

Scans

ARP Target Discovery

Tool: Netdiscover
Command: netdiscover -r 192.168.171.0/24
Intended Result: Find target through ARP requests in the network

Result:
Target IP address found.

IP Address: 192.168.171.129

File Edit View Search Terminal Help						
Currently scanning: Finished! Screen View: Unique Hosts						
8 Captured ARP Req/Rep packets, from 4 hosts. Total size: 480						
IP	At MAC Address	Count	Len	MAC Vendor / Hostname		
192.168.171.1	00:50:56:c0:00:08	1	60	VMware, Inc.		
192.168.171.2	00:50:56:f3:7e:19	4	240	VMware, Inc.		
192.168.171.129	00:0c:29:69:9d:5d	1	60	VMware, Inc.		
192.168.171.254	00:50:56:f9:92:05	2	120	VMware, Inc.		

NMAP Scans

2019/09/24 - 14:43:
Tool: NMAP
Command: nmap -T4 -p- 192.168.171.129
Intended Result: Find ports that are open on the target and get service information.

Result:
Found 2 ports open on the machine.

SSH on 22
HTTP on 80

```
root@TCK:~# nmap -T4 -p- 192.168.171.129
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-24 14:47 MST
Nmap scan report for 192.168.171.129
Host is up (0.00087s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:69:9D:5D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

Checking ports with -A for NMAP script enumeration

Command: `nmap -T4 -A -p22,80 192.168.171.129`

Intended Result: Find information about the ports and what services they are running.

Result:

Found Service information , will annotate in Services node, a quick summary

SSH Port 22: OpenSSH 6.6.1 p1 Ubuntu

HTTP Port 80: Apache (version is not disclosed)

Machine OS could be Ubuntu 2.13

```

root@TCK:~# nmap -T4 -A -p22,80 192.168.171.129
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-24 14:51 MST
Nmap scan report for 192.168.171.129
Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 1a:de:2a:25:2c:cc:51:4b:7a:a0:e0:73:23:b9:3a:64 (DSA)
|   2048 f4:67:d3:d3:e5:24:c0:fc:c4:60:07:1c:1a:34:e9:54 (RSA)
|   256 10:ce:a1:ee:54:27:03:2d:a0:b1:dc:75:80:f2:db:8b (ECDSA)
|_  256 6c:9d:b1:8d:ab:1f:3a:7c:e9:ad:bd:db:d8:81:d7:87 (ED25519)
80/tcp    open  http      Apache httpd
|_ http-robots.txt: 23 disallowed entries (15 shown)
|   /includes/ /scripts/ /js/ /secrets/ /css/ /themes/
|   /CHANGELOG.txt /underconstruction.html /info.php /hidden/note.txt
|   /INSTALL.mysql.txt /seeds/seed.txt.gpg /js/hidden.js /comment/reply/
|_  /filter/tips/
|_ http-server-header: Apache
|_ http-title: Mission-Pumpkin
MAC Address: 00:0C:29:69:9D:5D (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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   0.25 ms  192.168.171.129

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 8.79 seconds

```

Nikto Scan on Port 80

2019/09/29 - 10:51:

Tool: Nikto

Command: nikto -host 192.168.171.129

Intended Result: Find new directories and Apache version.

Result:

Same directories found.

