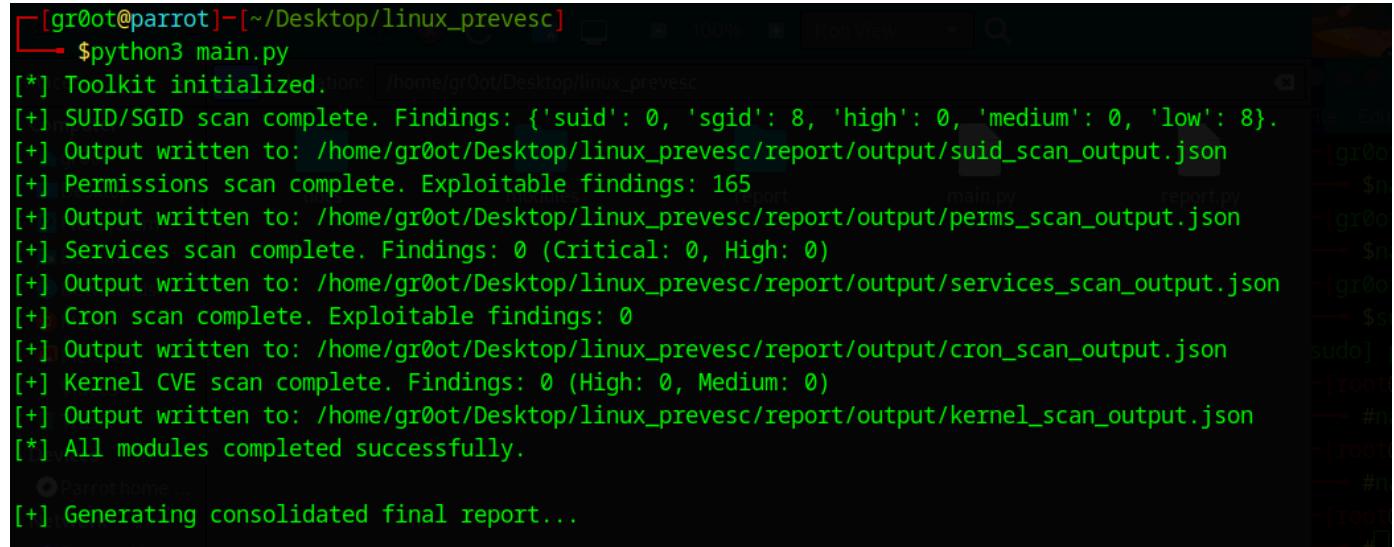


Linux_privesc_SS_file

Linux Privilege Escalation Toolkit

1. Toolkit Execution – Scanning in Progress :

This screenshot shows the toolkit being executed with main.py, where all modules begin scanning the system for privilege escalation vectors.



```
[gr0ot@parrot] -[~/Desktop/linux_prevesc]
└─$ python3 main.py
[*] Toolkit initialized.
[+] SUID/SGID scan complete. Findings: {'suid': 0, 'sgid': 8, 'high': 0, 'medium': 0, 'low': 8}.
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/suid_scan_output.json
[+] Permissions scan complete. Exploitable findings: 165
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/perms_scan_output.json
[+] Services scan complete. Findings: 0 (Critical: 0, High: 0)
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/services_scan_output.json
[+] Cron scan complete. Exploitable findings: 0
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/cron_scan_output.json
[+] Kernel CVE scan complete. Findings: 0 (High: 0, Medium: 0)
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/kernel_scan_output.json
[*] All modules completed successfully.

[+] Generating consolidated final report...
```

2. Consolidated Final Report (Terminal Output) :

Here the final report is displayed directly in the terminal, summarizing findings with severity levels in a color-coded format.

==== Linux PrivEsc Toolkit Final Report ====

Generated: 2026-02-04T20:49:11.533551Z

Overall Findings:

Total Findings: 173

High: 165

Medium: 0

Low: 8

[CRON_SCAN]

Findings: 0 (High: 0, Medium: 0, Low: 0)

No exploitable findings.

[KERNEL_SCAN]

Findings: 0 (High: 0, Medium: 0, Low: 0)

No exploitable findings.

