PET361@Assignment1

Pieter_Johannes_Swart(600640)

Table of Contents

Section A:

Question 1:

1.1 What is Metasploitable2?

Metasploitable 2 is a deliberately vulnerable Linux virtual machine designed for security professionals, ethical hackers, and students to practice penetration testing, to learn hack and vulnerability analysis. It is primarily used in conjunction with Metasploit, a popular penetration testing framework, to exploit vulnerabilities and simulate attacks in a controlled environment.

It comes with a wide range of security vulnerabilities, such as outdated services, insecure configurations, and known software bugs.

1.2 What is the Magical Code Injection rainbow (MCIr)?

It is a intentionally vulnerable web application designed to help users learn and practice various web exploitation techniques, especially those involving code injection vulnerabilities. It serves as a hands-on educational tool for security professionals, ethical hackers, and students to explore how different types of injections can be exploited in web applications.

MCIR allows ethical hackers to practice finding and exploiting code injection vulnerabilities. It's often used in security courses to teach students about injection flaws and how to avoid them through secure coding practices.

1.3 What is penetration testing and what is it's purpose?

Often referred to as pen testing or ethical hacking, is a simulated cyber attack performed on a computer system, network, or web application to identify and exploit security vulnerabilities. The primary goal is to evaluate the security of the system by discovering weaknesses that could be exploited by malicious attackers.

The purpose of penetration is to discover and document vulnerabilities that could be exploited by attackers. These can range from software bugs to misconfigurations and weak passwords.

1.4 What is malicious user testing?

It is a type of security testing that simulates the actions of a malicious insider or external attacker that have access to a system. The goal is to understand how a legitimate user, who has access to certain resources and privileges, could abuse their access or escalate privileges to compromise system security or perform unauthorized actions. Like example: insider threats, testing privilege misuse and social engineering.

1.5 What is the difference between phishing and spear phishing?

Phishing	Spear Phishing
A widespread form of cyber attack where attackers send out emails, messages, or websites to many people in an attempt to steal sensitive information like passwords, credit card numbers, or personal data.	It is focused on targets. Attackers create personalised messages aimed at a specific person, organisation, or group. The attacker often conducts research on the target to make the message more convincing.
It is not personalised and are often designed to appear as legitimate sources, like banks or popular online services.	Spear phishing emails often include specific details about the target, such as their name, job role, or even recent activities.
A phishing email might say, "Your bank account has been compromised. Click this link to verify your information." It's sent to thousands of people, hoping some will fall for it.	Example, "Hi Docter “Name”, I noticed you were recently working on this Patient. Can you go through this Patient report?" It looks personal and is designed to trick you into opening a malicious attachment or link.

Question 2:

2.1 Why is it a good idea to create a hacker toolbox on a virtual machine and not a physical computer or on the local host operating system?

A virtual machine provides a separate, isolated environment from your primary system. If you accidentally run a malicious program or script, it will only affect the virtual machine. This containment prevents damage or disruption to your host system or personal files. Any potentially dangerous software or malware that might be used in hacking exercises stays contained within the VM.

Many VMs allow you to configure different networking modes, which can isolate your testing environment from the main network. This minimizes the risk of exposing your personal IP address or network data when testing tools.

You can easily move your VM with all the configured tools between different machines. This portability allows you to work from different devices without having to reinstall or reconfigure everything.

Many penetration testing tools simulate attacks, and some may include actual malware. Running these on your local machine may lead to unintended consequences, including legal and security issues or breaking any law.

Virtual machines make it easy to set up different environments to practice hacking techniques or test new tools without impacting the main system.

2.2 Why is Kali Linux so sought-after in the hacking industry?

It is designed specifically for penetration testers and for hackers, so it has optimised settings for this use. Users can perform attacks like network scanning, wireless testing, vulnerability exploitation, and password cracking

The tools on Kali Linux are ready to use out of the box, eliminating the need for complex installations and configurations. This makes it convenient for ethical hackers to get started quickly.

Kali Linux includes dedicated wireless testing tools for attacks like Wi-Fi cracking, packet sniffing, and man-in-the-middle attacks. It's compatibility with diverse wireless chipsets makes it a favourite for wireless network testing.

While designed for advanced users, Kali Linux provides a clean, intuitive interface and extensive documentation, making it accessible to beginners.

Kali Linux comes with over 600 pre-installed tools for various security tasks, e.g. Penetration testing, Forensics, Reverse engineering, Vulnerability assessment. These tools cover nearly every aspect of cyber security, making it a comprehensive toolbox for both beginners and experts.

Section B:

Question 3:

3.1 Name the phases for the penetration test lifecycle.

1. Planning and Reconnaissance - This phase involves reconnaissance or information gathering, where the tester collects data on the target using both passive and active techniques. This could include information about the network

infrastructure, IP addresses, DNS records, employee information and software versions

Types of Reconnaissance (Cyber security):

- Passive Reconnaissance: Gathering publicly available information without interacting directly with the target, e.g. using WHOIS lookup, Google searches, or public databases

- Active Reconnaissance: Engaging with the target to collect information, e.g. pinging, port scanning.

2. Scanning - Testers probe the target systems more actively to discover exploitable services or software versions. Scanning helps map the attack surface and identify weak points for further exploitation.

3. Gaining Access - Penetration testers attempt to compromise the target by exploiting the vulnerable to discovered during the scanning phase. This may involve exploiting misconfiguration, weak credentials, unpatched software and specific security flaws.

