Tecnologia de Segurança

30 de Novembro de 2020

Ficha 3

a83899	André Morais
a84485	Tiago Magalhães

Testes de Penetração (PenTest)

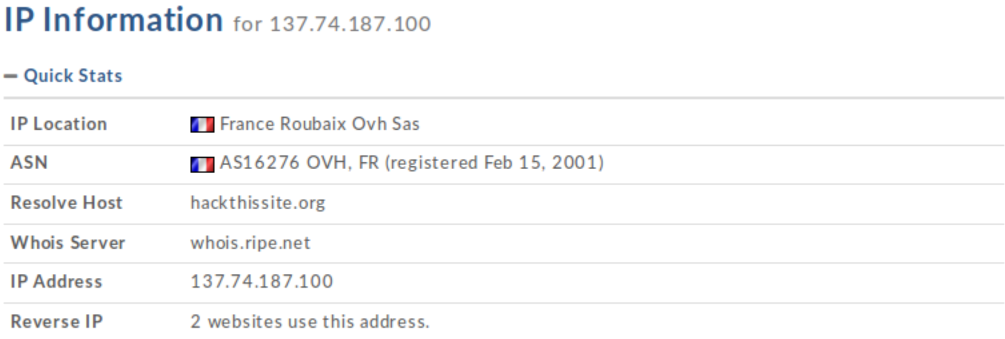
Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1 Teste de Penetração

1.1 Sistema 1 - 137.74.187.100

Como podemos verificar na Figura 1 e 2, o endereço IP pertence a um servidor na França, mais concretamente ao site hackthissite.org, mas nas informações do domínio não nos é revelada nenhuma informação pessoal que possa ser usada a posteriori.

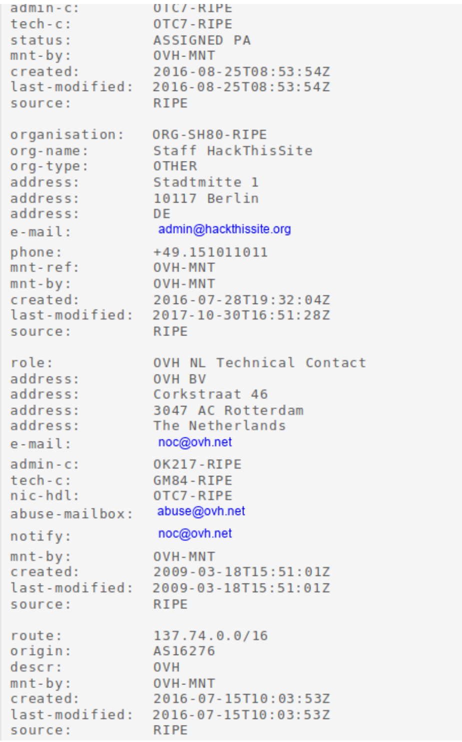


IP Information for 137.74.187.100

— Quick Stats

IP Location	France Roubaix Ovh Sas
ASN	AS16276 OVH, FR (registered Feb 15, 2001)
Resolve Host	hackthissite.org
Whois Server	whois.ripe.net
IP Address	137.74.187.100
Reverse IP	2 websites use this address.

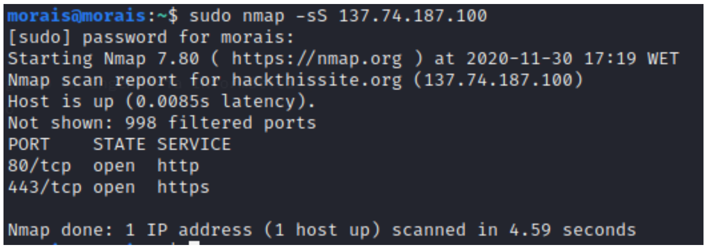
Figura 1



```
admin-c:        OTC7-RIPE
tech-c:         OTC7-RIPE
status:         ASSIGNED PA
mnt-by:         OVH-MNT
created:        2016-08-25T08:53:54Z
last-modified:  2016-08-25T08:53:54Z
source:         RIPE

organisation:   ORG-SH80-RIPE
org-name:       Staff HackThisSite
org-type:       OTHER
address:        Stadtmitte 1
address:        10117 Berlin
address:        DE
e-mail:         admin@hackthissite.org
phone:          +49.151011011
mnt-ref:        OVH-MNT
mnt-by:         OVH-MNT
created:        2016-07-28T19:32:04Z
last-modified:  2017-10-30T16:51:28Z
source:         RIPE

role:           OVH NL Technical Contact
address:        OVH BV
address:        Corkstraat 46
address:        3047 AC Rotterdam
address:        The Netherlands
e-mail:         noc@ovh.net
admin-c:        OK217-RIPE
tech-c:         GM84-RIPE
nic-hdl:        OTC7-RIPE
abuse-mailbox:  abuse@ovh.net
notify:         noc@ovh.net
mnt-by:         OVH-MNT
created:        2009-03-18T15:51:01Z
last-modified:  2009-03-18T15:51:01Z
source:         RIPE

route:          137.74.0.0/16
origin:         AS16276
descr:          OVH
mnt-by:         OVH-MNT
created:        2016-07-15T10:03:53Z
last-modified:  2016-07-15T10:03:53Z
source:         RIPE
```