[PERMS_SCAN]

Findings: 165 (High: 165, Medium: 0, Low: 0)

- /etc/systemd/system/dbus-f1.w1.wpa_supplicant1.service (High)
- /etc/systemd/system/dbus-org.bluez.service (High)
- /etc/systemd/system/dbus-org.freedesktop.ModemManager1.service (High)
- /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service (High)
- /etc/systemd/system/display-manager.service (High)

```
-[gr0ot@parrot]~[~]
--> $nano /etc/hosts
-[gr0ot@parrot]~[~]
--> $sudo su
[sudo] password for gr0ot:
-[root@parrot]~[/home/gr0ot]
--> #nano /etc/passwd
-[root@parrot]~[/home/gr0ot]
--> #nano /etc/hosts
-[root@parrot]~[/home/gr0ot]
--> #
```

```
[PERMS_SCAN]
Findings: 165 (High: 165, Medium: 0, Low: 0)
- /etc/systemd/system/dbus-f1.wl.wpa_supplicant1.service (High)
- /etc/systemd/system/dbus-org.bluez.service (High)
- /etc/systemd/system/dbus-org.freedesktop.ModemManager1.service (High)
- /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service (High)
- /etc/systemd/system/display-manager.service (High)

[sudo] password for gr0ot:
[gr0ot@parrot:~/Desktop/linux_prevesc/report/output]# nano /etc/passwd
[gr0ot@parrot:~/Desktop/linux_prevesc/report/output]# nano /etc/hosts
[gr0ot@parrot:~/Desktop/linux_prevesc/report/output]# nano /etc/hosts

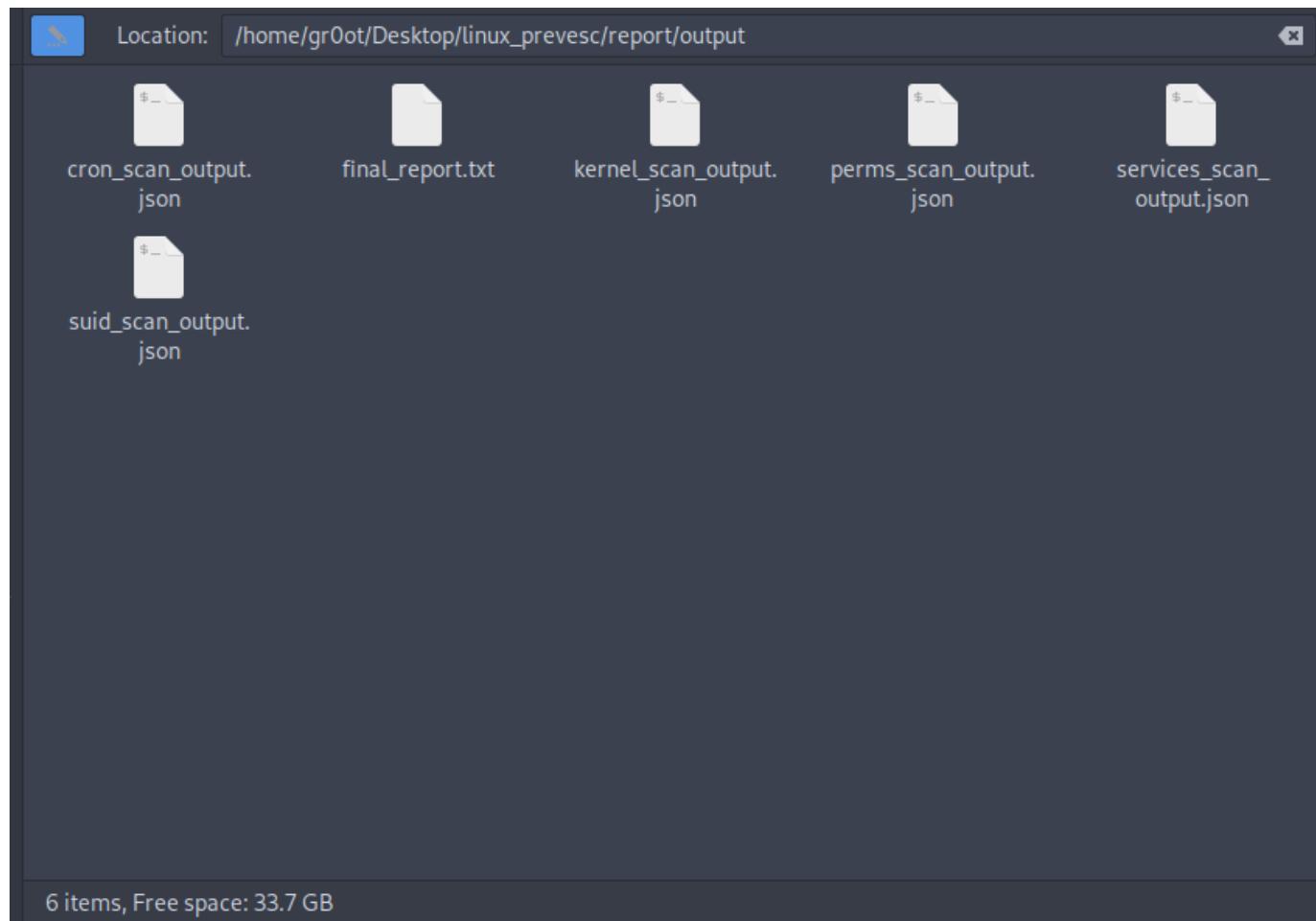
[SERVICES_SCAN]
Findings: 0 (High: 0, Medium: 0, Low: 0)
No exploitable findings.

[SUID_SCAN]
SUID Findings: 0
SGID Findings: 8
Severity -> High: 0, Medium: 0, Low: 8
- /usr/bin/chage (Low)
- /usr/bin/crontab (Low)
- /usr/bin/dotlockfile (Low)
- /usr/bin/expiry (Low)
- /usr/bin/ssh-agent (Low)

[+] Final report saved to /home/gr0ot/Desktop/linux_prevesc/report/output/final_report.txt
```

3. Report/Output Directory Overview (JSON Logs + Report) :

This view highlights the report/output/ directory, containing JSON logs from each module along with the consolidated final report file.



