Penetration Testing

Designed By:Tianna Green
Contributors: Jane Pierre, Frederick Asante, Shemar Brown, Mishelly Sandoval, Lucas Higgs, Elizabeth Bond and Aaron Kaah

What is Penetration testing?

- Penetration testing, also known as pen testing or ethical hacking, is a simulated attack on a computer system or network to identify vulnerabilities and weaknesses that could be exploited by malicious actors. The goal of penetration testing is to simulate a real-world attack to uncover security vulnerabilities before they can be exploited by actual attackers.
- Penetration testing typically involves using a combination of automated and manual techniques to identify vulnerabilities, such as insecure software configurations, weak passwords, and unpatched software. The results of a penetration test are typically reported to the organization that commissioned the test, along with recommendations for addressing any identified vulnerabilities.
- Penetration testing is an important component of an organization's overall security strategy, as it can help identify and remediate vulnerabilities before they are exploited by attackers and can help ensure compliance with regulatory requirements.

Why is penetration testing important to a secure program for a non-profit organization?

Identifying Vulnerabilities: Penetration testing helps identify vulnerabilities and weaknesses in the organization's systems and networks.

- According to a report by Trustwave, 98% of tested applications had at least one vulnerability, with the average number of vulnerabilities per application being 20.1 (Trustwave, 2020). By conducting penetration tests, a non-profit can proactively uncover and address these vulnerabilities before they are exploited by malicious actors.

Compliance Requirements: Many non-profit organizations are subject to compliance regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Penetration testing is often required to meet these compliance obligations.

- For example, PCI DSS Requirement 11.3 states that organizations must conduct external and internal penetration testing at least annually (PCI Security Standards Council, 2019). Failure to comply with such regulations can lead to legal consequences and reputational damage.

Why is penetration testing important to a secure program for a non-profit organization?

Risk Mitigation: Penetration testing allows non-profits to assess the potential impact of security vulnerabilities and prioritize their remediation efforts.

- According to a study by Ponemon Institute, organizations that conducted penetration testing reduced their risk of experiencing a data breach by 28% (Ponemon Institute, 2020). By identifying and addressing vulnerabilities through penetration testing, non-profits can significantly reduce the risk of data breaches and the associated financial and reputational damages.

Donor Trust and Reputation: Maintaining a secure program is crucial for non-profits to establish and retain donor trust.

- A survey by Edelman found that 81% of respondents said that trust in an organization is a deciding factor in their donation decisions (Edelman, 2021). By actively conducting penetration testing and demonstrating their commitment to security, non-profits can enhance their reputation and increase donor confidence.

Types of penetration Testing

- **White Box Testing**
  - Provides testers with all the details about an organization's system or target network and checks the code and internal structure of the product being tested. White box testing is also known as open glass, clear box, transparent or code-based testing. (Yasar & Mehta, 2022)
- **Black Box Testing**
  - Is a type of behavioral and functional testing where testers aren't given any knowledge of the system. Organizations typically hire ethical hackers for black box testing, where a real-world attack is carried out to get an idea of the system's vulnerabilities.(Yasar & Mehta, 2022)
- **Gray Box Testing**
  - Is a combination of white box and black box testing techniques. It provides testers with partial knowledge of the system, such as low-level credentials, logical flow charts and network maps. The main idea behind gray box testing is to find potential code and functionality issues. (Yasar & Mehta, 2022)

Stages of PenTesting

- Reconnaissance and planning
- Scanning
- Obtaining Entry
- Maintaining Access
- Analysis (Yasar & Mehta, 2022)
  - the vulnerabilities the testers exploited;
  - the type of sensitive data the testers accessed; and
  - the amount of time the testers stayed connected to the target.
- Cleanup and Remediation (Yasar & Mehta, 2022)

Social Engineering

- 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.
- According to the National Institute of Standards and Technology (NIST), social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes" (NIST SP 800-53). This can include techniques such as phishing emails, pretexting phone calls, baiting with USB drives, and physical impersonation.
- 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. However, it should only be conducted by trained professionals and with the organization's permission.

Social Engineering Tools

- Social-Engineer Toolkit (SET) - a popular open-source tool that allows security professionals to create a variety of social engineering attacks, such as phishing emails and USB drops.
- BeEF (Browser Exploitation Framework) - a tool that can be used to test an organization's vulnerability to browser-based attacks, such as clickjacking and cross-site scripting (XSS)
- Maltego - a data mining tool that can be used to gather information about individuals and organizations for use in social engineering attacks
- Recon-ng - a reconnaissance tool that can be used to gather information about an organization's employees, partners, and vendors, which can be used in spear-phishing attacks
- SETOOLKIT - a graphical user interface (GUI) for the Social-Engineer Toolkit, which simplifies the process of creating social engineering attacks.

