



Universidade do Minho
Escola de Engenharia

Universidade do Minho
Mestrado Integrado em Engenharia Informática

SSI

Segurança de Sistemas Informáticos

Trabalho Prático 2

Novembro 2020

Tânia Filipa Amorim Rocha
A85176

Maria Miguel Albuquerque Regueiras
A85242

Conteúdo

1	Introdução	3
2	Pentesting - <i>Footprinting</i>	3
3	Reconnaissance	3
3.1	Endereço 137.74.187.100	4
3.2	Endereço 216.58.215.148	7
3.3	Endereço 45.33.32.156	8
4	Scanning	9
4.1	Endereço 137.74.187.100	10
4.2	Endereço 216.58.215.148	11
4.3	Endereço 45.33.32.156	12
5	Conclusão	14

Lista de Figuras

1	Ciclo de Pentesting	3
2	Resultados do comando <i>host</i> para o endereço 137.74.187.100	4
3	Resultados do WHOIS para o endereço 137.74.187.100	5
4	Resultados da pesquisa de 137.74.187.100 no site WayBack Machine	6
5	Primeira e última captura	6
6	Resultados do comando <i>host</i> para o endereço 216.58.215.148	7
7	Resultados do WHOIS para o endereço 216.58.215.148	7
8	Resultados da pesquisa de 216.58.215.148 no site WayBack Machine	8
9	Resultados do comando <i>host</i> para o endereço 45.33.32.156	8
10	Resultados do WHOIS para o endereço 45.33.32.156	8
11	Resultados da pesquisa de 45.33.32.156 no site WayBack Machine	9
12	Primeira e última captura	9
13	Resultados do nmap -O para o endereço 137.74.187.100	10
14	Resultados do nmap -sA para o endereço 137.74.187.100	10
15	Resultados do nmap -sV para o endereço 137.74.187.100	11
16	Resultados do nmap -O para o endereço 216.58.215.148	11
17	Resultados do nmap -sN para o endereço 216.58.215.148	11
18	Resultados do nmap -sV para o endereço 216.58.215.148	12
19	Resultados do nmap -O para o endereço 45.33.32.156	13
20	Resultados do nmap -sX para o endereço 45.33.32.156	13
21	Resultados do nmap -A -T4 para o endereço 45.33.32.156	13

1 Introdução

Neste relatório apresenta-se a realização de *footprinting* de 3 sistemas hospedados em certos endereços (definidos pelos docentes).

Primeiramente, será explicado brevemente o que é *footprinting* e a sua utilidade, seguida da explicação dos seus passos. Por fim, serão apresentados os resultados da análise dos 3 endereços fornecidos, acompanhados pelas várias formas e técnicas utilizadas, e as nossas conclusões.

2 Pentesting - *Footprinting*

Pentesting (ou, em português, teste de intrusão) é uma simulação de um ataque intrusivo a um sistema como tentativa de explorar e identificar que vulnerabilidades e falhas este tenha. Esta técnica torna-se muito útil para desenvolver sistemas mais robustos e seguros contra possíveis ataques. Na figura 1 encontra-se o ciclo que representa o funcionamento de um teste de intrusão.