Figura 2

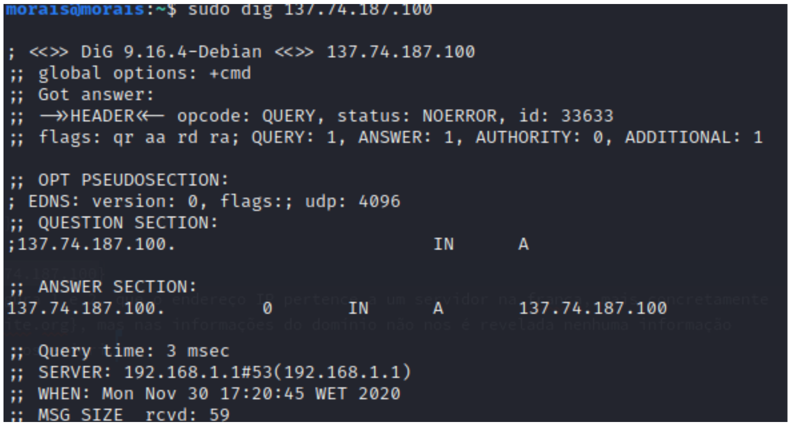
Através de uma ferramenta de *port scanning*, neste caso nmap, conseguimos saber que neste endereço a porta **80(HTTP)** e **443(HTPP)** encontram-se abertas.



```
morais@morais:~$ sudo nmap -sS 137.74.187.100
[sudo] password for morais:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 17:19 WET
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.0085s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds
```

Figura 3

De novo, através do comando ***dig ip*** observamos que este não é um servidor DNS.