4. Maintaining Access - After successfully gaining access, the tester may want to ensure the ability to return to the compromised system without being detected. This phase focuses on installing backdoors, establishing channels or using rootkits to maintain control over the system.

5. Privilege Escalation - Attackers often seek to increase their control over the system by leveraging vulnerabilities or misconfigure that allow them to execute commands with higher privileges. Privilege escalation can help hackers gain access to more sensitive data or control critical systems.

3.2 How does these phases of the penetration testing lifecycle work together?

Sequential Progression - Each phase builds on the one before it. For example, the reconnaissance and scanning phases identify entry points and vulnerabilities, which lead to exploitation and gaining access. After access is gained, phases like maintaining access and privilege escalation ensure deeper control over the target.

Feedback Loop - There is often a feedback loop between phases. For example, after exploiting a vulnerability and gaining access, the tester might return to the scanning

phase to look for new vulnerabilities in deeper system layers. Additionally, the post engagement phase often leads to follow up tests, where previously identified vulnerabilities are checked to ensure they have been moderated.

Comprehensive Testing - Together, these phases ensure a thorough assessment of a target's security. They test for weaknesses, exploit them to understand their impact, and provide actionable recommendations to improve security.

Question 4:

4.1 Give an example for each of the phases of the penetration testing lifecycle, as well as an explanation of the example.

Planning and Reconnaissance: A penetration tester is hired to assess the security of an e-commerce company. The tester begins by conducting passive reconnaissance, populating available information about the company's infrastructure. They use tools like WHOIS to look up domain details and Google Dorking to search for sensitive information that might be indexed in search engines.

Explanation: In this phase, the tester collects information without interacting directly with the target. This helps map out potential entry points and vulnerabilities, e.g. finding subdomains, identifying the technologies used, and uncovering potential usernames or email addresses that could be targeted

Scanning: Using Nmap, the tester scans the company's IP address range to identify open ports and the services running on them. They discover that the company is running an outdated version of Apache web server on port 80.

Explanation: The scanning phase helps the tester identify specific weaknesses in the target's systems. In this case, the outdated web server could have known vulnerabilities that the tester might exploit in the next phase. Nmap provides detailed information about open ports, services, and their versions, which helps narrow down attack vectors.

Gaining Access: The penetration tester identifies a known vulnerability in the outdated Apache version. Using Metasploit, they exploit this vulnerability to gain remote code execution on the web server, allowing them to execute commands on the target machine.

Explanation: This phase focuses on exploiting the vulnerabilities found in the scanning phase. In this example, the tester uses an exploit module from Metasploit

to gain unauthorised access to the system. This simulates how a real attacker could compromise the server and gain control over it.

Maintaining Access: After exploiting the Apache vulnerability, the tester installs a backdoor "reverse shell" on the compromised server. This allows the tester to maintain access to the system, even after a reboot or patching of the vulnerability.

Explanation: Maintaining access ensures that the tester can return to the system later without having to re-exploit the vulnerability. A reverse shell establishes a connection from the compromised machine back to the tester's machine, enabling remote control.

Privilege Escalation: The tester has gained access as a low-privileged web user on the server. To escalate privileges, they use a local Linux kernel exploit to elevate their permissions to the root user, gaining full control over the system.

Explanation: Privilege escalation takes the tester's access from a lower-level user to a more privileged user e.g., root or administrator. In this example, a known kernel vulnerability allows the tester to escalate their privileges and gain full control over the server, enabling them to manipulate critical files and settings.

References

Badman, A., 2023. Spear phishing vs. phishing: what's the difference?. 20 September, pp. https://www.ibm.com/think/topics/spear-phishing-vs-standard-phishing.

Basu, S., 2024. 7 Penetration Testing Phases Explained: Ultimate Guide. 8 August, pp. https://www.getastra.com/blog/security-audit/penetration-testing-phases/.

InfosecTrain, 2024. Why do Hackers Use Kali Linux?. 3 Jan, pp. https://medium.com/@Infosec-Train/why-do-hackers-use-kali-linux-5217e95e7a97#:~:text=Hackers%20use%20Kali%20Linux%20as,hacking%20for%20the%20first%20time..

Kumar, V., 2020. The Magical Code Injection Rainbow (MCIR) in Metasploitable2 Tutorial. 28 JAN, pp. https://www.cyberpratibha.com/blog/the-magical-code-injection-rainbow-mcir-in-metasploitable2/.

Mason, A., 2017. Malicious User Detection. 8 November, pp. https://www.rapidspike.com/blog/malicious-user-detection/.

McCarvil, A., 2022. What is Penetration Testing? Process, Types, and Tools. 29 May, pp. https://brightsec.com/blog/penetration-testing/.

Mifsud, F., 2022. Understanding the five stages of a penetration test.. 23 December, pp. https://cybergateinternational.com/blog/understanding-the-five-stages-of-a-penetration-test/.

Unknown, 2014. Pentest lab - Metasploitable 2. 3 Jun, pp. https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/.

Unknown, 2023. Understanding Virtual Machine Advantages and Disadvantages. 25 Sep, pp. https://www.scalecomputing.com/resources/understanding-virtual-machine-advantages-and-disadvantages.

Upadhyay, R., 2020. Phases of Penetration Testing. 11 Sep, pp. https://upadhyayraj.medium.com/life-cycle-of-penetration-testing-4e7d36a6f74.