```

root@TCK:~# nikto -host 192.168.171.129 -u http://192.168.171.129/ -p 80 -s 10000 -t 10000 -e Pumpkin Festival?
- Nikto v2.1.6
+ Target IP: 192.168.171.129
+ Target Hostname: 192.168.171.129
+ Target Port: 80
+ Start Time: 2019-09-29 10:55:02 (GMT-7)
-----
+ Server: Apache
+ 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
+ Entry '/underconstruction.html' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/hidden/note.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/seeds/seed.txt.gpg' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 25 entries which should be manually viewed.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Server may leak inodes via ETags, header found with file /, inode: 9de, size: 58b88b8ce763e, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8751 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2019-09-29 10:55:57 (GMT-7) (55 seconds)
-----
+ 1 host(s) tested

```

Still no apache version found.

OWASP ZAP scan

2019/09/29 - 11:12:

Tool: OWASP ZAP

GUI Tool URL Attacked: http://192.168.171.129

Intended Results: New directories and vulnerability assessment, maybe apache version.

Results:

Nothing interesting found from scan, except for a couple of hidden css pages.

Scan will be saved just in case.

The screenshot displays the Burp Suite application interface. The top toolbar includes buttons for 'Quick Start', 'Request', and 'Response'. The left sidebar shows a tree view of 'Contexts' and 'Sites'. The 'Sites' section is expanded, showing a list of files and folders. The 'GET:imagehover.min.css' file is selected. The main pane displays the HTTP response for this file, including headers and the CSS content. The bottom toolbar contains buttons for 'History', 'Search', 'Alerts', 'Output', 'Spider', and 'Active Scan'. The 'Alerts' tab is active, showing a list of security alerts. The 'X-Frame-Options Header Not Set (3)' alert is selected, and its details are shown in the right pane.

HTTP Response Headers:

```

HTTP/1.1 200 OK
Date: Sun, 29 Sep 2019 18:14:03 GMT
Server: Apache
Last-Modified: Fri, 14 Jun 2019 16:56:30 GMT
ETag: "36c8-58b4b87296b80"
Accept-Ranges: bytes
Content-Length: 14024
Vary: Accept-Encoding
Content-Type: text/css

```

HTTP Response Body:

```

@charset "UTF-8";
/*
 * ImageHover.css - http://www.imagehover.io
 * Version 1.0
 * Author: Ciarán Walsh

 * Made available under a MIT License:
 * http://www.opensource.org/licenses/mit-license.php

 */
[class*=" imghvr-"],[class^=imghvr-]{position:relative;display:
inline-block;margin:0;max-width:100%;background-color:#2266a5;color

```

Alerts (4):

- X-Frame-Options Header Not Set (3)
- Information Disclosure - Debug Error Messages
- Web Browser XSS Protection Not Enabled (26)
- X-Content-Type-Options Header Missing (15)

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.

Other Info:

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. http://www.example.com/iframe.html) then you will want

Dirbuster

2019/10/13 - 12:19: Dirbuster Scan

Tool: dirbuster

Command: GUI Interface

Intended Result: Find hidden AES256 key or other hidden information

Result:

No new directories found

Services

SSH on 22
HTTP on 80

SSH PORT 22

Service Information:

OpenSSH 6.6.1 p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)

```
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 1a:de:2a:25:2c:cc:51:4b:7a:a0:e0:73:23:b9:3a:64 (DSA)
|   2048 f4:67:d3:d3:e5:24:c0:fc:c4:60:07:1c:1a:34:e9:54 (RSA)
|   256  10:ce:a1:ee:54:27:03:2d:a0:b1:dc:75:80:f2:db:8b (ECDSA)
|_  256  6c:9d:b1:8d:ab:1f:3a:7c:e9:ad:bd:db:d8:81:d7:87 (ED25519)
```

Going to check for anonymous login

Tool: SSH

Command: `ssh anonymous@192.168.171.129`

Intended Result: Authenticate as the anonymous user account if available.

Result:

User account anonymous is not available or locked away with different password used.

Passwords used:

anonymous

password

blank

```
root@TCK:~# ssh anonymous@192.168.171.129
The authenticity of host '192.168.171.129 (192.168.171.129)' can't be established.
ECDSA key fingerprint is SHA256:FQpM7HKndPrLOXPDyJoBgEF3BkZVOP84CRC5j0lI3MI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.171.129' (ECDSA) to the list of known hosts.
anonymous@192.168.171.129's password:
Permission denied, please try again.
anonymous@192.168.171.129's password:
Permission denied, please try again.
anonymous@192.168.171.129's password:
anonymous@192.168.171.129: Permission denied (publickey,password).
```

Checking the credentials that I found

Tool: SSH

Command: `ssh robert@192.168.171.129`

Intended Result: Login as Robert

Result:

permission denied