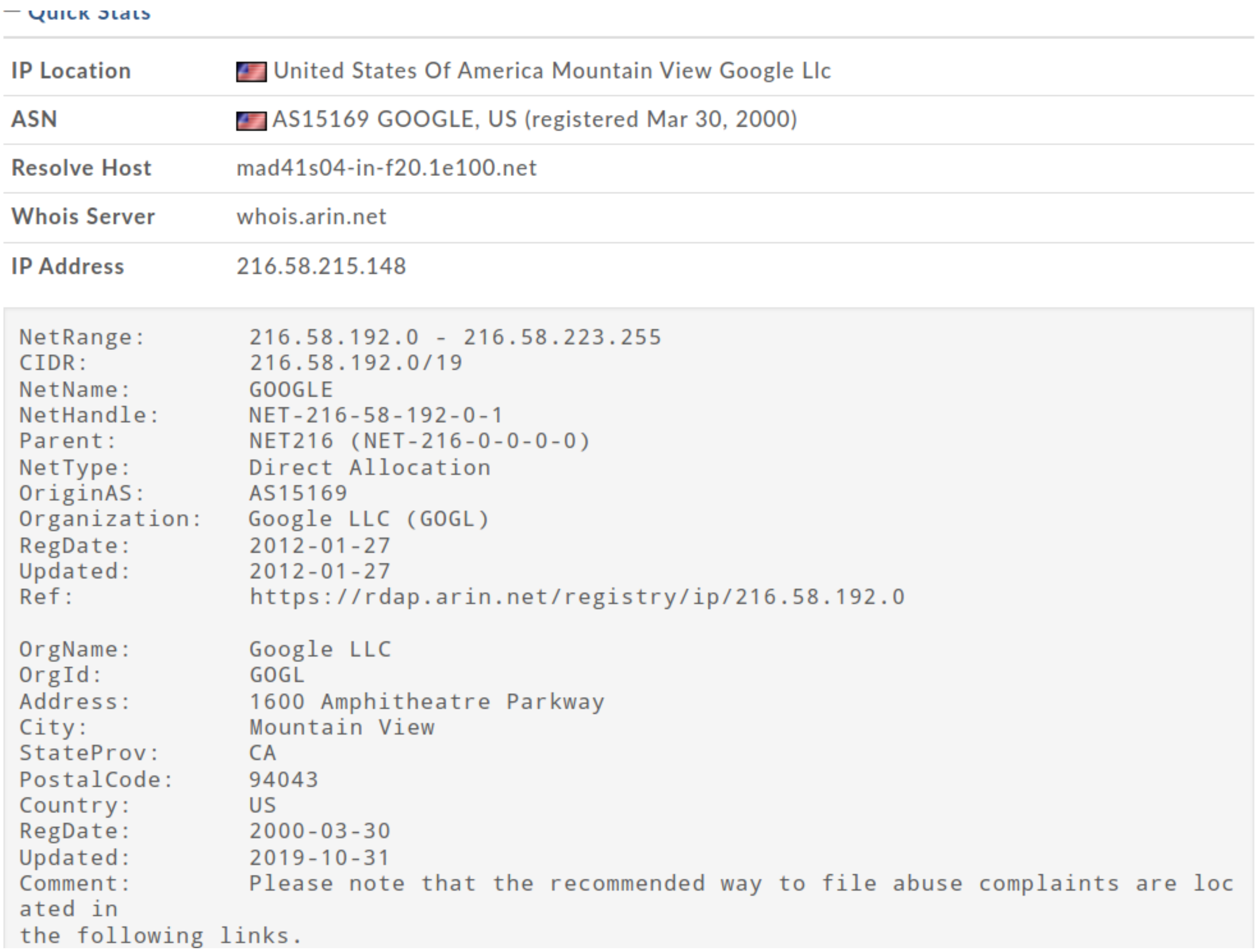


```
morais@morais:~$ sudo dig 137.74.187.100

; <<>> DiG 9.16.4-Debian <<>> 137.74.187.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33633
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;137.74.187.100.                        IN      A

;; ANSWER SECTION:
137.74.187.100.         0       IN      A       137.74.187.100

;; Query time: 3 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Nov 30 17:20:45 WET 2020
;; MSG SIZE  rcvd: 59
```

Figura 4

1.2 Sistema 2 - 216.58.215.148

Podemos ver pelas imagens abaixo que o sistema com o endereço 216.58.215.148, nas informações do domínio não é revelada qualquer informação acerca do responsável, conseguimos concluir que é um endereço pertencente à *google* e que a resolução de nomes é mad41s04-in-f20.1e100.ne .