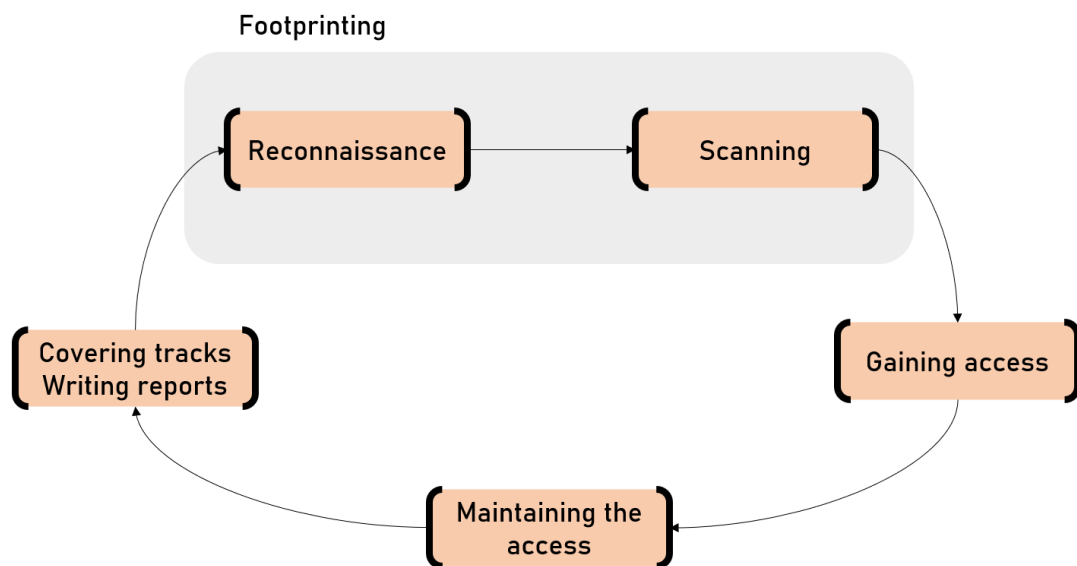


Figura 1: Ciclo de Pentesting

A primeira fase de um teste de intrusão chama-se de *footprinting* e passa por recolher informação sobre o sistema alvo. Esta pode ser dividida em duas partes: **Reconnaissance** e **Scanning**.

3 Reconnaissance

Para a fase de Reconnaissance, foram utilizadas várias ferramentas a fim de encontrar informação relacionada com os endereços em causa. Neste caso, não foi possível retirar informações de forma interna pois, obviamente, não conseguimos estar dentro das organizações em causa. As ferramentas são:

- **host**: comando do terminal que dado um endereço dá informações sobre este.
- **WHOIS**: protocolo de consulta orientado a transações baseadas em TCP. Este é utilizado como fonte de informação sobre endereços. Embora originalmente usado para fornecer informações sobre nomes de domínio registados, atualmente oferece um leque de serviços de informação.
- **WayBack Machine**: arquivo que contém informações sobre sites ao longo dos anos.

Nas secções seguintes apresenta-se a análise feita com ferramentas mencionadas aos endereços indicados.

3.1 Endereço 137.74.187.100

- *host*

Pelo comando *host* com o endereço 137.74.187.100 obtemos o nome associado a este (hackthissite.org.).

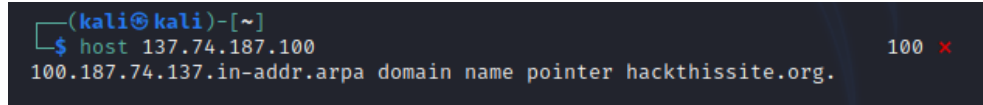
A terminal window with a dark background. The prompt is '(kali㉿kali)-[~]'. The command '\$ host 137.74.187.100' has been entered. The output is '100.187.74.137.in-addr.arpa domain name pointer hackthissite.org.' in green text. In the top right corner, there is a red '100' and a red 'x'.

Figura 2: Resultados do comando *host* para o endereço 137.74.187.100

- WHOIS

Em relação aos resultados do whois, como se pode observar pela figura 3, existe um leque de campos. No entanto, podemos retirar apenas as informações que considerarmos mais relevantes. Neste caso, para este endereço, obtiveram-se resultados extensos e bem detalhados. No entanto, os mais relevantes passam pela identificação da sua localização (Berlim e respetiva morada), o nome da organização (HackThisSite), número de telefone, datas de modificações, emails, etc.

