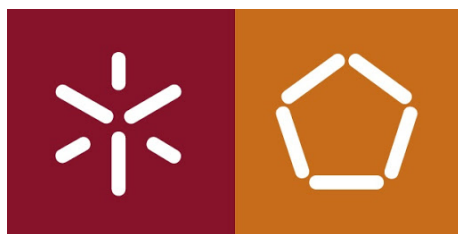


Segurança de Sistemas Informáticos

Trabalho Prático 2 Testes de Penetração (*Footprinting*)

pg42577 Daniel Regado
a85954 Luís Ribeiro



Mestrado em Engenharia Informática
Universidade do Minho

Conteúdo

1	Introdução	3
2	Parte A	4
2.1	Sintanet	4
2.1.1	Observações	11
2.2	Farfetch	12
2.2.1	Observações	18
3	Parte B	19
3.1	Questão 1	20
3.1.1	Exploração das portas TCP	22
3.2	Questão 2	25
3.2.1	Scan de vulnerabilidades no Nessus	25
3.2.2	Comparação com a Questão 1	27
3.3	Questão 3	28
3.3.1	Evento 1	28
3.3.2	Evento 2	29
3.4	Questão 4	30
3.5	Questão 5	32
4	Conclusões	39

1 Introdução

Este trabalho prático consiste na prática dos conceitos estudados previamente relativos ao **Footprinting**. *Footprinting* refere-se ao processo de colher o máximo de informação possível sobre um sistema destino, de modo a encontrar maneiras de penetrar o sistema. Um *hacker*, ou invasor, passa a maior parte do tempo traçando o perfil de uma organização, reunindo informações sobre o *host*, a rede e as pessoas relacionadas à organização.

Este processo de *Footprinting* divide-se em duas fases:

- **Reconnaissance**: Recolha **passiva** de informação. Aqui o atacante toma uma postura mais passiva e procura informação maioritariamente pública sobre a organização.
- **Scanning**: Recolha **ativa** de informação. Esta fase consiste no uso da informação da fase anterior, de modo a explorar vulnerabilidades e ameaças correntes no sistema ("Which risks might exist").

Este processo de *Footprinting* é um sub-processo do **Penetration Testing**. Os restantes sub-processos referem-se ao acesso e controlo da organização por parte do atacante.

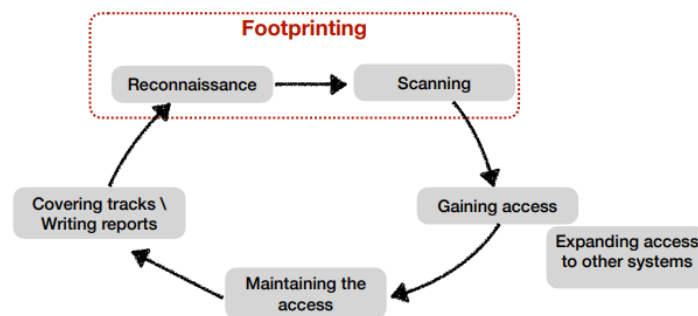


Figura 1: *Footprinting* e *Penetration Testing*

O trabalho está dividido em duas partes independentes, a primeira parte consiste no uso de técnicas para a recolha passiva de informação como ferramenta de análise da postura de segurança em sistemas e infra-estruturas reais. Na segunda parte, será configurado um ambiente de testes no qual técnicas e ferramentas de varredura activa serão usadas como estratégia de identificação de vulnerabilidades e fraquezas de um sistema remoto.

2 Parte A

Como já referido anteriormente, esta primeira parte do trabalho consiste na recolha passiva de informação de infra-estruturas, para uma análise posterior sobre a segurança interna da mesma. Para isto, escolhemos duas empresas com serviços *online*, de modo a conseguir explorar as suas infra-estruturas. As duas empresas escolhidas foram:

- Sintanet
- Farfetch

Nesta fase apresentaremos as estratégias usadas e os resultados obtidos relativos à recolha passiva de informação sobre estas empresas. De notar que esta varredura passiva passa por informação publicamente exposta, podemos não encontrar exposição de informação, mas vamos descrever, cuidadosamente, o processo de investigação.

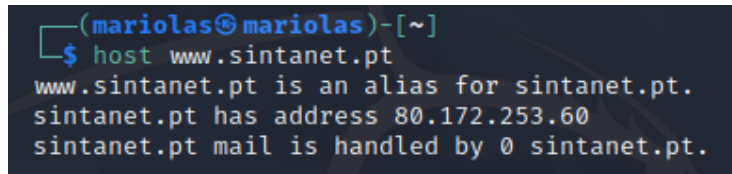
Para além disso, iremos sugerir possíveis melhorias, se possível, relativamente à postura de segurança destes domínios estudados.

2.1 Sintanet

A Sintanet.pt é uma loja online destinada a reparação e comércio de produtos na área das telecomunicações, informática e videojogos assim como dos respectivos acessórios e componentes.

Website: *www.sintanet.pt*

Inicialmente, identificamos o IP relativo ao *Domain name* *www.sintanet.pt*, através das ferramentas *host* e *dig*. Ambas as ferramentas são comandos/ferramentas para pedir informação aos DNS (*Domain Name System*) *nameservers*.



```
(mariolas@mariolas)-[~]  
$ host www.sintanet.pt  
www.sintanet.pt is an alias for sintanet.pt.  
sintanet.pt has address 80.172.253.60  
sintanet.pt mail is handled by 0 sintanet.pt.
```

Figura 2: *host* ao *Domain Name* *sintanet.pt*

O endereço IP com o *Domain Name* *sintanet.pt* é **80.172.253.60**, e *sintanet.pt* é um *alias* para *www.sintanet.pt*.