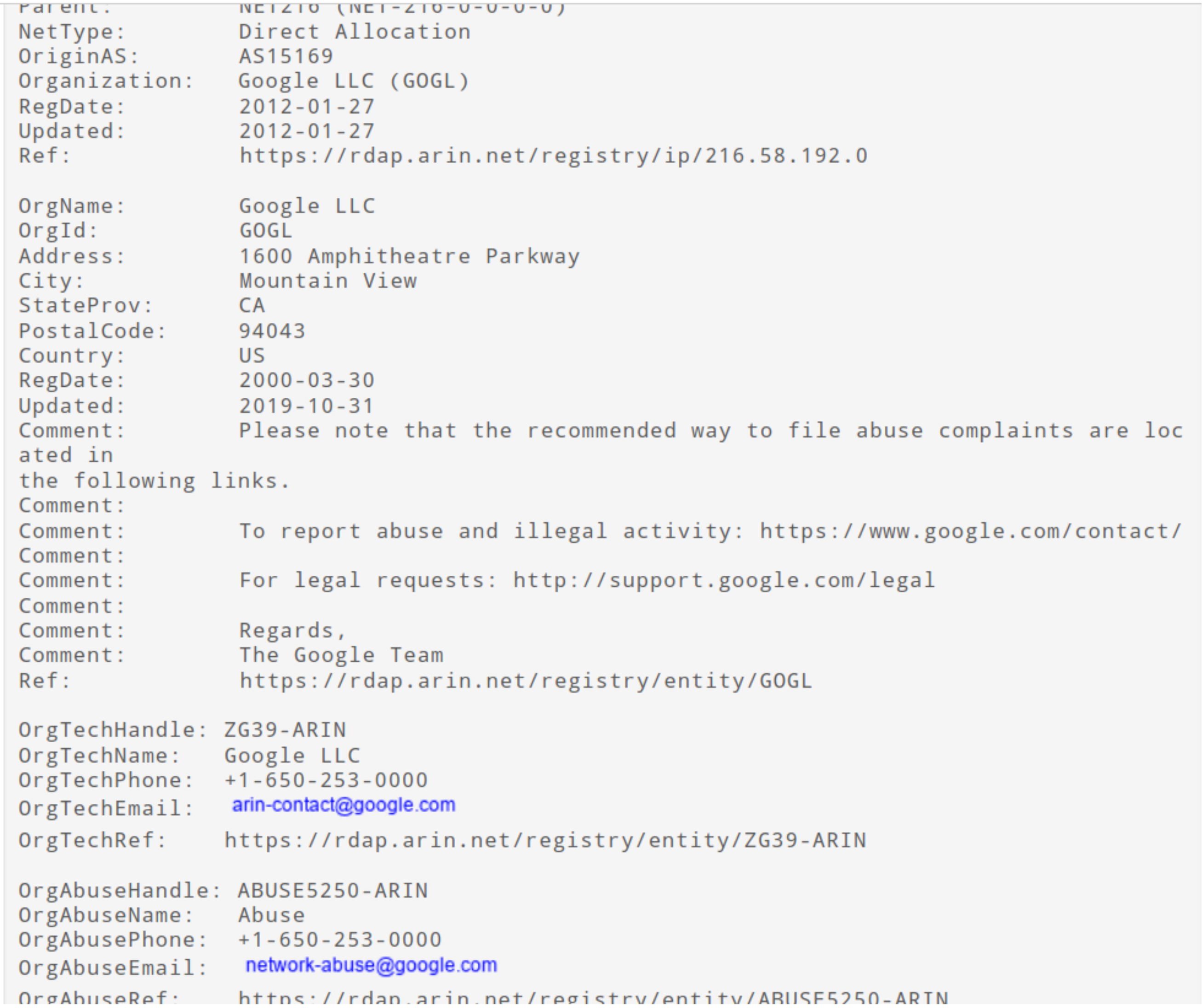


— Quick Stats

IP Location	United States Of America Mountain View Google Llc
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Resolve Host	mad41s04-in-f20.1e100.net
Whois Server	whois.arin.net
IP Address	216.58.215.148

```
NetRange:       216.58.192.0 - 216.58.223.255
CIDR:           216.58.192.0/19
NetName:        GOOGLE
NetHandle:      NET-216-58-192-0-1
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS15169
Organization:   Google LLC (GOGL)
RegDate:        2012-01-27
Updated:        2012-01-27
Ref:            https://rdap.arin.net/registry/ip/216.58.192.0

OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are loc
ated in
the following links.
```

