Kernel exploits

🐧 Linux Kernel Exploits (GitHub)

◇ 1. Dirty COW

- **CVE**: CVE-2016-5195
- **Desc**: Race condition in copy-on-write
- **Exploit**: https://github.com/firefart/dirtycow
- **Usage**: Escalates to root

```
gcc -pthread dirty.c -o dirty -lcrypt
./dirty
```

◇ 2. Dirty Pipe

- **CVE**: CVE-2022-0847
- **Desc**: Write arbitrary data to read-only files
- **Exploit**: https://github.com/Arinerron/CVE-2022-0847
- **Kernel**: Linux 5.8+

```
gcc dirtypipe.c -o dirtypipe
./dirtypipe /etc/passwd
```

◇ 3. Polkit (PwnKit)

- **CVE**: CVE-2021-4034
- **Desc**: Exploits `pkexec`
- **Exploit**: https://github.com/berdav/CVE-2021-4034

```
gcc pwnkit.c -o pwnkit
./pwnkit
```

◇ 4. Sudo Baron Samedit

- **CVE**: CVE-2021-3156
- **Desc**: Heap-based buffer overflow in `sudo`
- **Exploit**: https://github.com/blasty/CVE-2021-3156

```
./exploit
```

◇ 5. OverlayFS PrivEsc

- **CVE**: CVE-2021-3493
- **Exploit**: https://github.com/briskets/CVE-2021-3493
- **Affected**: Ubuntu 20.04+

```
make
./exploit
```

◇ 6. Retbleed (Speculative Execution)

- **CVE**: CVE-2022-29900
- **Desc**: Spectre-style attack
- **PoC**: https://github.com/IAIK/retbleed

  🧠 Requires understanding of CPU speculative exec

🪟 Windows Kernel Exploits (GitHub)

◇ 1. CVE-2022-21882

- **Desc**: Win32k LPE
- **Exploit**: https://github.com/KaLendsi/CVE-2022-21882
- **Works on**: Win10 21H1

```
exploit.exe
```

◇ 2. CVE-2021-1732

- **Desc**: Win32k Elevation
- **Exploit**: https://github.com/KaLendsi/CVE-2021-1732
- **Works on**: Windows 10

  Requires compiling with Visual Studio

◇ 3. Juicy Potato / Rogue Potato

- **Type**: Token impersonation via COM services
- **GitHub**:
  - https://github.com/ohpe/juicy-potato
  - https://github.com/antonioCoco/RoguePotato
- **Usage**:

```
JuicyPotato.exe -l 1337 -p cmd.exe -t *
```

◇ 4. PrintNightmare

- **CVE**: CVE-2021-1675 / CVE-2021-34527
- **Exploit**: https://github.com/calebstewart/CVE-2021-1675
- **Requirement**: Print Spooler enabled

🤖 Android Kernel Exploits (GitHub)

◇ 1. Binder PrivEsc

- **CVE**: CVE-2019-2215
- **Desc**: Use-after-free in Binder
- **Exploit**: https://github.com/tale/tale-cve-2019-2215
- **Usage**: Root access on vulnerable kernels

◇ 2. Dirty COW (Android Port)

- **Exploit**: https://github.com/timwr/CVE-2016-5195
- **Usage**: Android privilege escalation

◇ 3. MediaTek-su

- **Desc**: Root exploit for MediaTek devices
- **Exploit**: https://github.com/chiteroman/mtk-su
- **Note**: Works on many MTK SoCs

◇ 4. CVE-2020-0041

- **Exploit**: https://github.com/quarkslab/CVE-2020-0041
- **Desc**: Binder driver race condition
- **Target**: Android 9/10

⚠ Important Notes

- Always test these exploits in **controlled lab environments**.
- Match **kernel version and config** with what the exploit supports.
- Use **`uname -a`**, **`lsb_release -a`**, or **`ver`** to determine OS/kernel version.
- On Linux, `dmesg | grep -i linux` may also help identify version info.
