ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Reconnaissance

Introduction to Reconnaissance

Mastering Reconnaissance: The First Step in Ethical Hacking

DEFINITION

> Reconnaissance is the initial phase of ethical hacking where information about a target is gathered. This helps hackers understand the target's vulnerabilities and plan their approach.

KEY CONCEPTS

Passive Reconnaissance

Gathering information without direct interaction with the target, such as using public records.

Active Reconnaissance

Involves directly interacting with the target, like pinging servers or scanning networks.

Footprinting

The process of collecting details about a target's network and systems to identify potential vulnerabilities.

Social Engineering

Manipulating individuals to disclose confidential information that can aid in the attack.

WHOIS Lookup

A query that retrieves information about domain ownership and registration details.

EXAMPLES

→ Using Google to find information about a company's employees.

→ Running a WHOIS lookup to find domain registration details.

→ Scanning a network to identify active devices and services.

MEMORY TIPS

★ Remember 'P' for Passive and 'A' for Active to distinguish between reconnaissance types.

★ Use the acronym 'FOSS' for Footprinting, OSINT, Scanning, and Social Engineering.

★ Think of reconnaissance as 'researching' before 'attacking' to remember its purpose.

COMMON MISTAKES

✗ Confusing passive and active reconnaissance techniques.

✗ Neglecting to verify the legality of information gathering.

✗ Overlooking the importance of documenting gathered information.

QUICK RECAP

Reconnaissance is crucial for ethical hacking, involving both passive and active techniques. Understanding the target's vulnerabilities through methods like footprinting and social engineering sets the stage for effective penetration testing.