Detecting Lateral Movement and Pass-the-Hash Attacks in Networks

Lateral movement and Pass-the-Hash (PtH) attacks are key tactics used by attackers after initial compromise to escalate privileges, access sensitive resources, and spread through an environment. Understanding and detecting these behaviors is critical for defending modern enterprise networks.

2. What is Pass-the-Hash (PtH)?

Pass-the-Hash is a credential replay attack where an attacker uses stolen hashed credentials (typically NTLM hashes on Windows) to authenticate against other systems without cracking them.

How it works:

- Extract NTLM hashes from a compromised system (using tools like Mimikatz)
- Reuse the hash to authenticate via SMB or RDP on other machines
- No need to know the actual password

4. Indicators of Lateral Movement

- **Logons from unusual sources** (new IPs, user workstations logging onto servers)
- **Abnormal use of admin tools** (PsExec, WMI, WinRM)
- **Kerberos ticket anomalies** (unusual ticket-granting behavior)
- **High volume of SMB traffic**
- **Execution of remote commands**

6. Defense and Mitigation

- **Enforce least privilege**: Limit lateral movement by restricting admin access.

- **Credential hygiene**: Avoid credential reuse, disable legacy protocols like NTLM.
- **Enable Credential Guard**: Protect LSASS memory in Windows.
- **Segment the network**: Isolate systems to limit movement scope.
- **Log and alert** on suspicious authentication and remote execution behavior.
- **Patch regularly**: Prevent attackers from exploiting known vulnerabilities for pivoting.

Conclusion

Detecting lateral movement and Pass-the-Hash attacks requires a combination of strong logging, behavioral analysis, privilege control, and proactive threat hunting. Incorporating these detections into your security posture significantly increases your ability to stop an attacker before they reach critical assets.