Universidade do Minho

Mestrado integrado em Engenharia Informática

Ficha 3

Diogo Pinto Ribeiro, A84442

Luís Pedro Barbosa Ferreira, A86265

Segurança de Sistemas Informáticos
4th Year, 1st Semester
Departmento de Informática

November 30, 2020

Contents

1 Abstract

In this report we were given three different IP addresses, 137.74.187.100, 45.33.32.156 and 216.58.215.148, these were used as targets. The main objective proposed was to perform Footprinting on these targets using different tools while documenting what we found. With this tactic we will be able to know who these targets are and get information useful for Penetration Testing.

2 Footprinting

Footprinting consists in someone doing passive(reconnaissance) or active(scanning) information gathering about some target. This enables an attacker to create a near complete profile of an organisation's security posture.

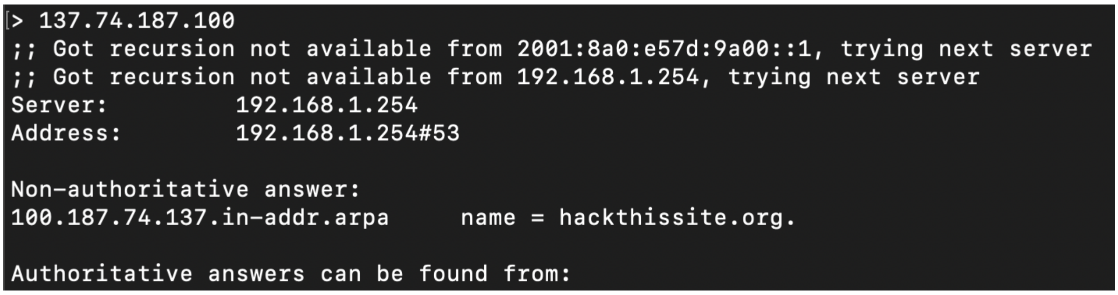
In our case, we will be Footprinting the following systems:

2.1 137.74.187.100

2.1.1 Hacker Target - Reverse DNS & nslookup

Using the Reverse DNS Lookup we were able to know to which domain this address belongs to:

```
137.74.187.100 hackthissite.org
```



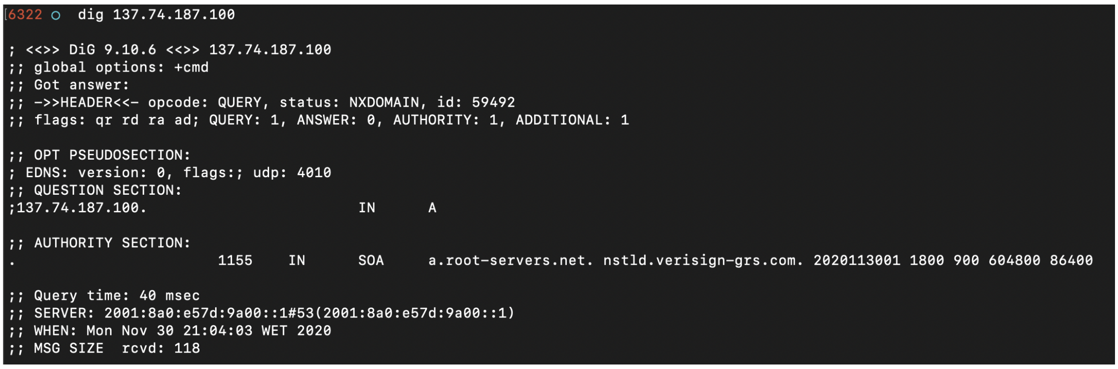
```
[> 137.74.187.100
;; Got recursion not available from 2001:8a0:e57d:9a00::1, trying next server
;; Got recursion not available from 192.168.1.254, trying next server
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
100.187.74.137.in-addr.arpa     name = hackthissite.org.

Authoritative answers can be found from:
```

Figure 1: nslookup result

Using nslookup we were also able to perform a reverse dns search, obtaining a non-authoritative answer with the same result.

