Phase 2: Identify Targets and Run Scans

1. ***Tool: Nmap***
    - Purpose: Nmap is a widely used network scanning tool for host discovery, port scanning, service enumeration, and OS fingerprinting.
    - Usage: Utilize Nmap to identify live hosts, open ports, and services running on those hosts. Commonly used commands include nmap -sn for host discovery, nmap -sV for version detection, and nmap -O for OS fingerprinting.
2. ***Tool: Nessus***
    - Purpose: Nessus is a comprehensive vulnerability scanning tool that can assist in host discovery, vulnerability assessment, and enumeration of security weaknesses.
    - Usage: Utilize Nessus to perform in depth vulnerability scans on discovered hosts, identifying potential security issues, misconfigurations, and outdated software versions.
3. ***Tool: OpenVAS***
    - Purpose: OpenVAS (Open Vulnerability Assessment System) is an open source vulnerability scanner that can perform network scanning, vulnerability detection, and reporting.
    - Usage: Utilize OpenVAS to conduct network scans, identify potential vulnerabilities, and generate comprehensive reports on the security posture of the target hosts.
4. ***Tool: Nikto***

- Purpose: Nikto is a web server scanning tool designed to identify common vulnerabilities and misconfigurations in web applications and servers.
- Usage: Employ Nikto to perform comprehensive scans of web servers, including detection of outdated software versions, insecure configurations, and potential vulnerabilities in web applications.

5. ***Tool: Metasploit Framework***
    - Purpose: Metasploit Framework is a powerful exploitation framework that can be used for host discovery, vulnerability validation, and penetration testing.
    - Usage: Utilize Metasploit to validate identified vulnerabilities, test for potential exploitation, and demonstrate the impact of security weaknesses to the client.

Challenges and Potential Limitations:

- Network Segmentation: Host discovery and enumeration may be challenging in networks with strict segmentation, firewalls, or access controls that limit visibility and scanning capabilities.
- False Positives and False Negatives: Scans may occasionally produce false positives or negatives due to factors such as network latency, intermittent connectivity, or misconfigurations, requiring manual verification and validation of results.
- Network Performance Impact: Intensive scanning activities may consume network resources, negatively impact network performance, or trigger security

alerts, requiring the utmost precise and careful planning and in sync coordination with the client's information technology (IT) team.