ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Post Exploitation

Introduction to Post Exploitation

Mastering Post Exploitation for Effective Ethical Hacking

DEFINITION

> Post exploitation refers to the actions taken after gaining unauthorized access to a system. It involves maintaining access, gathering data, and covering tracks.

KEY CONCEPTS

Privilege Escalation

This involves gaining higher access rights on a compromised system to exploit it further.

Data Exfiltration

The process of transferring sensitive data from the compromised system to an external location.

Persistence

Techniques used to maintain access to a system even after it has been rebooted or updated.

Covering Tracks

Actions taken to erase or alter logs and evidence of unauthorized access.

Network Pivoting

Using a compromised system to access other systems within the same network.

EXAMPLES

→ Using a rootkit to maintain access after a system reboot.

→ Extracting user credentials from a compromised database.

→ Setting up a backdoor for future access to a target system.

MEMORY TIPS

★ Remember 'PEP' for Privilege, Exfiltration, Persistence.

★ Use 'CNP' to recall Covering tracks and Network Pivoting.

★ Think of 'DPC' for Data, Persistence, and Covering tracks.

COMMON MISTAKES

✗ Neglecting to secure the backdoor after gaining access.

✗ Failing to document actions taken during post exploitation.

✗ Overlooking the importance of stealth in covering tracks.

QUICK RECAP

Post exploitation is crucial for maximizing the benefits of a successful hack. It involves maintaining access, gathering valuable data, and ensuring stealth to avoid detection.