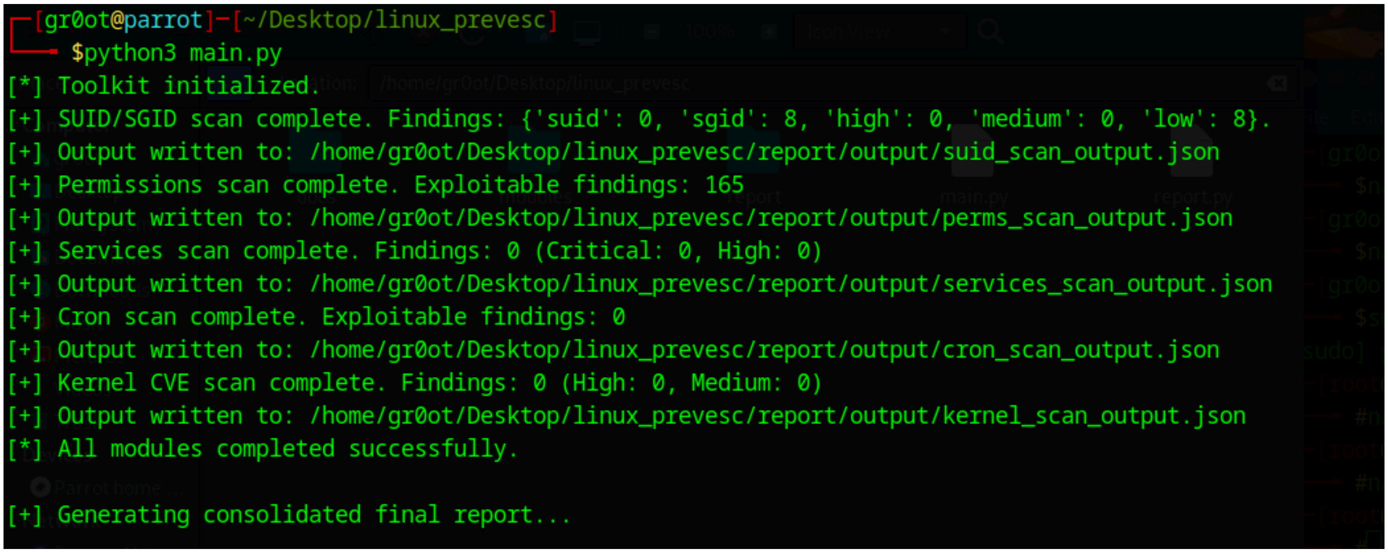
Linux_privesc_SS_file

Linux Privilege Escalation Toolkit

1. **Toolkit Execution – Scanning in Progress** :

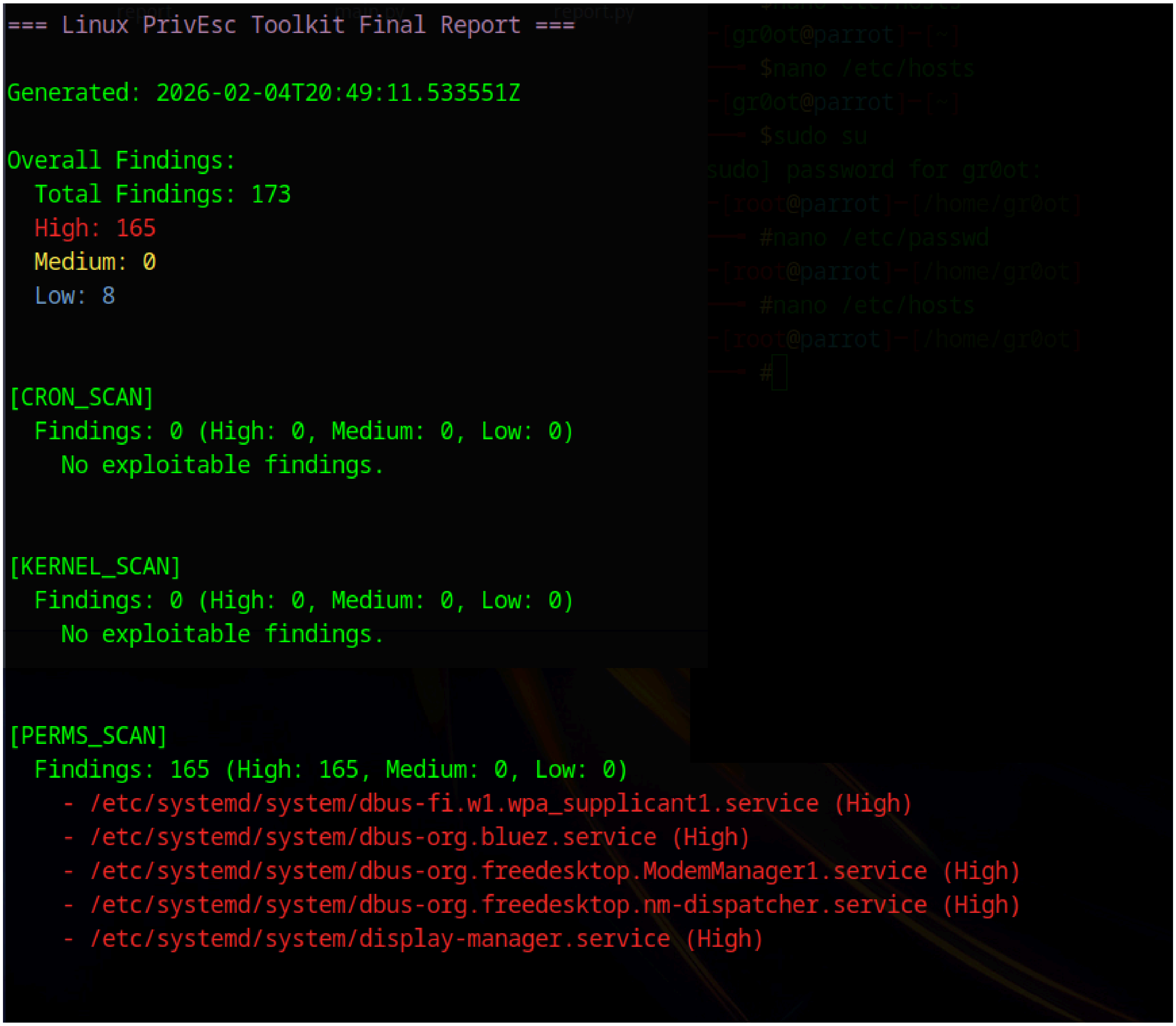
   This screenshot shows the toolkit being executed with main.py, where all modules begin scanning the system for privilege escalation vectors.



