Ficha 3
Tecnologia de Segurança

Ana Margarida Campos A85166
Nuno Pereira PG42846

30 de Outubro de 2020

Nesta ficha prática são nos forneceidos três endereços IP e o objetivo é descobrir, a partir de técnicas e ferramentas apresentadas na aula, os sistemas hospedados nesses endereços. Para tal recorremos à téncica de *Footprinting*.

Footprinting consiste num método de recolha passiva (reconhecimento) ou ativa (*scanning*) de informações sobre um determinado alvo. Permite que um atacante crie um perfil quase completo do sistema de segurança da organização.

As técnicas e ferramentas que usamos nesta ficha prática para a fase de reconhecimento do *Footprinting* são:

- **whois**: é um protocolo de consulta e resposta baseado em TCP que é normalmente usado para fornecer serviços de informação aos utilizadores. Retorna informações sobre os nomes de domínio registados, um bloco de endereços IP, servidores de nomes e mais informações relativas ao domínio;
- **WayBackMachine**: é uma biblioteca digital que contém sites da Internet e outros artefactos culturais em formato digital;
- **host**: este comando é utilizado para encontrar o endereço IP de um domínio particular;
- **nslookup**: é uma ferramenta utilizada para se obter informações sobre registos de DNS de um determinado domínio, host ou ip.

Na parte de *Scanning* do *Footprinting* foi utilizado nomeadamente o comando *nmap* com as suas variências:

- **nmap -sS**: é um *security scanner* que neste caso comunica a partir da comunicação TCP e usa *TCP three-way handshake* para identificar portas abertas;
- **nmap -O**: dá as versões dos sistemas operativos o que faz com que os falsos positivos sejam reduzidos porque sabemos que uma dada versão do sistema operativo tem determinadas vulnerabilidades;

De seguida são apresentados os endereços e os dados obtidos relativos aos mesmos através da análise de *Footprinting*.

137.74.187.100

Primeiramente, de maneira a decobrir qual o sistema associado a este endereço, recorreu-se ao comando *nmap -sS 137.74.187.100*.

```
margarida@Kali:~$ sudo nmap -sS 137.74.187.100
[sudo] senha para margarida:
Enganou-se, tente de novo.
[sudo] senha para margarida:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-27 09:37 WET
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.058s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp open   https
```

Figura 1: nmap -sS 137.74.187.100

De modo a confirmar que o endereço associado a *hackthissite.org* era o 137.74.187.100 ,foi utilizado o comando host:

```
np@np:~$ host hackthissite.org
hackthissite.org has address 137.74.187.100
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:100
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:104
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:103
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:101
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:102
hackthissite.org mail is handled by 30 aspmx5.googlemail.com.
hackthissite.org mail is handled by 10 aspmx.l.google.com.
hackthissite.org mail is handled by 20 alt1.aspmx.l.google.com.
hackthissite.org mail is handled by 20 alt2.aspmx.l.google.com.
hackthissite.org mail is handled by 30 aspmx2.googlemail.com.
hackthissite.org mail is handled by 30 aspmx3.googlemail.com.
hackthissite.org mail is handled by 30 aspmx4.googlemail.com.
```

Figura 2: host hackthissite.org

Após descobrir qual o domínio, *hackthissite.org*, foi utilizado o comando *whois* para obter variadas informações. Conseguimos obter informações como datas de criação, de atualizações, de expiração, o endereço de email, o contacto telefónico, os nomes de servidores e outras informações pretinentes. O resultado é visível na figura seguinte:

```
margarida@Kali:~$ whois hackthissite.org
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2020-07-12T08:05:03Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2021-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Data Protected
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2020-11-27T09:38:47Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of
a domain name registration record in the Public Interest Registry registry database. The data in this record is pr
ovided by Public Interest Registry for informational purposes only, and Public Interest Registry does not guarante
e its accuracy. This service is intended only for query-based access. You agree that you will use this data only f
or lawful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise supp
ort the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitatio
ns to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, elect
ronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Afilias except as r
easonably necessary to register domain names or modify existing registrations. All rights reserved. Public Interes
t Registry reserves the right to modify these terms at any time. By submitting this query, you agree to abide by t
his policy.

The Registrar of Record identified in this output may have an RDDS service that can be queried for additional info
rmation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
```

Figura 3: whois hackthissite.org

Para acrescentar mais informação no que toca à fase de reconhecimento, recorremos ao arquivo da Internet *WayBackMachine* onde nos mostra, através da visualização de calendários, o número de vezes que o *hackthissite.org* foi rastreado pela Wayback Machine.

