall-back measures to mitigate the risks if avoidance actions fail
7. The determination of the imminence of the risk and of taking appropriate countermeasures

It is recommended that those who will be carrying out the security audit familiarise themselves further with risk management and analysis theory before commencing.

3.3 Security Audit Tools

Several security audit tools are available to aid security auditors to find vulnerabilities in systems and services. These tools run on Windows and Unix-based operating systems. The choice of security audit tools depends on the security assessment needed. For instance, some security scanning tools that can check for vulnerabilities on the network (network-based) or specific hosts (host-based) through scanning and launching simulated attacks. Table 1 shows some security audit tools.

Table 1: Security Audit Tools

Security Audit Tool	**Platform**	**Type**
COPS/Tiger	Linux and Unix	Intrusion detection
Crack	Linux, Unix and Windows	Password cracking
Nmap	Linux, Unix and Windows	Port scanner
tcpdump	Linux, Unix and Windows	Network monitoring
snifit	Linux, Unix and Windows	Network monitoring
CyberCop	Linux and Windows	Password cracking, port scanning and network monitoring
Nessus	Linux, Unix and Windows	Exploit tester
Metasploit	Linux, Unix and Windows	Exploit tester
TripWire	Linux, Unix and Windows	Intrusion detection

3.4 Security Audit Stages

A security audit comprises several stages, as shown in Figure 19.

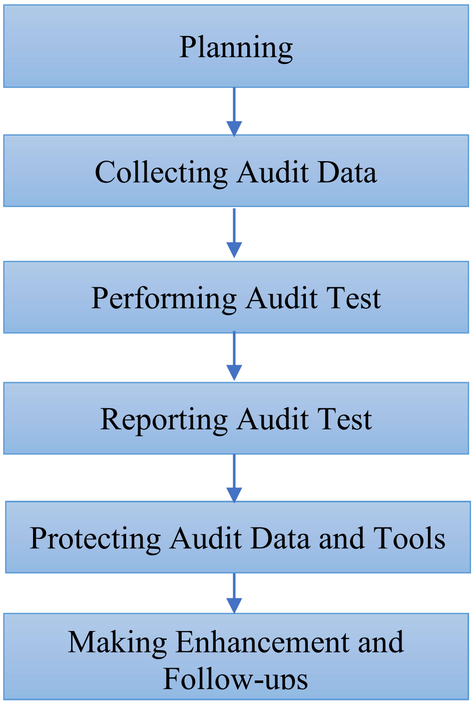

Fig. 19: Security Audit Stages

Planning

This is the process of selecting the effective and efficient methods of performing security audit and obtaining all necessary information. The required time for planning depends on the nature, extent and complexity of the audit. In this stage, the security audit scopes are clearly defined and established. Examples of security audit scopes include:

1. Internet security
2. General security of an internal network
3. Mission-critical systems
4. Hosts security
5. Network server's security such as web servers and email servers
6. Network components and devices such as firewalls and routers
7. General security of a computer room
8. Network services such as directory services and mailing services

Collecting audit data

This stage determines the amount and type of information to capture, and how to filter, store, access and review the audit data and logs. The amount of data collected depends on the audit scope and data availability. Audit data can be collected and stored in different ways such as log files, reports and storage media. Apart from electronic data collection, some physical or manual events should also be recorded and collected. These includes:

1. Computer equipment repair and maintenance activities such as date, time, supporting vendor information and the activity's description.
2. Change control and administration events such as configuration changes, installation of new software, data conversion or patches updating.
3. Physical site visit by external parties such as security auditors or guests.
4. Procedure and policy changes.
5. Operation logs.
6. Security incident records.

Performing audit tests

This stage involves technical investigation using different automated security audit tools for diagnostic review and penetration tests. The security audit tools are useful in gathering information because they require little user intervention, which saves time. It is important to check systems against know vulnerability advisories from groups such as Computer Emergency Readiness Team (CERT), Common Vulnerabilities and Exposures (CVE), bugtraq and National Vulnerability Database (NVD).

Reporting Audit Results

This stage involves writing a comprehensible security audit report after completion of the audit work. Security auditors should analyse the auditing results and provide a report, which reflects the current security status. The report should be presented in a way that explains your findings clearly to your intended audience. The audience may comprise executive members of an organisation, information technology managers and staff. It is essential to present the report in a clear and non-technical language.