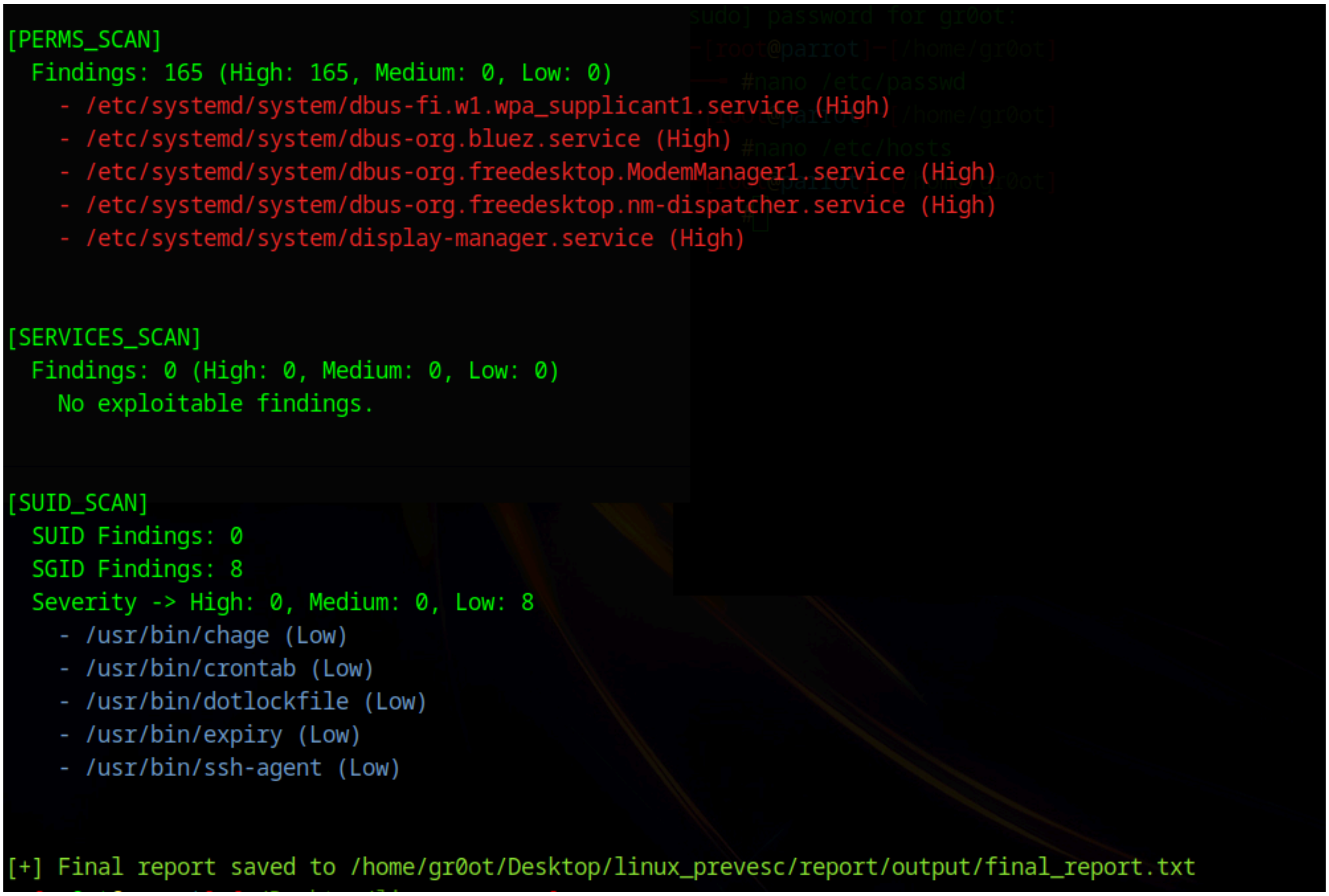
```
┌─[gr0ot@parrot]─[~/Desktop/linux_prevesc]
└──╼ $python3 main.py
[*] Toolkit initialized.
[+] SUID/SGID scan complete. Findings: {'suid': 0, 'sgid': 8, 'high': 0, 'medium': 0, 'low': 8}.
[+] Output written to: /home/gr0ot/Desktop/linux_prevesc/report/output/suid_scan_output.json
