

Ignition

Methodology

Step By Step

- First enumerate to find port 80 open so we know there is a website
- Curl'd the IP and got a 302 code found
- It's brute forcing time, I use gobuster
- Ran my trusty directory buster command
- 302 code prevented this, drats
- Just remembered I have to assign the IP's in Linux, nice
- Added the ip and domain to my hosts now time to brute force it
- Found an admin page in the directories so just going to manually brute force it with common login
- User:admin Pass:qwerty123
- Hacker voice "Im in"
- Found the flag on the admin panel

Walkthrough

Step By Step

Enumeration

nmap -sC -sV -p- -T5 10.129.79.194 -v

```
andrew@jarvis:~$ nmap -sC -sV -p- -T5 10.129.79.194 -v
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-26 22:28 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:28
Completed NSE at 22:28, 0.00s elapsed
Initiating NSE at 22:28
Completed NSE at 22:28, 0.00s elapsed
Initiating NSE at 22:28
Completed NSE at 22:28, 0.00s elapsed
Initiating Ping Scan at 22:28
Scanning 10.129.79.194 [2 ports]
Completed Ping Scan at 22:28, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:28
Completed Parallel DNS resolution of 1 host. at 22:28, 0.01s elapsed
Initiating Connect Scan at 22:28
Scanning 10.129.79.194 [65535 ports]
Discovered open port 80/tcp on 10.129.79.194
Completed Connect Scan at 22:29, 11.59s elapsed (65535 total ports)
Initiating Service scan at 22:29
Scanning 1 service on 10.129.79.194
Completed Service scan at 22:29, 6.57s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.79.194.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.92s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.19s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Nmap scan report for 10.129.79.194
Host is up (0.015s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.14.2
|_http-title: Did not follow redirect to http://ignition.htb/
|_http-methods:
|_ Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.14.2

NSE: Script Post-scanning.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.71 seconds

andrew@jarvis:~$
```

```

—(andrew@jarvis)-[~]
$ curl -v http://10.129.79.194
  Trying 10.129.79.194:80 ...
  Connected to 10.129.79.194 (10.129.79.194) port 80 (#0)
  GET / HTTP/1.1
  Host: 10.129.79.194
  User-Agent: curl/7.85.0
  Accept: */*

  Mark bundle as not supporting multiuse
  HTTP/1.1 302 Found
  Server: nginx/1.14.2
  Date: Thu, 27 Apr 2023 02:34:50 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  Set-Cookie: PHPSESSID=dsbm43jalo79jhe8h9maccuphe; expires=Thu, 27-Apr-2023 03:34:50 GMT; Max-Age=3600; path=/; domain=10.129.79.194; HttpOnly; SameSite=Lax
  Location: http://ignition.htb/
  Pragma: no-cache
  Cache-Control: max-age=0, must-revalidate, no-cache, no-store
  Expires: Wed, 27 Apr 2022 02:34:50 GMT
  Content-Security-Policy-Report-Only: font-src data: 'self' 'unsafe-inline'; form-action secur
  authorize.net test.authorize.net geostag.cardinalcommerce.com geo.cardinalcommerce.com leafst
  g.cardinalcommerce.com leaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com centinel
  bi.cardinalcommerce.com 'self' 'unsafe-inline'; frame-ancestors 'self' 'unsafe-inline'; frame-
  rc fast.amc.demdex.net secure.authorize.net test.authorize.net geostag.cardinalcommerce.com ge
  .cardinalcommerce.com leafstag.cardinalcommerce.com leaf.cardinalcommerce.com centinelapistag.
  cardinalcommerce.com centinelapi.cardinalcommerce.com www.paypal.com www.sandbox.paypal.com pla
  er.vimeo.com *.youtube.com 'self' 'unsafe-inline'; img-src assets.adobedtm.com amcgloba.sc.om
  rdc.net dpm.demdex.net cm.everesttech.net widgets.magentocommerce.com data: www.googleadservic
  s.com www.google-analytics.com www.paypalobjects.com t.paypal.com www.paypal.com fpdbs.paypal.
  om fpdbs.sandbox.paypal.com *.vimeocdn.com i.ytimg.com s.ytimg.com data: 'self' 'unsafe-inline
  ; script-src assets.adobedtm.com secure.authorize.net test.authorize.net www.googleadservices.
  om www.google-analytics.com www.paypalobjects.com js.braintreegateway.com www.paypal.com geost
  g.cardinalcommerce.com leafstag.cardinalcommerce.com geoapi.cardinalcommerce.com leafapi.cardi
  alcommerce.com songbird.cardinalcommerce.com includetest.ccdc02.com www.sandbox.paypal.com t.
  aypal.com s.ytimg.com www.googleapis.com vimeo.com www.vimeo.com *.vimeocdn.com www.youtube.co
  video.google.com 'self' 'unsafe-inline' 'unsafe-eval'; style-src getfirebug.com 'self' 'unsaf
  -inline'; object-src 'self' 'unsafe-inline'; media-src 'self' 'unsafe-inline'; manifest-src 's
  lf' 'unsafe-inline'; connect-src dpm.demdex.net amcgloba.sc.omtrdc.net www.google-analytics.c
  n geostag.cardinalcommerce.com geo.cardinalcommerce.com leafstag.cardinalcommerce.com leaf.car
  inalcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com 'self'
  unsafe-inline'; child-src http: https: blob: 'self' 'unsafe-inline'; default-src 'self' 'unsaf
  -inline' 'unsafe-eval'; base-uri 'self' 'unsafe-inline';
  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block
  X-Frame-Options: SAMEORIGIN

  Connection #0 to host 10.129.79.194 left intact