Junto com algumas informações sobre o registo do domínio, é também possível observar os nameServers que estão neste domínio. Os nameServers basicamente informam onde os registos DNS de um domínio são armazenados. Frequentemente, mas nem sempre, isso também pode indicar em qual empresa o domínio está hospedado, já que muitas pessoas optam por manter seus registos DNS e registos de hospedagem juntos.

```
NetRange:      137.74.0.0 - 137.74.255.255
CIDR:          137.74.0.0/16
NetName:       RIPE
NetHandle:     NET-137-74-0-0-1
Parent:        NET137 (NET-137-0-0-0-0)
NetType:       Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:  RIPE Network Coordination Centre (RIPE)
RegDate:       2016-08-29
Updated:       2016-08-29
Ref:           https://rdap.arin.net/registry/ip/137.74.0.0

OrgName:       RIPE Network Coordination Centre
OrgId:         RIPE
Address:       P.O. Box 10096
City:          Amsterdam
StateProv:
PostalCode:    1001EB
Country:       NL
RegDate:
Updated:       2013-07-29
Ref:           https://rdap.arin.net/registry/entity/RIPE

ReferralServer: whois://whois.ripe.net
ResourceLink:   https://apps.db.ripe.net/search/query.html

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName:   Abuse Contact
OrgAbusePhone:   +31205354444
OrgAbuseEmail:   abuse@ripe.net
OrgAbuseRef:     https://rdap.arin.net/registry/entity/ABUSE3850-ARIN

OrgTechHandle:  RNO29-ARIN
OrgTechName:    RIPE NCC Operations
OrgTechPhone:   +31 20 535 4444
OrgTechEmail:   hostmaster@ripe.net
OrgTechRef:     https://rdap.arin.net/registry/entity/RNO29-ARIN

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '137.74.187.96 - 137.74.187.127'

% 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
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 # Filtered

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

% Information related to '137.74.0.0/16AS16276'

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

% This query was served by the RIPE Database Query Service version 1.98 (BL AARKOP)
```

Figura 3: Resultados do WHOIS para o endereço 137.74.187.100

- WayBack Machine

O site WayBack Machine permite realizar várias pesquisas. Neste caso pesquisou-se pelo nome associado ao endereço na barra de pesquisa e obteve-se o resultado da figura 4. Aqui observa-se o fluxo de capturas feitas ao longo dos anos ao site em causa.

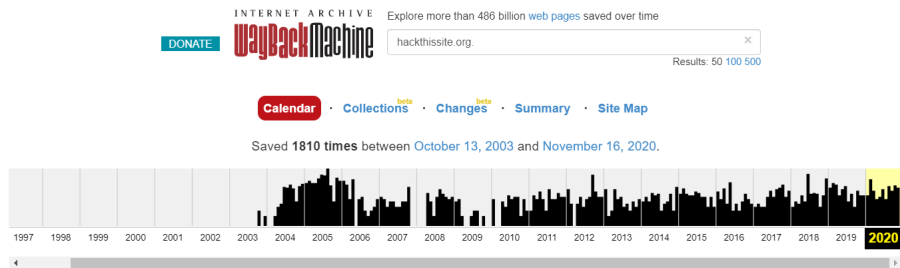


Figura 4: Resultados da pesquisa de 137.74.187.100 no site WayBack Machine

Para além disso, explorou-se a primeira captura realizada e a mais recente (até à data) e obtiveram-se os seguintes resultados:



Figura 5: Primeira e última captura

Deste modo é possível procurar por vulnerabilidades numa página web que poderiam não existir na página actual ou a ter acesso a informação que já não está disponível.

3.2 Endereço 216.58.215.148

- *host*

Ao efetuar o comando *host* neste link é obtido o nome do site em questão.

```
(kali@kali)-[~]  
$ host 216.58.215.148  
148.215.58.216.in-addr.arpa domain name pointer mad41s04-in-f20.1e100.net. 1 x
```