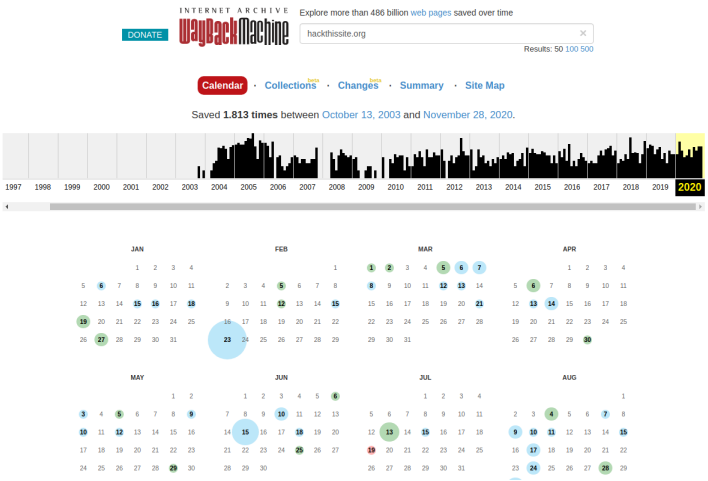

Figura 4: Utilização de *WayBackMachine*

Seguidamente utilizou-se o comando nslookup para obter informações sobre registos de DNS:

```
np@np:~$ nslookup hackthissite.org
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   hackthissite.org
Address: 137.74.187.100
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:100
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:104
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:102
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:103
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:101
```

Figura 5: nslookup hackthissite.org

Por último, utilizou-se o comando *nmap -o 137.74.187.100* para descobrir quais os sistemas operativos e os servidores associados ao mesmo.

```
np@np:~$ sudo nmap -O 137.74.187.100
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-29 10:01 WET
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.022s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Network
s BayStack 450 switch (software version 3.1.0.22) (88%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds
np@np:~$
```

Figura 6: nmap -O 137.74.187.100

256.58.215.148

De forma a decobrir qual o sistema associado a este endereço, recorreu-se ao comando *nmap -sS 256.58.215.148*. O domínio associado a este endereço é o *mad41.s04-in-f20.1e100.net*.

```
np@np:~$ sudo nmap -sS 216.58.215.148
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-29 10:29 WET
Nmap scan report for mad41s04-in-f20.1e100.net (216.58.215.148)
Host is up (0.0049s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

Figura 7: nmap -sS 256.58.215.148

De modo a confirmar que o endereço associado a *mad41.s04-in-f20.1e100.net* era o 256.58.215.148,foi utilizado o comando host:

```
margarida@Kali:~$ host mad41s04-in-f20.1e100.net
mad41s04-in-f20.1e100.net has address 216.58.215.148
```

Figura 8: host mad41.s04-in-f20.1e100.net

De modo a retirar informações específicas como contactos ou servidores, foi utilizado o comando *whois*. No entanto a utilização deste comando não teve sucesso uma vez que não deu nenhum *match*. O mesmo aconteceu ao recorrer ao *WayBackMachine*.

```
margarida@Kali:~$ whois mad41s04-in-f20.1e100.net
No match for "MAD41S04-IN-F20.1E100.NET".
```

Figura 9: whois mad41.s04-in-f20.1e100.net

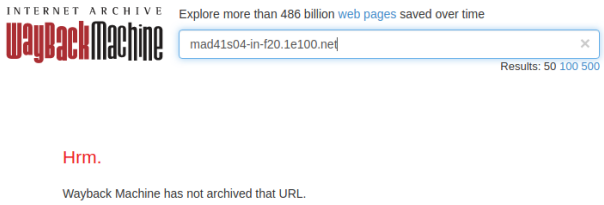

Figura 10: *WayBackMachine* mad41.s04-in-f20.1e100.net

Seguidamente utilizou-se o comando nslookup para tentar obter informações sobre registos de DNS:

