Two Extra Network Protocol Attacks

1.1 DHCP Starvation Attack

Overview: This attack targets the DHCP server by sending many fake requests with different MAC addresses until no more IP addresses are available.

How it's executed: An attacker runs a script or tool (like Yersinia) that sends DHCP requests using random MAC addresses.

Impact: Legitimate devices can't get an IP, causing a denial of service on the network.

Fix/Mitigation: - Use DHCP Snooping on switches. - Limit the number of MAC addresses per port.

Example: Seen in internal penetration tests at universities.

1.2 SMB Relay Attack

Overview: This attack tricks a system into authenticating to a fake SMB server, then relays the credentials to another system.

How it's executed: An attacker uses tools like ntlmrelayx to capture and forward SMB authentication to another machine.

Impact: Can get unauthorized access to shared folders or run commands with victim's privileges.

Fix/Mitigation: - Disable SMBv1. - Enable SMB signing. - Disable LLMNR and NetBIOS over TCP/IP.

Example: Used in the spread of Petya/NotPetya malware.

Two Privilege Escalation Techniques

2.1 Windows: Token Impersonation

Method: Attacker uses a tool like Mimikatz to impersonate another user's token (like SYSTEM) to gain higher privileges.

Vulnerabilities Used: Abuse of available tokens in processes or services.

How Attackers Escalate: Steal a token, then start a new process or command with it.

Fix/Mitigation: - Apply security patches. - Limit unnecessary services. - Monitor token usage.

2.2 Linux: Abusing Wildcard Injection in Scheduled Tasks

Method: Attackers exploit scheduled scripts (like cron jobs) that use wildcards (`*`) unsafely in commands such as `tar`, `chown`, or `cp`, letting them inject malicious

files and commands.

Vulnerabilities Used: - Misuse of wildcards in system maintenance scripts. - Overly permissive directory write permissions.

How Attackers Escalate: - Find writable directories with scheduled scripts. - Drop a malicious file named something like `--checkpoint-action=exec=sh shell.sh` in the directory. - When a command like `tar` runs with wildcards (`tar czf backup.tar.gz *`), it interprets the injected filename as a parameter and executes the payload.

Fix/Mitigation: - Avoid using wildcards in privileged cron jobs. - Use absolute paths and safe practices. - Restrict write permissions on sensitive directories.