Scans

NMAP SYN SCAN

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-15 09:43 MST
Nmap scan report for 192.168.171.145
Host is up (0.00033s latency).
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 192.168.171.146
|      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 2
|      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:
|   1024 d8:8d:e7:48:3a:3c:91:0e:3f:43:ea:a3:05:d8:89:e2 (DSA)
|   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: 00:0C:29:29:91:56 (VMware)
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 192.168.171.145

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
```

SERVICES

FTP vsftpd 2.0.8 or later : PORT 21

HTTP Apache 2.4.7 : PORT 1515

SSH OpenSSH 6.6.1 p1 : PORT 3535

FTP

VSFTPD found on port 21

Enum

Anonymous login is available

There is some kind of text file in the directory, the shell seems busted.
I connected with netcat the first time, shell was busted, I could not access anything

Oopened new connection with ftp command and got access.
Got the note.txt
<---
Hello Dear!
Looking for route map to PumpkinGarden? I think jack can help you find it.--->

jack could be a user

HTTP APACHE

Apache Server found on port 1515

Nikto Scan

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.171.145
+ Target Hostname:    192.168.171.145
+ Target Port:        1515
+ Start Time:         2019-09-15 10:17:04 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 387, size: 58ab693542700, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7918 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2019-09-15 10:17:58 (GMT-7) (54 seconds)
---------------------------------------------------------------------------
```

Enum

The page revealed there was something hiding in the “source”.
I inspected the source page and a clue was found.

<!-- searching for the route map? Pumpkin images may help you find the way -->

The images were coming from the same directory.

I performed a Nikto scan to find any other directories.
Whent to the /img/ directory since it was available.
found a folder called “hidden secret”
found a code inside.

Clue: c2NhcmVjcm93IDogNVFuQCR5

Base64 Encoded, got some creds after decoding on a website.

Creds

scarecrow : 5Qn@$y

SSH

OpenSSH found on port 3535

Enum

Found creds in the HTTP server
logged in with the creds

No sudo priveleges, decided to look around.
Home directory has 3 folders
Note in FTP stated I should check with "jack"
One of the directories is called jack

permission denied on jack

two more directories:
goblin - denied
scarecrow - open
jack - denied

another note.txt in scarecrow

<---
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 LordPumpkin.
--->

Tried user goblin with the password found in note and logged in as goblin
another note.txt

<---
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 LordPumpkin 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
--->

leads to an exploit
"Todd Miller Sudo 'sudoedit' Local Privilege Escalation Vulnerability"

going to start HTTP server with python and wget file.
python -m SimpleHTTPServer

wget file in goblin user

run file, had to run a couple of times to get it to execute
got root access

root:6budH0KF3$qgLCqvPB9y3Qqi5MzQH0v55imm8YOwNZ9ehldQ6hAH5bNkP1HkdekxEn0i/5tHg
code in hidden directory: File name : PumpkinGarden_Key
Q29uZ3JhdHVsYXRpb25zIQ==
Base64 Encoded for:
Congratulations!

Creds

goblin : Y0n$M4sy3D1t

root:6budH0KF3$qgLCqvPB9y3Qqi5MzQH0v55imm8YOwNZ9ehldQ6hAH5bNkP1HkdekxEn0i/5tHg