

## Lab06      **Vulnerability Analysis**

### Objective

- In this lab, I will identify and analyze vulnerabilities using a scripting tool and a vulnerability scanner. This process helps assess system weaknesses and understand their severity.

### Tools

- We were given the Cisco's Ethical Hacker VM
- Nmap + nmap scripts
- GVM Vulnerability Scanner

### **Step1 Target Fingerprinting**

Scanned the target system using nmap to find two FTP services running on different ports. Once identified, i performed a version scan to determine the exact service versions for further analysis.

```
(root@Kali)-[/home/kali/Desktop]
# nmap -sT 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-10 17:00 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000093s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5667/tcp  open  irc
MAC Address: 02:42:AC:11:00:02 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

```
(root@Kali)-[/home/kali/Desktop]
# nmap -sV -p 21,2121 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-10 17:02 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000034s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
2121/tcp  open  ftp      ProFTPD 1.3.1
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

- Step 1. Target Fingerprinting
- Step 2. Known Vulnerabilities
- Step 3. Verify the Vulnerabilities
- Step 4. Vulnerability Exploitation
- Clean-up
- Submission

## Step2. Known Vulnerabilities

For this step, i used again nmap and vulners script to check whether the vulners.com database contains know vulnerabilities for the founded FTP services. As i found some information from the database, i compared the CVE details with Packetstrom records.

```
(root@Kali)-[/home/kali/Desktop]
# nmap -sV -p 21,2121 172.17.0.2 --script vulners --script-args mincvss=8.0
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-10 17:05 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000029s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|   | PACKETSTORM:162145      10.0      https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|   |
|   | EDB-ID:49757      9.8      https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|   | CVE-2011-2523      9.8      https://vulners.com/cve/CVE-2011-2523
|   | 1337DAY-ID-36095      9.8      https://vulners.com/zdt/1337DAY-ID-36095      *EXPLOIT*
|   |
| 2121/tcp open  ftp      ProFTPD 1.3.1
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.1:
|   | SAINT:FD1752E124A72FD3A26EEB9B315E8382      10.0      https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382      *EXPLOIT*
|   | SAINT:ECC52DD75C7865AF72D358DC03E39270      10.0      https://vulners.com/saint/SAINT:ECC52DD75C7865AF72D358DC03E39270      *EXPLOIT*
|   | SAINT:C38482A29286C4F6E5C4BD19DFFEC245      10.0      https://vulners.com/saint/SAINT:C38482A29286C4F6E5C4BD19DFFEC245      *EXPLOIT*
```

## Step3. Verify the Vulnerability

This step was used nmap to check whether the service allows anonymous FTP logins. I you can see from picture, the port 21 allows Anonymous FTP logins.

```
(root@Kali)-[/home/kali/Desktop]
# nmap -p 21 172.17.0.2 --script ftp-anon
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-10 17:10 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000038s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

After this i verified the vulnerability even further.

```
root@Kali: /home/kali/Desktop
File Actions Edit View Help

(root@Kali)~/Desktop
# nmap -p 21 172.17.0.2 --script "ftp-* and vuln"
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-10 17:13 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000036s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:   BID:48539 CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_23
|   4_backdoor.rb
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

(root@Kali)~/Desktop
```

#### Step4. Vulnerability Scanner

This was the final step of the lab. I used the GVM scanner to analyze the previous target, including the host and FTP services. The main goal of this step was to familiarize myself with a vulnerability scanner and automate the scanning process.

