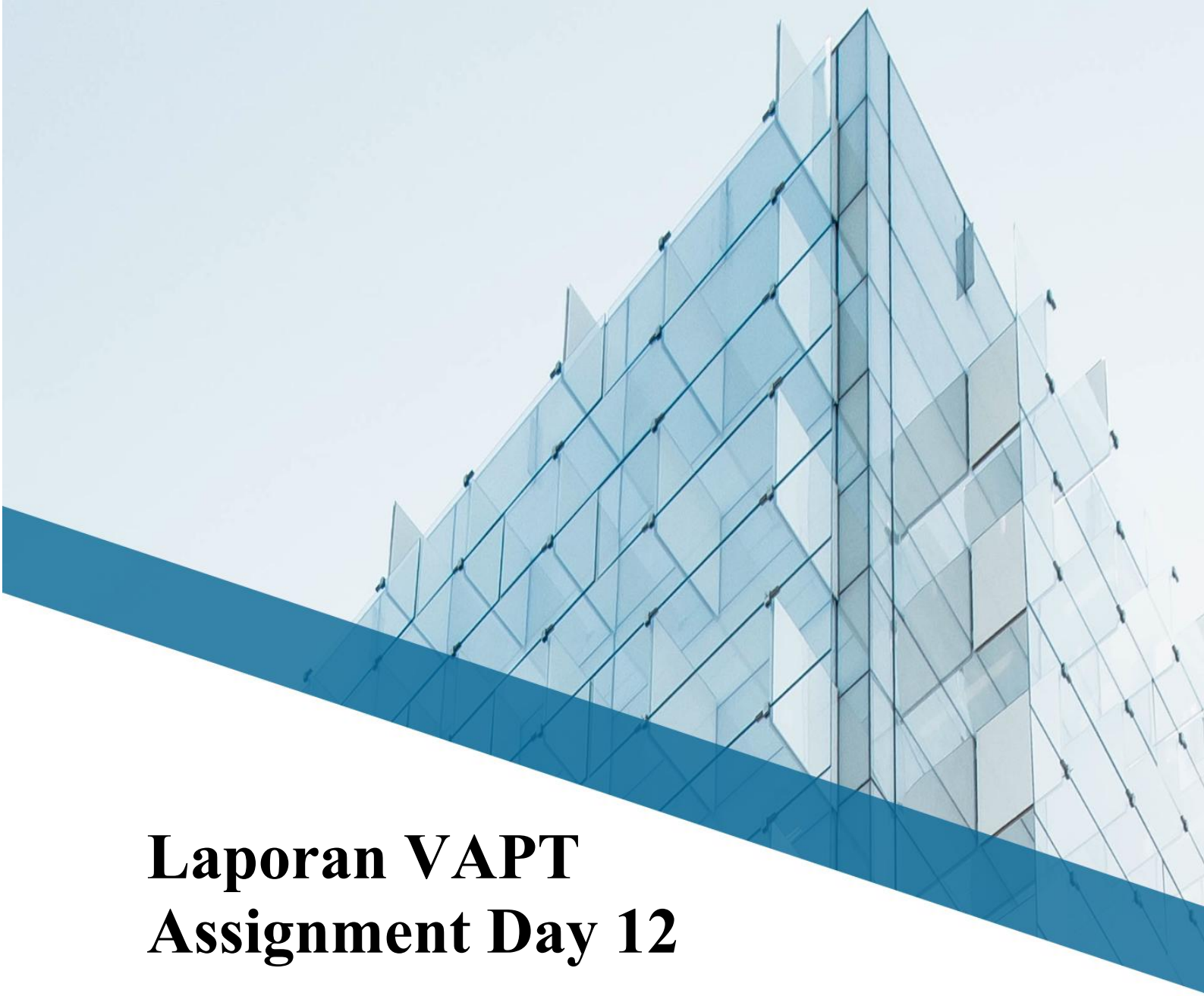


Laporan VAPT
Assignment Day 12

Bootcamp Cyber Security Batch 4

Disusun oleh: Sabilillah Ramaniya Widodo

!!Catatan: Diharapkan seluruh pengerjaan Assignment tidak sepenuhnya mengandalkan penggunaan AI!!