Relativamente à último registo dado pela ferramenta *host* refere-se a um **Mail Exchange (MX) record** necessário para o encaminhamento de *emails*, dentro do domínio. O '0' corresponde à prioridade (quanto mais baixo for o número, maior a prioridade), e o *sintanet.pt* seguido corresponde ao domínio ou ao servidor de *email* (*Mail Server*).

```
(mariolas@mariolas)-[~]
$ dig www.sintanet.pt

; <<>> DiG 9.16.8-Debian <<>> www.sintanet.pt
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 40495
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.sintanet.pt.                493     IN      CNAME   sintanet.pt.
sintanet.pt.                    9893    IN      A       80.172.253.60

;; AUTHORITY SECTION:
sintanet.pt.                    2051    IN      NS      ns1.bsolus.pt.
sintanet.pt.                    2051    IN      NS      ns2.bsolus.pt.

;; ADDITIONAL SECTION:
ns2.bsolus.pt.                  9770    IN      A       80.172.253.60
ns1.bsolus.pt.                  9770    IN      A       80.172.253.62

;; Query time: 20 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: qua dez 16 14:05:46 WET 2020
;; MSG SIZE rcvd: 149
```

Figura 3: *dig* ao Domain Name *sintanet.pt*

A ferramenta *dig* dá-nos mais informação relativamente ao *host*. A primeira parte do resultado corresponde a detalhes da resposta do servidor DNS, e a *QUESTION SECTION* corresponde à *query* que fizemos, portanto estes campos podem ser ignorados. A *ANSWER SECTION* dá-nos o mesmo resultado que o *host*, isto é, devolve-nos o endereço (*address(A)*) relativo ao *www.sintanet.pt*, sendo o *sintanet.pt* um *alias(CNAME)* para este.

As secções a seguir, *AUTHORITY SECTION* e *ADDITIONAL SECTION* correspondem a respostas DNS. A *AUTHORITY SECTION* diz-nos quais os servidores DNS (NS), *ns1.bsolus.pt* e *ns2.bsolus.pt*, responsáveis pelo *Domain Name* *www.sintanet.pt*. A *ADDITIONAL SECTION* dá-nos os endereços correspondentes a esses NS responsáveis.

De seguida, usamos a ferramenta *nslookup*, sendo esta também uma ferramenta para se obter informação sobre registos DNS de um determinado *host*. Através desta, podemos confirmar que existe um servidor DNS autoritativo relacionado com o *Domain Name* *www.sintanet.pt*.

```
(mariolas@mariolas)-[~]
$ nslookup
> server ns1.bsolus.pt
Default server: ns1.bsolus.pt
Address: 80.172.253.62#53
> www.sintanet.pt
Server:      ns1.bsolus.pt
Address:     80.172.253.62#53

www.sintanet.pt canonical name = sintanet.pt.
Name:  sintanet.pt
Address: 80.172.253.60
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> www.sintanet.pt
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.sintanet.pt canonical name = sintanet.pt.
Name:  sintanet.pt
Address: 80.172.253.60
> 
```

Figura 4: *nslookup*

Acima podemos ver que, foram feitas 2 *queries* ao *nslookup*, usando 2 servidores diferentes. Estes 2 servidores foram definidos através do comando *server* do *nslookup*, que muda o servidor por omissão para os que definimos. Neste caso, referimos o IP relativo ao servidor DNS *ns1.bsolus.pt* e o servidor **8.8.8.8**, que corresponde ao servidor DNS público da *Google*.

Se mudarmos o servidor por omissão para o endereço IP relativo à *ns1.bsolus.pt*, e questionarmos o endereço IP relativo ao *www.sintanet.pt*, o servidor responde diretamente, por se tratar do servidor DNS autoritativo. Esta resposta "direta" corresponde a *Authoritative answer*. No entanto, quando mudamos o servidor para o endereço relativo ao servidor DNS público da *Google* e o questionamos com a mesma *querie*, este responde com uma ***Non-authoritative answer*** com a informação do *Domain Name* *www.uminho.pt*. A informação *Non-authoritative answer* significa que o servidor DNS do provedor de acesso não responde por este domínio, isto significa que uma consulta externa foi realizada.

Um possível passo, no processo de varredura passiva, passa pela análise do *Website*, na esperança de encontrar informação relativo ao trabalho ou trabalhadores da empresa. Para isto, vamos comparar 2 versões do *Website*, uma capturada em 2013 pelo *archive.org* e a versão atual.

Precisa de Ajuda? <ul style="list-style-type: none"> De meus pedidos Onde estou e Rembolso Termos & Condições Como Comprar 	Mais Informação <ul style="list-style-type: none"> A empresa Contactos Recomendações Reparações Portos Pick-up 	Join Us <ul style="list-style-type: none"> Facebook 	sintonet <small>uma loja online</small> Centro Comercial Passarela Loja Nº 74 4895-121 Caldas das Taipas
---	--	---	--

A loja da sua Internet!

APOIO AO CLIENTE ?

Sintonet

A Sintonet.pt é uma loja online destinada a reparação e comércio de produtos na área das telecomunicações, informática e videogames assim como dos respectivos acessórios e componentes.

Apresentamos preços muito competitivos num mercado que se mostra cada vez mais exigente, assegurando elevados padrões de qualidade nos produtos apresentados e um serviço de excelência, rigoroso, seguro, eficaz, apostando no cumprimento rigoroso dos serviços solicitados pelo cliente, prestando todo o apoio necessário para que comodamente nos escolha como seu parceiro no dia-a-dia.