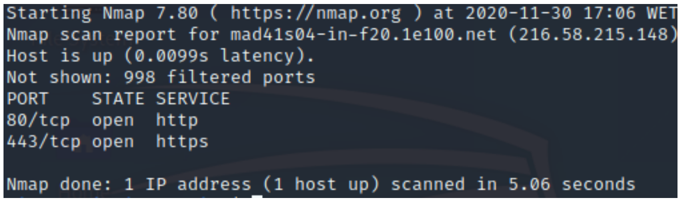
Figura 5



```
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS15169
Organization:   Google LLC (GOGL)
RegDate:        2012-01-27
Updated:        2012-01-27
Ref:            https://rdap.arin.net/registry/ip/216.58.192.0

OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are loc
ated in
the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

Figura 6

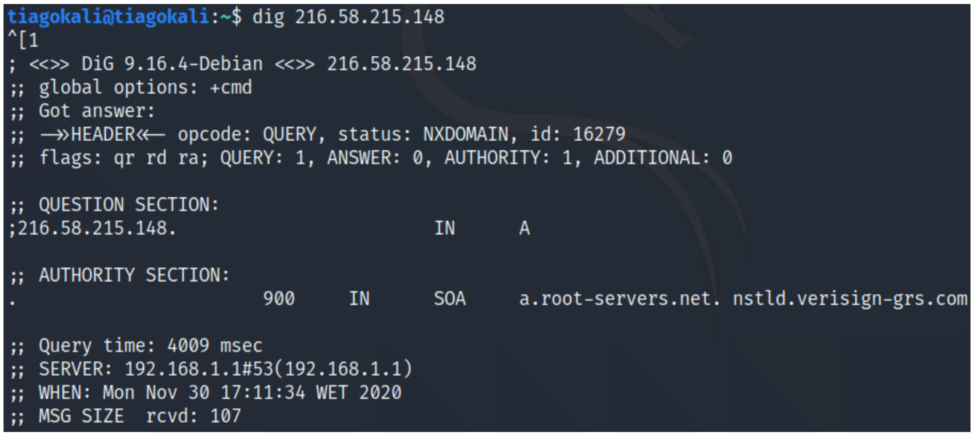
Tal como no sistema anterior, a porta **80** e **443** encontram-se também abertas, o que nos indica que poderá ser um servidor *web*.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 17:06 WET
Nmap scan report for mad41s04-in-f20.1e100.net (216.58.215.148)
Host is up (0.0099s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```

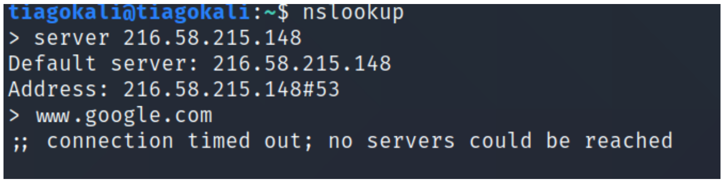
Figura 7

Através do comando ***dig ip*** e ***nslookup***observamos que este é não é um servidor DNS.



```
tiagokali@tiagokali:~$ dig 216.58.215.148
^[1
; <<>> DiG 9.16.4-Debian <<>> 216.58.215.148
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16279
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;216.58.215.148.                        IN      A

;; AUTHORITY SECTION:
.                       900     IN      SOA     a.root-servers.net. nstld.verisign-grs.com

;; Query time: 4009 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Nov 30 17:11:34 WET 2020
;; MSG SIZE  rcvd: 107
```

Figura 8

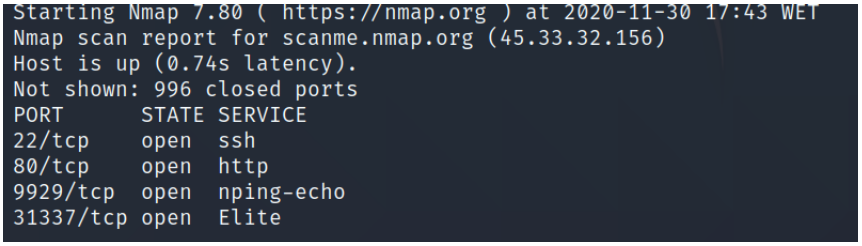


```
tiagokali@tiagokali:~$ nslookup
> server 216.58.215.148
Default server: 216.58.215.148
Address: 216.58.215.148#53
> www.google.com
;; connection timed out; no servers could be reached
```

Figura 9

1.3 Sistema 3 - 45.33.32.156

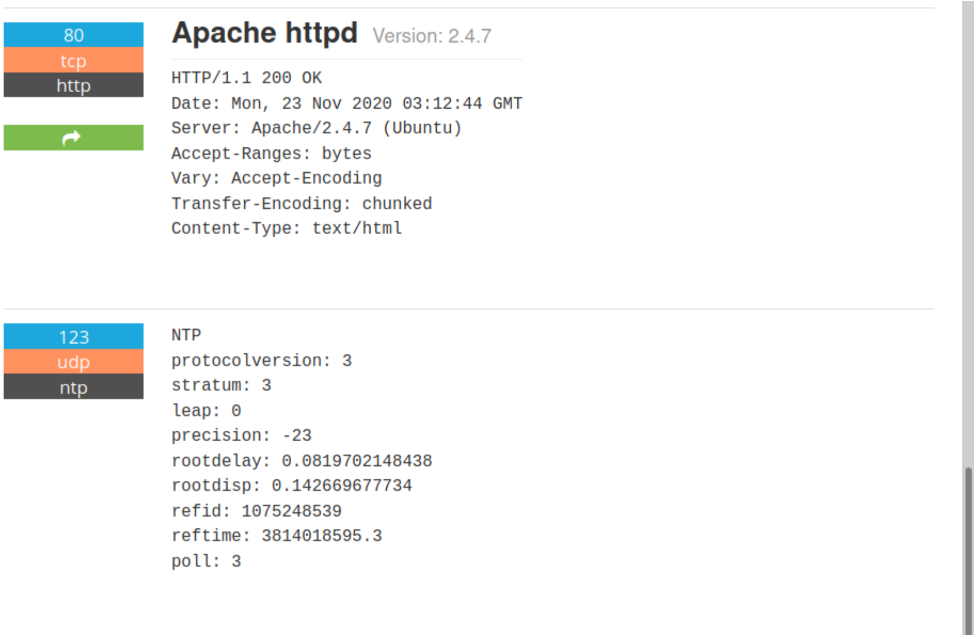
Podemos ver que este sistema tem as portas **22(TCP)**, **80(HTTP)**, **9929(NPING-ECHO)**, **313337(Elite)** abertas.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 17:43 WET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.74s 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
```

