Scanning & Vulnerability Analysis: Part 2

Phase 1: Reconnaissance and Information Gathering

- Collecting public information about the target.
- Identifying vulnerabilities and formulating a testing strategy.
- Using Passive information gathering to reduce risk of detection.
- Open-Source Intelligence (OSINT): Gathering information from public sources.
  - Techniques: Web Scraping, Google Dorking, Social Media Profiling.
  - Tools: host, nslookup, dig, whois, knockpy, netdiscover, traceroute, whatweb, theHarvester, sherlock, wfw00f, Google Dorking, OSINT framework

Phase 2: Scanning and Vulnerability Analysis

- Objective of scanning: Identify system services and potential entry points.
  - Techniques: NW scanning, Port scanning, Services detection.
  - Tools: nmap, zenmap, unicorn, nikto.
- Objective of vulnerability analysis: Deep examination to uncover known vulnerabilities.
  - Tools: nessus, searchsploit, OpenVAS, Metasploit Framework.
- Scanning and Vulnerability Analysis Tools:
  - OS and NW: nmap, nessus, openVAS, tripwire, wireshark, MSF
  - Web Applications: Burp Suite, nikto, OWASP ZAP
  - Mobile Applications: frida, drozer, MobSF, Burp Suite
- Vulnerability Analysis Steps:
  1. Scanning for vulnerabilities using databases like NVD.
  2. Assessing severity using metrics like CVSS/VPR.
  3. Submitting report with vulnerability, risk levels, and mitigation.
- Reference: Rapid7 vulnerability management fundamentals.

Environment Setup

- Kali Linux (Attacker)
- Metasploitable 2 (Target)

Metasploit Framework (MSF) Overview

- Open-source penetration testing and exploitation platform.
- Developed by H.D. Moore; acquired by Rapid7.
- Comprehensive tools for penetration testing, from info gathering to post-exploitation.
- Kali Linux includes a command-line version (free). Commercial version with GUI available.

- Key concepts:
  - Vulnerability
  - Exploit
  - Payload

Accessing Metasploit Framework (MSF) using msfconsole

- Interfaces: msfconsole, msfcli, msfgui, msfweb, armitage.
- msfconsole: Centralized console for accessing MSF options.
- Run `sudo msfconsole` in Kali Linux.
- `help` command to check available commands.

Anatomy and Structure of Metasploit in Kali Linux

- Metasploit files located in `/usr/share/metasploit-framework/`
- Interaction primarily through seven modules in `/usr/share/metasploit-framework/modules/`

Metasploit Modules

1. **Auxiliary:** Information gathering and vulnerability analysis.
   - Port scanners, sniffers, fuzzers.
   - Example: `scanner/portscan/syn.rb` (SYN scan).
2. **Exploits:** Exploiting vulnerabilities in OS, network services, and applications.
3. **Payloads:** Code that runs on compromised systems.
   - **Singles:** Self-contained, single-task payloads.
   - **Stagers:** Establishes connection back to attacker.
   - **Stages:** Larger payloads sent over established connection.
4. **Encoders:** Encoding payloads to evade detection.
5. **Nops:** Generates NOP sleds to modify payload signature.
6. **Evasion:** Evades detection by security mechanisms (firewalls, IDS).
7. **Post:** Post-exploitation activities (privilege escalation, data exfiltration, persistence).

Basic Commands of msfconsole

- Run `msfconsole` as `sudo`
- `help`: Lists available commands.
- `banner`: Displays ASCII art banner with version information.
- `exit/quit`: Exits msfconsole.
- `show nops`: Displays scripts names, disclosure date, rank, check, and description of each
- `search telnet`: Searches for exploits, payloads, auxiliary modules.
- `searchsploit telnet`: Searches Exploit Database (EDB) for exploits.

- `info auxiliary/scanner/portscan/syn`: Provides info about a specific module.
- `use auxiliary/scanner/portscan/syn`: Changes context to specific module.
- `show options`: Displays module parameters.
- `show advanced`: Displays advanced module options.
- `set <param> <value>`: Sets a parameter value.
- `unset <param>`: Removes a parameter value.
- `unset all`: Removes all assigned variables.
- `setg RHOSTS <ip>`: Sets a global parameter value.
- `run`: Executes the loaded module.

Performing Port Scanning on Metasploitable2

- Run nmap within msfconsole: `msf6> nmap -sV <ip of M2>`

- Using Metasploit auxiliary modules for port scanning.

    - `msf6> search portscan`
    - `msf6> use auxiliary/scanner/portscan/syn`
    - `msf6 auxiliary(scanner/portscan/syn)> show options`

Performing Port Scanning on Metasploitable2 using Metasploit Auxiliary Modules

- Set `RHOSTS` to the Metasploitable2 IP address.
- Set `THREADS` for scan speed (e.g., `set THREADS 50`).

- Execute the module with `run`.

- Other scripts can be run like `ack.rb` and `tcp.rb`.

Performing Version Scanning on Metasploitable2

- Objective: Determine the versions of services running on open ports.

- **SMB Version Scanning:**

    - Module: `auxiliary/scanner/smb/smb_version`
    - Sets `RHOSTS` to Metasploitable2 IP.
    - Identifies SMB service version.

- **FTP Version Scanning:**

    - Module: `auxiliary/scanner/ftp/ftp_version`
    - Sets `RHOSTS` to Metasploitable2 IP.
    - Identifies FTP service version (e.g., vsftpd 2.3.4).

- **HTTP Version Scanning:**
  - Module: `auxiliary/scanner/http/http_version`
  - Sets `RHOSTS` to Metasploitable2 IP.
  - Identifies web server version (e.g., Apache 2.2.8 with PHP 5.2.4).
  - Verification: Confirmed by navigating to `http://<IP of M2>/phpinfo.php`.
- Students should identify the versions of ssh, smb, mysql, and postgres.