Todos os nossos clientes poderão realizar as suas compras online, sem necessidade de se deslocar a uma loja e desta forma não estar sujeito a horários de abertura e fecho, encontrando uma disponibilidade 24 horas por dia apenas à distância de um clique. Podendo receber as suas encomendas comodamente em sua casa, através de pagamento no ato de entrega, ou via transferência bancária, evitando desta forma o risco de exposição de dados bancários na Web e de burocracias.

O catálogo de produtos apresentado é baseado em informações oriundas dos fabricantes dos produtos por forma a fazer chegar toda a informação que necessita para efetuar as suas compras na nossa loja.

A LOJA DO SEU TELEFONE

Centro Comercial Passarela Loja Nº 74
4895-121 Caldas das Taipas

Tel: 351 252 050 549

encomendas@sintonet.pt

GPS: N41°53.180 W-8.347048

NOME *

EMAIL *

ASSUNTO *

MENSAGEM *

☐ CÓPIA PARA MIM

PODE ENVIAR INDIAR OS CARACTERES QUE VOCÊ VÊ NA CAIXA DE TEXTO ADJUNTO

ENVIAR

Figura 5: Sintonet 2013

Precisa de Ajuda? <ul style="list-style-type: none"> De meus pedidos Onde estou e Rembolso Termos & Condições Como Comprar Informações do Consumidor Lista de Recomendações 	Mais Informação <ul style="list-style-type: none"> A empresa Contactos Recomendações Reparações Reparação Remotiva no mesmo dia Informações de Catálogo 	Join Us <ul style="list-style-type: none"> Facebook 	Sintonet.pt Centro Comercial Passarela Loja Nº 62 4895-121 Caldas das Taipas Domínio Social N.º de Identificação de Segurança (N.º de Segurança) encomendas@sintonet.pt GPS: N41°53.180 W-8.347048
--	--	---	---

SINTANET © 2012 TODOS OS DIREITOS RESERVADOS DEVELOPED BY BICOLUP PT

Sintonet

A Sintonet.pt é uma loja online destinada a reparação e comércio de produtos na área das telecomunicações, informática e videogames assim como dos respectivos acessórios e componentes.

Apresentamos preços muito competitivos num mercado que se mostra cada vez mais exigente, assegurando elevados padrões de qualidade nos produtos apresentados e um serviço de excelência, rigoroso, seguro, eficaz, apostando no cumprimento rigoroso dos serviços solicitados pelo cliente, prestando todo o apoio necessário para que comodamente nos escolha como seu parceiro no dia-a-dia.

Todos os nossos clientes poderão realizar as suas compras online, sem necessidade de se deslocar a uma loja e desta forma não estar sujeito a horários de abertura e fecho, encontrando uma disponibilidade 24 horas por dia apenas à distância de um clique. Podendo receber as suas encomendas comodamente em sua casa, através de pagamento no ato de entrega, ou via transferência bancária, evitando desta forma o risco de exposição de dados bancários na Web e de burocracias.

O catálogo de produtos apresentado é baseado em informações oriundas dos fabricantes dos produtos por forma a fazer chegar toda a informação que necessita para efetuar as suas compras na nossa loja.

Like **Share** It jumps like this. Be the first of your friends.

A LOJA DO SEU TELEFONE

Centro Comercial Passarela Loja Nº 62
4895-121 Caldas das Taipas

encomendas@sintonet.pt

GPS: N41°53.180 W-8.347048

NOME *

EMAIL *

ASSUNTO *

MENSAGEM *

☐ CÓPIA PARA MIM

ENVIAR EMAIL

Google

Não é possível carregar constantemente o Google Maps nesta página.

E proprietário deste Website? **OK**

Figura 6: Sintonet 2020

Este tipo de análise é frequente, porque pode estar exposta informação sobre colaboradores ou trabalhadores da empresa. Informação como, *email*, morada e outros tipos de dados que podem ser usados para comprometer os mesmos.

Como podemos ver, não existe nenhuma informação exposta nos *Websites* que pode ser comprometida ou explorada. A rede social *Facebook* está associada,

no entanto é apenas exposto fotos de produtos que estão à venda, ou seja, serve apenas como um acrescento ao *Website*.

A base de dados *whois* e a ferramenta <https://whois.domaintools.com/> permitem-nos tirar informação correspondente ao domínio que inserimos, sendo neste caso *www.sintanet.pt*. Em baixo, apresenta-se uma imagem seguida de uma observação dos seus dados.



Whois Record for SintaNet.pt	
— Domain Profile	
Registrar Status	taken
Name Servers	NS1.BSOLUS.PT (has 78 domains) NS2.BSOLUS.PT (has 78 domains)
Tech Contact	—
IP Address	80.172.253.60 - 22 other sites hosted on this server
IP Location	Porto - Maia - Claranet Portugal S.a
ASN	AS8426 CLARANET-AS ClaraNET LTD, GB (registered Aug 15, 1997)
Hosting History	5 changes on 2 unique name servers over 7 years
— Website	
Website Title	Sintanet.pt - Venda de telemóveis, Acessórios e Reparação de Smartphones - Home
Server Type	Apache
Response Code	200
Terms	1,563 (Unique: 399, Linked: 1,319)
Images	25 (Alt tags missing: 0)
Links	779 (Internal: 779, Outbound: 0)
Whois Record (last updated on 2020-12-18)	
% NOTE: The registry for this domain name does not publish ownership records (whois records) in the standard format. This data represents the most likely status of the domain based on information provided by the Internet's domain name servers (DNS). domain: sintanet.pt status: taken nameserver: ns1.bsolus.pt nameserver: ns2.bsolus.pt % For more information, please visit http://www.dns.pt/	

Figura 7: *Whois Record* relativo ao *www.sintanet.pt*

Como já tínhamos visto através das ferramentas acima referidas, os servidores *ns1.bsolus.pt*, *ns2.bsolus.pt* correspondem aos servidores de nome (servidores DNS) responsáveis pelo domínio estudado. O campo correspondente ao **ASN** vai ser explicado mais à frente. O campo *Server Type* não nos dá nenhuma informação relevante que possa ajudar na exploração.

