ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Network Penetration Testing

Introduction to Network Penetration Testing

Unlocking Network Security: The Art of Penetration Testing

DEFINITION

> Network penetration testing is a simulated cyber attack to identify vulnerabilities in a network. It helps organizations strengthen their defenses against real threats.

KEY CONCEPTS

Reconnaissance

The process of gathering information about the target network to identify potential vulnerabilities.

Exploitation

The act of taking advantage of identified vulnerabilities to gain unauthorized access to systems.

Post-Exploitation

Activities performed after gaining access, such as maintaining access or extracting sensitive data.

Reporting

Documenting findings, vulnerabilities, and recommendations for remediation to improve security.

Tools and Techniques

Utilizing software and methodologies like Metasploit, Nmap, and social engineering to conduct tests.

EXAMPLES

→ Using Nmap to scan for open ports on a network.

→ Executing a phishing attack to test employee awareness.

→ Attempting to exploit a known vulnerability in outdated software.

MEMORY TIPS

★ Remember 'R-E-P' for Reconnaissance, Exploitation, and Post-Exploitation.

★ Think of 'Report' as the final step to complete the cycle.

★ Use the acronym 'T.E.A.R.' for Tools, Exploitation, Access, Reporting.

COMMON MISTAKES

✗ Neglecting to get proper authorization before testing.

✗ Failing to document findings thoroughly.

✗ Overlooking the importance of post-exploitation activities.

QUICK RECAP

Network penetration testing is essential for identifying and fixing security vulnerabilities. It involves reconnaissance, exploitation, and thorough reporting to enhance network security.