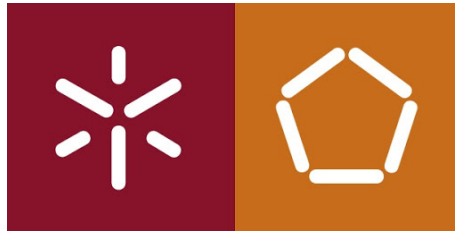


Segurança de Sistemas Informáticos

TPC3
Testes de Penetração (*PenTest*)

a85954 Luís Ribeiro



Mestrado em Engenharia Informática
Universidade do Minho

Conteúdo

1	Sistema 137.74.187.100	3
2	Sistema 216.58.215.148	5
3	Sistema 45.33.32.156	7

1 Sistema 137.74.187.100

Através da *Domain Tools* disponibilizado pela *Whois*, uma das possíveis ferramentas para revelar informações sobre um endereço IP, concluí que este endereço IP está "alocado" num servidor francês, concretamente ao *host* **hackthis-site.org**.

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.

% Abuse contact for '137.74.187.96 - 137.74.187.127' is 'abuse@ovh.net'	
inetnum:	137.74.187.96 - 137.74.187.127
netname:	OVH_113911647
descr:	OVH Static IP
country:	NL
org:	ORG-SH80-RIPE
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:	3947 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 1: Informação sobre o domínio do endereço IP 137.74.187.100

É possível identificar as portas abertas através de ferramentas de *port scanning*, neste caso usei **nmap** com as *flags -sS*, para a identificação de portas associadas ao *TCP three-way handshake*.

Como podemos ver, as portas **80 - HTTP** e **443 - HTTP** encontram-se abertas.

```
(mariolas@kali)-[~]
└─$ sudo nmap -sS 137.74.187.100
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 21:25 WET
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.0084s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Figura 2: 137.74.187.100 *Port Scanning*

A ferramenta **dig** permite identificar se um servidor é **DNS Server**. Com a ajuda do **nslookup** concluímos que não se trata de um servidor DNS.

```
(mariolas@kali)-[~]
└─$ sudo dig 137.74.187.100

;<<>> DIG 0.16.8-Debian <<>> 137.74.187.100
;; global options: +cmd
;; Got answer:
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 26983
;; 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: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: seg nov 30 21:26:54 WET 2020
;; MSG SIZE rcvd: 59
```

Figura 3: Ferramenta *dig*

```
(mariolas@kali)-[~]
└─$ nslookup
> 137.74.187.100
100.187.74.137.in-addr.arpa    name = hackthissite.org.

Authoritative answers can be found from:
187.74.137.in-addr.arpa nameserver = dns16.ovh.net.
187.74.137.in-addr.arpa nameserver = ns16.ovh.net.
ns16.ovh.net      internet address = 213.251.128.135
dns16.ovh.net     internet address = 213.251.188.135
ns16.ovh.net      has AAAA address 2001:41d0:1:1987::1
dns16.ovh.net     has AAAA address 2001:41d0:1:4a87::1
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> 137.74.187.100
100.187.74.137.in-addr.arpa    name = hackthissite.org.

Authoritative answers can be found from:
>
```

Figura 4: Ferramenta *nslookup*

2 Sistema 216.58.215.148

Através da *Domain Tools* disponibilizado pela *Whois*, uma das possíveis ferramentas para revelar informações sobre um endereço IP, apenas conseguimos concluir que é um endereço pertencente à *Google*.



IP Information for 216.58.215.148	
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
<pre>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 located 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</pre>	

Figura 5: Informação sobre o domínio do endereço IP 216.58.215.148

É possível identificar as portas abertas através de ferramentas de *port scanning*, neste caso usei **nmap** com as *flags* **-sS**, para a identificação de portas associadas ao *TCP three-way handshake*.

Como podemos ver, as portas **80 - HTTP** e **443 - HTTP** encontram-se abertas, podendo ser um servidor *Web*.

```
(mariolas@kali)-[~]
└─$ sudo nmap -sS 216.58.215.148
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 22:04 WET
Nmap scan report for mad41s04-in-f20.1e100.net (216.58.215.148)
Host is up (0.0043s 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 5.18 seconds
```

Figura 6: 216.58.215.148 *Port Scanning*

A ferramenta **dig** permite identificar se um servidor é *DNS Server*. Com a ajuda do **nslookup** concluímos que não se trata de um servidor DNS.

```
(mariolas@kali)-[~]
└─$ sudo dig 216.58.215.148

;<>> Dig 9.16.8-Debian <>> 216.58.215.148
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 15539
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;216.58.215.148.                IN      A
;; ANSWER SECTION:
216.58.215.148.                0      IN      A      216.58.215.148

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: seg nov 30 22:05:22 WET 2020
;; MSG SIZE rcvd: 59
```

Figura 7: Ferramenta *dig*

```
(mariolas@kali)-[~]
└─$ nslookup
> 216.58.215.148
148.215.58.216.in-addr.arpa      name = mad41s04-in-f20.1e100.net.