[+] Permissions scan 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-fi.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)
```

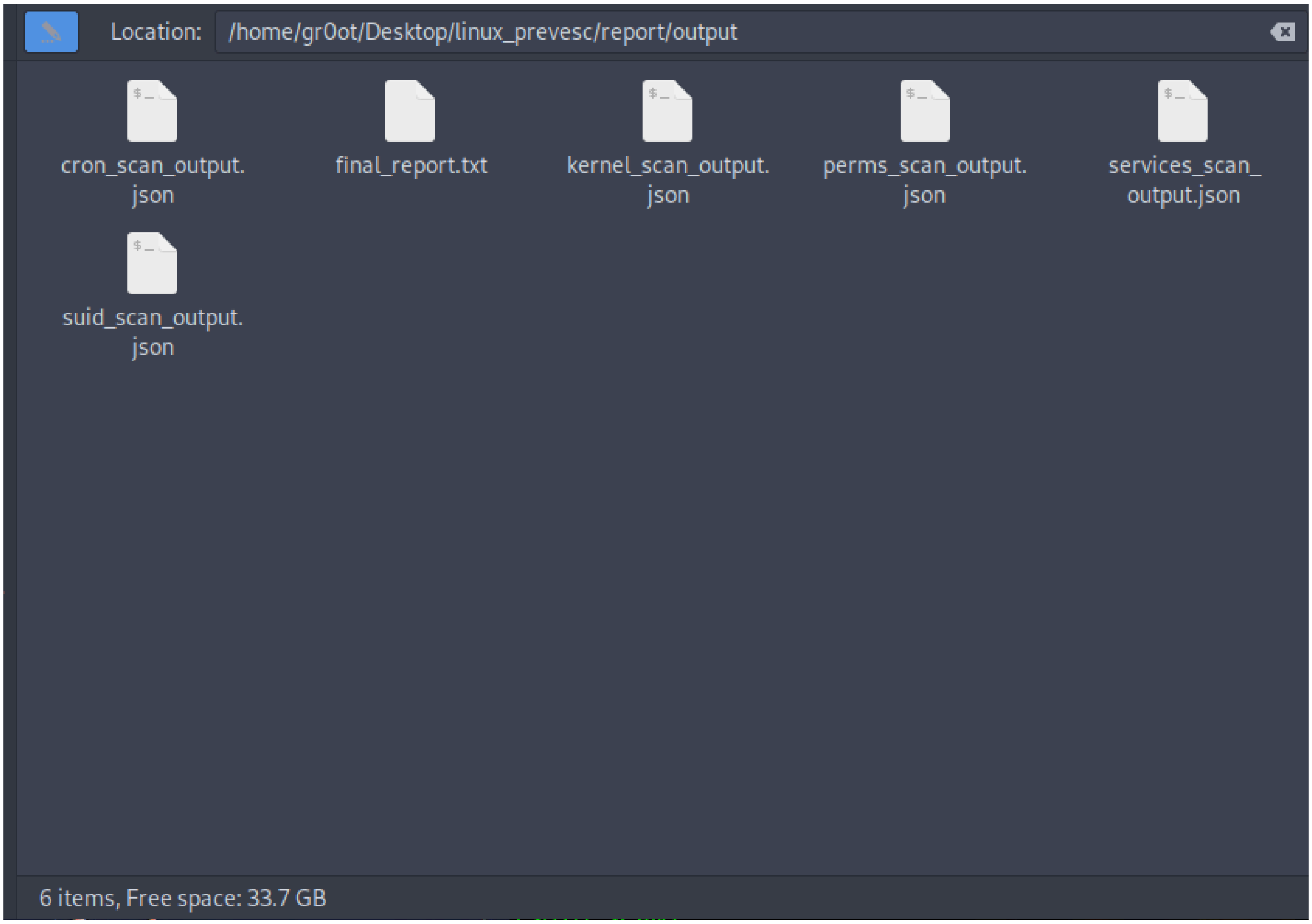


```
[PERMS_SCAN]
  Findings: 165 (High: 165, Medium: 0, Low: 0)
    - /etc/systemd/system/dbus-fi.w1.wpa_supplicant1.service (High)
    - /etc/systemd/system/dbus-org.bluez.service (High)
    - /etc/systemd/system/dbus-org.freedesktop.ModemManager1.service (High)
    - /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service (High)
    - /etc/systemd/system/display-manager.service (High)


[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.