```
root@TCK:~# ssh robert@192.168.171.129
robert@192.168.171.129's password:
Permission denied, please try again.
robert@192.168.171.129's password:
Permission denied, please try again.
robert@192.168.171.129's password:
robert@192.168.171.129: Permission denied (publickey,password).
root@TCK:~# ssh Robert@192.168.171.129
Robert@192.168.171.129's password:
Permission denied, please try again.
Robert@192.168.171.129's password:
Permission denied, please try again.
Robert@192.168.171.129's password:
Robert@192.168.171.129: Permission denied (publickey,password).
```

Tool: SSH

Command: ssh mark@192.168.171.129

Intended Result: Login as Mark

Result:

permission denied

```
root@TCK:~# ssh mark@192.168.171.129
mark@192.168.171.129's password:
Permission denied, please try again.
mark@192.168.171.129's password:
Permission denied, please try again.
mark@192.168.171.129's password:
mark@192.168.171.129: Permission denied (publickey,password).
root@TCK:~# ssh Mark@192.168.171.129
Mark@192.168.171.129's password:
Permission denied, please try again.
Mark@192.168.171.129's password:
Permission denied, please try again.
Mark@192.168.171.129's password:
Mark@192.168.171.129: Permission denied (publickey,password).
```

Tool: SSH

Command: ssh goblin@192.168.171.129

Intended Result: Login as goblin

Result:

permission denied

```

root@TCK:~# ssh goblin@192.168.171.129
goblin@192.168.171.129's password:
Permission denied, please try again.
goblin@192.168.171.129's password:
Permission denied, please try again.
goblin@192.168.171.129's password:
goblin@192.168.171.129: Permission denied (publickey,password).
root@TCK:~#

```

HTTP PORT 80

Service Information:
Apache <version>

```

80/tcp open  http      Apache httpd
| http-robots.txt: 23 disallowed entries (15 shown)
| /includes/ /scripts/ /js/ /secrets/ /css/ /themes/
| /CHANGELOG.txt /underconstruction.html /info.php /hidden/note.txt
| /INSTALL.mysql.txt /seeds/seed.txt.gpg /js/hidden.js /comment/reply/
| /filter/tips/
| http-server-header: Apache
| http-title: Mission-Pumpkin

```

Going to the site for further investigation leads us to a homepage that has a link attached to some text.
Looking at the source page we can see an encrypted message that translates to:
"This is just to remind you that it's Level 2 of Mission-Pumpkin! ;)"

```

</div>
<!-- VGhpcyBpcyBqdXN0IHRvIHJlbWVpbnQgew91IHRoYXQgaXQncyBMZXZlbCAyIG9mIE1pc3Npb24tUHVtcGtpbiEgOyk= -->
v class="demo">

```

Clicking on the hyperlinked text takes you to another page with another link:
<http://192.168.171.129/pumpkin.html>
Looking at the source page reveals another message:

```

F5ZWG4TJOB2HGL3TOB4S44DDMFYA====

```

The decoder I am using seems to be having a hard time decoding this,
I cannot place the output due to corruption problems, but some of the visible items included:
880V

The page takes you to another page via a link, this page is "under construction", the source for the page has nothing interesting.

Performing a Nikto scan gave me similar results to what the nmap scan gave me, so I will start visiting those directories.

/includes:
Error 404

/scripts:
Error 404

/js:
Error 404

/secrets:
Error 404

/css:
Error 403: Forbidden but exists

/themes:
Error 404

/CHANGELOG.txt:
Error 404

/info.php:
Error 404

/hidden/note.txt:
Robert : C@43r0VqG2=
Mark : Qn@F5zMg4T
goblin : 79675-06172-65206-17765

/INSTALL.mysql.txt:
Error 404

/seeds/seed.txt.gpg:
Interesting find, text seems to be encrypted, will not paste due to corruption.

/js/hidden.js:
Error 404

/comment/reply/:
Error 404

/filter/tips/:
Error 404

Interesting finds on two of those directories. Found what looks like creds, will try them out while I do a OWASP ZAP scan.

2019/10/13 - 11:19: The /seeds directory is forbidden, but the file at /seeds/seed.txt.gpg is available.

Tool: wget

Command: wget 192.168.171.129/seeds/seed.txt.gpg

Intended Result: Retrieve the file.

Result:

Saved the file onto my machine.

Creds

Robert : C@43r0VqG2=
Mark : Qn@F5zMg4T
goblin : 79675-06172-65206-17765

Acorn Pumpkin Seeds ID: 96454

Enum/Other

IP Address: 192.168.171.129

Machine OS could be Ubuntu 2.13

"This is just to remind you that it's Level 2 of Mission-Pumpkin! ;)"

F5ZWG4TJOB2HGL3TOB4S44DDMFYA====

2019/10/13 - 11:40:

Downloaded PGPTool to decrypt the pgp file I found.
The tool required a key for decryption.
Will try to create key with creds found.

Robert attempt:

Mark attempt:

golbin attempt

2019/10/13 - 12:04

I read the file extension wrong, the actual extension is .pgp not .pgp
Linux has a decryption tool that can be used in terminal.

Tool: gpg

Command: gpg --output seedDecrypt.txt --decrypt seed.txt.gpg

Intended result: Decrypt the file with the creds I have

Result:

Robert: Failed

Mark: Failed

goblin: Failed

Need to look for a AES256 looking key.

"An AES 256-bit key can be expressed as a hexadecimal string with 64 characters. It will require 44 characters in base64." - Some smarter guy on StackExchange

Going to run a dirbuster scan because I am clearly missing something.

2019/10/14 - 13:48

I opened up my OWASP scan again to look over all of the websites responses and I found a strange response from /pumpkin.html

At the bottom of the page's source info I found this:

<!--

59 61 79 21 20 41 70 70 72 65 63 69 61 74 65 20 79 6f 75 72 20 70 61 74 69 65 6e 63 65 20 3a 29 0a 41 6c 6c 20 74 68 69 6e 67 73 20 61
72 65 20 64 69 66 66 69 63 75 6c 74 20 62 65 66 6f 72 65 20 74 68 65 79 20 62 65 63 6f 6d 65 20 65 61 73 79 2e 0a 41 63 6f 72 6e 20 50 75
6d 70 6b 69 6e 20 53 65 65 64 73 20 49 44 3a 20 39 36 34 35 34 0a 0a 44 6f 2c 20 72 65 6d 65 6d 62 65 72 20 74 6f 20 69 6e 66 6f 72 6d 20
4a 61 63 6b 20 74 6f 20 70 6c 61 6e 74 20 61 6c 6c 20 34 20 73 65 65 64 73 20 69 6e 20 74 68 65 20 73 61 6d 65 20 6f 72 64 65 72 2e

-->

Im going through all of the possibilites found on this site: <https://tech.pookey.co.uk/non-wp/encoder-decoder.php>

Here are some interesting results:

Standard MD5 hash: 65580d8cf73187d1c94ad11ec3c52d82

MD5 password hash: \$1\$4b38dcd6\$PCf2Bj/DN6FRpYG0wQPTK0

SHA1 hash: 2885f48cc33a747a357047e1ec9ecf527ede5fba

SHA256 hash: 61e205ade79c763af190c9056e5cebb6f6f1a6223555c9b7b54a278e2c6c5a14

SHA512 hash:

adf9cba87d0f817709608369db40ce613bce08629a3c3d2eb47f73420b64f5cfec8b0cc78a8ae3363ee5969bf08c82d16bcd1f0949c67173016f0a1064e27

These can be the passwords used for the gpg file, im going to try them out:

No luck.

2019/10/14 - 14:10:

Looking at other conversion methods I am dumb and forgot this is hex, running it through hexadecimal to text you get:

”

Yay! Appreciate your patience :)

All things are difficult before they become easy.

Acorn Pumpkin Seeds ID: 96454

Do, remember to inform Jack to plant all 4 seeds in the same order.

”

Well I guess that was a flag? Saving it in creds. Going to use the seed ID as a password for the gpg file:
No luck.