Network Scanning

- Network scanning is a technique used in penetration testing to identify open ports, active hosts, and other network infrastructure details. It involves systematically scanning a target network for vulnerabilities an attacker could exploit.
- Network scanning tools can perform various types of scans, including port scans, operating system detection, service discovery, and vulnerability scans. These scans can be either passive, where the scanning tool listens for responses from the network, or active, where the tool sends packets to the web to elicit a response.
- The goal of network scanning in penetration testing is to identify potential vulnerabilities in the target network that attackers could exploit. This information can then be used to strengthen the network's security posture and mitigate any potential risks.

Network Scanning Tool (Nmap)

- **Nmap, or network mapper**, is a toolkit for functionality and penetration testing throughout a network, including port scanning and vulnerability detection and assessment.
- Nmap scripting engine (NSE) Script is one of Nmap's most popular and powerful capabilities. These Nmap vulnerability scan scripts are used by hackers to examine commonly known vulnerabilities.
- Nmap-vulners, vulscan, and vuln are the common and most popular CVE detection scripts in the Nmap search engine. These scripts allow you to discover important information about system security flaws.
  - Common Vulnerabilities and Exposures (CVE); is a database of publicly disclosed data security issues. It serves as a reference model for detecting vulnerabilities and threats related to the security of information systems.

Web Application Testing Tool (Burp Suite)

- Burp Suite is a popular web application security testing tool widely used by security professionals, web developers, and penetration testers. It includes a range of features, including a proxy server, scanner, intruder, and repeater, which can be used to identify and exploit vulnerabilities in web applications.
- Burp Suite can intercept and modify HTTP/HTTPS traffic between the client and server, allowing users to analyze and adjust requests and responses. The scanner feature can automatically identify vulnerabilities in web applications, such as SQL injection, cross-site scripting, and file inclusion vulnerabilities. The intruder feature can automate attacks against web applications, such as brute force attacks and parameter manipulation.

Exploitation

- Exploitation is the step after scanning, where the penetrator attempts to gain access to the target system so they can then exploit the identified vulnerabilities (this is where Metasploit is used). It is the most delicate of the steps within penetration testing because it requires bypassing security restrictions. Penetrators must be cautious that they don't compromise or damage the system.

- Exploitation works by a cyber criminal using some tool to find vulnerabilities within a system. Methods: hacking of social media and email passwords, phishing- fake emails asking for security information and personal details, malicious software- including ransomware that allows criminals to hijack files and hold them ransom and distributed denial of service (ddos) attacks against websites. Cyber criminals exploit security and human vulnerabilities so they can steal passwords, data, or money.

Exploitation Tool (John the Ripper)

- John the ripper is a password cracking tool that can be used to perform brute force attacks using different encryption technologies and helpful wordlists. Penetration testers and ethical hackers use this to find the “true passwords” behind hashes. It can help to show how easy it is to reveal weak passwords as well as sophisticated ones.

- How to crack passwords with John the Ripper : “The “john” command has an extensive range of options and flags you can use to run accurate sessions and match the specific format and encryption of your targeted password. The tool has built-in wordlists that automatically apply by default, but you can specify your own with –wordlist and the path to your custom wordlist”

Exploitation Tool (MetaSploit)

- Metasploit is an open-source penetration framework that is used by security engineers to find vulnerabilities on servers and networks. Once vulnerabilities are found the user can take that information to address the weaknesses within a system and find a solution. Metasploit is easily customizable and can be used with most operating systems because it is open-source.
- Metasploit has over 1677 exploits organized over 25 platforms. THis framework consists of 5 parts which are:
    - Interfaces- different platforms used to access the metasploit framework
    - Libraries- contains different functions that allow users to run exploits without the need of having to write additional code themselves
    - Modules- software used to perform task like target exploitation and scanning
    - Tools & Plugins - an addon to the framework that is used to extend its functionality

Password Cracking

- 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.
- As technology advanced, so did the techniques used by cyber criminals to crack passwords. Security professionals developed various password cracking tools to test the security of password systems.
- Password crackers can be used as a part of a penetration testing exercise to identify vulnerabilities in computer systems and networks.
- By attempting to crack passwords, security professionals can determine if there are any weak passwords that could be exploited by attackers.

Password Cracking Tool (John the Ripper)

- 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.