“Proses belajar ibarat menanam pohon. Jika hanya mengandalkan AI tanpa memahami esensinya, yang berkembang bukan kompetensimu, melainkan ketergantungan yang melemahkan.”
- Learning Design Dibimbing

1. Scope

Pengujian ini mencakup 1 mesin Debian di room Linux PrivEsc TryHackMe. Akses dilakukan menggunakan OpenVPN. Aktivitas ini fokus pada analisis permission file, hak sudo, binary SUID, dan aset auth di dalam sistem. Aset lain di luar mesin ini tidak termasuk cakupan asesmen.

2. Methodology

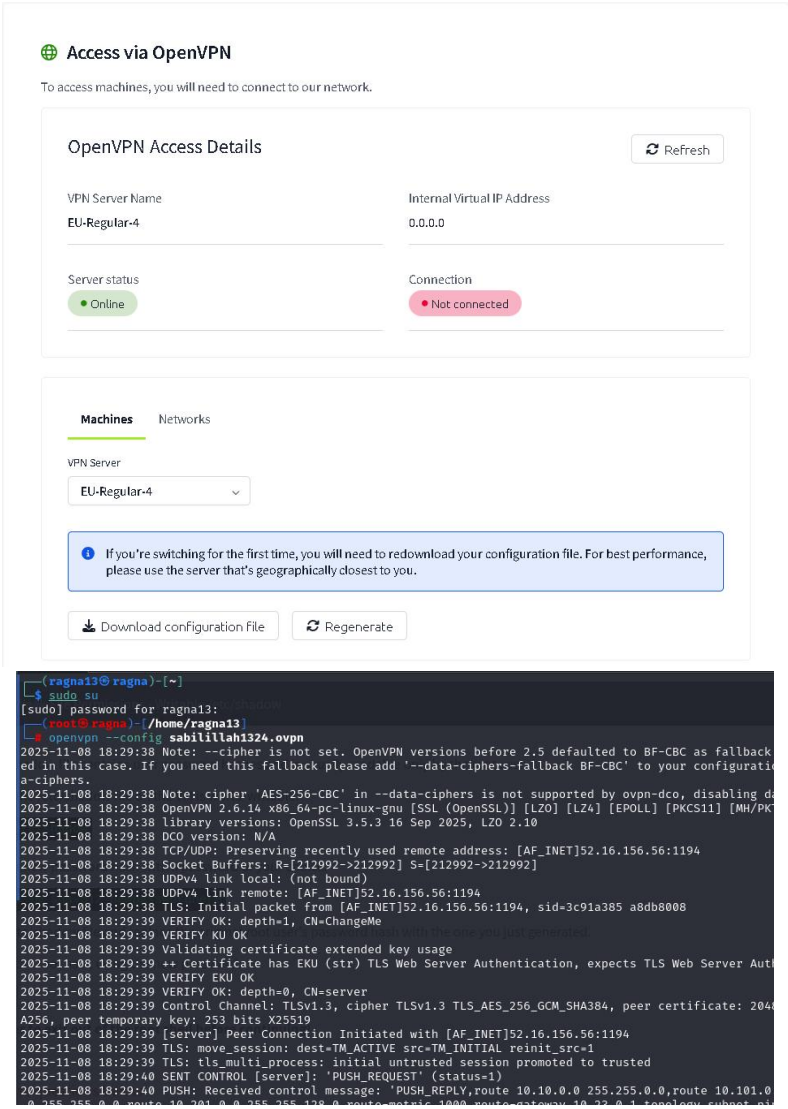
Proses asesmen keamanan dilakukan dengan mengikuti metodologi standar yang mencakup beberapa fase, yaitu:
Fase 1: Konfigurasi akses
- Mesin diaktifkan dari task page TryHackMe.
- Koneksi dibuat menggunakan OpenVPN.
- SSH digunakan untuk akses awal.

