Phase 2: Identify Targets and Run Scans

Objective

This phase aims to identify the tools and techniques to be used for host discovery and enumeration. This involves performing network scans to gather detailed information about hosts, services, and operating systems in the target environment.

Procedure and Tools

1. Nmap: Nmap is a popular network scanning tool. Nmap is used to find open ports on the network and identify services. Nmap also includes many preconfigured scripts that can detect vulnerabilities and exploit them. Nmap is a great tool for initial host discovery and collecting information about operating systems and services running in the system. However, Nmap scans can be easily detected by IPS or IDS. Additionally, in large networks, Nmap scans can be time-consuming. Though Nmap is a great resource for network scanning, its exploiting capabilities are limited and can disrupt the target system.
    - Usage:
        1. nmap -sn <target ip>

           Scans for live hosts in the network.
        2. nmap <target ip>

           Scans target IP for open ports.
        3. nmap -sV <target ip> -p <port number>

           Returns basic information about the target port.
        4. nmap -sV --script=banner <target ip>

It grabs banners from every service discoverable in the target IP.

5. nmap --script=vuln <target ip>

   Runs all scripts in the vulnerabilities category against the target IP.

2. OpenVAS: OpenVAS is a free, open-source tool for scanning networks, systems, and software for vulnerabilities. OpenVAS comes with a large database of vulnerability signatures. After each vulnerability assessment, OpenVAS lists the vulnerabilities along with a risk rating. CVSS (Common Vulnerability Scoring System) value and CVE (Common Vulnerabilities and Exposures) number detailed in the report can be crucial information for exploitation. However, configuring and using openVAS can be a challenge for non-technical personnel. Moreover, the vulnerability signature database may not always include the latest vulnerabilities. Although vulnerability scanners like Nessus can be considered a better alternative, OpenVAS is the go-to solution for dealing with a low budget.
   - Usage: OpenVAS’s full scan capability can be used to scan the entire network for vulnerabilities. Web server scan is useful to find vulnerabilities in web applications running in the system.
3. Metasploit: Metasploit is a penetration testing framework used for exploitation and post-exploitation activities. In addition, it can enumerate services and check for known vulnerabilities. Metasploit comes with a wide range of exploits and is very easy to use. Although it is a very powerful weapon in a penetration tester’s arsenal, it can be easily detected by antivirus and firewalls.
   - Usage: Metasploit contains hundreds of auxiliary modules to perform network scanning, vulnerability scanning, sniffing, etc. These modules can be used to perform port scans, enumerate services, and search for exploitable vulnerabilities.

4. Netcat: Netcat is used for manual enumeration of network services. It can be used to connect to open ports and retrieve banner information, which may reveal service versions and other useful details. Netcat is a great tool for creating remote (bind/reverse) shells. However, using Netcat for port scanning on a large network can be less efficient than Nmap.
    - Usage:
        1. Port scan: nc -nv -w 1 -z <target-ip> <port range>
        2. Banner grabbing: nc -v <target> <port>
5. Masscan: Masscan is a high-speed port scanner. It is highly used for scanning large networks efficiently. The biggest disadvantage of Masscan is that, unlike Nmap, it lacks advanced functionality.
    - Usage:
        1. Basic scan : masscan -p0-65535 <target>

Conclusion

Each of these tools listed above comes with unique strengths and weaknesses. By combining these tools, we can construct a detailed network profile, identifying potential security weaknesses for further investigation.