Protecting audit data and tools

This stage involves safeguarding the audit data and tools. Audit data and all physical documents relating to the audit shall also be classified to an appropriate level and protected according to their classification. The auditing tools should be properly maintained, controlled and monitored to avoid misuse. The security auditors should only use such tools in a controlled manner. These tools should also be removed immediately after use unless proper control has been made to protect them from unauthorized access. Security auditors shall also return all audit information.

Making enhancements and follow-up

This stage involves discussing the action that should be taken based on the results of the security audit. If corrective actions are required, resources should be allocated to ensure that the enhancements could be performed at the earliest opportunity.

4.0 Self-Assessment Exercise(s)

3. One of the following is not included in the activities you need to perform in conducting a security audit for an organisation?
    A. Performing Audit Tests
    B. Modifying Audit Results
    C. Protecting Audit Data and Tools
    D. Planning

    Answer: B

4. Security audit is conducted__________?
    A. Annually
    B. Daily
    C. Periodically
    D. Monthly

    Answer: C

5.0 Conclusion

In this unit, you have learned the stage and processes of measuring the compliance of organisation security with standard security policies and procedures. Several security audit tools are available. However, the use of an audit tool depends on the type of security audit you will conduct and the platform used by the organisation.

6.0 Summary

In this unit, I discussed the security audit and the activities performed at each stage of the audit process. A security audit is conducted to identify the strength and weakness of an organisation regarding compliance with security policies. I also highlight some security audit tools used to facilitate conducting a security audit for an organisation.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Hall, G. & Watson, E. (2016). *Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

IGeorgia, W. G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Kapp, J. (2000). "How to Conduct a Security Audit. PC Network Advisor." (120), 3-8.

SPG-SM01 (2017). Practice Guide for Security Risk Assessment and Audit

Unit 2: Vulnerability Assessment

Contents

1.0 Introduction

In this unit, I will explain how the assessment vulnerabilities in applications, systems, services and network infrastructure. In Unit 1, you learned how to perform a security audit to determine compliance with security policy. In this unit, I will take you through how to find a weakness, not in compliance with security policy as in security audit, but in the design of systems and network infrastructure. I will also take you through the activities performed at the stages of vulnerability assessment and approached used in assessing vulnerabilities.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- explain vulnerability assessment
- discuss the types of vulnerability assessments
- describe approaches to vulnerability assessment.

3.0 Main Content

3.1 Vulnerability Assessment

Vulnerability is a weakness in software design, network services, operations, control and procedure that could be exploited to gain unauthorised access or compromise a system. This includes anything from a weak password on a router to an unpatched programming flaw in an exposed network service. Vulnerability assessments are the process of locating and reporting vulnerabilities. The assessment is used to detect and resolve security problems before being exploited by a hacker. Once vulnerabilities are identified, the affected systems and services can be fixed by patching the vulnerabilities. Then, the assessment can be repeated to verify the effectiveness of the fixes. This is the standard method for many organisations to manage their security issues.

3.2 Types of Vulnerability Assessment

There are two types of vulnerability assessment; host vulnerability assessment and network vulnerability assessment.

3.2.1 Host Vulnerability Assessments

In a host vulnerability assessment, you analyse the security of a single system. The assessment is conducted on the systems using specialised tools and an administrative user account. The host vulnerability assessment tools are installed on the system(s) you want to assess or linked to a central system on the network. A host vulnerability assessment looks for system-level vulnerabilities such as insecure file permissions, missing software patches, noncompliant security policies, and outright backdoors and Trojan horse installations.

Host vulnerability assessment provides an in-depth test of the host, which is good for monitoring the security of critical systems. However, host vulnerability assessment requires administrative access and specialised tools for the operating system and software packages installed on the system under test. Thus, host assessments are often reserved for a few critical systems.

3.2.2 Network Vulnerability Assessments

In a network vulnerability assessment, you used to test an entire network of systems at once. A network vulnerability assessment identifies all live systems on a network, determines what network services are running on the systems, and then analyses the services for potential vulnerabilities.

Network vulnerability assessment differs from host vulnerability assessment because it does not require any configuration changes on the systems being assessed. Network vulnerability assessments provide the feasible of testing the security of large, complex networks of heterogeneous systems. The strength of network vulnerability assessment is its effectiveness in identifying vulnerabilities in a large number of systems at a time. However, network vulnerability assessment has limitations that include:

- Inability to detect certain types of backdoors
- Complications with the firewall.
- Disruption of normal operations
- Interference with many devices such as printers
- Network bandwidth consumption.