Figura 10

Podemos ver pelo site **https://www.shodan.io/** (Figura 11) que o servidor na porta 80 é um apache, bem como as vulnerabilidade associadas (Figura 12).

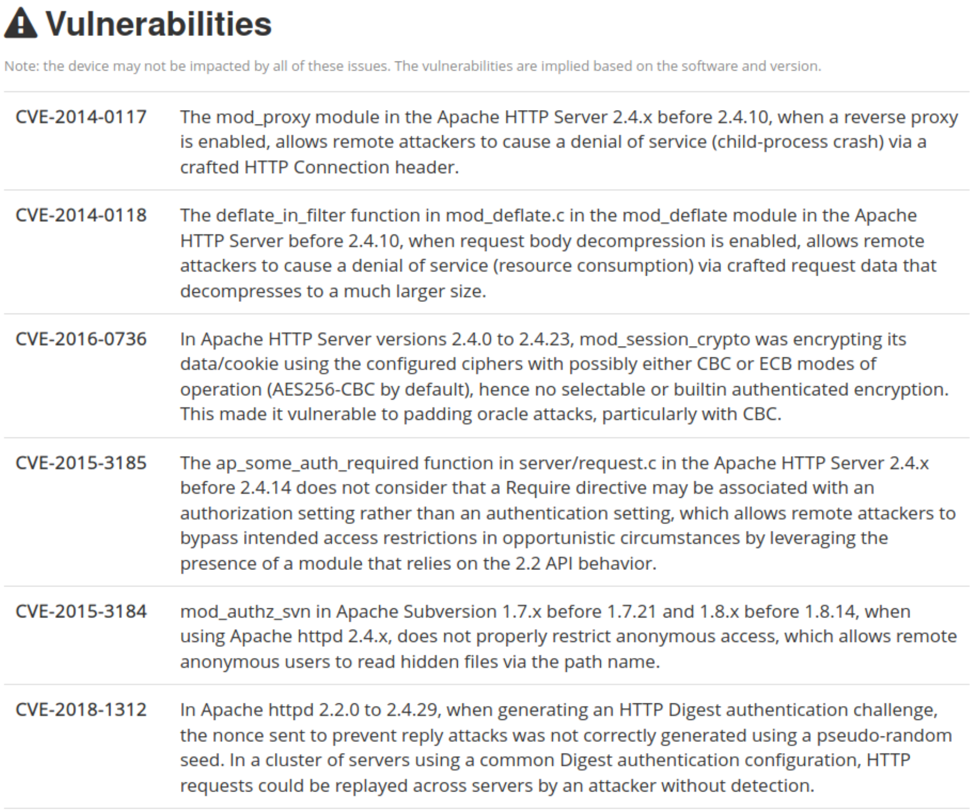


Apache httpd Version: 2.4.7

```
HTTP/1.1 200 OK
Date: Mon, 23 Nov 2020 03:12:44 GMT
Server: Apache/2.4.7 (Ubuntu)
Accept-Ranges: bytes
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html
```

```
NTP
protocolversion: 3
stratum: 3
leap: 0
precision: -23
rootdelay: 0.0819702148438
rootdisp: 0.142669677734
refid: 1075248539
reftime: 3814018595.3
poll: 3
```

Figura 11



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-0117	The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.
CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.
CVE-2015-3184	mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Figura 12

Referências

[1] Domain Tool:
`https://whois.domaintools.com/`

[2] Shodan:
`https://www.shodan.io/`