Discovery

In the discovery phase of an attack, attackers **gather information about the compromised environment to understand its layout, identify high-value assets, and locate other systems they may wish to target**. Discovery is essential for planning lateral movement and for gaining the context needed to elevate privileges or execute further attacks. Common discovery tactics include **network scanning, account and policy enumeration, and identifying remote systems, installed software, and system details**.

1. Network Scanning

- Definition: Network scanning involves probing the network to identify active hosts, open ports, and available services. This information helps attackers **map out the network and locate potential targets**.
- Types of Network Scanning:
  - **Ping Sweeps**: Attackers use ping sweeps to find live hosts on a network.
  - **Port Scanning**: Tools like **Nmap** allow attackers to scan for open ports on discovered hosts, revealing which services are running.
  - **Service Identification**: By analyzing responses, attackers can determine specific versions of services, which can help them identify known vulnerabilities.
- Security Implications: Network scanning is often a prelude to lateral movement and privilege escalation. **Detecting unauthorized scans can be an early indicator of compromise**, as attackers try to gather information on internal resources.

2. Find Accounts by Listing Policies

- Definition: Attackers enumerate user accounts, permissions, and policies within the environment to understand access control structures and identify privileged accounts.
- Techniques:
  - **Enumerating Group Policies**: Attackers may check for existing group policies in Active Directory (AD) to see which accounts have elevated privileges or access to sensitive systems.
  - **Listing Accounts and Permissions**: By listing user accounts and groups, attackers can identify high-value accounts, such as administrators or service accounts with broad access rights.
  - **Policy Details**: Attackers may look at password policies, account lockout thresholds, and auditing settings to plan their attack without triggering alerts.
- Security Implications: By gathering information on accounts and policies, attackers can target specific users for credential access or privilege escalation. It also helps them tailor their approach based on the environment's access control policies.

3. Find Remote Systems, Software, and System Information

- **Find Remote Systems**:
  - Definition: Attackers search for other accessible devices on the network, such as servers, workstations, or IoT devices, to identify potential lateral movement targets.
  - Tools and Techniques: They may use tools like **net view (Windows)** or **arp-scan (Linux)** to find remote systems within the same subnet or across network boundaries.
- **Discover Installed Software and System Information**:

    - Definition: Attackers gather information about the installed software, system configurations, and OS versions on devices within the environment.
    - Purpose: Identifying installed software helps attackers pinpoint specific applications and versions that may have vulnerabilities. System information, like OS type and version, can indicate available exploits.
    - Tools: Commands like systeminfo (Windows) or uname (Linux) reveal operating system details and system architecture.
- Detect Virtual Machines and Sandboxes:
    - Purpose: Attackers check if they're operating within a virtual environment or sandbox, as many security solutions use VMs or sandboxes to analyze malware behavior.
    - Techniques: Attackers look for VM-specific artifacts like Hyper-V processes or VMware directories, which could indicate a sandbox or security monitoring environment.
- Security Implications: Discovering information about remote systems, software, and system environments gives attackers insight into potential weaknesses. Additionally, detecting a sandbox environment may prompt attackers to delay their payload execution or adjust their methods to avoid detection.

Summary

- Network Scanning helps attackers map out the network, locate active hosts, and identify services and ports that may be vulnerable.
- Finding Accounts by Listing Policies enables attackers to identify privileged accounts and understand the environment's access control structure, aiding in privilege escalation.
- Finding Remote Systems, Software, and System Information provides attackers with details on potential lateral movement targets, vulnerable software, and OS versions, as well as the ability to detect VM or sandbox environments to avoid security monitoring.

Discovery tactics give attackers a comprehensive understanding of the environment, enabling them to refine their approach, locate targets, and plan further steps. Security teams can detect discovery activities by monitoring for abnormal scanning behavior, unexpected account enumeration, and excessive access requests to sensitive system information.