Figura 6: Resultados do comando *host* para o endereço 216.58.215.148

- WHOIS

De forma semelhante ao link anterior, quando é efetuado o comando *whois* para o mesmo é devolvido um output com varias informações desde sobre o proprio *whois* até ao nome da organização, IDs, endereços físicos etc.

```
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 complain  
ts are located in the following links.  
Comment:  
Comment: To report abuse and illegal activity: https://www.google.co  
m/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 7: Resultados do WHOIS para o endereço 216.58.215.148

- WayBack Machine

No caso deste endereço, não se obteve nenhum resultado no site WayBack Machine.



Hrm.

Wayback Machine has not archived that URL.
Click here to search for all archived pages under <http://mad41s04-in-f20.1e100.net/>

Figura 8: Resultados da pesquisa de 216.58.215.148 no site WayBack Machine

3.3 Endereço 45.33.32.156

- *host*

Através do comando *host* foi possível obter o nome do website que é *scanme.nmap.org*.

```
(kali㉿kali)-[~]
$ host 45.33.32.156
156.32.33.45.in-addr.arpa domain name pointer scanme.nmap.org.
```

Figura 9: Resultados do comando *host* para o endereço 45.33.32.156

- WHOIS

Através do comando *whois* é novamente obtido output com varia informações relativamente ao website nomeadamente nome e id da organização, onde se encontra sediada, números e emails de contacto etc.

```
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-45-0-0-0-0)
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

OrgNOCHandle: LNO21-ARIN
OrgNOCName: Linode Network Operations
OrgNOCPhone: +1-609-380-7304
OrgNOCEmail: support@linode.com
OrgNOCRef: https://rdap.arin.net/registry/entity/LNO21-ARIN

OrgAbuseHandle: LAS12-ARIN
OrgAbuseName: Linode Abuse Support
OrgAbusePhone: +1-609-380-7100
OrgAbuseEmail: abuse@linode.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/LAS12-ARIN