Fase 2: Information Gathering
- Pemeriksaan identitas user dengan id
- Identifikasi group dan permission default

Fase 3: Vulnerability Identification
- Pemeriksaan izin file sensitif seperti /etc/shadow.
- Pengecekan hak sudo dengan sudo -l.
- Pemindaian binary SUID.
- Inspeksi direktori root untuk mencari file berisiko.

Fase 4: Exploitation & Verification
- Crack hash /etc/shadow menggunakan John The Ripper.
- Escalation dari sudo NOPASSWD
- Eksploitasi exim-4.84 (CVE-2016-1531).

Fase 5: Analysis & Reporting
- Analisis risiko menggunakan CVSS
- Penyusunan rekomendasi mitigasi prioritas



3. Executive Summary

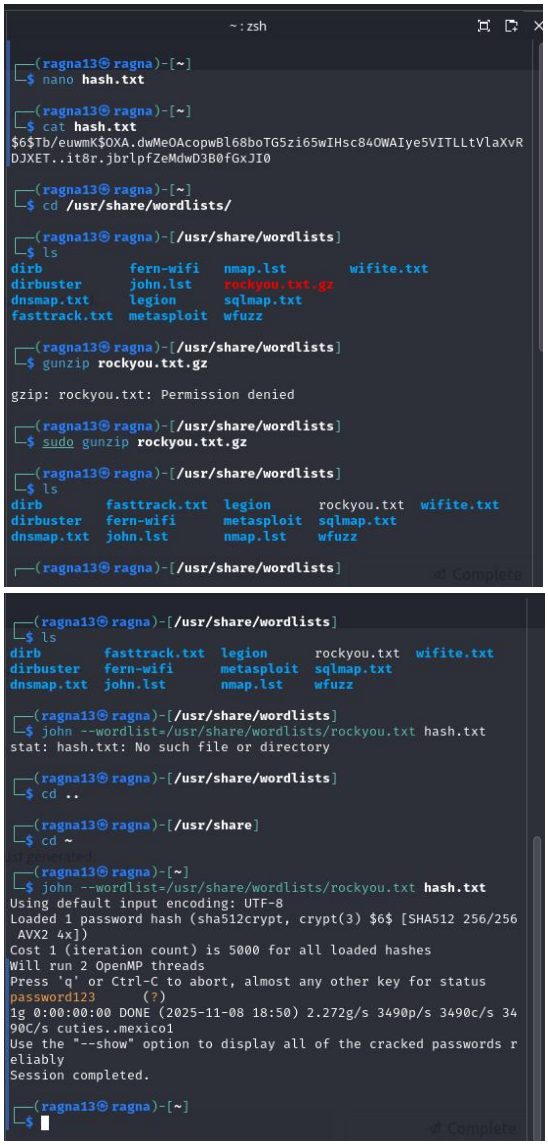
Pengujian keamanan pada mesin Linux PrivEsc TryHackMe menemukan empat temuan risiko tinggi dan kritis yang memungkinkan akses root tanpa autentikasi. Vulnerability ini disebabkan oleh permisson file sensitif yang salah, konfigurasi sudo yang terlalu longgar, binary SUID yang rentan, dan kebocoran kunci private. Semua celah bisa dimanfaatkan dengan langkah langsung tanpa hambatan teknis yang berarti.

Risiko bisnis mencakup pengambilalihan sistem, modifikasi konfigurasi yang kritis, pencurian data, dan potensi lateral movement ke sistem lain. Tindakan mitigasi bisa dilakukan melalui pembatasan izin file, pembaruan binary, penghapusan akses sudo yang tidak perlu, dan pengamanan aset autentikasi.

