Phase 2: Network Scanning Tools

The primary goal of Phase 2 is to identify live hosts, open ports, services, and potential vulnerabilities within Artemis's external network. To achieve this, I've selected five essential tools available in Kali Linux: Nmap, OpenVAS, Metasploit, Nikto, and Lynis. Each tool serves a specific function in the network scanning process and provides critical data that will inform later stages of the penetration test. Below is an in-depth description of each tool, the rationale for its selection, and its intended usage.

---

1. Nmap (Network Mapper)

- **Purpose**: Nmap is a versatile network scanning tool that allows for host discovery, service detection, and operating system fingerprinting. It provides foundational insights into the structure and configuration of the network by identifying live hosts, open ports, and the services running on those ports.
- **Reasoning for Selection**: Nmap is a cornerstone tool in network reconnaissance and is widely trusted due to its effectiveness and flexibility. It offers a range of scanning techniques, from simple pings to detailed scans that reveal service versions and OS information, making it ideal for initial host discovery and enumeration.
- **Usage**:
    - **Ping Sweep**: `nmap -sn <target_IP_range>` — Used to identify active hosts within the target's IP range.
    - **Service Version Detection**: `nmap -sV <target_IP>` — Determines the versions of services running on open ports.
    - **OS Fingerprinting**: `nmap -O <target_IP>` — Attempts to detect the operating system of the target host.
    - **Comprehensive Scans**: `nmap -A <target_IP>` — Provides a detailed scan with service detection and OS fingerprinting, often combined with scripting to detect specific vulnerabilities.
- **Challenges and Limitations**: Nmap scans can generate detectable traffic, especially when used on large networks. This may alert network monitoring systems (IDS/IPS) and reduce the stealth of the penetration test. Additionally, advanced scans with OS fingerprinting can be time-consuming on larger networks.

---

2. OpenVAS (Open Vulnerability Assessment System)

- **Purpose**: OpenVAS is a full-featured vulnerability scanner that identifies known vulnerabilities within networked systems and services. It is particularly useful for mapping security flaws and associating risk levels with detected services.

- **Reasoning for Selection**: OpenVAS is an established tool with an extensive library of vulnerability tests, which are continuously updated to reflect new threats. This makes it an excellent choice for pinpointing specific vulnerabilities that can be prioritized in the risk assessment phase.
- **Usage**:
    - **Vulnerability Scan**: OpenVAS can be configured through its GUI to scan specific IP ranges or hosts identified during the Nmap scans. It checks each host against its database of vulnerabilities, providing detailed reports.
    - **Risk Assessment**: Each detected vulnerability is assigned a risk level, which helps in prioritizing remediation efforts.
- **Challenges and Limitations**: OpenVAS scans consume significant processing power and bandwidth, potentially causing slowdowns on the network. Its activity is also highly detectable, which could alert Artemis's monitoring systems if stealth is a requirement. Setup can be time-intensive, requiring proper configuration to run efficiently.

---

3. Metasploit Framework

- **Purpose**: Metasploit is an exploitation framework with extensive auxiliary and exploitation modules. In the context of network scanning, Metasploit can be used for banner grabbing, service detection, and testing the exploitability of identified vulnerabilities.
- **Reasoning for Selection**: Metasploit is highly valuable in simulating real-world attacks and validating the presence of vulnerabilities. By mapping vulnerabilities to specific exploits, it provides insights into how exposed systems could be compromised.
- **Usage**:
    - **Service Enumeration**: `use auxiliary/scanner/portscan/tcp` to scan open TCP ports and identify services on target hosts.
    - **Banner Grabbing**: `use auxiliary/scanner/http/http_version` to detect HTTP version information and service banners, which may reveal software versions.
    - **Exploit Testing**: If allowed by engagement rules, Metasploit modules can be used to test the exploitability of vulnerabilities discovered by OpenVAS.
- **Challenges and Limitations**: Metasploit's scans are detectable by network defenses. Additionally, its effectiveness depends on the compatibility of discovered vulnerabilities with available exploit modules. Misuse of Metasploit can also cause unintended disruptions to services if exploits are tested without authorization.

---

4. Nikto

- **Purpose**: Nikto is a web server scanner designed to detect common vulnerabilities, outdated software, and misconfigurations in web applications. It quickly identifies issues that may be present on public-facing web servers.
- **Reasoning for Selection**: Nikto is highly effective for quickly assessing web servers for basic vulnerabilities. Since Artemis has several publicly accessible systems, Nikto will provide valuable information on potential weaknesses in the web layer.
- **Usage**:
    - **Basic Web Scan**: `nikto -h <target_IP>` — Scans the web server for known vulnerabilities, such as outdated software, open directories, and server misconfigurations.
    - **Customization**: Additional plugins and configurations in Nikto allow for specific vulnerability checks based on Artemis's web server setup.
- **Challenges and Limitations**: Nikto is a noisy tool and easily detectable by IDS/IPS, as it generates a high number of HTTP requests. Its findings are limited to known vulnerabilities, meaning it may miss novel or custom-coded web application flaws.

---

5. Lynis

- **Purpose**: Lynis is a Unix-based auditing tool that performs extensive system checks, assessing compliance, configuration issues, and security settings. It helps identify internal weaknesses and provides system-hardening recommendations.
- **Reasoning for Selection**: Since Artemis uses Linux systems within its infrastructure, Lynis offers valuable insights for identifying misconfigurations and potential security issues specific to Unix-based systems. It is particularly helpful for internal auditing if SSH access to systems is available.
- **Usage**:
    - **System Audit**: `lynis audit system` — This command initiates a comprehensive audit of the Unix/Linux system, examining configuration files, permissions, installed software, and system logs for security weaknesses.
    - **Hardening Recommendations**: Lynis provides actionable suggestions for improving the security posture of the audited system, which can help with remediation planning.
- **Challenges and Limitations**: Lynis requires SSH access to the target systems, so it may not be feasible for purely external scans. Additionally, while it's effective for Unix-based systems, it cannot be applied to non-Unix operating systems (e.g., Windows).

Summary of Network Scanning Strategy

Each tool in this selection addresses a different layer of network scanning, from host discovery to vulnerability detection and system configuration auditing:

1. **Nmap**: Establishes a foundational map of live hosts, services, and operating systems.
2. **OpenVAS**: Identifies known vulnerabilities within network services and assigns risk levels for prioritization.
3. **Metasploit**: Tests the exploitability of identified vulnerabilities, providing insights into real-world risks.
4. **Nikto**: Focuses on web server security, detecting common misconfigurations and vulnerabilities in publicly accessible web applications.
5. **Lynis**: Completes system audits for Unix-based targets, identifying hardening opportunities and configuration issues.

Challenges and Limitations

- **Detectability**: Tools like Nmap, Nikto, and Metasploit can be easily flagged by network monitoring systems, which could impact the stealth of the assessment.
- **Resource Consumption**: OpenVAS and Metasploit require significant processing power, which may slow down scanning processes on larger networks.
- **Tool-Specific Scope**: Lynis and Nikto have focused areas of application, meaning they may not cover broader network vulnerabilities but are essential for in-depth audits within their domains.