```
np@pop-os:~/Desktop$ sudo nslookup mad41s04-in-f20.1e100.net.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mad41s04-in-f20.1e100.net
Address: 216.58.215.148
```

Figura 11: nslookup mad41.s04-in-f20.1e100.net

Por último, utilizou-se o comando *nmap -O 256.58.215.148* para descobrir quais os sistemas operativos e os servidores associados ao mesmo. Como é possível verificar na imagem seguinte não conseguimos obter resposta.

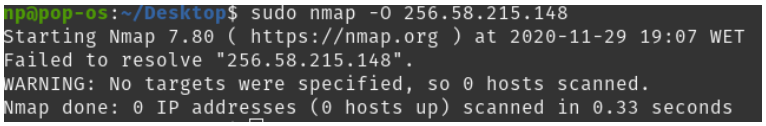

Figura 12: nmap -O 256.58.215.148

45.33.32.156

De forma a decobrir qual o sistema associado a este endereço, recorreu-se ao comando *nmap -sS 45.33.32.156*. O domínio associado é *scanme.nmap.org*.

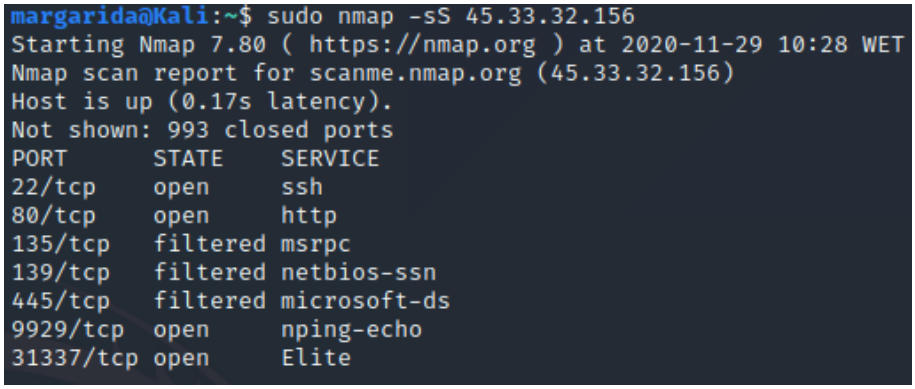

Figura 13: nmap -sS 45.33.32.156

De modo a confirmar que o endereço associado a *scanme.nmap.org* é o 45.33.32.156 ,foi utilizado o comando host:

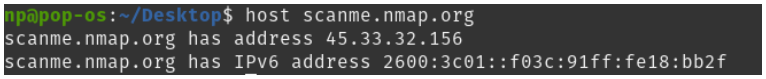

Figura 14: host scanme.nmap.org

Para tentar obter várias informações sobre este domínio foi usado o comando *whois scanme.nmap.org* mas este não teve sucesso.

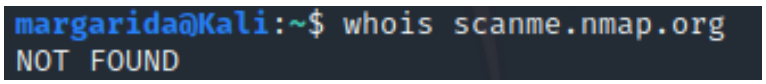

Figura 15: whois scanme.nmap.org

Recorremos ao arquivo da Internet *WayBackMachine* onde nos mostra, através da visualização de calendários, o número de vezes que o domínio *scanme.nmap.org* foi rastreado pela Wayback Machine.

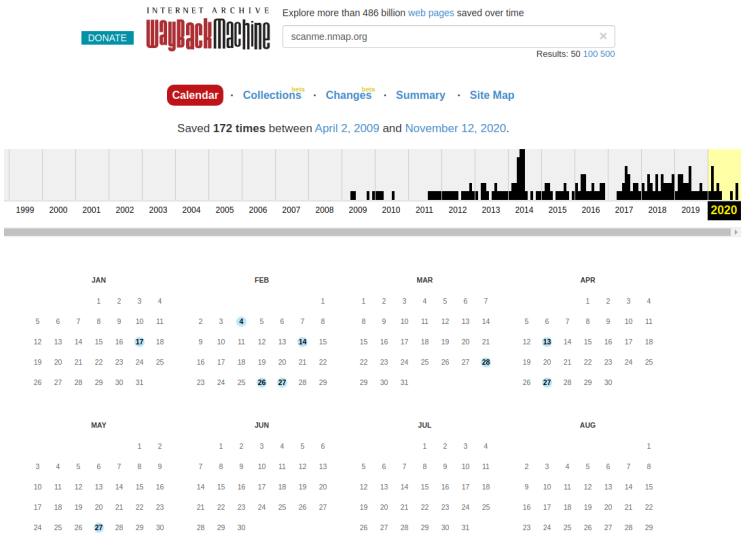

Figura 16: Utilização de *WayBackMachine*

Seguidamente utilizou-se o comando nslookup para tentar obter informações sobre registos de DNS:

```
margarida@Kali:~$ nslookup scanme.nmap.org
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   scanme.nmap.org
Address: 45.33.32.156
Name:   scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
```

Figura 17: nmap -sS 45.33.32.156

Por último, utilizou-se o comando *nmap -O 45.33.32.156* para descobrir quais os sistemas operativos e os servidores associados ao mesmo.

```
ap@pop-os:~/Desktop$ sudo nmap -O 45.33.32.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-29 19:39 WET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s 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 2.6.32 - 3.13 (96%), Linux 2.6.22 - 2.6.36 (95%), Linux 3.10 -
4.11 (95%), Linux 3.10 (94%), Linux 2.6.32 (94%), Linux 3.2 - 4.9 (94%), Linux 2.6.32 - 3.10
 (93%), HP P2000 G3 NAS device (93%), Linux 2.6.18 (93%), Linux 3.16 - 4.6 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.21 seconds
```

Figura 18: nmap -O 45.33.32.156