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 discover active devices and gather information about them on a network. These processes help identify vulnerabilities that can be exploited in ethical hacking.

KEY CONCEPTS

Network Scanning

The process of identifying active devices on a network to understand its structure.

Port Scanning

A method to check which ports on a device are open and listening for connections.

Service Enumeration

Gathering detailed information about the services running on open ports to identify potential vulnerabilities.

OS Fingerprinting

The technique used to determine the operating system of a device based on its responses.

Vulnerability Scanning

Automated tools that scan systems for known vulnerabilities to assess security risks.

EXAMPLES

→ Using Nmap to scan a network for active IP addresses.

→ Enumerating user accounts on a web application to find weak passwords.

→ Performing a port scan to identify open ports on a server.

MEMORY TIPS

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

★ Use the acronym 'NPS' for Network, Port, and Service to recall key scanning types.

★ Visualize a detective gathering clues to remember the information-gathering aspect of enumeration.

COMMON MISTAKES

✗ Neglecting to obtain permission before scanning a network.

✗ Overlooking firewall settings that may block scanning attempts.

✗ Failing to interpret scan results accurately, leading to incorrect conclusions.

QUICK RECAP

Scanning and enumeration are essential steps in ethical hacking to identify devices and their vulnerabilities. Understanding network structures, open ports, and services helps in assessing security risks effectively.