OrgTechHandle: LNO21-ARIN
OrgTechName: Linode Network Operations
OrgTechPhone: +1-609-380-7304
OrgTechEmail: support@linode.com
OrgTechRef: https://rdap.arin.net/registry/entity/LNO21-ARIN
```

Figura 10: Resultados do WHOIS para o endereço 45.33.32.156

- **WayBack Machine**

Semelhante ao primeiro link, este quando é procurado no WayBackMachine tem vários registos em diferentes alturas possíveis de aceder. Escolhendo uma data possível é possível ser redireccionado ao website em questão nesta mesma data como era sendo possível ter acesso a informação disponível nessa dada altura que actualmente não é possível.

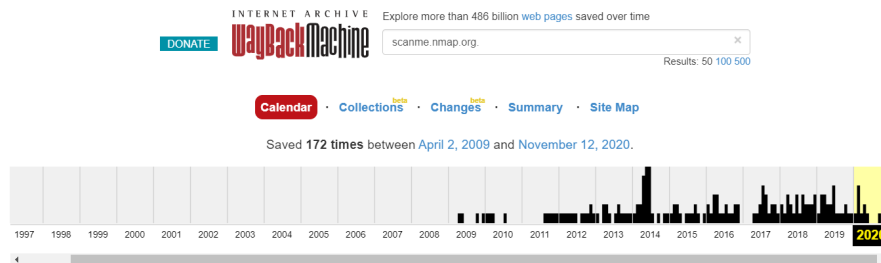


Figura 11: Resultados da pesquisa de 45.33.32.156 no site WayBack Machine

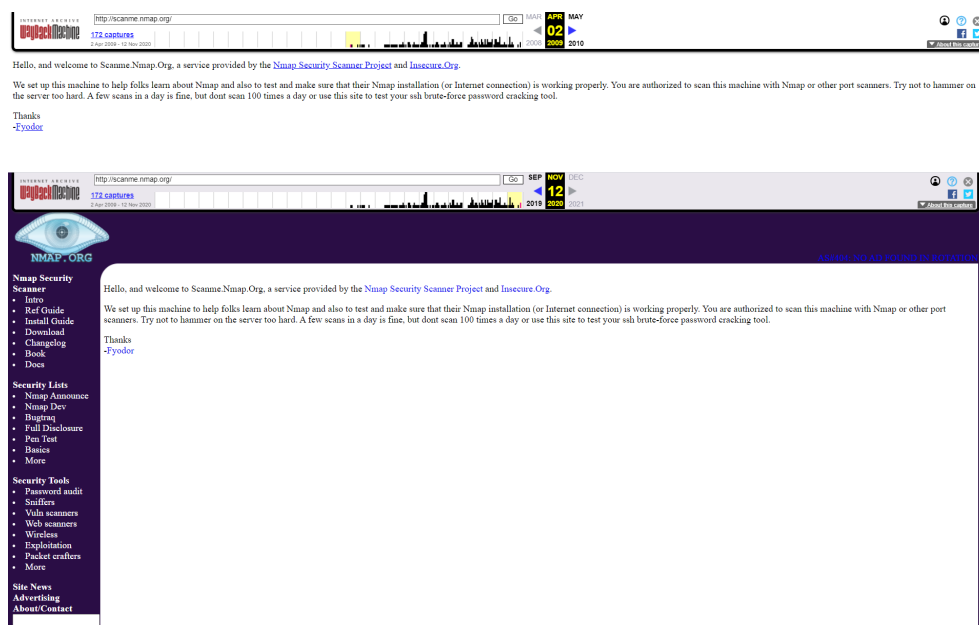


Figura 12: Primeira e última captura

4 Scanning

A realização de *Scanning* passa por recolher informações sobre os já conhecidos sistemas de forma passiva ou ativa. Isso envolve descobrir o sistema operativo em causa, que portas estão disponíveis ou não, identificar vulnerabilidades existentes, entre outros.

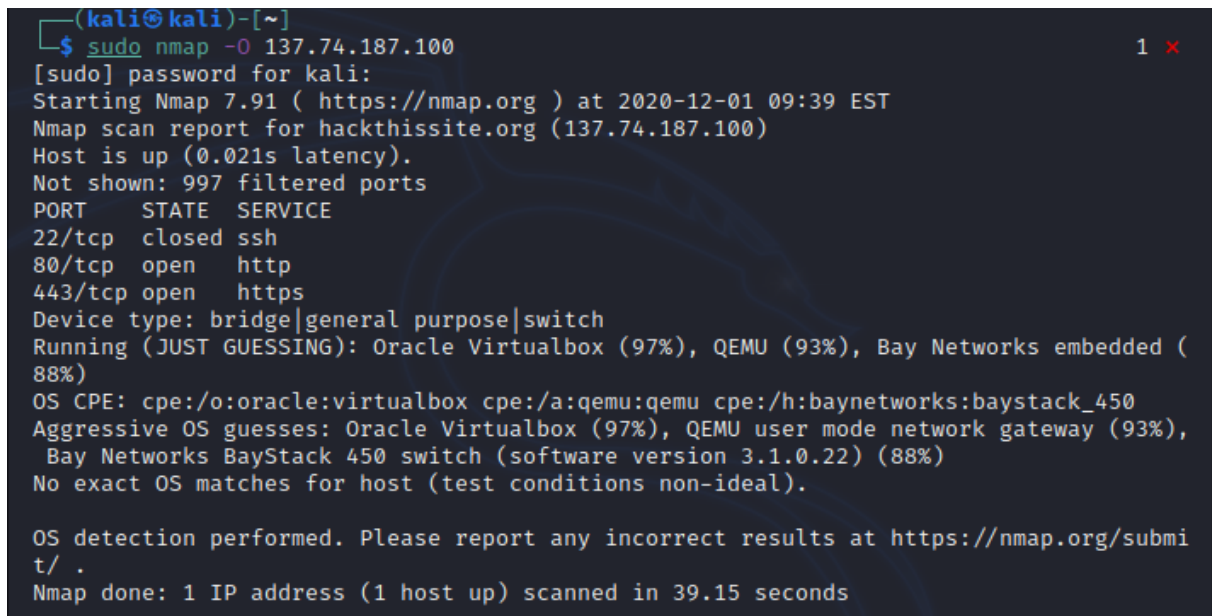
Para o caso em estudo utilizaram se as seguintes ferramentas:

- **NMap:** Software que permite explorar redes e sistemas em vários aspetos, tais como que portas de um sistema existem, o seu estado atual (disponíveis ou não), qual o sistema operativo em causa, que serviços existem, entre outras informações.