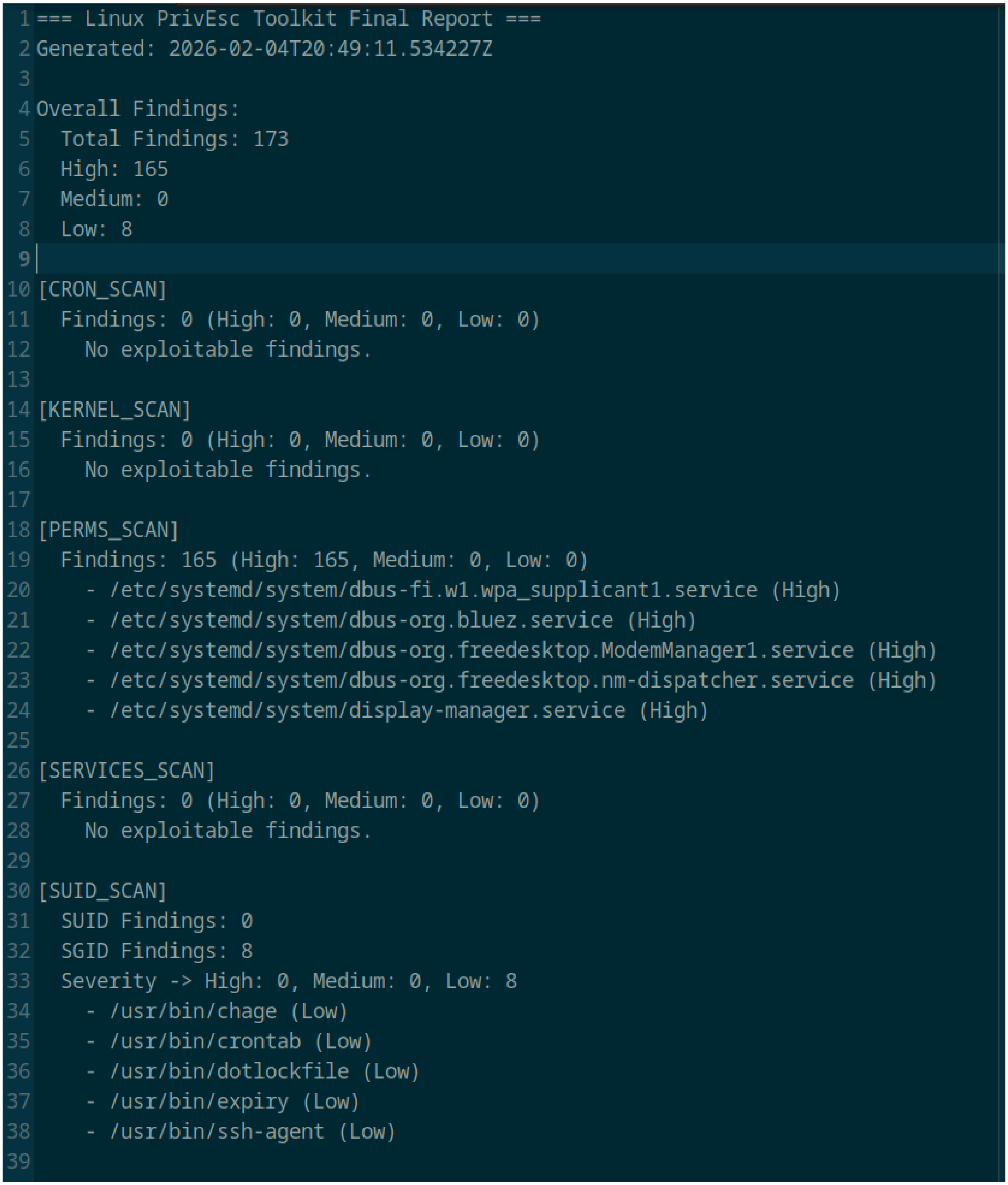
Location: /home/gr0ot/Desktop/linux_prevesc/report/output

6 items, Free space: 33.7 GB

---

4. **Saved Final Report (final_report.txt)** :

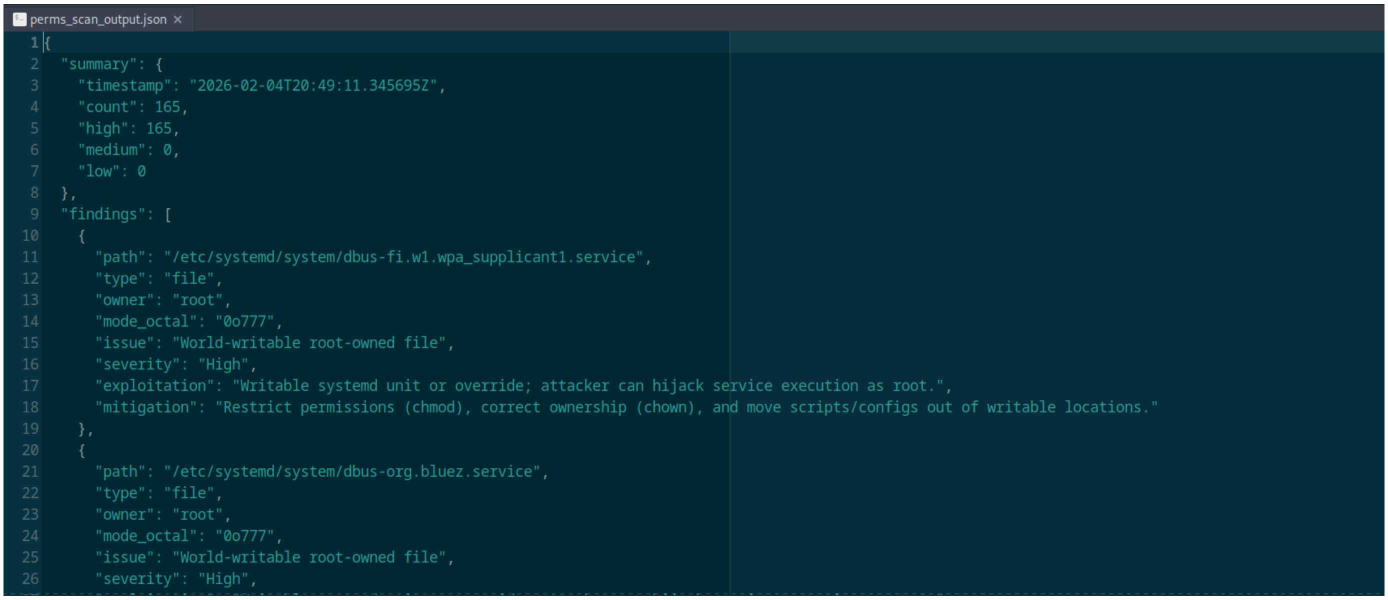
   This screenshot shows the generated final_report.txt, which provides a structured summary of all findings for offline review.



```
=== Linux PrivEsc Toolkit Final Report ===
Generated: 2026-02-04T20:49:11.534227Z

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-fi.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)

[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)

```

5. **Permissions Scan Results (perms_scan_output.json)** :

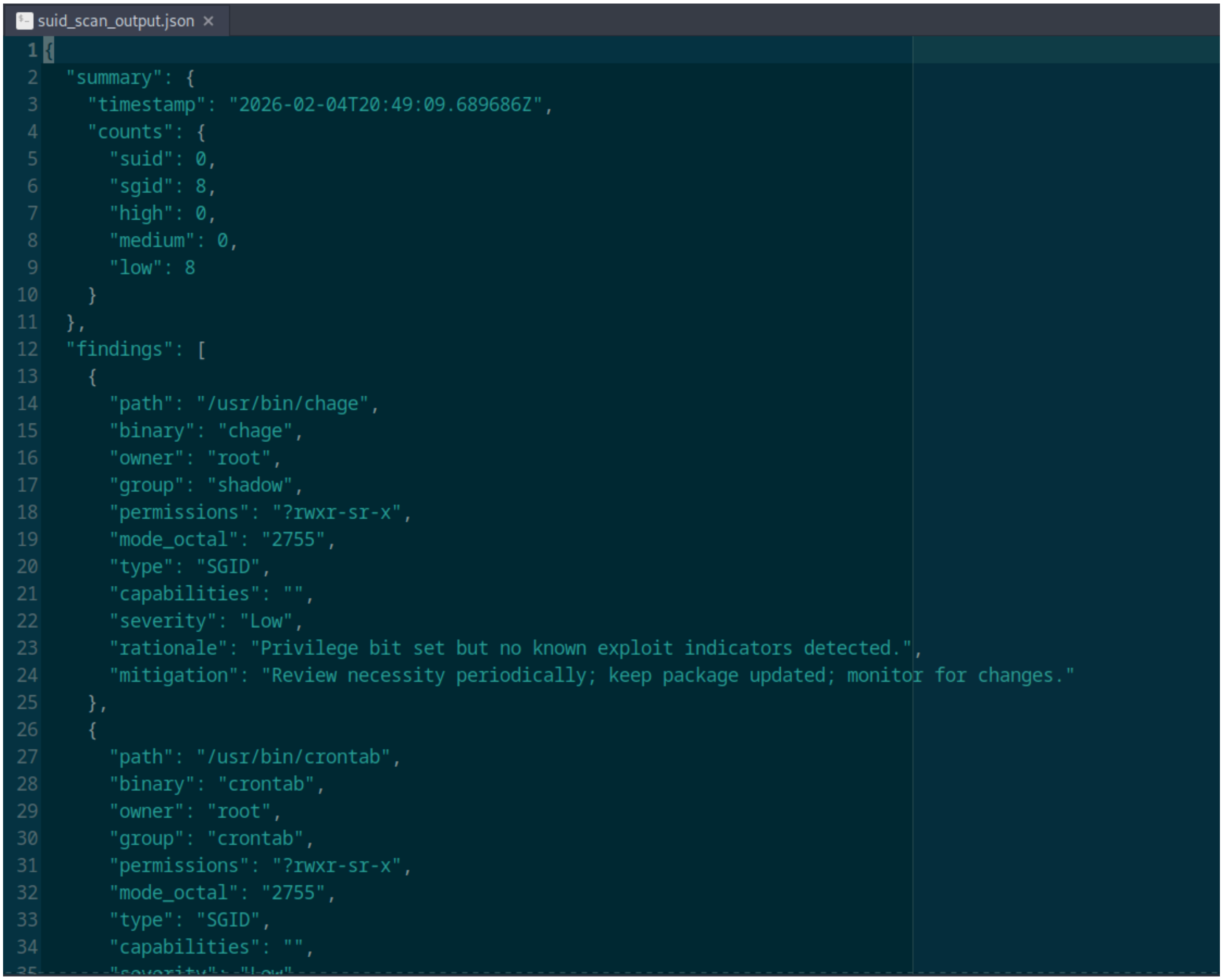
   This JSON output captures the results of the permissions scan, listing misconfigured files or directories with severity ratings.



```
{
  "summary": {