2.1.2 dig

Using dig, we can retrieve DNS records related to our targets IP address. By querying dig with our target it returns the following response:



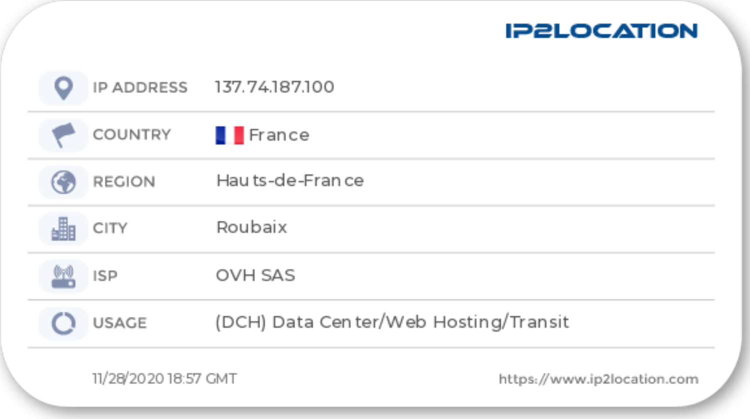
```
[6322 ○  dig 137.74.187.100

; <<>> DiG 9.10.6 <<>> 137.74.187.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59492
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4010
;; QUESTION SECTION:
;137.74.187.100.                        IN      A

;; AUTHORITY SECTION:
.                       1155    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2020113001 1800 900 604800 86400

;; Query time: 40 msec
;; SERVER: 2001:8a0:e57d:9a00::1#53(2001:8a0:e57d:9a00::1)
;; WHEN: Mon Nov 30 21:04:03 WET 2020
;; MSG SIZE  rcvd: 118
```

Figure 2: dig result

In this case, we were able to retrieve a SOA record.

2.1.3 IP2Location.com

Using the IP2Location tool we were able to know exactly where in the world this IP address is located and we can also get a lot of information about its ISP and its ASN number.



IP2LOCATION

IP ADDRESS	137.74.187.100
COUNTRY	France
REGION	Hauts-de-France
CITY	Roubaix
ISP	OVH SAS
USAGE	(DCH) Data Center/Web Hosting/Transit

11/28/2020 18:57 GMT https://www.ip2location.com

Figure 3: IP2Location result

Other information gathered includes:

- City Coordinates: 50°41’39"N 3°10’28"E
- Local Time: 28 Nov, 2020 07:55 PM (UTC +01:00)
- ZIP Code: 59689

- Elevation: 32m
- ASN: 16276 OVH
- Proxy Type: (DCH) Hosting Provider, Data Center or CDN Range

2.1.4 Spyse

Using the Spyse tool we were able to discover open ports and technologies being used with related CVE's as well:

- Open Ports: 80 (uses http protocol) and 443
- Technologies Used: jQuery Ver 1.8.1

There were listed 6 CVE, but the free tier only shows the first 4:

- CVE-2020-11022
- CVE-2020-11023
- CVE-2020-7656
- CVE-2012-6708

2.1.5 nmap

Using the nmap tool we were able to scan ports on the targeted IP, as well as seeing what service is using it. Nmap was only able of doing a guess about possible Operation Systems because the fingerprint wasn't ideal. The command for running nmap with OS detection (-O) and to use the TCP SYN technique (-sS) is:

```
nmap –v –sS –O 137.74.187.100
```

The report that nmap returned gave us information

```
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.040s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
22/tcp   closed ssh
```

```
80/tcp  open   http
443/tcp open   https

Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses:
    - Oracle Virtualbox (98%),
    - QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
```

2.1.6 Shodan

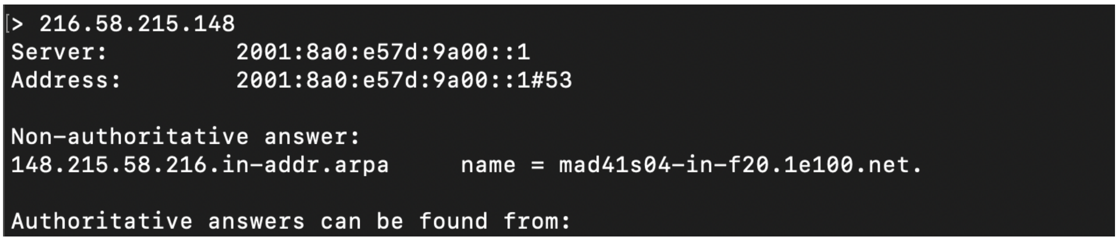
Using the Shodan website we were able to scan ports as before and get information about the SSL certificate. The majority of information that Shodan retrieved we already had uncovered.