Esta ferramenta foi usada em 3 casos distintos. Primeiro para obter informações sobre o sistema operativo do sistema em questão. De seguida, foram exploradas que portas existiam e o seu estado. Por fim, experimentou-se um comando para obter ainda mais informação sobre as portas em questão.

4.1 Endereço 137.74.187.100

Para obter o sistema operativo usou-se o comando `nmap -O`. Na figura 13 podemos observar que o `nmap` tentou adivinhar primeiro que sistemas operativos estavam a correr ("JUST GUESSING") sendo estes "Oracle Virtualbox", QEMU ou "Bay Networks embedded". Ele concluiu que não existiam resultados exatos para o sistema operativo mas adivinhou estes 3 referidos. Para além disso, ele mostra também algumas portas: 22, 80 e 443. A primeira suporta o serviço `ssh` e encontra-se `closed` e as duas últimas estão abertas e suportam `http` e `https` respetivamente.

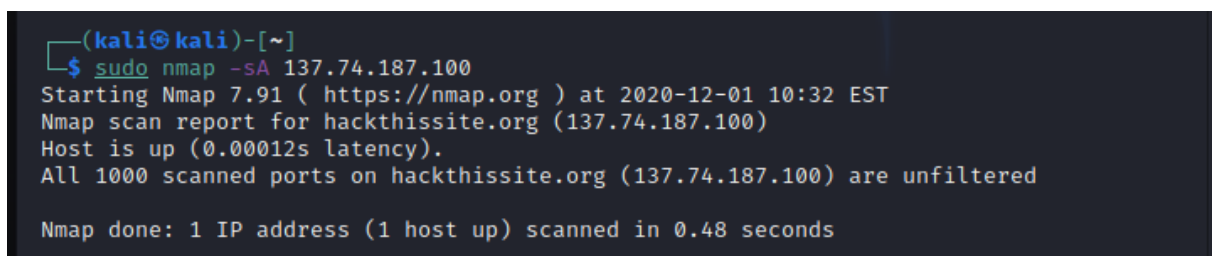
A terminal window with a dark background and light-colored text. The prompt is (kali@kali)-[~]. The command executed is sudo nmap -O 137.74.187.100. The output shows the nmap scan report for hackthissite.org (137.74.187.100). It indicates the host is up with a latency of 0.021s. A table shows the state of ports 22/tcp (closed, ssh), 80/tcp (open, http), and 443/tcp (open, https). It also shows OS detection results, including guesses for Oracle Virtualbox (97%), QEMU (93%), and Bay Networks embedded (88%). The scan took 39.15 seconds.

