Sprint 3 Summary:
Penetration Testing

Authors: Jane Pierre and Elizabeth Bond

Contributors: Frederick Asante, Shemar Brown, Tianna Green, Lucas Higgs, Aaron Kaah and Mishelly Sandoval

Cyber Security & Networking

The Knowledge House

Instructor: George Robbins

May 14, 2023

Penetration testing, also known as pen testing or ethical hacking, is an approach that simulates a real-world attack on a computer system or network to detect vulnerabilities and weaknesses that could be exploited by malicious actors. Penetration testing has a long history, dating back to the 1970s and evolving into a crucial component of modern security practices. This paper defines penetration testing, describes its history, different types, stages, and the tools used today. Furthermore, this summary explains the importance of penetration testing and why it is a vital component of any organization's security strategy.

Penetration testing is critical in any secure program as it helps to identify potential vulnerabilities that attackers could exploit. According to research conducted by IBM, the average cost of a data breach in 2020 was approximately $3.86 million, with 52% of breaches resulting from malicious attacks.

According to a recent study:

- 71% of businesses consider cybersecurity as their top priority.(Abdalslam, 2023)
- 77% of companies use penetration testing to evaluate their security measures.(Abdalslam, 2023)
- The global penetration testing market size is expected to reach USD 4.5 billion by 2025.(Abdalslam, 2023)
- 57% of organizations have experienced a cybersecurity attack in the last year.(Abdalslam, 2023)
- 68% of businesses believe that a cyber-attack is inevitable.(Abdalslam, 2023)
- The average cost of a data breach in the US is $8.19 million.(Abdalslam, 2023)
- 90% of cyber attacks start with a phishing email.(Abdalslam, 2023)
- 69% of organizations do not have a formal incident response plan.
- 43% of cyber attacks target small businesses (Abdalslam, 2023).
- 60% of small businesses go out of business within six months of a cyber attack. (Abdalslam, 2023).

Regular penetration testing can help The Knowledge House detect security weaknesses, prioritize remediation efforts, and reduce the risk of a data breach.

Furthermore, compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA), mandate penetration testing as part of their security requirements.

Social engineering is a method of penetration testing that involves exploiting human psychology and behavior to gain access to sensitive information or systems. It is a non-technical approach to penetration testing that relies on tricking people rather than hacking technology.

Social engineering works by exploiting human psychology and emotions to manipulate individuals into divulging sensitive information or performing actions that compromise security (Verizon, 2021). Cyber criminals use social engineering because it is often easier to trick a person into revealing information or taking an action than it is to hack into a system (Verizon, 2021).

Several techniques are used by cyber criminals use to carry out social engineering attacks such as phishing, pretexing, baiting and spear phishing (Verizon, 2021). According to the 2021 Verizon Data Breach Investigations Report, social engineering was the second most common tactic used by cyber criminals in data breaches, accounting for 17% of all incidents. The report notes that social engineering attacks are becoming increasingly sophisticated, and that cyber criminals are using a combination of tactics to achieve their goals.

The SANS Institute recommends several social engineering tools that can be used for pen testing. These tools can help security professionals simulate social engineering attacks and assess the vulnerability of an organization to these types of attacks. Some of the tools recommended by SANS include: Social-Engineer Toolkit (SET), BeEF (Browser Exploitation Framework), Maltego, Recon-ng and SETOOLKIT. Social engineering is an important component of any comprehensive penetration testing

program, as it can help identify weaknesses in an organization's security culture and employee training.

Exploitation is the act of leveraging vulnerabilities or weaknesses in a system or network to gain unauthorized access, escalate privileges, or execute malicious actions (Infosec Institute, n.d.). Exploits are specific pieces of code or techniques that take advantage of software flaws, misconfigurations, or design weaknesses to compromise the security of a target system (Infosec Institute, n.d.). Penetration testers use exploitation as a tool to simulate real-world attacks and identify the impact and severity of vulnerabilities (Infosec Institute, n.d.).

Exploitation is an essential component of penetration testing because it helps assess the effectiveness of security controls and identify potential risks in a system or network (Infosec Institute, n.d.). By exploiting vulnerabilities, testers can demonstrate the impact of successful attacks, validate the presence of vulnerabilities, and provide actionable recommendations for improving security defenses (Infosec Institute, n.d.).

Metasploit is a widely used penetration testing framework and exploitation tool (Metasploit Unleashed, n.d.). It provides a comprehensive suite of tools, exploits, and payloads that assist security professionals in identifying and exploiting vulnerabilities in target systems (Metasploit Unleashed, n.d.). Metasploit simplifies the process of launching and managing exploitation attempts, making it a valuable tool in penetration testing (Metasploit Unleashed, n.d.). Metasploit enables penetration testers to automate and streamline the process of discovering and exploiting vulnerabilities (Rapid7, n.d.). It offers a vast collection of exploits, both pre-built and user-contributed, that target specific vulnerabilities in various software applications and systems (Rapid7, n.d.). By leveraging these exploits, testers can simulate real-world attack scenarios and assess the security posture of the target environment (Rapid7, n.d.).

In the early days of computing, passwords were often stored in plaintext, meaning, anyone with access to the password file could easily read the passwords. As computer

systems became more widespread, users started to use more complex passwords, and administrators began to use various encryption methods to keep passwords secure. Nevertheless, as technology advanced, so did the techniques used by cyber criminals to crack passwords (Lainhart, 2020).