Whois Record for bsolus.pt

Domain Profile

Registrar Status	taken
Name Servers	NS1.BSOLUS.PT (has 78 domains) NS2.BSOLUS.PT (has 78 domains)
Tech Contact	—
IP Address	80.172.253.153 - 4 other sites hosted on this server
IP Location	 Porto - Maia - Claranet Portugal S.a
ASN	 AS8426 CLARANET-AS ClaraNET LTD, GB (registered Aug 15, 1997)

Website

Website Title	B BSOLUS - web engineering
Server Type	nginx/1.12.2
Response Code	200
Terms	181 (Unique: 119, Linked: 52)
Images	3 (Alt tags missing: 0)
Links	33 (Internal: 30, Outbound: 3)

Whois Record (last updated on 2020-12-18)

```
% NOTE: The registry for this domain name does not publish ownership
% records (whois records) in the standard format. This data
% represents the most likely status of the domain based on
% information provided by the Internet's domain name servers (DNS).

domain: bsolus.pt
status: taken
nameserver: ns1.bsolus.pt
nameserver: ns2.bsolus.pt

% For more information, please visit http://www.dns.pt/
```

Figura 8: Whois Record relativo ao *ns1.bsolus.pt*

Acima, numa tentativa de encontrar mais informação sobre o domínio, usamos a mesma ferramenta para analisar o domínio correspondente ao servidor DNS *ns1.bsolus.pt*. Podemos ver que tem um *Website* correspondente (<https://www.bsolus.pt/>). O campo *Server Type* dá-nos mais informação que no *record* anterior, pois dá-nos a versão do servidor **nginx** (**nginx/1.12.2**), facilitando na procura por vulnerabilidades. Em baixo, apresentam-se algumas vulnerabilidades associadas a esta versão.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publication Date	Update Date	Score	Gain Access Level	Access	Complexity	Authentication	Cert.	Http	Avail.
1	CVE-2018-16865	AS2			2018-11-07	2019-10-02	5.8	None	Remote	Medium	Not required	Partial	None	Partial
nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mpm_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mpm file. The issue only affects nginx if it is built with the ngx_http_mpm_module (the module is not built by default) and the .mpm directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mpm file with the ngx_http_mpm_module.														
2	CVE-2018-16866	AS2			2018-11-07	2019-09-10	7.8	None	Remote	Low	Not required	None	None	Complete
nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.														
3	CVE-2018-16862	AS2			2018-11-07	2019-09-10	7.8	None	Remote	Low	Not required	None	None	Complete
nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.														

Figura 9: CVEs relativos ao *nginx/1.12.2*

O campo ASN, em ambos os registos, é referente à **Claranet**. Os ASN, ou Sistemas Autónomos, são redes roteáveis na Internet pública, administradas pelos RIRs locais e atribuídas aos proprietários das redes. A **Claranet** é um *Service Provider*, que oferece serviços completamente administrados e seguros. A segurança dos serviços é praticamente garantida pela **Claranet**, para

além disso, efetuam testes de penetração com especialistas para assegurar o maior *range* de possibilidades de ataques, Portanto aumenta a dificuldade de exploração destes domínios, no entanto, existe informação relativo aos colaboradores e *CEOs* da Claranet, no *Website* oficial, que pode ser usado para exploração de dados privados expostos publicamente.