2.2 216.58.215.148

2.2.1 Hacker Target - Reverse DNS & nslookup

Using the Reverse DNS Lookup we were able to know to which domain this address belongs to:

```
216.58.215.148 mad41s04-in-f20.1e100.net
```



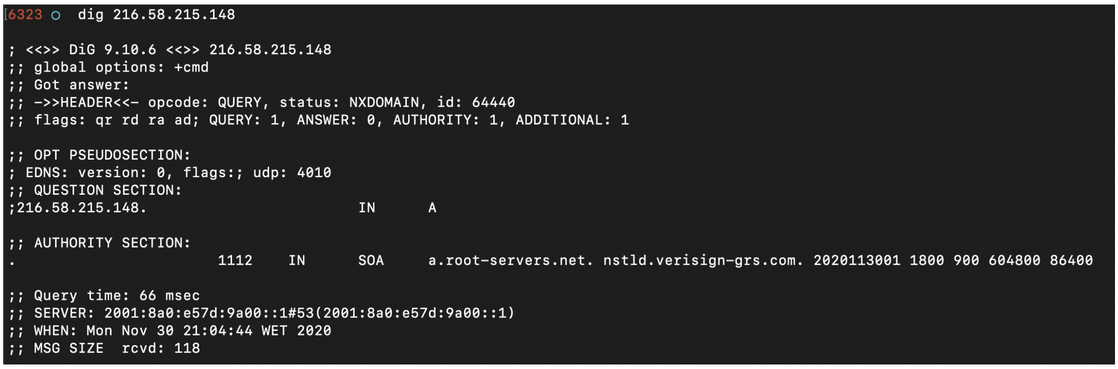
```
[> 216.58.215.148
Server:         2001:8a0:e57d:9a00::1
Address:        2001:8a0:e57d:9a00::1#53

Non-authoritative answer:
148.215.58.216.in-addr.arpa     name = mad41s04-in-f20.1e100.net.

Authoritative answers can be found from:
```

Figure 4: nslookup result

Using nslookup we were also able to perform a reverse dns search, obtaining a non-authoritative answer with the same result.

2.2.2 dig

Using dig, we can retrieve DNS records related to our targets IP address. By querying dig with our target it returns the following response:



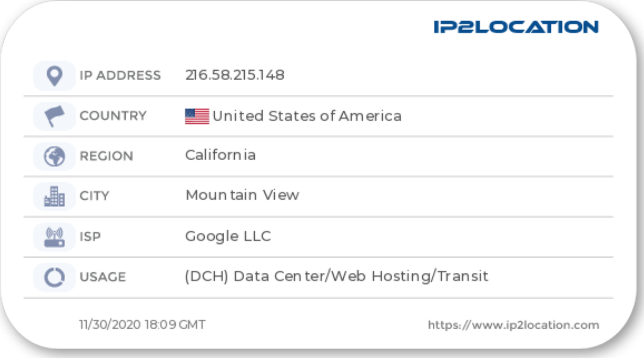
```
[6323 ○  dig 216.58.215.148

; <<>> DiG 9.10.6 <<>> 216.58.215.148
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64440
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4010
;; QUESTION SECTION:
;216.58.215.148.                        IN      A

;; AUTHORITY SECTION:
.                       1112    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2020113001 1800 900 604800 86400

;; Query time: 66 msec
;; SERVER: 2001:8a0:e57d:9a00::1#53(2001:8a0:e57d:9a00::1)
;; WHEN: Mon Nov 30 21:04:44 WET 2020
;; MSG SIZE  rcvd: 118
```

Figure 5: dig result

In this case, we were able to retrieve a SOA record.

2.2.3 IP2Location.com

Using the IP2Location tool we were able to know exactly where in the world this IP address is located and we can also get a lot of information about its ISP and its ASN number.



IP2LOCATION

IP ADDRESS	216.58.215.148
COUNTRY	United States of America
REGION	California
CITY	Mountain View
ISP	Google LLC
USAGE	(DCH) Data Center/Web Hosting/Transit

11/30/2020 18:09 GMT https://www.ip2location.com

Figure 6: IP2Location result

Other information gathered includes:

- City Coordinates: 37°24'22"N 122°4'43"W
- Local 30 Nov, 2020 09:55 AM (UTC -08:00)
- ZIP Code: 94043
- Elevation: 32m
- ASN: 15169 Google
- Proxy Type: (DCH) Hosting Provider, Data Center or CDN Range

2.2.4 Spyse

Using the Spyse tool we were able to discover only open ports, no technologies being used, nor CVE's:

- Open Ports: 80 (uses http protocol) and 443

This site couldn't find any vulnerabilities to the given IP. Awarding a Security Score of 100, meaning it has a low security risk.