3.3 Network Vulnerability Assessment Process

There are a set of activities that you conduct when assessing network vulnerabilities. The activities are as shown in Figure 20.

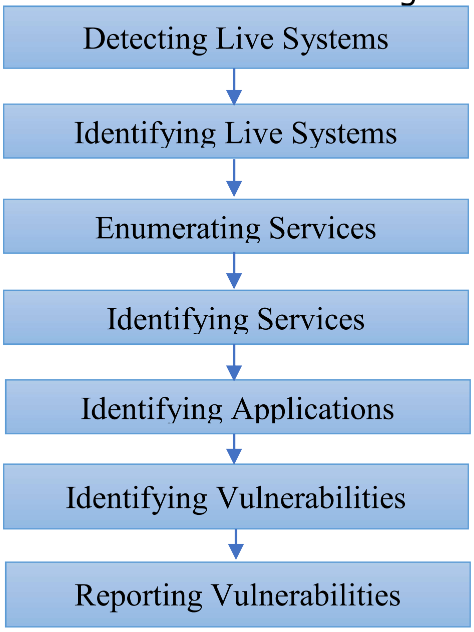

Fig. 20: Vulnerability Assessment Process

Detecting live systems

This is to identify the systems being assessed using Internet Protocol (IP) addresses to determine whether the systems are accessible. Several probes are sent to the systems for responses. If a response is received, the system is considered reachable and valid.

Identifying live systems

In this stage, the systems being assessed are probed to identify their types and platforms used by the systems. Do you remember fingerprinting in Unit 2 of Module 1? Fingerprinting techniques are used here to detect system type and platform. The fingerprinting techniques used from Simple Network Management Protocol (SNMP) queries to complex TCP/IP stack-based operating system identification.

Enumerating services

Once a system is detected and identified, the activity that follows is an enumeration, that is, port scan. A port scan is a process of determining what TCP and UDP services are open on the system being assessed. Do you remember port scanning in Unit 2 of Module 1? TCP and UDP port scanning are used to send connection requests to the systems. There are 65,536 available TCP ports; however, limiting the scan to a subset of the available ports reduces the amount of time it takes to perform the assessment and substantially decreases the bandwidth required.

Identifying services

After enumerating services on network systems, the next activity is to identify the services that are in use on each open port. This process starts with sending some common application requests, such as HyperText Transfer Protocol (HTTP) on port 80, and analysing the responses against a set of signatures. When a signature matches a known application, this information is stored for the later use and the next service is tested.

Identifying applications

Once the service detection phase is complete, the next step is to determine the actual application in use for each detected service. The goal of this stage is to identify the vendor, type, and version of every service detected in the previous stage.

Identifying vulnerabilities

After identifying systems and applications, the systems are now ready to begin testing for vulnerabilities. This process often starts with basic information-gathering techniques, followed by active configuration probes, and finally a set of custom attacks that can identify whether a particular vulnerability exists on the tested system.

Reporting vulnerabilities

After the analysis is finished, the final stage of the assessment process is reporting. The assessment report lists the systems discovered during the assessment and any vulnerabilities that were identified on them.

3.4 Vulnerability Assessment Approaches

When performing a vulnerability assessment, the actual perspective of the test can have a huge impact on the depth and quality of the results. Essentially, there are three different approaches to vulnerability testing: administrative, outsider and hybrid.

3.4.1 Administrative Approach

The administrative approach performs the assessment from the perspective of a normal, authenticated system administrator. The assessment tool might require that it be launched by an authenticated administrative user or provided with a user account and password. These credentials can be used to detect missing patches, insecure configuration settings, and potentially vulnerable client-side software. This is useful when trying to detect and resolve client-side vulnerabilities on a network of computer systems.

3.4.2 The Outsider Approach

The outsider approach takes the perspective of the unauthenticated malicious intruder who is trying to break into the network. The assessment process can make decisions about the security of a system only through a combination of application fingerprinting, version identification, and actual exploitation attempts. Assessment tools built on this approach have the capabilities of detecting vulnerabilities across a wider range of operating systems and devices than the administrative approach.

3.4.3 The Hybrid Approach

In this approach, the assessment tools use administrative credentials when possible but fall back to remote fingerprinting techniques if an account is either not available or not accepted on the tested system. The hybrid approach provides results that are often better than those using administrative or outsider approach.