Como último passo, voltamos a usar a ferramenta *whois*, mas em vez de questionar a um domínio, usamos esta para questionar o endereço IP relativo ao domínio *sintanet.pt* (**80.172.253.60**).

```
(mariolas@mariolas)-[~]
$ whois 80.172.253.60
% 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 '80.172.253.51 - 80.172.253.255'
% Abuse contact for '80.172.253.51 - 80.172.253.255' is 'abuse@pt.clara.net'

inetnum:      80.172.253.51 - 80.172.253.255
netname:      PT-WEBLEVEL
descr:        Weblevel - Tecnologias de Informacao, Lda.
descr:        *****
descr:        * for abuse or spam complains
descr:        * abuse@weblevel.pt
descr:        *****
country:      PT
admin-c:      PN5053-RIPE
tech-c:       PN5053-RIPE
status:       ASSIGNED PA
mnt-by:       CLARANET-MNT
created:      2013-07-04T16:47:14Z
last-modified: 2019-08-13T16:48:56Z
source:       RIPE

person:       PT Networks
address:      Claranet, Av. D. Joao II, 1.07 - 2.1, 4, 1998-014 Lisboa
phone:        +351 21 319 92 00
nic-hdl:      PN5053-RIPE
mnt-by:       CLARANET-MNT
mnt-by:       ESOTERICA-MNT
created:      2019-07-15T11:47:54Z
last-modified: 2019-07-15T11:48:34Z
source:       RIPE # Filtered

% Information related to '80.172.0.0/16AS8426'

route:        80.172.0.0/16
descr:        Claranet Portugal
descr:        Lisboa, Portugal
origin:       AS8426
mnt-by:       CLARANET-MNT
created:      2008-07-09T16:19:33Z
last-modified: 2013-07-04T17:36:57Z
source:       RIPE

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

Figura 10: *Whois Record* relativo ao **80.172.253.60**

Uma informação que pode ser explorada, é o campo referente ao *Abuse contact*. Neste campo é indicado o *email* de abuso do Claranet, e este serve para reportar ataques como os de *spam* (***abuse@pt.clara.net***). No entanto, este *email* pode ter informações, não só dos ataques que foram reportados, mas também das pessoas que os reportaram, podendo estes ser colaboradores ou

utilizadores.

Para a exploração deste *email*, usamos o Website *haveibeenpwned.com*, que nos permite saber se houve exposição de palavras-passe do *email* dado.



Figura 11: Resultados do *haveibeenpwned.com*

Como podemos ver em cima, houve exposição da palavra-passe deste *email* em duas *Breaches*. Uma *breach* corresponde ao incidente em que os dados foram expostos ao público. Estes dados podem continuar expostos, portanto, se não houve o cuidado, podem continuar vulneráveis a ataques de exposição.

De notar que estas palavras-passe estão expostas em base de dados públicas, ou seja, se houver palavras-passe repetidas dentro do mesmo *email*, podem ser usadas para obter informação dentro de outros domínios,

2.1.1 Observações

Após esta varredura passiva ao domínio *Sintanet.pt*, passamos agora a uma breve análise dos resultados obtidos. Relativamente à exposição de dados privados relativos a colaboradores da empresa, podemos encontrar dentro da página *Facebook* da empresa alguma informação do responsável de loja, no entanto, dentro da página *Web*, não tem nenhuma informação exposta.

A informação mais relevante é o facto do *email* de abuso ter sido exposto, juntamente com a sua palavra-passe, como podemos ver acima. A melhor maneira de reagir a estes *leaks* é alterar as palavras-passe de acesso deste *email*, para que não esteja vulnerável a acessos não autorizados. Técnicas como o uso de *proxys* externos e de servidores *DNS* no endereço IP do domínio *Sintanet.pt*, são possíveis melhorias a ter em conta na administração deste tipo de domínios.

2.2 Farfetch

A abordagem relativamente à análise desta empresa espera-se ser mais curta em comparação com a anterior porque podemos ser mais diretos no uso de ferramentas. Primeiro vamos apresentar, de uma forma breve, do que se trata a empresa que vamos analisar e o *Website* correspondente.

Farfetch é uma plataforma líder mundial no mercado on-line de moda de luxo. O site foi fundado em 2008 pelo empresário português José Neves, com sede fiscal em Londres.

Website: *www.farfetch.com*

Inicialmente, identificamos o endereço IP relativo ao *Domain name* *www.farfetch.com*. Para isso usamos apenas a ferramenta *dig*, pois podemos extrair informações relativos aos endereços e *Name Servers* (servidores DNS).

```
(mariolas@mariolas)~$ dig www.farfetch.com

; <<>> DiG 9.16.8-Debian <<>> www.farfetch.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3416
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 10

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

;; ANSWER SECTION:
www.farfetch.com.      157     IN      CNAME   farfetch.edgekey.net.
farfetch.edgekey.net.  3155    IN      CNAME   e2866.a.akamaiedge.net.
e2866.a.akamaiedge.net. 1         IN      A       23.216.98.95

;; AUTHORITY SECTION:
a.akamaiedge.net.      602     IN      NS       n5a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n2a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n4a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n1a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n0a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n3a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n7a.akamaiedge.net.
a.akamaiedge.net.      602     IN      NS       n6a.akamaiedge.net.

;; ADDITIONAL SECTION:
n0a.akamaiedge.net.    2525    IN      A       88.221.81.192
n3a.akamaiedge.net.    1004    IN      A       2.16.65.55
n7a.akamaiedge.net.    2061    IN      A       2.17.47.4
n2a.akamaiedge.net.    1764    IN      A       2.16.65.36
n4a.akamaiedge.net.    1594    IN      A       2.16.65.79
n5a.akamaiedge.net.    3074    IN      A       2.16.65.86
n6a.akamaiedge.net.    2670    IN      A       2.22.245.172
n1a.akamaiedge.net.    2032    IN      A       2.16.65.53
n0a.akamaiedge.net.    2525    IN      AAAA    2600:1480:e800::c0