2.2.5 nmap

Using the nmap tool we were able to scan ports on the targeted IP, as well as seeing what service is using it. This time, Nmap was able to obtain the Operation System. The command for running nmap with OS detection (-O) and to use the TCP SYN technique (-sS) is:

```
nmap -v -sS -O 216.58.215.14
```

The report that nmap returned gave us information

```
Nmap scan report for fra21s02-in-f14.1e100.net (216.58.215.14)
Host is up (0.0055s latency).
Not shown: 991 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
```

```
110/tcp open  pop3
119/tcp open  nntp
143/tcp open  imap
465/tcp open  smtps
563/tcp open  snews
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
TCP Sequence Prediction: Difficulty=18 (Good luck!)
IP ID Sequence Generation: Incremental
```

2.2.6 Shodan

Using the Shodan website we were able to scan ports as before, get information about the SSL certificate. The majority of information that Shodan retrieved we already had uncovered.

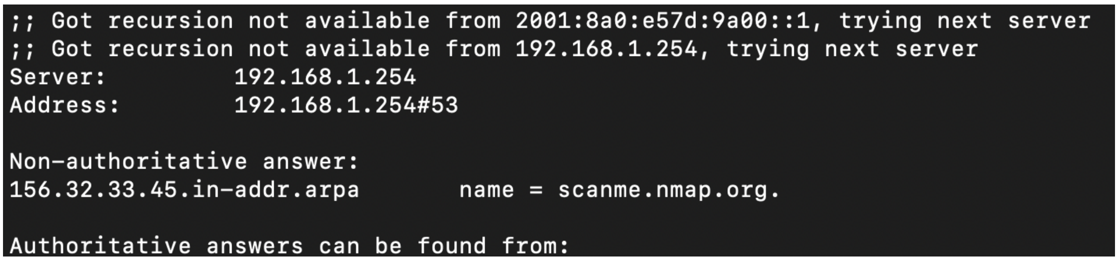
2.3 45.33.32.156

2.3.1 Hacker Target - Reverse DNS & nslookup

Using the Reverse DNS Lookup we were able to know to which domain this address belongs to:

```
45.33.32.156 scanme.nmap.org
```

Using nslookup we were also able to perform a reverse dns search, obtaining a non-authoritative answer with the same result.

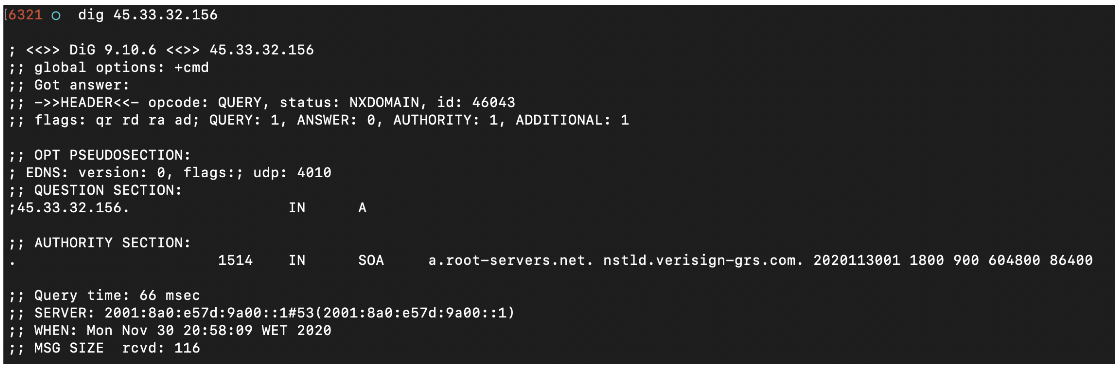


```
;; Got recursion not available from 2001:8a0:e57d:9a00::1, trying next server
;; Got recursion not available from 192.168.1.254, trying next server
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
156.32.33.45.in-addr.arpa       name = scanme.nmap.org.

Authoritative answers can be found from:
```

Figure 7: nslookup result

2.3.2 dig

Using dig, we can retrieve DNS records related to our targets IP address. By querying dig with our target it returns the following response:



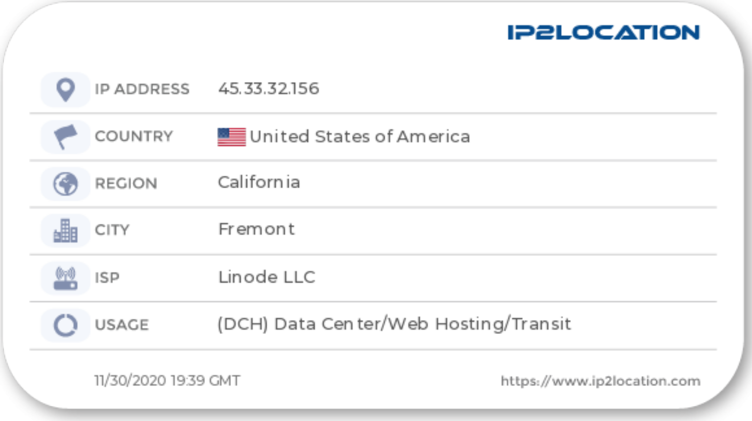
```
[6321 ○  dig 45.33.32.156

; <<>> DiG 9.10.6 <<>> 45.33.32.156
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46043
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4010
;; QUESTION SECTION:
;45.33.32.156.                  IN      A

;; AUTHORITY SECTION:
.                       1514    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2020113001 1800 900 604800 86400

;; Query time: 66 msec
;; SERVER: 2001:8a0:e57d:9a00::1#53(2001:8a0:e57d:9a00::1)
;; WHEN: Mon Nov 30 20:58:09 WET 2020
;; MSG SIZE  rcvd: 116
```

Figure 8: dig result

In this case, we were able to retrieve a SOA record.

2.3.3 IP2Location.com

Using the IP2Location tool we were able to know exactly where in the world this IP address is located and we can also get a lot of information about its ISP and its ASN number.



IP2LOCATION

IP ADDRESS	45.33.32.156
COUNTRY	United States of America
REGION	California
CITY	Fremont
ISP	Linode LLC
USAGE	(DCH) Data Center/Web Hosting/Transit

11/30/2020 19:39 GMT https://www.ip2location.com

Figure 9: IP2Location result

Other information gathered includes:

- City Coordinates: 37°32'54"N 121°59'19"W
- Local Time: 30 Nov, 2020 11:15 AM (UTC -08:00)
- ZIP Code: 94536
- Elevation: 16m
- ASN: 63949 Linode LLC
- Proxy Type: (VPN) VPN Server

2.3.4 Spyse

Using the Spyse tool we were able to discover open ports and technologies being used with related CVE's as well:

- Open Ports: 80 (uses http protocol) and 22
- Technologies Used: Google AdSense, OpenSSH Ver 6.6.1p1 and Apache Ver 2.4.7

There were listed 6 CVE, but the free tier only shows the first 4:

- CVE-2019-0217

- CVE-2016-2161
- CVE-2015-8325
- CVE-2016-3115

We were also able to see the Banners on ports 80 and 22:

```
Port 80:
    HTTP/1.1 200 OK
    Date: Tue, 03 Nov 2020 21:30:32 GMT
    Server: Apache/2.4.7 (Ubuntu)
    Accept-Ranges: bytes
    Vary: Accept-Encoding
    Connection: close
    Content-Type: text/html

Port 22:
    SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
```

2.3.5 nmap

Using the nmap tool we were able to scan ports on the targeted IP, as well as seeing what service is using it. Just like the first IP address, nmap was only able of doing a guess about possible Operation Systems, because the fingerprint wasn't ideal. The command for running nmap with OS detection (-O) and to use the TCP SYN technique (-sS) is:

```
nmap -v -sS -O 45.33.32.156
```

The report that nmap returned gave us information

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Linux 5.0 - 5.4 (96%), Linux 5.4 (95%), Linux
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 15.079 days (since Sun Nov 15 18:01:15 2020)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
```

Using nmap we discovered 2 new open ports and we use it's OS prediction to have a slight idea of the targets OS type(Linux).

2.3.6 Shodan

Using the Shodan website we were able to scan ports as before, including a new one (port 123), get information about the OpenSSH, and we discovered a lot of CVE's. The majority of information that Shodan retrieved we already had uncovered.

3 Conclusions

After performing Footprinting on all of our targets, we were able to extract a lot of sensitive and specific information. From physical information to software versions, every single detail that we got our hands on, could also be used by an attacker to launch an attack. With this report we gained a new insight about the exposure of systems connected to the internet and the dangers of not securing sensitive information.