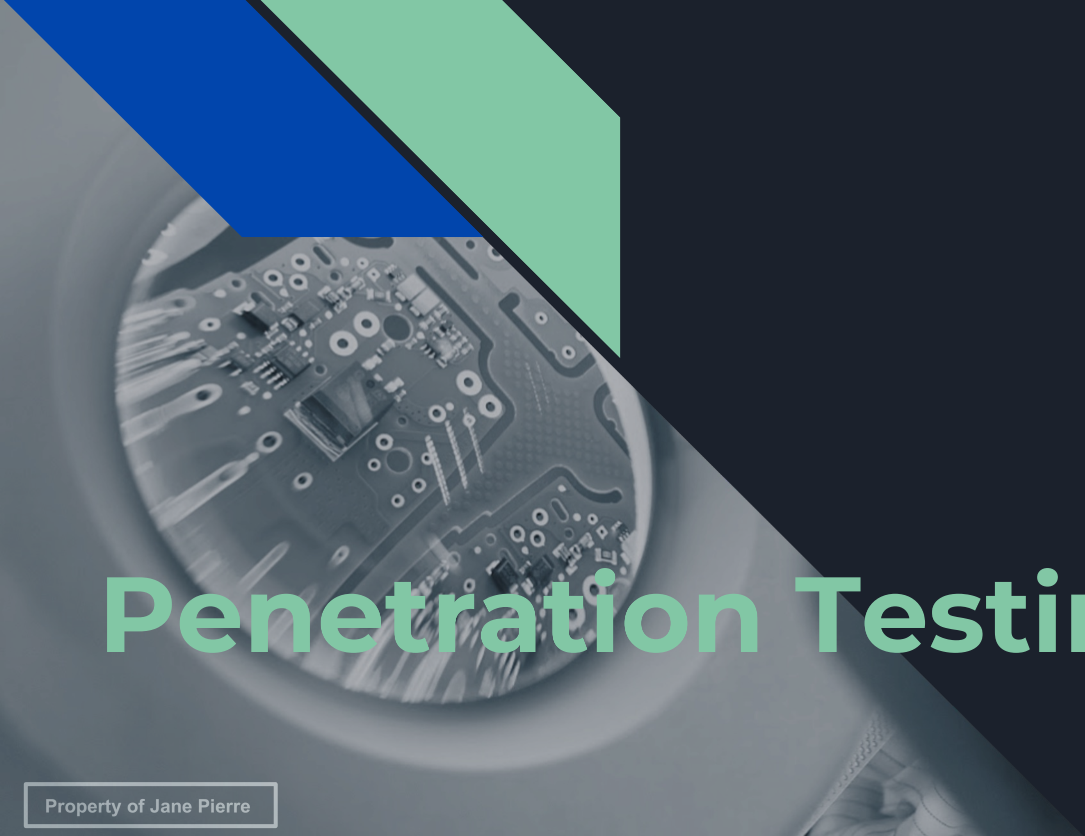

Penetration Testing

Property of Jane Pierre

What is Penetration Testing?

Penetration testing or ethical hacking, simulates a real-world attack on a computer system or network to identify vulnerabilities and weaknesses that could be exploited by malicious actors.

Is Penetration Testing Important?

Penetration testing is vital to a secure program for numerous reasons. It helps identify vulnerabilities - with a report by Trustwave indicating that 98% of tested applications have at least one vulnerability. Moreover, compliance regulations like the PCI DSS or NIST often mandate penetration testing. Lastly, penetration testing assists in risk mitigation, reducing the risk of data breaches by 28% as per a study by the Ponemon Institute.

Penetration Testing for Non-Profit Organizations: Preserving Donor Trust

For non-profits, maintaining a secure program is crucial to establish and retain donor trust. According to a survey by Edelman, 81% of respondents consider trust in an organization a decisive factor in their donation decisions. Regular penetration testing demonstrates a non-profit's commitment to security, enhancing their reputation and boosting donor confidence.

Types of Penetration Testing

There are three main types of penetration testing:

1. **White Box Testing: Tests the internal structure and code of the product with complete system knowledge.**

   Black Box Testing: Involves a real-world attack scenario without any prior knowledge of the system.

1. **Gray Box Testing: Combines white and black box testing techniques with partial knowledge of the system.**

Stages of Penetration Testing

Penetration testing involves several stages:

1. Reconnaissance and Planning
2. Scanning
3. Obtaining Entry
4. Maintaining Access
5. Analysis
6. Cleanup and Remediation

The Penetration Testing Report

The final deliverable of a penetration test is the report. This report typically includes details of the tests carried out, the vulnerabilities discovered, their severity, potential impact, and recommended remediation steps.

Remediation Process

Remediation is the process of fixing the vulnerabilities found during the penetration test. It involves addressing each vulnerability in order of its severity and potential impact. Periodic re-testing is necessary to ensure that the fixes have been effective and that no new vulnerabilities have been introduced.

Penetration Testing:
Visiting The Knowledge House

Our team's primary objective during the visit to The Knowledge House was to conduct a thorough penetration test as a part of their threat and vulnerability assessment.

Property of Jane Pierre

Penetration Testing: Visiting The Knowledge House

This involved using penetration testing tools like:

- NMAP for network exploration, Wireshark for packet analysis;
- Metasploit Framework for assessing security vulnerabilities;
- Burp Suite for web application security testing;
- Additional assessments from PentestTools.com.

Penetration Testing:
Visiting The Knowledge House

Our goal was to scan the networks and website of The Knowledge House to identify any vulnerabilities, particularly focusing on server-side software and security headers, which are common points of exploitation.

NMAP: A Versatile Network Scanning Tool

Nmap, or Network Mapper, is a powerful tool for functionality and penetration testing, including port scanning and vulnerability detection. Its scripting engine allows hackers to examine known vulnerabilities, aiding in detecting system security flaws.

Penetration Testing with NMAP: A Demonstration

- The command '`db_nmap -sV -sC 69.23.187.194*`' was used during our assessment.
- The '`-sV`' flag is used to determine the version of the services running on the open ports, providing insights into potential vulnerabilities associated with specific versions.
- The '`-sC`' flag indicates a script scan using Nmap's default set of scripts, which can perform a variety of checks and returns useful diagnostic information about the target.

*IP address changed for confidentiality.

Penetration Testing with NMAP: A Demonstration

- The Our scan revealed 10 open/filtered ports on the host, indicating potential entry points for attackers.
- We identified services including SSH, Telnet, DNS, HTTP, HTTPS, and others running on these ports.
- The server appeared to be running a Linux distribution, which was further specified by the version number.
- These details are crucial in understanding the attack surface and potential vulnerabilities of the system.

Penetration Testing with NMAP: A Demonstration

- The open ports discovered could serve as entry points for attackers if they are not adequately secured.
- The SSL certificate's issues, being self-signed and dated from 1970, present a severe security risk as they can be easily compromised.
- The http-title information suggests redirection and potential misconfiguration, which could be indicative of security weaknesses or intentional obfuscation efforts.

Penetration Testing with NMAP: A Demonstration

While the specifics of our findings are confidential, we identified several vulnerabilities in their server-side software and security headers. These vulnerabilities were detailed in a separate confidential report, which also includes the necessary steps to mitigate these vulnerabilities and enhance The Knowledge House's security posture.

Penetration Testing – Facing Forward

Penetration testing is a critical component of any cybersecurity strategy. For nonprofit organizations, this practice helps identify vulnerabilities, maintain compliance with regulations, and build donor trust. The insights and vulnerabilities identified through penetration testing are not only vital for maintaining our technical defenses but also for ensuring our compliance with various laws and regulations.