4.0 Self-Assessment Exercise(s)

1. What are the strengths of using the hybrid approach of vulnerability assessment compared to a single approach?
2. Identify the limitations of network vulnerability assessment
   a. Ability to detect certain types of backdoors
   b. Complications with antivirus
   c. Disruption of normal operations
   d. Interference with many devices, such as printers.

5.0 Conclusion

In this unit, you have learnt how to assess vulnerabilities in applications, systems, services and network infrastructure. To assess vulnerabilities, you need to determine the systems to be assessed in order to apply the relevant type and approach of vulnerability assessment.

6.0 Summary

In this unit, I have discussed vulnerability assessment and the activities performed at each stage of the assessment process. I also explored the types and approaches used by security administrators to assess vulnerabilities in systems, applications, services, and network infrastructure.

7.0 References/Further Reading

Beale, J., Meer, H., van der Walt, C., & Deraison, R. (2004). Nessus Network Auditing: Jay Beale Open-Source Security Series. Elsevier.

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia Weidman G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

ISPG-SM01 (2017). Practice Guide for Security Risk Assessment and Audit.

Unit 3: Penetration Testing Roadmap

Contents

1.0 Introduction

In Unit 2, you learned vulnerability assessment. Unlike vulnerability assessment that focuses on identifying vulnerabilities on a network, a penetration test focuses on gaining unauthorised access to the tested systems by exploiting the vulnerabilities identified during assessment. In this unit, I will discuss the roadmap for conducting a penetration test.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- describe the rules for a successful penetration test
- discuss how to develop penetration testing plan.

3.0 Main Content

3.1 Penetration Testing Roadmap

Penetration testing is an authorised attempt to locate and successfully exploit vulnerabilities in computer systems to make the systems more secure. Penetration testing provides proof of concept attacks to demonstrate the vulnerabilities in computer systems.

What is the difference between vulnerability assessment and penetration testing?

A vulnerability assessment reviews services and systems for potential security issues, whereas a penetration test performs exploitation and proof of concept attacks to prove that a security issue exists. Penetration tests go a step beyond vulnerability assessments by simulating the hacker activity and delivering live payloads.

3.2 Penetration Testing Rules

Before conducting a penetration test, there are certain rules you need to know. These are:

1. **Set a goal**: If you have planned to evaluate the security of an online system or network, you must first try to answer three questions:
   a. What information does a hacker see when they look at the target network?
   b. Can the hacker misuse that information?
   c. Is the target aware of any attempts to penetrate their system?
2. **Plan ahead**: A penetration testing plan must be defined. The plan should include:
   - Identifying the networks to be tested
   - Determining the intervals of the tests
   - Clearly defining the testing procedure
   - Creating a plan that you can share with stakeholders
   - Getting the plan approved.
3. **Get authorisation**: Before conducting a penetration test, you must obtain the necessary authorisation from the organisation. An authorisation document must be issued by the organisation showing that you have the approval to test the system according to an approved plan and that the organisation will support you in case of any legal charges.
4. **Be ethical**: Before conducting a penetration test, you must bound by the code of professionalism, confidentiality and conscience. Make sure that you always stick to the plan that was previously approved and avoid adding any new details to it down the road. You are not to release or share the results of your security test with unauthorised persons both within and outside the organisation. Any information you discover should be treated as sensitive. It is also important to be aware of any local laws or governance regulations within the organisation that relate to hacking.
5. **Maintain good records**: Some basic rules should be followed when it comes to record-keeping:
   - Note down every task performed.
   - Log every piece of information directly.
   - Always have a backup copy of the log.
   - Note down every test performed, including the dates.

