

# Privacy Escalation

local Linux privilege-escalation discovery

Python :

```
#!/usr/bin/env python3
```

```
"""
```

Local privesc info gatherer. Run this on the target Linux VM (lab).

Collects: kernel info, sudo -l, world-writable files, SUID binaries.

Usage: python3 privesc\_local.py

```
"""
```

```
import os, subprocess, json
```

```
def run(cmd):
```

```
    try:
```

```
        return subprocess.check_output(cmd, shell=True, stderr=subprocess.DEVNULL).decode()
```

```
    except Exception as e:
```

```
        return str(e)
```

```
info = {}
```

```
info['uname'] = run("uname -a")
```

```
info['os_release'] = run("cat /etc/os-release")
```

```
info['sudoers'] = run("sudo -l 2>&1") # will prompt if sudo needs password - run as permitted user
```

```
info['suid'] = run("find / -perm -4000 -type f -exec ls -ld {} \; 2>/dev/null | head -n 200")
```

```
info['world_writable'] = run("find / -xdev -type f -perm -0002 -ls 2>/dev/null | head -n 200")
```

```
info['crontab'] = run("ls -la /etc/cron* 2>/dev/null || true")
```

```
# Save
```

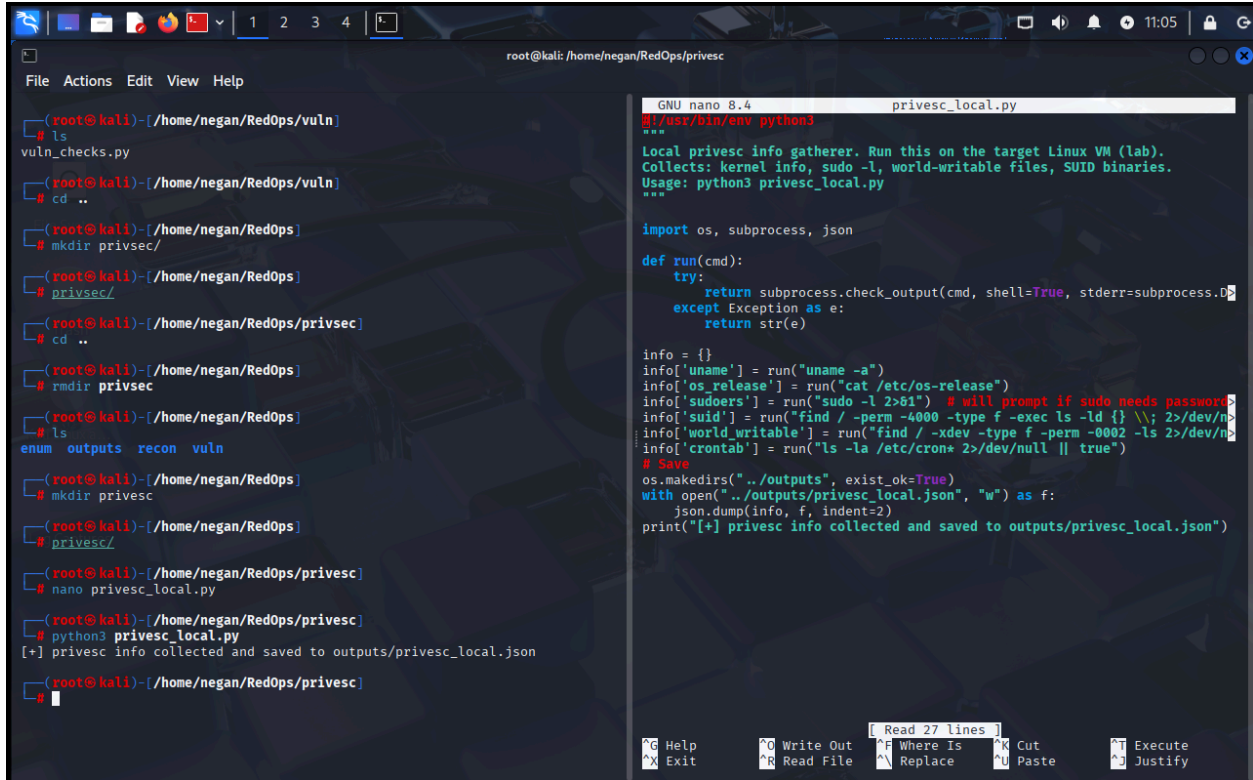
```
os.makedirs("../outputs", exist_ok=True)
```

```
with open("../outputs/privesc_local.json", "w") as f:
```

```
    json.dump(info, f, indent=2)
```

```
print("[+] privesc info collected and saved to outputs/privesc_local.json")
```

Working :



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
root@kali: ~/home/negan/RedOps/privsec
File Actions Edit View Help
root@kali)~/home/negan/RedOps/vuln
# ls
vuln_checks.py
root@kali)~/home/negan/RedOps/vuln
# cd ..
root@kali)~/home/negan/RedOps
# mkdir privsec/
root@kali)~/home/negan/RedOps
# cd privsec/
root@kali)~/home/negan/RedOps/privsec
# cd ..
root@kali)~/home/negan/RedOps
# rmdir privsec
root@kali)~/home/negan/RedOps
# ls
enum outputs recon vuln
root@kali)~/home/negan/RedOps
# mkdir privsec
root@kali)~/home/negan/RedOps/privsec
# cd privsec/
root@kali)~/home/negan/RedOps/privsec
# nano privsec_local.py
root@kali)~/home/negan/RedOps/privsec
# python3 privsec_local.py
[+] privsec info collected and saved to outputs/privsec_local.json
root@kali)~/home/negan/RedOps/privsec
#
```

The nano editor shows the content of `privsec_local.py`:

```
GNU nano 8.4 privsec_local.py
#!/usr/bin/env python3
"""
Local privsec info gatherer. Run this on the target Linux VM (lab).
Collects: kernel info, sudo -l, world-writable files, SUID binaries.
Usage: python3 privsec_local.py
"""

import os, subprocess, json

def run(cmd):
    try:
        return subprocess.check_output(cmd, shell=True, stderr=subprocess.STDOUT)
    except Exception as e:
        return str(e)

info = {}
info['uname'] = run("uname -a")
info['os_release'] = run("cat /etc/os-release")
info['sudoers'] = run("sudo -l 2>&1") # will prompt if sudo needs password
info['suid'] = run("find / -perm -4000 -type f -exec ls -ld {} \; 2>/dev/null")
info['world_writable'] = run("find / -xdev -type f -perm -0002 -ls 2>/dev/null")
info['crontab'] = run("ls -la /etc/cron* 2>/dev/null || true")

# Save
os.makedirs("../outputs", exist_ok=True)
with open("../outputs/privsec_local.json", "w") as f:
    json.dump(info, f, indent=2)
print("[+] privsec info collected and saved to outputs/privsec_local.json")
```

The bottom status bar of the nano editor shows: `[ Read 27 lines ]` and navigation shortcuts: `^G Help`, `^O Write Out`, `^F Where Is`, `^X Cut`, `^H Read File`, `^_ Replace`, `^U Paste`, `^J Execute`, `^_ Justify`.