    "timestamp": "2026-02-04T20:49:11.345695Z",
    "count": 165,
    "high": 165,
    "medium": 0,
    "low": 0
  },
  "findings": [
    {
      "path": "/etc/systemd/system/dbus-fi.w1.wpa_supplicant1.service",
      "type": "file",
      "owner": "root",
      "mode_octal": "0o777",
      "issue": "World-writable root-owned file",
      "severity": "High",
      "exploitation": "Writable systemd unit or override; attacker can hijack service execution as root.",
      "mitigation": "Restrict permissions (chmod), correct ownership (chown), and move scripts/configs out of writable locations."
    },
    {
      "path": "/etc/systemd/system/dbus-org.bluez.service",
      "type": "file",
      "owner": "root",
      "mode_octal": "0o777",
      "issue": "World-writable root-owned file",
      "severity": "High",
```

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.



```
{
  "summary": {
    "timestamp": "2026-02-04T20:49:09.689686Z",
    "counts": {
      "suid": 0,
      "sgid": 8,
      "high": 0,
      "medium": 0,
      "low": 8
    }
  },
  "findings": [
    {
      "path": "/usr/bin/chage",
      "binary": "chage",
      "owner": "root",
      "group": "shadow",
      "permissions": "?rwxr-sr-x",
      "mode_octal": "2755",
      "type": "SGID",
      "capabilities": "",
      "severity": "Low",
      "rationale": "Privilege bit set but no known exploit indicators detected.",
      "mitigation": "Review necessity periodically; keep package updated; monitor for changes."
    },
    {
      "path": "/usr/bin/crontab",
      "binary": "crontab",
      "owner": "root",
      "group": "crontab",
      "permissions": "?rwxr-sr-x",
      "mode_octal": "2755",
      "type": "SGID",
      "capabilities": "",
      "severity": "Low"
```