```
(kali@kali)-[~]
$ sudo nmap -O 137.74.187.100
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 09:39 EST
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.021s 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|switch
Running (JUST GUESSING): Oracle Virtualbox (97%), 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 (97%), QEMU user mode network gateway (93%),
Bay Networks 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/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 39.15 seconds
```

Figura 13: Resultados do `nmap -O` para o endereço 137.74.187.100

Com o comando `nmap -sA` escolhemos testar as suas portas com pacotes do tipo `ACK`, sendo que este conseguiu fazer scan das 1000 portas dizendo que são `unfiltered`.

A terminal window with a dark background and light-colored text. The prompt is (kali@kali)-[~]. The command executed is sudo nmap -sA 137.74.187.100. The output shows the nmap scan report for hackthissite.org (137.74.187.100). It indicates the host is up with a latency of 0.00012s. The message states that all 1000 scanned ports are unfiltered. The scan took 0.48 seconds.

```
(kali@kali)-[~]
$ sudo nmap -sA 137.74.187.100
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 10:32 EST
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.00012s latency).
All 1000 scanned ports on hackthissite.org (137.74.187.100) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

Figura 14: Resultados do `nmap -sA` para o endereço 137.74.187.100

Por fim, correu-se o comando `nmap -sV` como tentativa para obter mais informações sobre as portas. Este liga-se a um serviço e verifica se a porta dá alguma informação extra sobre si. Neste caso, são mencionadas as versões e refere ainda proxys.

```
(kali㉿kali)-[~]
$ sudo nmap -sV 137.74.187.100
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 10:33 EST
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http-proxy   HAProxy http proxy 1.3.1 or later
443/tcp   open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.58 seconds
```

Figura 15: Resultados do nmap -sV para o endereço 137.74.187.100

4.2 Endereço 216.58.215.148

Tal como para o endereço anterior, realizaram-se os mesmos passos. Neste caso, existem apenas duas portas (80 e 443) como no anterior. Ambas open e http e https respetivamente. Mais uma vez, o nmap tentou adivinhar que sistema operativo estava a correr adivinhando "Oracle Virtualbox" e QEMU.

```
(kali㉿kali)-[~]
$ sudo nmap -O 216.58.215.148
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 09:40 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.60% done
Nmap scan report for mad41s04-in-f20.1e100.net (216.58.215.148)
Host is up (0.013s 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
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
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 11.86 seconds
```

Figura 16: Resultados do nmap -O para o endereço 216.58.215.148

À semelhança do anterior, todas as 1000 portas foram scanned com sucesso mas neste caso estão todas closed. Desta vez usou-se o comando nmap -sN que apenas muda o tipo de pacote usado para testar.

```
(kali㉿kali)-[~]
$ sudo nmap -sN 216.58.215.148
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 10:33 EST
Nmap scan report for mad41s04-in-f20.1e100.net (216.58.215.148)
Host is up (0.00043s latency).
All 1000 scanned ports on mad41s04-in-f20.1e100.net (216.58.215.148) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Figura 17: Resultados do nmap -sN para o endereço 216.58.215.148


```
(kali@kali)-[~]
$ sudo nmap scanme.nmap.org.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 09:52 EST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).
```

Figura 19: Resultados do nmap -O para o endereço 45.33.32.156

Assim, experimentou-se o comando nmap -sX para testar as portas, e à semelhança do anterior, todas estavam closed.

```
(kali@kali)-[~]
$ sudo nmap -sX 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 10:31 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00013s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Figura 20: Resultados do nmap -sX para o endereço 45.33.32.156

Para o comando nmap -sV, este também estava a falhar nas portas como o comando -O. Assim, por investigação na documentação do nmap, correu se o comando nmap -A -T4 para saber o sistema operativo e acelerar o processo (-T4). Este foi bem sucedido e observamos que a porta 22 suporta o serviço ssh e encontra-se aberta. Para além disso, ainda menciona informações sobre que versão do serviço está a ser usada. Revela ainda as ssh.hostkey (DSA, RSA, ECDSA). Observamos também a porta 80 open com o serviço http e a respetiva versão, a porta 9929 open com o serviço nping-echo e a porta 31337 open com o serviço tcpwrapped.

Neste caso o nmap conseguiu com certeza identificar o sistema operativo em causa sendo este Linux.

```
(kali@kali)-[~]
$ nmap -A -T4 scanme.nmap.org.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 10:49 EST
Nmap scan report for scanme.nmap.org. (45.33.32.156)
Host is up (0.47s latency).
Other addresses for scanme.nmap.org. (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.08 seconds
```

Figura 21: Resultados do nmap -A -T4 para o endereço 45.33.32.156

5 Conclusão

Com este exercício, ficou-se a entender como se processa a primeira fase de um teste de intrusão, o *fingerprinting*. Para isso, foram utilizadas várias ferramentas novas ao grupo e aprendeu-se o seu funcionamento. Foi ainda útil a interpretação dos resultados e a tentativa de perceber como encaixar as informações todas para gerar um conjunto de dados sobre os sistemas investigados.