ONE PAGE SUMMARY

IT & Software › Ethical Hacking › Privilege Escalation

Introduction to Privilege Escalation

Unlocking higher access: Understanding privilege escalation in ethical hacking.

DEFINITION

Privilege escalation is a technique used by attackers to gain elevated access to resources. It allows them to perform actions that are normally restricted to higher-level users.

KEY CONCEPTS

Types of Escalation

There are two main types: vertical escalation, which increases user privileges, and horizontal escalation, which accesses other users' privileges.

Exploiting Vulnerabilities

Attackers often exploit software vulnerabilities or misconfigurations to escalate privileges and gain unauthorized access.

User Privileges

Understanding user roles and permissions is crucial, as attackers target accounts with insufficient security.

Common Tools

Tools like Metasploit and Mimikatz are frequently used to automate privilege escalation attacks.

Defense Strategies

Implementing least privilege access, regular updates, and monitoring can help prevent privilege escalation.

EXAMPLES

→ Using a software bug to gain admin rights.

→ Accessing another user's account through session hijacking.

→ Exploiting weak passwords to elevate privileges.

MEMORY TIPS

★ Remember 'Vertical vs. Horizontal' to distinguish types of escalation.

★ Use the acronym 'VULN' for Vulnerabilities, User roles, Least privilege, and Networking.

★ Think of 'Privilege' as a key that unlocks doors to restricted areas.

COMMON MISTAKES

✗ Confusing vertical and horizontal escalation.

✗ Overlooking the importance of user roles.

✗ Neglecting to patch known vulnerabilities.

QUICK RECAP

Privilege escalation is a critical concept in ethical hacking that involves gaining unauthorized access to higher privileges. Understanding the types, common tools, and defense strategies is essential for preventing such attacks.