ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Scanning and Enumeration

Introduction to Scanning and Enumeration

Master the Basics of Scanning and Enumeration in Ethical Hacking!

DEFINITION

> Scanning and enumeration are techniques used to identify active devices and gather information about them in a network. They help ethical hackers assess security vulnerabilities.

KEY CONCEPTS

Scanning Techniques

Methods like ping sweeps and port scans are used to discover live hosts and open ports.

Enumeration

This involves extracting detailed information from a system, such as user accounts and services.

Network Mapping

Creating a visual representation of a network's layout to identify devices and connections.

Vulnerability Scanning

Automated tools assess systems for known vulnerabilities that could be exploited.

OS Fingerprinting

Determining the operating system of a device based on its responses to network requests.

EXAMPLES

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

→ Enumerating user accounts on a Windows machine with Net User command.

→ Creating a network map using tools like Zenmap.

MEMORY TIPS

★ Remember 'S' for Scanning and 'E' for Enumeration to link the two processes.

★ Use the acronym 'NVE' for Network Mapping, Vulnerability Scanning, and Enumeration.

★ Visualize a treasure map where scanning finds the treasure spots and enumeration reveals the treasure details.

COMMON MISTAKES

✗ Neglecting to use proper permissions when scanning networks.

✗ Overlooking the importance of stealth during scanning to avoid detection.

✗ Failing to update scanning tools, leading to outdated vulnerability databases.

QUICK RECAP

Scanning and enumeration are essential steps in ethical hacking to identify and assess vulnerabilities. Mastering these techniques enhances your ability to secure networks effectively.