Phase 2: Identify Targets and Run Scans

Goal:
Identify the tools and techniques used to perform host discovery and enumeration.

Procedure:
List the tools used to perform network scans, the purpose for using them, and how they will be used.

Tools and Techniques

---

1. Nmap (Network Mapper)

Purpose:
Nmap is a powerful and versatile open-source network scanning tool, widely used for discovering hosts, identifying open ports, and gathering information about the services and operating systems running on target hosts.

Commands:

- **Identify Live Hosts**:

```bash
nmap -sn <target-ip-range>
```

- **Comprehensive Scan with OS Fingerprinting and Service Detection**:

```bash
nmap -A -T4 <target -ip>
```

- **Scan for Specific Ports**:

```bash
map -p 22, 89, 443 <target ip>
```

Banner Grabbing:

```bash
nmap -sV —script-banner <target ip>
```

Challenges and Limitations:

- The accuracy of OS fingerprinting may vary depending on the target's configuration.
- Nmap scans can be noisy and easily detectable by intrusion detection systems (IDS).

---

2. Masscan

Purpose:
Masscan is a high-speed network scanning tool designed to perform large-scale scans. It can identify a large number of hosts quickly and scan the entire internet in a short amount of time.

Commands:

Scan a Large Range of IPs:

```bash
masscan -p0-65536 <target-ip-range> -- rate=1000
```

Challenges and Limitations:

- Masscan's speed can overwhelm networks and cause disruptions.
- It may produce false positives and lack the depth of information that Nmap provides.

---

3. OpenVAS (Open Vulnerability Assessment Scanner)

Purpose:
OpenVAS is an open-source vulnerability scanner that performs comprehensive scans to identify known vulnerabilities on target hosts.

Commands:

Launch a Scan:
Use the OpenVAS web interface to create and start a new scan targeting the IP range.

View Results:
Analyze the scan results in the OpenVAS dashboard.

Challenges and Limitations:

- OpenVas scans can be time-consuming and resource-intensive.
- There can be a high number of false positives.

---

4. Nikto

Purpose:
Nikto is a web server scanner designed to identify vulnerabilities, outdated software, and configuration issues on web servers.

Commands:

Scan a Web Server**:**

```bash
nikto -h <target ip>
```

Challenges and Limitations:

- Nikto is limited to web servers and cannot scan other types of hosts.
- It can be noisy and easily detectable by web application firewalls (WAF).

---

5. Amass

Purpose:
Amass is a powerful tool for performing DNS enumeration and subdomain discovery. It helps identify additional targets by mapping out the DNS infrastructure.

Commands:

```bash
amass enum -d <target-domain>
```

Selection Reasoning:

Nmap: Selected for its versatility and detailed output, essential for in-depth analysis of target hosts.

Masscan: Chosen for its speed and efficiency in quickly identifying a large number of live hosts across vast IP ranges.

OpenVAS: included for its ability to detect known vulnerabilities, providing a comprehensive security assessment.

Nikto: Used to identify vulnerabilities and issues specific to web servers, which are often critical targets.

Amass: Essential for mapping out the DNS landscape and identifying additional targets that might be missed by other tools.

Potential Drawbacks and Limitations:

- **Detection**: Many of these tools, especially Nmap and Masscan, can be easily detected by IDS and IPS systems, which could alert the target of the scanning activity.

- **False Positives**: Tools like OpenVAS may generate false positives, requiring additional validation and analysis.

- **Resource Intensive**: Comprehensive scans, particularly with OpenVAS and Nmap's aggressive options, can be resource-intensive and time-consuming.

- **Legal and Ethical Considerations**: Ensure that all scanning activities are conducted within the legal and ethical boundaries agreed upon in the engagement scope.

Usage Strategy:

- **Stealth Scanning**: Use timing and evasion options in Nmap to reduce detectability.

- **Rate Limiting**: Control the scan rate in Masscan to avoid overwhelming the network.

- **Target Validation**: Validate findings from vulnerability scanners (e.g., OpenVAS) with manual testing or additional tools to reduce false positives.

- **Layered Approach**: Combine different tools to provide a comprehensive view of the target network, leveraging the strengths of each tool.

By carefully selecting and utilizing these tools, you can effectively identify targets and gather detailed information to aid in the subsequent phases of the penetration test.