Lateral Movement

In the lateral movement phase, attackers leverage their initial foothold to move within the network, **accessing additional systems and resources**. This phase enables them to spread throughout the environment, often with the goal of reaching high-value assets, escalating privileges, or maintaining persistent access. Common lateral movement techniques include **remote access protocols like SSH, RDP, and SMB**, compromising shared content and using internal spear phishing, and advanced credential theft methods like pass the hash/ticket and token/cookie theft.

1. SSH, RDP, SMB

- Definition: Attackers use remote access protocols—SSH (Secure Shell), RDP (Remote Desktop Protocol), and SMB (Server Message Block)—to access and control other systems within the network.
- Usage in Lateral Movement:
    - SSH: Primarily used on Unix-based systems, SSH provides secure, command-line access to other systems. Attackers may use stolen credentials to log in to Unix/Linux servers.
    - RDP: Commonly used for remote access on Windows systems, RDP allows full graphical access, which attackers can exploit to interact with Windows desktops and run applications.
    - SMB: A file-sharing protocol for Windows environments, SMB enables access to shared files and printers. Attackers use SMB to map network drives, move files, and execute remote commands.
- Security Implications: Attackers using these protocols can blend in with legitimate network activity, as they are commonly used by administrators. Unauthorized use of these protocols allows attackers to execute commands, install tools, and gather information on target systems, often without raising alerts.

2. Compromise Shared Content and Internal Spear Phishing

- Compromise Shared Content:
    - Definition: Attackers access shared files, folders, and network drives that multiple users have access to. By modifying these resources, **attackers can spread malware or collect additional credentials**.
    - Examples: Inserting malicious scripts or macros into shared documents, spreading trojans on network drives, or using shared folders to stage and move data.
- Internal Spear Phishing:
    - Definition: Attackers use compromised accounts to send targeted, phishing-like emails within the organization. By **posing as a trusted internal user**, they attempt to trick others into revealing credentials, opening malicious attachments, or clicking on links.
    - Techniques: Crafting emails that request access to sensitive resources or contain infected attachments, often with personalized details to make the messages appear legitimate.
- Security Implications: By compromising shared content, attackers can increase their access across the network while minimizing their footprint. Internal spear phishing often succeeds because recipients recognize the sender as an internal contact, lowering suspicion and bypassing typical email security controls.

3. Pass the Hash/Ticket, Tokens, and Cookies

- **Pass the Hash (PTH)**:
    - Definition: Pass the Hash is a technique that **uses password hashes instead of plaintext passwords to authenticate to other systems**. Attackers capture a hash from one system and reuse it to access other systems without needing the plaintext password.
    - Usage: Typically used on Windows networks, where attackers extract NTLM hashes and use them to move laterally without needing to decrypt the password.
- **Pass the Ticket (PTT)**:
    - Definition: Pass the Ticket is a similar technique, but with Kerberos tickets instead of hashes. Attackers steal a valid Kerberos ticket (TGT or TGS) from one system and use it to authenticate to other systems in the network.
    - Usage: Kerberos tickets allow access to services within a Windows Active Directory environment, making it easy for attackers to bypass multi-factor authentication and other security controls once they possess a ticket.
- **Tokens and Cookies**:
    - Definition: Attackers steal session tokens or cookies, which represent authenticated sessions. This tactic allows attackers to impersonate the user whose token or cookie they have stolen.
    - Usage: Once attackers acquire these tokens, they can authenticate as the compromised user without re-entering credentials. **Common in web applications and cloud environments**.
- Security Implications: Pass the Hash, Pass the Ticket, and token/cookie theft allow attackers to bypass traditional authentication, moving laterally as trusted users. Because they rely on legitimate authentication methods, these techniques often evade detection.

Summary

- **SSH, RDP, and SMB allow attackers to move to additional systems through standard remote access protocols, enabling stealthy command execution and access to network resources**.
- **Compromising Shared Content and Internal Spear Phishing** allow attackers to spread malware and collect credentials by leveraging trust within the organization, bypassing perimeter defenses.
- **Pass the Hash, Pass the Ticket, Tokens, and Cookies** provide attackers with authenticated access, bypassing password requirements by reusing credentials or session data. These techniques are effective in Active Directory environments, as they mimic legitimate network activity.

By understanding these lateral movement techniques, defenders can implement countermeasures such as **monitoring for unusual access patterns, restricting access to shared content, and enabling credential guard technologies like Microsoft's LSA Protection**. These steps can help detect and prevent attackers from spreading across the network and accessing sensitive systems.