4. Saved Final Report (final_report.txt) :

This screenshot shows the generated final_report.txt, which provides a structured summary of all findings for offline review.

```
1 === Linux PrivEsc Toolkit Final Report ===
2 Generated: 2026-02-04T20:49:11.534227Z
3
4 Overall Findings:
5   Total Findings: 173
6   High: 165
7   Medium: 0
8   Low: 8
9
10 [CRON_SCAN]
11   Findings: 0 (High: 0, Medium: 0, Low: 0)
12     No exploitable findings.
13
14 [KERNEL_SCAN]
15   Findings: 0 (High: 0, Medium: 0, Low: 0)
16     No exploitable findings.
17
18 [PERMS_SCAN]
19   Findings: 165 (High: 165, Medium: 0, Low: 0)
20     - /etc/systemd/system/dbus-fi.wl.wpa_supplicant1.service (High)
21     - /etc/systemd/system/dbus-org.bluez.service (High)
22     - /etc/systemd/system/dbus-org.freedesktop.ModemManager1.service (High)
23     - /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service (High)
24     - /etc/systemd/system/display-manager.service (High)
25
26 [SERVICES_SCAN]
27   Findings: 0 (High: 0, Medium: 0, Low: 0)
28     No exploitable findings.
29
30 [SUID_SCAN]
31   SUID Findings: 0
32   SGID Findings: 8
33   Severity -> High: 0, Medium: 0, Low: 8
34     - /usr/bin/chage (Low)
35     - /usr/bin/crontab (Low)
36     - /usr/bin/dotlockfile (Low)
37     - /usr/bin/expiry (Low)
38     - /usr/bin/ssh-agent (Low)
39
```

5. Permissions Scan Results (perms_scan_output.json) :

This JSON output captures the results of the permissions scan, listing misconfigured files or directories with severity ratings.

```
perms_scan_output.json x
1|{
2  "summary": {
3    "timestamp": "2026-02-04T20:49:11.345695Z",
4    "count": 165,
5    "high": 165,
6    "medium": 0,
7    "low": 0
8  },
9  "findings": [
10  {
11    "path": "/etc/systemd/system/dbus-fi.wl.wpa_supplicant.service",
12    "type": "file",
13    "owner": "root",
14    "mode_octal": "0o777",
15    "issue": "World-writable root-owned file",
16    "severity": "High",
17    "exploitation": "Writable systemd unit or override; attacker can hijack service execution as root.",
18    "mitigation": "Restrict permissions (chmod), correct ownership (chown), and move scripts/configs out of writable locations."
19  },
20  {
21    "path": "/etc/systemd/system/dbus-org.bluez.service",
22    "type": "file",
23    "owner": "root",
24    "mode_octal": "0o777",
25    "issue": "World-writable root-owned file",
26    "severity": "High",
27  }
28]
```

6. SUID/SGID Scan Results (suid_scan_output.json) :

This JSON output displays the findings from the SUID/SGID scan, identifying binaries with special permission bits that may be exploitable.

```
suid_scan_output.json x
1 {
2   "summary": {
3     "timestamp": "2026-02-04T20:49:09.689686Z",
4     "counts": {
5       "suid": 0,
6       "sgid": 8,
7       "high": 0,
8       "medium": 0,
9       "low": 8
10    }
11  },
12  "findings": [
13    {
14      "path": "/usr/bin/chage",
15      "binary": "chage",
16      "owner": "root",
17      "group": "shadow",
18      "permissions": "?rwxr-sr-x",
19      "mode_octal": "2755",
20      "type": "SGID",
21      "capabilities": "",
22      "severity": "Low",
23      "rationale": "Privilege bit set but no known exploit indicators detected.",
24      "mitigation": "Review necessity periodically; keep package updated; monitor for changes."
25    },
26    {
27      "path": "/usr/bin/crontab",
28      "binary": "crontab",
29      "owner": "root",
30      "group": "crontab",
31      "permissions": "?rwxr-sr-x",
32      "mode_octal": "2755",
33      "type": "SGID",
34      "capabilities": "",
35      "severity": "Low"
36    }
37  ]
38 }
```