4. Tools

- SSH
- John the Ripper
- Rockyou Wordlist

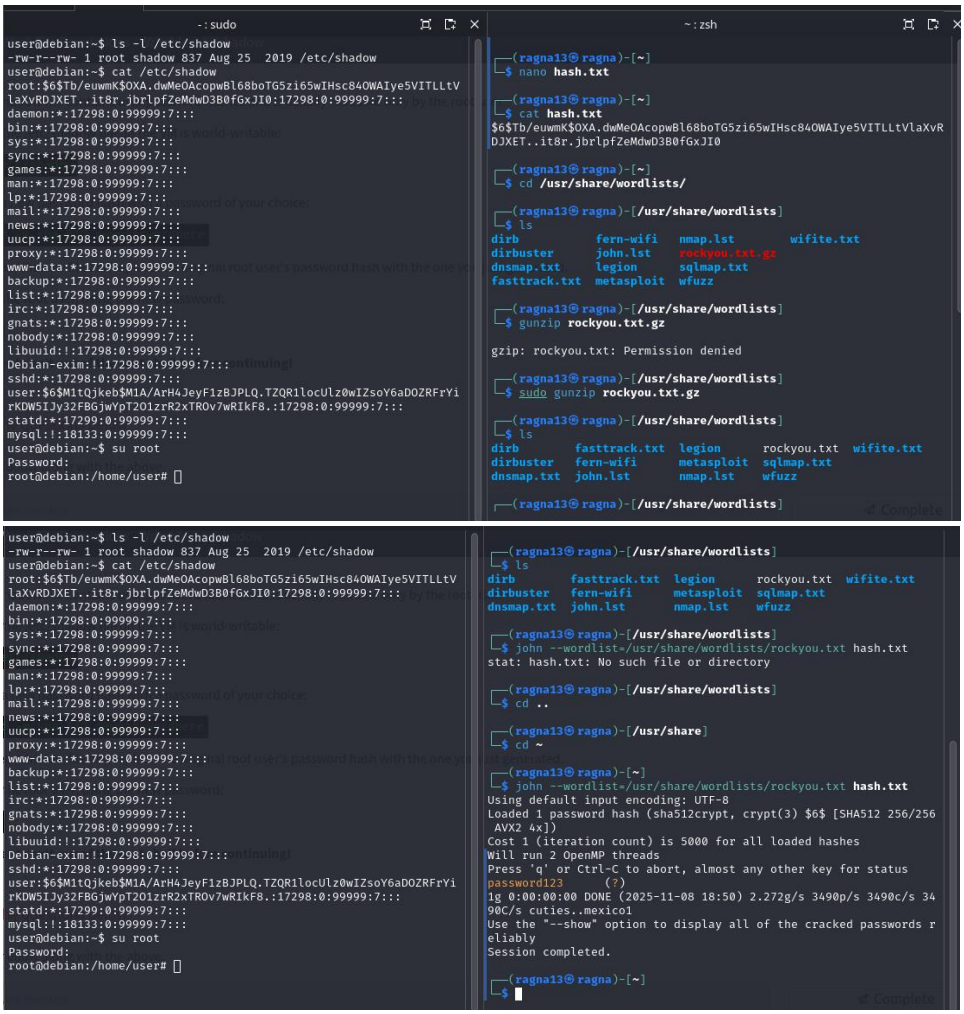
- Find (binary search)
- OpenVPN
- CVSS Calculator