Authoritative answers can be found from:
215.58.216.in-addr.arpa nameserver = ns2.google.com.
215.58.216.in-addr.arpa nameserver = ns4.google.com.
215.58.216.in-addr.arpa nameserver = ns1.google.com.
215.58.216.in-addr.arpa nameserver = ns3.google.com.
ns3.google.com internet address = 216.239.36.10
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns4.google.com internet address = 216.239.38.10
ns3.google.com has AAAA address 2001:4860:4802:36::a
ns1.google.com has AAAA address 2001:4860:4802:32::a
ns2.google.com has AAAA address 2001:4860:4802:34::a
ns4.google.com has AAAA address 2001:4860:4802:38::a
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> 216.58.215.148
148.215.58.216.in-addr.arpa      name = mad41s04-in-f20.1e100.net.

Authoritative answers can be found from:
>
```

Figura 8: Ferramenta *nslookup*

3 Sistema 45.33.32.156

Através da *Domain Tools* disponibilizado pela **Whois**, uma das possíveis ferramentas para revelar informações sobre um endereço IP, podemos ver que se trata de um servidor americano com domínio **scanme.nmap.org**.



IP Information for 45.33.32.156	
— Quick Stats	
IP Location	 United States Of America Fremont Linode Llc
ASN	 AS63949 LINODE-AP Linode, LLC, US (registered Feb 16, 2015)
Resolve Host	scanme.nmap.org
Whois Server	whois.arin.net
IP Address	45.33.32.156
Reverse IP	1 website uses this address.
NetRange:	45.33.0.0 - 45.33.127.255
CIDR:	45.33.0.0/17
NetName:	LINODE-US
NetHandle:	NET-45-33-0-0-1
Parent:	NET45 (NET-45-0-0-0)
NetType:	Direct Allocation
OriginAS:	AS3595, AS21844, AS6939, AS8001
Organization:	Linode (LINOD)
RegDate:	2015-03-20
Updated:	2015-03-20
Comment:	Linode, LLC
Comment:	http://www.linode.com
Ref:	https://rdap.arin.net/registry/ip/45.33.0.0
OrgName:	Linode
OrgId:	LINOD
Address:	249 Arch St
City:	Philadelphia
StateProv:	PA
PostalCode:	19106
Country:	US
RegDate:	2008-04-24
Updated:	2019-06-28
Comment:	http://www.linode.com
Ref:	https://rdap.arin.net/registry/entity/LINOD
OrgAbuseHandle:	LAS12-ARIN
OrgAbuseName:	Linode Abuse Support
OrgAbusePhone:	+1-609-380-7180
OrgAbuseEmail:	abuse@linode.com
OrgAbuseRef:	https://rdap.arin.net/registry/entity/LAS12-ARIN
OrgNOCHandle:	LNO21-ARIN
OrgNOCHandle:	Linode Network Operations
OrgNOCHandle:	+1-609-380-7384
OrgNOCHandle:	support@linode.com
OrgNOCHandle:	https://rdap.arin.net/registry/entity/LNO21-ARIN
OrgTechHandle:	LNO21-ARIN
OrgTechName:	Linode Network Operations
OrgTechPhone:	+1-609-380-7384
OrgTechEmail:	support@linode.com
OrgTechRef:	https://rdap.arin.net/registry/entity/LNO21-ARIN

Figura 9: Informação sobre o domínio do endereço IP 45.33.32.156

A ferramenta **dig** permite identificar se um servidor é *DNS Server*. Com a ajuda do **nslookup** concluímos que não se trata de um servidor DNS.

```
(mariolas@kali)-[~]
$ sudo dig 45.33.32.156

; <<> Dig 9.16.8-Debian <<> 45.33.32.156
;; global options: +cmd
;; Got answer:
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 24888
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;45.33.32.156.                IN      A
;; ANSWER SECTION:
45.33.32.156.                0      IN      A      45.33.32.156

;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ter dez 01 03:23:32 WET 2020
;; MSG SIZE rcvd: 57
```

Figura 10: Ferramenta *dig*

```
(mariolas@kali)-[~]
$ nslookup
> 45.33.32.156
156.32.33.45.in-addr.arpa      name = scanme.nmap.org.

Authoritative answers can be found from:
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> 45.33.32.156
156.32.33.45.in-addr.arpa      name = scanme.nmap.org.

Authoritative answers can be found from:
>
```

Figura 11: Ferramenta *nslookup*