6. **Protect confidential information**: You are likely to come across a lot of personal and private information during your penetration testing. You must respect people's privacy and treat every piece of information with confidentiality. Passwords, encryption keys, and other sensitive information must not be abused. Always treat other people's personal or confidential information with the same respect you would want others to treat your own.
7. **Do not cause harm**: There are times when you may get excited about the job and the positive test results you are receiving, so you keep plugging away. However, you may accidentally cause some kind of outage or even interfere with another's rights. This is why you should always have a plan and then commit to sticking to it. Be knowledgeable about the tools you are using, especially their implications. Choose your tools wisely and always read the documentation.
8. **Always be empirical**: If you want your test results to be accepted, you need to use a scientific process that is characterised by these features:
    a. Quantifiable goals: Set a goal that you will be able to quantify. You can set task goals or time-related goals.
    b. Consistency and repeatability: Every test that you perform must produce the same results. If they do not, then your results are inconsistent and probably invalid. If you repeat a test over and over, you should get the same results every time. Consistency and repeatability of tests are critical features of an empirical process.
    c. The permanence of results: The client that you work for will look forward to your test results if you focus on fixing persistent problems for good, instead of solving temporary ones that may recur later on.
9. **Do not use any random tool**: There are a lot of hacking tools in the market today. It is easy to be tempted to try them all out, probably since most of them are free. However, it is advisable to just focus on a few tools that you know are effective, and you are familiar with.
10. **Report all your findings**: If you are hired for penetration systems, and the process takes longer than a week, you need to give your clients weekly status updates. If you discover any high-risk weaknesses and vulnerabilities in the system during your tests, you need to report them to those concerned. The reports that you issued is what the client will use to determine how thorough and sincere you are in your work. A report will also help during the analysis and critique of your results.

3.3 Penetration Testing Plan

Having learned the rules for conducting a penetration test, it is important to take you through the steps that guide you through planning the penetration testing process. The penetration testing plan steps include:

i. Determine the most critical and vulnerable systems to be tested first. These can include server passwords or email phishing. Once the core areas have been tested, you can then cascade down to all the other systems.

ii. Assess the risks involved. It is important to always have a contingency plan in case the penetration testing process goes wrong. Determine how people and systems will be affected beforehand.

iii. Determine testing schedule. It could be during regular business hours, early mornings, or maybe late at night. The best way to test the system would be to launch any type of test at any time of day. The only exceptions would typically be full DoS attacks, physical security and social engineering tests.

iv. Have a basic understanding of the system being tested. You may need to get more details of the systems to be tested.

v. Define the actions to be taken in case major vulnerabilities are found. If you discover a couple of security weaknesses, let the key players know about it immediately. Keep testing the system until you find it impenetrable.

vi. Determine the deliverables. These include detailed scanning reports containing information about vulnerabilities and recommendations on how to fix them.

vii. Determine the specific set of tools that you will need for your task. Always ensure that you are using the appropriate tool for the right task.

4.0 Self-Assessment Exercise(s)

What is the major difference between internal penetration testing and external penetration test?

Answer:
the major difference between internal and external penetration testing is that with internal penetration testing, it is assumed the attacker already has access. In contrast, external penetration testing is the ability of a remote attacker to get to the internal network.

5.0 Conclusion

In this unit, I explored the concept of a penetration test, rules and steps that you need to follow to achieve a successful penetration test. A penetration test is a great way to determine how well the security measures of an organisation respond to a real-life attack.

6.0 Summary

In this unit, you learnt the concept of exploiting the weaknesses identified during vulnerability assessment to gain unauthorised access to systems. It is important to note that you need to properly plan and follow the rules of a penetration test to achieve successful results.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *HACKING: Computer Hacking, Security Testing, Penetration Testing and Basic Security.*

Unit 4: Penetration Test Plan

Contents

1.0 Introduction

In Unit 2, you learnt the roadmap to carry out a penetration test. In this unit, I will take you through the main steps of the penetration test plan from information gathering to the actual test.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be able to:

- perform reconnaissance
- conduct penetration testing
- evaluate system vulnerabilities.

3.0 Main Content

3.1 Penetration Test Plan

A penetration test plan is an essential step-by-step procedure used to prepare for a penetration test. Penetration test exploits every potential entry point into the network, such as customer networks, wireless networks, or mobile devices. Testing everything is important because hackers use people, physical components, or computer systems to launch an attack. The primary aim is to figure out how hackers can exploit the vulnerabilities in the systems and other network components. You can decide to simulate a restricted attack on a single computer or comprehensively attack the whole system.

There are two ways to test a system; a covert test and an over test. The overt test is where you have some inside knowledge of the system you intend to test. In the covert test, you do not know much information apart from the name of the organisation. In the covert test, you have to search for information on your own, the same way a hacker will do. This enables you to see what a hacker would see when they try to gain access. However, a covert test takes more time, and there is a higher chance of overlooking certain vulnerabilities.

There are three main steps for conducting a penetration test. These are reconnaissance/information gathering, evaluating system vulnerability and penetration test.

3.2 Reconnaissance/ Information Gathering

This is the process of collecting information about the person or organisation that you want to test. It is a passive approach that mainly involves using publicly available resources to find information about something. There are some techniques that you can use to gather information. These include:

Web Searches
These involve using the target's website and browse around as you try to collect as much useful information as possible. If you are using Google, you can use keywords to get the most relevant information.