5. Technical Findings

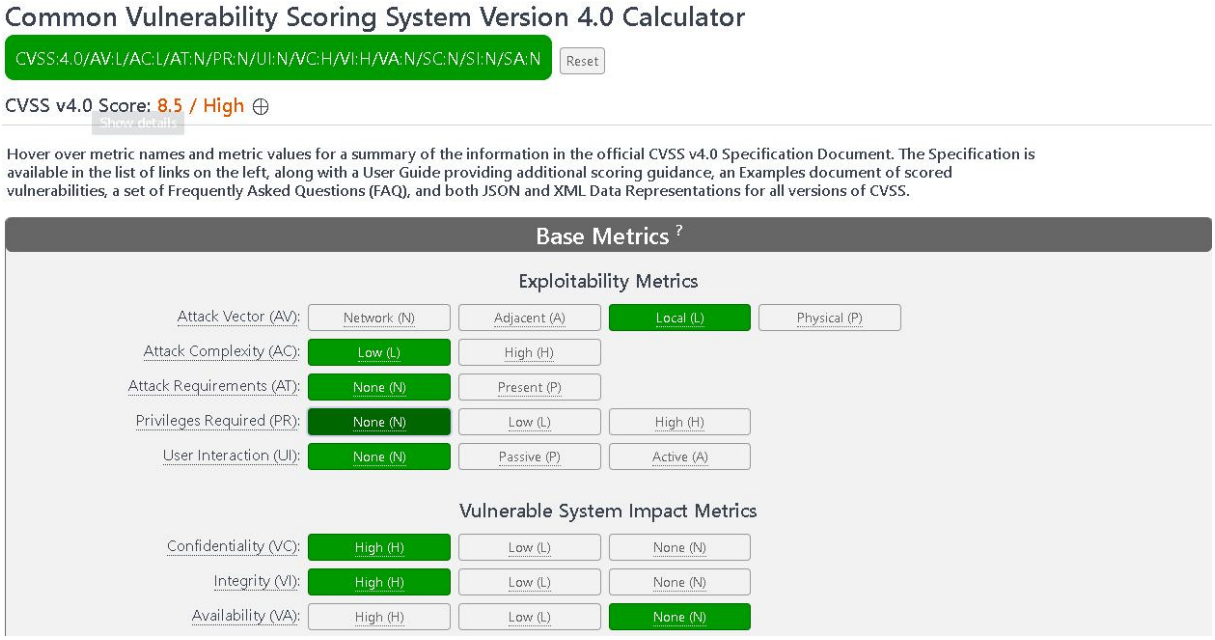
Temuan 1

World-Readable /etc/shadow
Tingkat Risiko: Kritis
Deskripsi: File /etc/shadow dapat dibaca oleh semua user. Hal ini memungkinkan user non-root mengakses hash password root.
Evidence/PoC:



- ls -l /etc/shadow menunjukkan bit r-- pada world
- Hash root dapat dibaca
- Hash berhasil dicrack menjadi password123

Risk (CVSS): Skor 8.5 (High)



Impact -> Teknis: Pengambilalihan akun root.

Bisnis: Kompromi penuh layanan dan data.

Rekomendasi Mitigasi:
- Ubah permission ke 640.
- Batasi group ke shadow.