Understanding password cracking tools are crucial in identifying and mitigating security vulnerabilities. Password cracking tools are applications designed with the purpose of revealing or recovering password authentications used for access to networks, web applications, files and more.

Security professionals developed various password cracking tools to test the security of password systems. John the Ripper is a popular password cracking tool that can crack passwords from various operating systems, including Linux, macOS, and Windows (J. the Ripper, n.d.). This tool can also use different hashing algorithms, including MD5, SHA-1, and bcrypt. To use John the Ripper, the program needs to be provided with a password file, which contains hashed passwords. A hashed password is a one-way cryptographic function that transforms a password into a fixed-length string of characters that represents the original password. The program then uses the selected cracking method to try and crack the passwords. John the Ripper can also use wordlists and rulesets to modify dictionary words and increase the likelihood of cracking passwords.

Network scanning is the process of troubleshooting the active devices on your system for vulnerabilities (Whitaker, Newman, & Whitaker, 2014). It is the process of systematically identifying active hosts, open ports, and services on a network. It involves sending probes or requests to target hosts and analyzing the responses received to gather information about the network infrastructure (Gordon, Loeb, Lucyshyn, & Richardson, 2017). It identifies and examines the connected devices by deploying one or more features in the network protocol (Whitaker, Newman, & Whitaker, 2014). These features pick up vulnerability signals and give you feedback on the security status of your network (Whitaker, Newman, & Whitaker, 2014).

The purpose of network scanning is to manage, maintain, and secure the system using data found by the scanner. There are two types of network scanning: passive and active. Active scanning refers to the process of actively probing a network or system to identify vulnerabilities, open ports, and potential security weaknesses (Whitaker, Newman, & Whitaker, 2014). It involves sending deliberate network traffic or probes to target hosts and analyzing the responses received (Whitaker, Newman, & Whitaker, 2014). Active scanning is commonly used as a form of penetration testing to assess the security posture of a network or system (Whitaker, Newman, & Whitaker, 2014).

Nmap (Network Mapper) is a popular and powerful open-source network scanning tool used in penetration testing to discover and analyze hosts, open ports, and services on a network (nmap.org, n.d.). It provides a comprehensive set of features for network exploration, vulnerability scanning, and security auditing (nmap.org, n.d.).
Nmap is primarily used as a network scanner in penetration testing due to its ability to efficiently probe networks and gather information about the target environment (Rapid7 Blog, 2016). It employs various scanning techniques, such as TCP, UDP, and ICMP scans, to identify hosts, detect open ports, and determine the services running on those ports (Rapid7 Blog, 2016). Nmap also offers advanced features like OS fingerprinting, version detection, and script scanning, allowing penetration testers to gather detailed intelligence about the target network's infrastructure (Rapid7 Blog, 2016). Nmap and other network scanning tools are used to recognize available network services, discover, and recognize any filtering systems in place, look at what operating systems are in use, and to protect the network from attacks. It can also be used to determine the overall health of the network.

In conclusion, penetration testing is an essential part of The Knowledge House's security strategy. Through the different types of penetration testing, such as white box, black box, and gray box testing, the organization can simulate real-world attacks on its computer systems and networks. By identifying potential vulnerabilities, prioritizing remediation efforts, and reducing the risk of a data breach, penetration testing is a

cost-effective way to strengthen The Knowledge House's overall security posture. As such, the organization should prioritize regular penetration testing to ensure the safety and security of its systems and protect its stakeholders' sensitive information.

References:

Abdalslam. (2023, April 13). Penetration testing statistics, trends and facts 2023. Abdalslam. Retrieved May 1, 2023, from https://abdalslam.com/penetration-testing-statistics#:~:text=77%25%20of%20companies%20use%20penetration,a%20cyber%20attack%20is%20inevitable.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2017). Evaluating and Managing the Security of the Internet of Things. In The Economic Benefits and Costs of Entrepreneurship (pp. 187-213). University of Chicago Press.

Infosec. (2021, September 4). The history of penetration testing. Infosec Resources. Retrieved
May 1, 2023, from
https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing/

Infosec Institute. (n.d.). Understanding Exploits in Penetration Testing. Retrieved from https://resources.infosecinstitute.com/topic/understanding-exploits-in-penetration-testing/

J. the Ripper. (n.d.). Retrieved April 7, 2023, from https://www.openwall.com/john/

Lainhart, J. (2020). Passwords and Their History. Retrieved April 7, 2023, from https://www.ntp.gov/docs/internetworks/PasswordHistory.pdf
nmap.org. (n.d.). Nmap - The Network Mapper. Retrieved from https://nmap.org/

Metasploit Unleashed. (n.d.). Metasploit Unleashed. Retrieved from https://www.metasploitunleashed.org/

Rapid7. (n.d.). Introduction to Metasploit. Retrieved from https://www.rapid7.com/learn/metasploit/

Rapid7 Blog. (2016, November 15). Using Nmap for Security Auditing: Official Nmap Project Guide. Retrieved from https://www.rapid7.com/blog/post/2016/11/15/using-nmap-for-security-auditing-official-nmap-project-guide/

TechTarget. Security. Retrieved May 1, 2023, from https://www.techtarget.com/searchsecurity/definition/penetration-testing

Whitaker, A., Newman, J., & Whitaker, B. (2014). Principles of Computer Security: CompTIA Security+ and Beyond (Fourth Edition). McGraw-Hill Education.

Yasar, K., & Mehta, P. (2022, November 18). What is penetration testing?: Definition from IBM. (2021). Cost of a Data Breach Report 2021. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/