;; Query time: 12 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: sáb dez 19 16:48:22 WET 2020
;; MSG SIZE rcvd: 428
```

Figura 12: *dig* ao *Domain Name* *www.farfetch.com*

Analisando a *Figure* acima, podemos retirar informação sobre os *alias* do *Domain Name* *www.farfetch.com* (que não é muito relevante), sobre o seu en-

dereço IP e os servidores DNS responsáveis por este domínio.

O endereço IP associado a este domínio é **23.216.98.96**. Os servidores DNS autoritativos deste domínio estão associados a uma empresa de Internet chamada **Akamai**. Esta empresa é responsável por mais de 60 domínios, subdomínios e servidores DNS em toda a Internet, sendo um destes o *akamai-edge.net*. Esta informação vai ser útil quando usarmos a ferramenta *whois*, pois podemos explorar detalhadamente os domínios relativos ao endereço IP e aos servidores DNS responsáveis.

Como na análise anterior, vamos a seguir explorar o *Website* oficial, na esperança de encontrar informação relativo a colaboradores ou trabalhadores, ou até sobre a infra-estrutura. Tipicamente a informação associada à empresa dentro do *Website*, encontra-se na secção **About Us**, que se pode encontrar no rodapé da página.

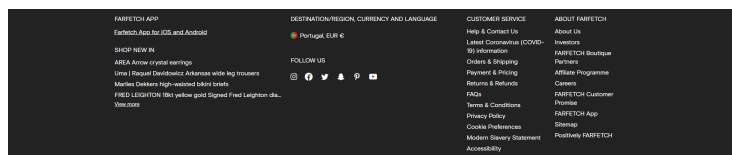


Figura 13: Rodapé do *Website* da Farfetch

Dentro da parte *About Farfetch*, a secção que nos permite tirar mais dados é a subsecção **Careers**, que corresponde à disponibilidade de emprego dentro das várias equipas de desenvolvimento da empresa. As restantes subsecções, apesar de parecerem ter potencial, não apresentam qualquer exposição pública de informação que pode ser usada posteriormente.

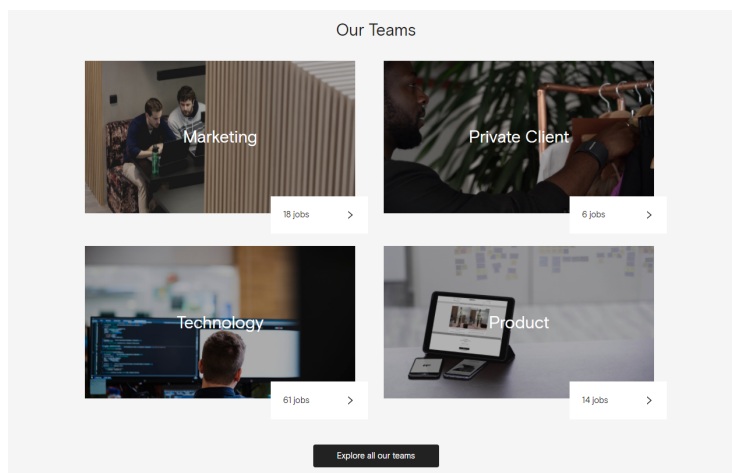


Figura 14: Equipas de desenvolvimento da Farfetch

A equipa de desenvolvimento mais relevante é a parte da **Tecnologia**, porque

pode ter detalhes sobre os sistemas e infra-estrutura da Farfetch. Aqui, o nosso objetivo foi tentar encontrar estes detalhes dentro das várias ofertas de emprego. Em baixo encontram-se exemplos destas ofertas.

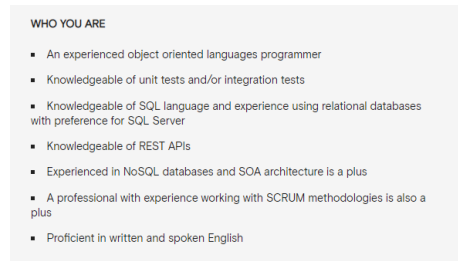


Figura 15: Oferta de emprego a um Engenheiro de *Software* especializado em *Backend*

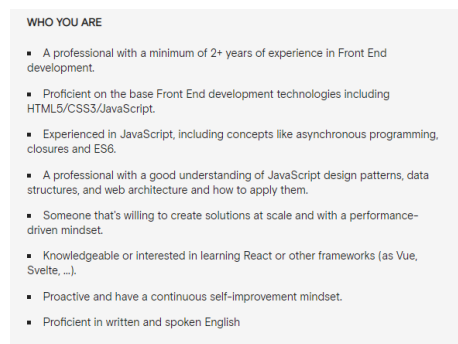


Figura 16: Oferta de emprego a um Engenheiro de *Software* especializado em *Frontend*

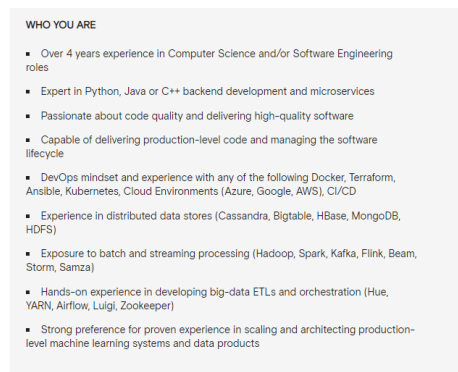


Figura 17: Oferta de emprego a um Engenheiro de Dados

Como podemos ver, a informação não é assim tão útil porque, apesar de sabermos quais são as ferramentas que usam dentro de cada área da Tecnologia, não sabemos as versões destas, portanto torna-se complicado a exploração das vulnerabilidades do sistema.

A base de dados *whois* e a ferramenta <https://whois.domaintools.com/> permitem-nos tirar informação correspondente ao domínio que inserimos, sendo neste caso o endereço IP em cima referido, *23.216.98.96*. Em baixo, apresenta-se uma imagem seguido de uma observação dos seus dados.

```

NetRange: 23.192.0.0 - 23.223.255.255
CIDR: 23.192.0.0/11
NetName: AKAMAI
NetHandle: NET-23-192-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate: 2013-07-12
Updated: 2013-08-09
Ref: https://rdap.arin.net/registry/ip/23.192.0.0

OrgName: Akamai Technologies, Inc.
OrgId: AKAMAI
Address: 145 Broadway
City: Cambridge
StateProv: MA
PostalCode: 02142
Country: US
RegDate: 1999-01-21
Updated: 2020-08-26
Ref: https://rdap.arin.net/registry/entity/AKAMAI

OrgTechHandle: S3598-ARIN
OrgTechName: Schechter, Steven Jay
OrgTechPhone: +1-617-274-7134
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/S3598-ARIN

OrgAbuseHandle: NUS-ARIN
OrgAbuseName: NOC United States
OrgAbusePhone: +1-617-444-2535
OrgAbuseEmail: abuse@akamai.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NUS-ARIN

OrgTechHandle: IPADM11-ARIN
OrgTechName: ipadmin
OrgTechPhone: +1-617-444-0017
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPADM11-ARIN

OrgTechHandle: YKS-ARIN
OrgTechName: Yeung, Kam Sze
OrgTechPhone: +852-92813828
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/YKS-ARIN

NetRange: 23.216.96.0 - 23.216.111.255
CIDR: 23.216.96.0/20
NetName: AIBV
NetHandle: NET-23-216-96-0-1
Parent: AKAMAI (NET-23-192-0-0-1)
NetType: Reassigned
OriginAS:
Organization: Akamai International, BV (AIB-17)
RegDate: 2014-07-08
Updated: 2014-07-08
Ref: https://rdap.arin.net/registry/ip/23.216.96.0