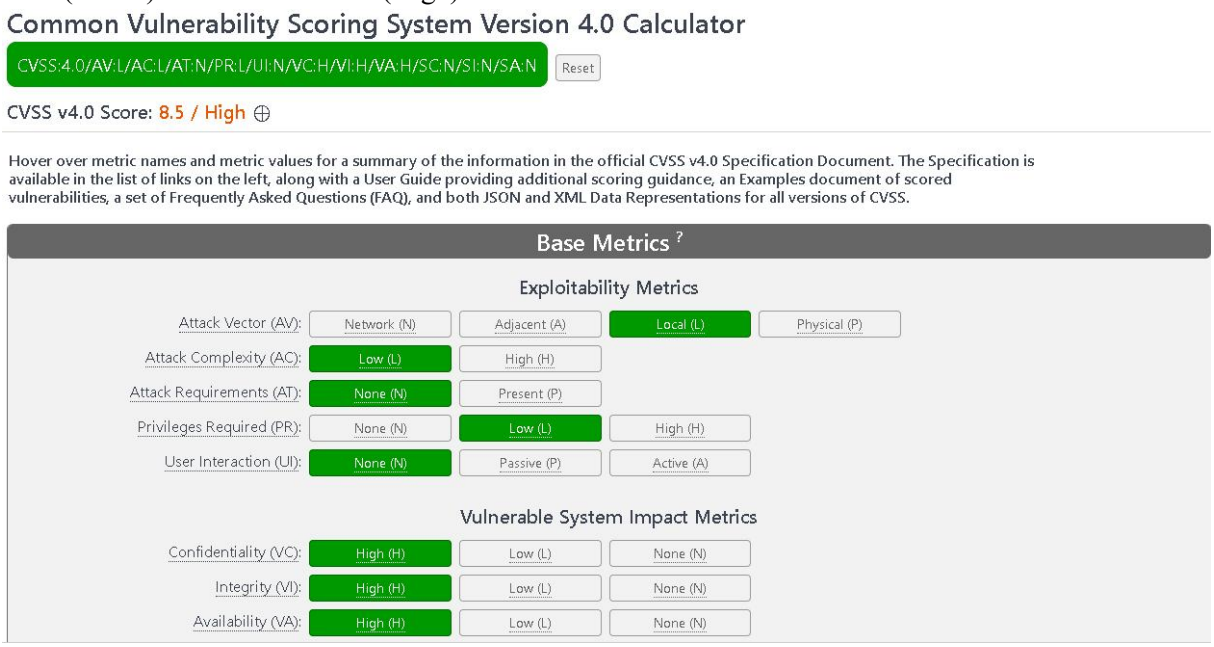
Temuan 2

Sudo NOPASSWD pada program exploitable
Tingkat Risiko: Kritis
Deskripsi: User dapat menjalankan iftop, find, nano, vim, awk, nmap, ftp, more, dan lainnya sebagai root tanpa password. Banyak program tersebut memberi akses ke shell.
Evidence/PoC:

