Penetration Testing

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.

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

3. 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:

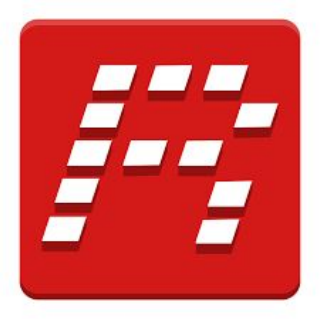
1. Reconnaissance and Planning
2. Scanning
3. Obtaining Entry
4. Maintaining Access
5. Analysis
6. Cleanup and Remediation

Social Engineering in Penetration Testing

Social engineering is a non-technical approach to penetration testing that exploits human psychology to gain access to sensitive information. It includes techniques such as phishing, pretexting, and physical impersonation, and helps identify weaknesses in an organization's security culture and employee training.

Tools for Social Engineering

Several tools aid in social engineering attacks, such as the Social-Engineer Toolkit (SET), BeEF, Maltego, and Recon-ng. These tools facilitate the creation of various social engineering attacks and the gathering of valuable information for the same.



Network Scanning in Penetration Testing

Network scanning identifies open ports, active hosts, and other network infrastructure details to find vulnerabilities that an attacker could exploit. It involves various types of scans like port scans, operating system detection, service discovery, and vulnerability scans.

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.

Wireless Network Testing: Aircrack-ng

Aircrack-ng is a suite of tools for monitoring and testing wireless network security. It can crack keys, capture packets, analyze them, and perform attacks like deauthentication.

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 – 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.