OrgName: Akamai International, BV
OrgId: AIB-17
Address: Prins Bernhardplein 200
City: Amsterdam
StateProv:
PostalCode: 1097 JB
Country: NL
RegDate: 2013-09-19
Updated: 2016-12-14
Ref: https://rdap.arin.net/registry/entity/AIB-17

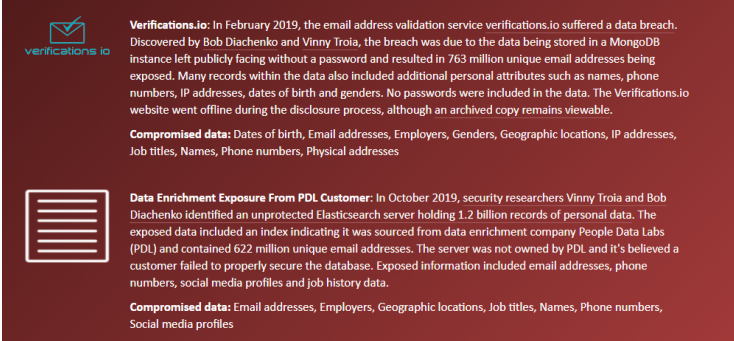
OrgTechHandle: AIBVH-ARIN
OrgTechName: AIBV Hostmaster
OrgTechPhone: +1-617-444-4699
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/AIBVH-ARIN