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
user@debian:~$ sudo iftop
interface: eth0
IP address is: 10.201.0.241
MAC address is: 16:ff:e2:4f:cf:c7
sh-4.1# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.1# exit
exit
user@debian:~$ sudo find . -exec /bin/sh \; -quit
sh-4.1# whoami
root
sh-4.1# exit
exit
user@debian:~$ sudo nano
user@debian:~$
```

- sudo -l menampilkan 11 program root tanpa autentikasi
- Eksploitasi berhasil dengan iftop, find, dan nano.
Risk (CVSS): Skor estimasi 8.5 (High).

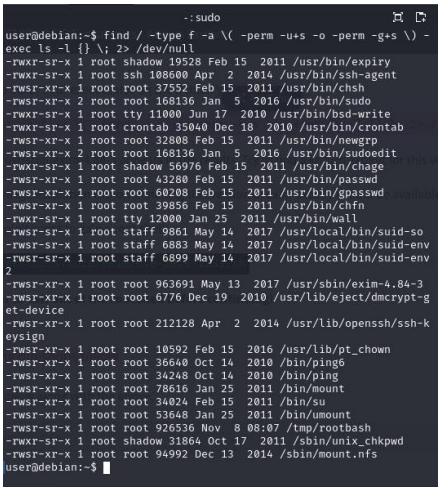


Impact -> Teknis: Shell root instan

Bisnis: Pengambilalihan server dan konfigurasi.
Rekomendasi Mitigasi:
- Hapus seluruh entri NOPASSWD yang tidak diperlukan
- Terapkan prinsip least privilege.

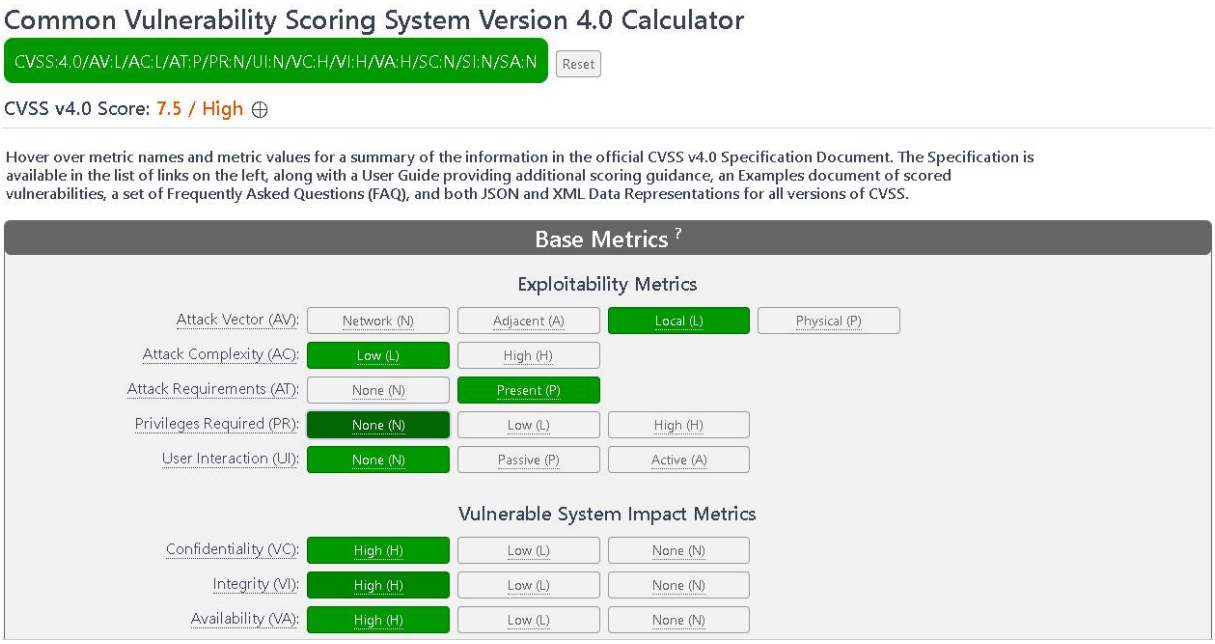
Temuan 3

SUID Exim 4.84 Vulnerable (CVE-2016-1531)
Tingkat Risiko: Tinggi
Deskripsi: Binary exim versi lama memiliki bit SUID dan rentan local privilege escalation
Evidence/PoC:



- Ditemukan melalui find.
- Eksploitasi PoC pada direktori tools/suid/exim menghasilkan shell root

Risk (CVSS): Skor 7.5 (High)

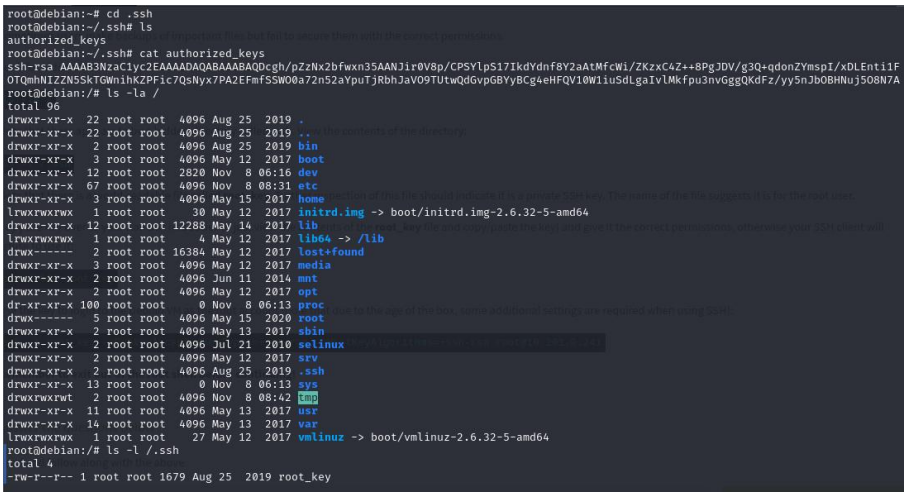


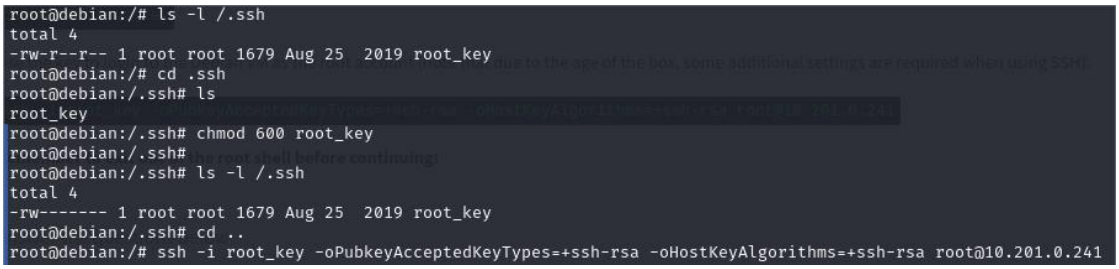
Impact -> Teknis: Eksekusi kode sebagai root

