Simeon Hawkins
Capstone Phase 2: Identify Targets and Run Scans

Tools for Network Scans

1. **Nmap:**

Purpose: Obtain information on hosts and the services and operating systems they are running.
Commands:

- **Host Discovery:** nmap -sn 192.168.1.0/24
    - This command performs a ping scan to identify live hosts within the specified subnet.

- **Service Version Detection:** nmap -sV 192.168.1.1
    - This command detects services and their versions running on open ports.

- **Operating System Detection:** nmap -0 192.168.1.1
    - This command attempts to identify the operating system of the target host.

- **Aggressive Scan:** nmap -A 192.168.1.1
    - This command combines OS detection, version detection, script scanning, and traceroute

Reasoning: Nmap is a versatile and powerful tool for network discovery and security auditing. It is widely used due to its comprehensive feature set and ability to perform detailed scans.

Challenges and Limitations:

- **Detection by IDS/IPS:** Aggressive scans can trigger intrusion detection and prevention systems.
- **Stealth Scanning:** Stealth techniques may require more time and expertise to execute effectively.

2. **Masscan**

Purpose: Perform high-speed port scanning across large IP ranges.
Commands:

- **Basic Port Scan:** masscan -p1-65535 192.168.1.0/24 –rate=10000

- This common scans all 65535 TCP ports on the specified subnet at a rate of 10,000 packets per second.

Reasoning: Masscan is designed for high-speed scanning and can scan the entire Internet in under six minutes, making it ideal for large-scale reconnaissance.

Challenges and Limitations:

- **Accuracy:** Massscan can produce false positives due to its speed.
- **Detection:** High-speed scanning is easily detectable and can lead to IP blacklisting.

3. **Nessus**

Purpose: Perform vulnerability scanning and identify potential security issues.
Commands:

- **Scan Configuration:** Utilize the Nessus web interface to configure and run scans against the target network.

Reasoning: Nessus is a comprehensive vulnerability scanner that can identify a wide range of security issues, from missing patches to configuration vulnerabilities.

Challenges and Limitations:

- **False Positives:** Nessus scans can generate false positives, requiring manual verification.
- **Resource Intensive:** Scans can be resource-intensive and may impact network performance.

4. **OpenVAS**

Purpose: Perform vulnerability scanning and identify security issues, similar to Nessus.
Commands:

- **Scan Configuration:** Utilize the OpenVAS web interface to configure and run scans against the target network.

Reasoning: OpenVAS is an open-source alternative to Nessus, providing similar functionality for identifying vulnerabilities.

Challenges and Limitations:

- **Setup Complexity:** Setting up and configuring OpenVAS can be complex and time-consuming.
- **False Positives:** Similar to Nessus, OpenVAS can generate false positives.

5. **Amass**

Purpose: Perform subdomain enumeration and infrastructure mapping
Commands:

- **Passive Enumeration:** amas enum -passive -d example.com
    - This command performs passive reconnaissance, avoiding direct interaction with the target.

- **Active Enumeration:** amass enum -active -d example.com
    - This command uses active techniques to gather more detailed information about the target.

Reasoning: Amass is highly effective at discovering subdomains and mapping infrastructure, providing valuable insights into the external attack surface.

Challenges and Limitations:

- **Data Overload:** Amass can generate large amounts of data, requiring effective filtering and analysis.
- **API Rate Limits:** Using multiple APIs can result in rate limiting, slowing down the enumeration process.