Web Crawling
A **Web crawler** sometimes called a **spider** or **spiderbot** and often shortened to **crawler**, is an Internet bot that systematically browses the World Wide Web, typically for Web indexing (*web spidering*).

Web search engines and some other sites use Web crawling or spidering software to update their web content or indices of other sites' web content. Web crawlers copy pages for processing by a search engine which indexes the downloaded pages so users can search more efficiently. Certain web crawling tools can mirror a website and download all the publicly accessible files from the target website. This then allows you to scan the copy offline.

Websites
There are certain websites that contain information about different organisations and their employees. You can even do a people search if you just know which websites to use.

Network mapping
This is the process of searching public databases to discover the information available about a particular network such as Whois. Whois

enables you to obtain information that will help you scan a network or prepare a social engineering attack. You will be able to get the names, phone numbers, and addresses linked to a specific Internet domain registration.

System scanning
The information gathered from external sources can provide you with a map of the entire network, revealing how the systems are interconnected. You should be able to see the hostnames, IP addresses, open ports, running protocols and applications.

Hosts
Scan and record those hosts that can be accessed externally via the Internet and internally by an insider. Begin by pinging the IP addresses or the hostnames. You can use either the standard ping tool that comes with operating systems or a 3rd party tool such as SuperScan or fping.

Open ports
Several networking tools can be used to scan for open ports. These include OmniPeek, Wireshark, SuperScan, among others. It is easier to perform a scan internally than externally. To scan internally, connect your computer to the local network and run the software. To scan externally, just assign the computer you are using a public IP address and connect it to a hub that is not within the firewall.

3.3 Evaluating System Vulnerabilities

After discovering a potential vulnerability, it is time to start testing. However, you should confirm if the vulnerability is real. There are several websites and hacker message boards that you can manually search to determine whether what you have discovered is on the list of classified vulnerabilities. These websites include www.sans.org, nvd.nist.gov, and cve.mitre.org/cve.

The next step is to start testing right away. You can either perform a manual evaluation or an automated evaluation. In manual evaluation, the potential vulnerabilities are assessed by linking to the ports that can be exploited by hackers. Automated evaluations involve the use of tools that test for weaknesses on a platform or network. Though these tools make work easier and much faster, most of them only can test for specific and individual system vulnerabilities.

3.4 Penetration Testing

Once you have discovered the major security vulnerabilities, the next step is to penetrate the vulnerable system using the available tools or a tool you develop for a penetration test. After penetrating the system, you should carry out the following:

1. Gather more information from the host system
2. Access other interconnected systems in the network
3. Start and stop specific services
4. Get a remote command prompt
5. Launch a denial of service attack
6. Gain access to confidential files
7. Disable inbuilt logging security checks
8. Perform SQL injection attacks
9. Take screenshots
10. Send emails to people as the administrator
11. Upload a file.

Generally, your job is to expose the presence of system vulnerabilities, so there is no need actually to exploit them and mess around with people. Unless for some reason, it is necessary to show the management just how serious system flaws are.

4.0 Self-Assessment Exercise(s)

1. _____________ is an Internet bot that systematically browses the World Wide Web, typically for Web indexing.
   E. Zombie
   F. Botnet
   G. Spider
   H. Hosting

2. Which of the following statements is true about a penetration testing plan?
   A. It is an essential plan used to conduct a vulnerability assessment.
   B. It is an essential step-by-step procedure used to prepare for a penetration test.
   C. It is the plan for gathering information from external sources, revealing how the systems are interconnected.

   Answer: B

3. There are four main steps for conducting a penetration test, true or false?

   Answer: True

Mini-project

A Nigerian bank has been using online banking for ten years now. They have their web servers at the head office in Abuja. The bank wishes to understand their current level of risk. They contact you with an offer to carry out a penetration test. They provide you with the IP address of their web servers. Develop a penetration testing plan to assess the security risk of their web servers.

5.0 Conclusion

In this unit, you learnt how to develop a penetration test plan to assess the security risk of an organisation.

6.0 Summary

In this unit, I explored the necessary step needed by a security expert to develop a plan for a penetration test.

7.0 References/Further Reading

Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Inc.

Georgia, W. G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc.

Hall, G. & Watson, E. (2016). *HACKING: Computer Hacking, Security Testing, Penetration Testing and Basic Security*