Bisnis: Kontrol penuh terhadap host
Rekomendasi Mitigasi:
- Hapus SUID
- Update exim ke versi terbaru

Temuan 4

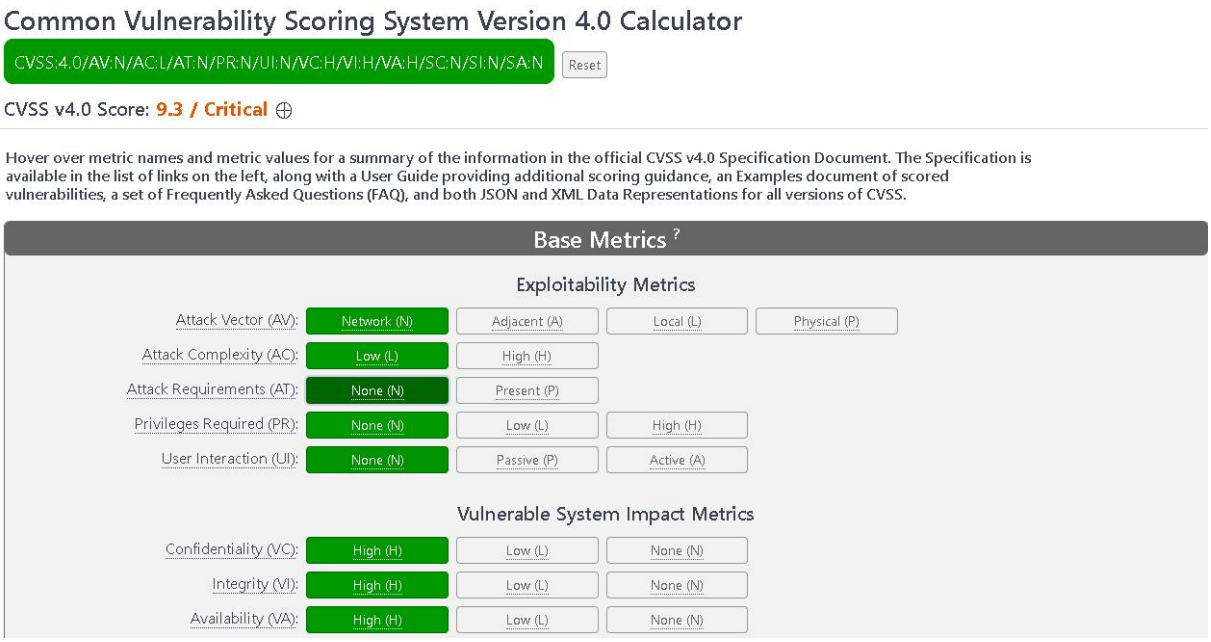
SSH Private Key root readable
Tingkat Risiko: Kritis
Deskripsi: File /.ssh/root_key dapat dibaca oleh siapapun. Kunci ini dapat digunakan untuk login sebagai root.
Evidence/PoC:





- Permission -rw-r--r-- pada root_key
- Login root berhasil menggunakan kunci tersebut.

Risk (CVSS): Skor 9.3 (Critical)



Impact -> Teknis: Akses penuh tanpa password
Bisnis: Risiko tinggi pencurian data dan persistence malware
Rekomendasi Mitigasi:
- Pindahkan ke /root/.ssh dengan permission 600
- Buat kunci baru dan cabut kunci lama.

6. Rekomendasi Mitigasi

Prioritas 1 - Kritis:
- Perbaiki permission /etc/shadow
- Hapus seluruh sudo NOPASSWD yang tidak diperlukan
- Update exim dan nonaktifkan binary lama
- Amankan dan regenerasi SSH key

Prioritas 2 - Tinggi:
- Audit ulang permission direktori sensitif
- Terapkan hardening sistem

Prioritas 3 - Medium:
- Tambahkan logging akses file
- Terapkan monitoring host

7. Retesting Plan

- Verifikasi ulang permission file yang diperbaiki
- Test sudo untuk memastikan tidak ada akses root tidak sah
- Dokumentasi hasil validasi