Performing Directory Scanning on Metasploitable2

- Objective: Scan for directories, files, or shares on network services.
- **HTTP Directory Scanning:**
  - Module: `auxiliary/scanner/http/dir_scanner`
  - Sets `RHOSTS` to Metasploitable2 IP.
  - Reveals directories (e.g., phpMyAdmin).
- **Tomcat Directory Scanning:**
  - Metasploitable2 runs tomcat on port 8180.
  - Module: `auxiliary/scanner/http/dir_scanner`
  - Sets `RHOSTS` to Metasploitable2 IP.
  - Identifies Tomcat directories (e.g., `/admin/`, `/webdav/`, `/tomcat-docs/`).
  - Example: Manual brute-forcing login to `http://<IP of M2>:8180/admin`.

Anonymous User Access Without Password

- Objective: Identify services configured for anonymous access.
- **FTP Anonymous Access Check:**
  - Module: `auxiliary/scanner/ftp/anonymous`
  - Sets `RHOSTS` to Metasploitable2 IP.
  - Checks if FTP service allows anonymous login.
- Verification:
  - Connect using `ftp <ip of M2>`
  - Username: `anonymous`
  - Blank password.

Brute-Force Login on Metasploitable2

- Tomcat server running on port 8180.
- Admin panel accessible at `http://<IP of M2>:8180/admin` (requires credentials).
- `tomcat_mgr_login.rb` script for brute-force attacks.

- Parameters: `RHOSTS`, `RPORT`, `USERNAME`, `PASSWORD`, `USER_FILE`, `PASS_FILE`, `USERPASS_FILE`.

```
msf6> use auxiliary/scanner/http/tomcat_mgr_login msf6
auxiliary(scanner/http/tomcat_mgr_login)> show options
```

- Default username/password lists: `/usr/share/Metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt`, `/usr/share/Metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt`

```
msf6> set --clear username msf6> set --clear password msf6> set
--clear user_file msf6> set --clear pass_file msf6> set --clear
userpass_file msf6> set user_file /usr/share/Metasploit-
framework/data/wordlists/tomcat_mgr_default_users.txt msf6> set
user_file /usr/share/Metasploit-framework/data/wordlists/
tomcat_mgr_default_pass.txt msf6> set RHOSTS <IP of M2> msf6> set
RPORT 8180 msf6> run
```

- Example Credentials found: tomcat:tomcat
- Students advised to perform similar brute-force login scans using `ssh_login.rb`, `mysql_login.rb`, and `postgres_login.rb`.

Summary of Vulnerable Services Running on Metasploitable2

1. **TCP Port 21 - vsftpd 2.3.4 (FTP Server)**
   - CVE: CVE-2011-2523
   - Attack Vector: Backdoor allows reverse shell on port 6200/tcp with username ending in ":)".
2. **TCP Port 22 - OpenSSH 4.7p1 (SSH Server)**
   - CVE: No specific CVE, susceptible to brute-force.
   - Attack Vector: Brute-force attacks to guess SSH credentials.
3. **TCP Port 23 - Telnet (Remote Login Service)**
   - CVE: No specific CVE, transmits data in plaintext.
   - Attack Vector: Interception of credentials through network sniffing.
4. **TCP Port 25 - Postfix (SMTP Server)**
   - CVE: No specific CVE, misconfiguration leads to open relay.
   - Attack Vector: Exploitation of open mail relay for spam.
5. **TCP Port 53 - BIND 9.4.2 (DNS Server)**
   - CVE: CVE-2009-0025
   - Attack Vector: Denial of service via DNSSEC validation issues.

6. **TCP Port 80 - Apache 2.2.8 (HTTP Server)**

   ◦ CVE: CVE-2007-6750
   ◦ Attack Vector: Denial of service via partial HTTP requests.

7. **TCP Ports 139 & 445 - Samba 3.0.20 (SMB/CIFS)**

   ◦ CVE: CVE-2007-2447
   ◦ Attack Vector: Remote code execution via "username map script" parameter.

8. **TCP Ports 512, 513, 514 - Rexec, Rlogin, Rsh (Remote Execution Services)**

   ◦ CVE: No specific CVEs, inherently insecure.
   ◦ Attack Vector: Plaintext transmission of data, susceptible to interception and unauthorized remote command execution.

9. **TCP Port 2049 - NFS (Network File System)**

   ◦ CVE: No specific CVE, misconfigurations lead to unauthorized access.
   ◦ Attack Vector: Remote attackers can mount NFS shares and access sensitive files.

10. **TCP Port 2121 - ProFTPD 1.3.1 (FTP Server)**

    ◦ CVE: CVE-2006-5815
    ◦ Attack Vector: Command injection flaw allows remote command execution.

11. **TCP Port 3306 - MySQL 5.0.51a (Database Server)**

    ◦ CVE: No specific CVE, weak default configurations.
    ◦ Attack Vector: Unauthorized database access due to weak or missing passwords.

12. **TCP Port 5432 - PostgreSQL 8.3.0 (Database Server)**

    ◦ CVE: No specific CVE, potential for weak configurations.
    ◦ Attack Vector: Unauthorized database access due to default or weak passwords.

13. **TCP Port 5900 - VNC (Virtual Network Computing)**

    ◦ CVE: No specific CVE, depends on configuration.
    ◦ Attack Vector: Unauthorized remote desktop access if not properly secured.

14. **TCP Port 6667 - UnrealIRCd 3.2.8.1 (IRC Server)**

    ◦ CVE: CVE-2010-2075
    ◦ Attack Vector: Remote command execution via crafted commands to the server.

Disclaimer: The information provided is for educational purposes only. Misuse of this information can result in criminal charges.