ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Post Exploitation

Introduction to Post Exploitation

Mastering Post Exploitation: The Key to Ethical Hacking Success

DEFINITION

> Post exploitation refers to the actions taken after successfully breaching a system. It involves maintaining access, gathering information, and escalating privileges.

KEY CONCEPTS

Privilege Escalation

Gaining higher access rights on a system to perform more sensitive actions.

Data Exfiltration

The process of extracting sensitive data from a compromised system.

Persistence Mechanisms

Techniques used to maintain access to a system even after a reboot or logout.

Covering Tracks

Actions taken to erase signs of intrusion to avoid detection.

Post Exploitation Frameworks

Tools and scripts designed to automate post-exploitation tasks and streamline the process.

EXAMPLES

→ Using a backdoor to maintain access after a successful breach.

→ Extracting user credentials from a compromised database.

→ Installing a rootkit to hide malicious activities.

MEMORY TIPS

★ Remember 'PEP' for Post Exploitation Processes: Privilege, Exfiltration, Persistence.

★ Visualize a 'trapdoor' for persistence: it lets you back in anytime.

★ Think of 'CATS' for Covering Tracks: Clean, Anonymize, Tidy, Secure.

COMMON MISTAKES

✗ Neglecting to secure the access point after exploitation.

✗ Failing to document actions taken during post-exploitation.

✗ Overlooking the importance of stealth in covering tracks.

QUICK RECAP

Post exploitation is crucial for maintaining access and gathering data after a breach. Key actions include privilege escalation, data exfiltration, and covering tracks to avoid detection.