```

Gobuster originally did not work cause I did not setup the hosts correctly, 2nd screenshot is the correct output

```

(andrew@jarvis)-[~]
$ gobuster dir --url http://10.129.79.194 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.79.194
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php,html
[+] Timeout: 10s
=====
2023/04/26 22:39:58 Starting gobuster in directory enumeration mode
=====
Error: the server returns a status code that matches the provided options for non existing urls
. http://10.129.79.194/752389ba-7204-432a-91fe-13db7df5c6d4 => 302 (Length: 0). To continue please exclude the status code or the length
=====
(andrew@jarvis)-[~]

```

gobuster dir --url <http://ignition.htb/> --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html

```

(andrew@jarvis)-[~]
$ gobuster dir --url http://ignition.htb/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://ignition.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php,html
[+] Timeout: 10s
=====
2023/04/26 22:45:01 Starting gobuster in directory enumeration mode
=====
/index.php (Status: 200) [Size: 25815]
/contact (Status: 200) [Size: 28673]
/home (Status: 200) [Size: 25802]
/media (Status: 301) [Size: 185] [→ http://ignition.htb/media/]
/0 (Status: 200) [Size: 25803]
/catalog (Status: 302) [Size: 0] [→ http://ignition.htb/]
/admin (Status: 200) [Size: 7095]
/static (Status: 301) [Size: 185] [→ http://ignition.htb/static/]
/Home (Status: 301) [Size: 0] [→ http://ignition.htb/home]
/cms (Status: 200) [Size: 25817]
/checkout (Status: 302) [Size: 0] [→ http://ignition.htb/checkout/cart/]
/robots (Status: 200) [Size: 1]
/setup (Status: 301) [Size: 185] [→ http://ignition.htb/setup/]
Progress: 6643 / 262995 (2.53%)

```

🔗 Hacking

📁 CTF

🐧 Kali Linux

🔧 Kali Tools

📄 Kali Docs


🗨️ Kali Forums

🔒 Kali Net-Tools

🔍 Exploit-DB

🔍 Google Hacking DB

🔒 OnSec



DASHBOARD

SALES

CATALOG

CUSTOMERS

MARKETING

CONTENT

REPORTS

STORES

SYSTEM

FIND PARTNERS & EXTENSIONS

⚠️ One or more Indexers are invalid. Make sure your Magento cron job is running.

System Messages: 1

Dashboard

🔍 🔔 3 👤 admin

Scope: All Store Views ?

Reload Data

Advanced Reporting

Congratulations, your flag is: 797d6c988d9dc5865e010b9410f247e0

Go to Advanced Reporting

Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data.

Lifetime Sales

Chart is disabled. To enable the chart, click [here](#).

Revenue

Tax

Shipping

Quantity

€0.00

€0.00

€0.00

0

Average Order

€0.00

Last Orders

We couldn't find any records.

Bestsellers

Most Viewed Products

New Customers


Customers

Last Search Terms

We couldn't find any records.

Top Search Terms

We couldn't find any records.

 Copyright © 2023 Magento Commerce Inc. All rights reserved.

Magento ver. dev-2.4-develop

[Privacy Policy](#) | [Account Activity](#) | [Report an Issue](#)