OrgAbuseHandle: NUS-ARIN
OrgAbuseName: NOC United States
OrgAbusePhone: +1-617-444-2535
OrgAbuseEmail: abuse@akamai.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NUS-ARIN

```

Figura 18: *Whois Record* relativo ao **23.216.98.96**

Dentro deste registo podemos observar a exposição de 2 *emails*. Para a exploração destes *emails*, usamos o Website ***haveibeenpwned.com***, que nos permite saber se houve exposição de palavras-passe do *email* dado. Os *emails* questionados foram os seguintes: *abuse@akamai.com* e *ip-admin@akamai.com*. O primeiro corresponde ao *email* de denúncia de abusos, poderá ter alguma informação sobre quem enviou as denúncias, sendo a maior parte intervenientes do Akamai. O último corresponde a um *email* de organização, portanto a descoberta de informações sobre este domínio pode comprometer informação privada.



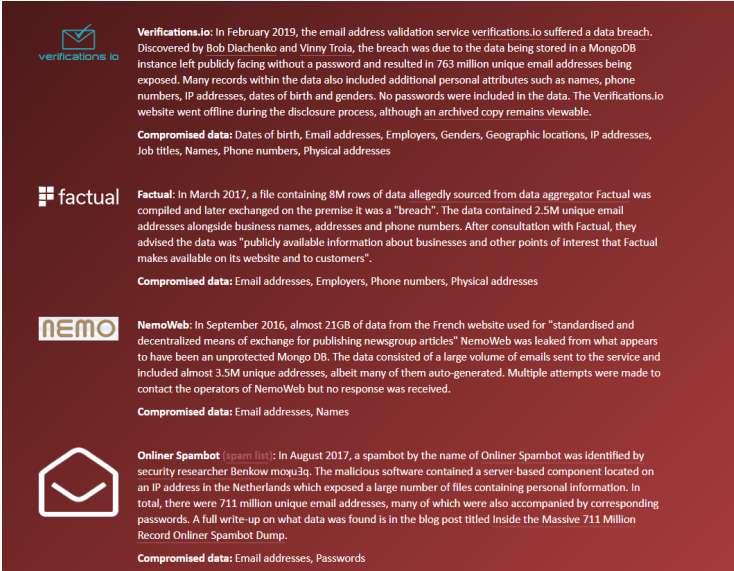
Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Figura 19: Resultados do *haveibeenpwned.com* (*ip-admin@akamai.com*)



Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

factual: In March 2017, a file containing 8M rows of data allegedly sourced from data aggregator Factual was compiled and later exchanged on the premise it was a "breach". The data contained 2.5M unique email addresses alongside business names, addresses and phone numbers. After consultation with Factual, they advised the data was "publicly available information about businesses and other points of interest that Factual makes available on its website and to customers".

Compromised data: Email addresses, Employers, Phone numbers, Physical addresses

NEMO: In September 2016, almost 21GB of data from the French website used for "standardised and decentralized means of exchange for publishing newsgroup articles" NemoWeb was leaked from what appears to have been an unprotected Mongo DB. The data consisted of a large volume of emails sent to the service and included almost 3.5M unique addresses, albeit many of them auto-generated. Multiple attempts were made to contact the operators of NemoWeb but no response was received.

Compromised data: Email addresses, Names

Onliner Spambot [spam list]: In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moqu3q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

Figura 20: Resultados do *haveibeenpwned.com* (*abuse@akamai.com*)

Como podemos ver em cima, houve exposição de palavras-passe em ambos

emails em diferentes *Breaches*. Uma *breach* corresponde ao incidente em que os dados foram expostos ao público. Estes dados podem continuar expostos, portanto, se não houve o cuidado, podem continuar vulneráveis a ataques de exposição.

Para obter mais informações também questionamos ao *whois*, sobre o domínio respetivo ao servidor DNS responsável pela Farfetch, sendo este um dos servidores apresentados na ferramenta *dig* em cima referida.

Whois Record for AkamaiEdge.net	
— Domain Profile	
Registrant	Hostmaster Billing
Registrant Org	Akamai Technologies, Inc.
Registrant Country	us
Registrar	Akamai Technologies, INC. Akamai Technologies, Inc. IANA ID: 2480 URL: http://www.akamai.com Whois Server: whois.akamai.com registrars-abuse@akamai.com (p) 16174443076
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	7,017 days old Created on 2001-10-03 Expires on 2022-10-03 Updated on 2020-10-07
Name Servers	A1-192.AKAMAIEDGE.NET (has 5 domains) A11-192.AKAMAIEDGE.NET (has 5 domains) A12-192.AKAMAIEDGE.NET (has 5 domains) A13-192.AKAMAIEDGE.NET (has 5 domains) A28-192.AKAMAIEDGE.NET (has 5 domains) A6-192.AKAMAIEDGE.NET (has 5 domains) LA1.AKAMAIEDGE.NET (has 5 domains) LA3.AKAMAIEDGE.NET (has 5 domains) LAR2.AKAMAIEDGE.NET (has 5 domains) NS3-194.AKAMAIEDGE.NET (has 5 domains) NS5-194.AKAMAIEDGE.NET (has 5 domains) NS6-194.AKAMAIEDGE.NET (has 5 domains) NS7-194.AKAMAIEDGE.NET (has 5 domains)
Tech Contact	Hostmaster Billing Akamai Technologies, Inc. 145 Broadway, Cambridge, MA, 02142, us hostmaster-billing@akamai.com (p) 16174443000 (f) 16174443001
Registrar History	2 registrars with 2 drops
— Website	
Website Title	None given.
Whois Record (last updated on 2020-12-19)	

Figura 21: *Whois Record* relativo ao servidor DNS autoritativo

Dentro deste registo podemos observar a exposição de 2 *emails*. Para a exploração destes *emails*, usamos o *Website haveibeenpwned.com*, que nos permite saber se houve exposição de palavras-passe do *email* dado.

O *email* relativo ao *email* de abuso, *registrars-abuse@akamai.com*, de acordo com o *Website*, não tem exposto nenhuma palavra-passe relativo a este mesmo. No entanto, o *email* abaixo referido, corresponde a um *email* de uso administrativo, e como se pode ver abaixo, houve exposição de palavras-passe em duas *breaches*.

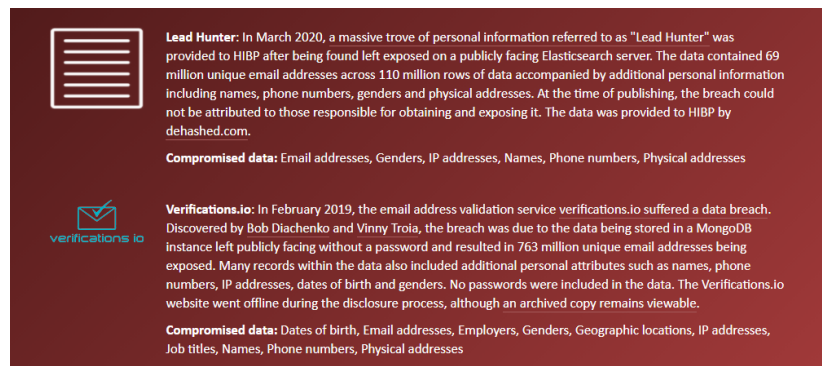


Figura 22: Resultados do *haveibeenpwned.com*

De notar que estas palavras-passe estão expostas em base de dados públicas, ou seja, se houver palavras-passe repetidas dentro do mesmo *email*, podem ser usadas para obter informação dentro de outros domínios,

2.2.1 Observações

Após esta varredura passiva ao domínio *Farfetch.com*, passamos agora a uma breve análise dos resultados obtidos. Relativamente à exposição de dados privados relativos a colaboradores da empresa, dentro da página *Web*, não tem nenhuma informação exposta. Existe também uma secção, dentro da página *Web*, destinada à oferta de emprego, no entanto não há nenhuma informação relevante que permite explorar este domínio.

A informação mais relevante é o facto de *emails* terem sido expostos, juntamente com as suas palavra-passe, como podemos ver acima. A melhor maneira de reagir a estes *leaks* é alterar as palavras-passe de acesso destes *emails*, para que não esteja vulnerável a acessos não autorizados. Técnicas como o uso de *proxys* externos e de servidores *DNS* no endereço IP do domínio *Farfetch.com*, são possíveis melhorias a ter em conta na administração deste tipo de domínios.

3 Parte B

Para esta segunda parte do trabalho é necessário a configuração de um ambiente remoto de testes, denominado como sistema **Metasploitable 3**, para que o sistema **Auditor** (*KALI Linux*) use ferramentas de recolha ativa de modo a explorar as vulnerabilidades e ameaças dos serviços a correr no sistema de ambiente de testes.

As ferramentas necessárias para o *scan* ativo do *Metasploitable 3*, foram as seguintes:

- **Nessus:** *Scanner* de vulnerabilidade.
- **Wireshark:** Analisador de tráfego.
- **Snort:** Sistema de Detecção de Intrusão - IDS.

Esta parte consiste na resolução de 5 questões. Relativamente à Questão 1, foi usado ferramentas e técnicas de recolha ativa de informação, de forma a detalhar vulnerabilidades e fraquezas para as quais o sistema *Metasploitable 3* está exposto. Nesta questão, não será permitido usar um *scanner* de vulnerabilidades. Para as restantes questões é necessário a instalação e o uso das ferramentas acima referidas.

Para além disso, tivemos que estabelecer uma conexão privada entre as duas máquinas, para simular uma rede interna, com o objetivo de manter o ambiente de teste isolado da rede local e, portando, evitando riscos de ataques externos, deverá ser configurada uma rede virtual através do VMWare ou do VirtualBox. Em baixo, está ilustrado esta rede virtual interna.

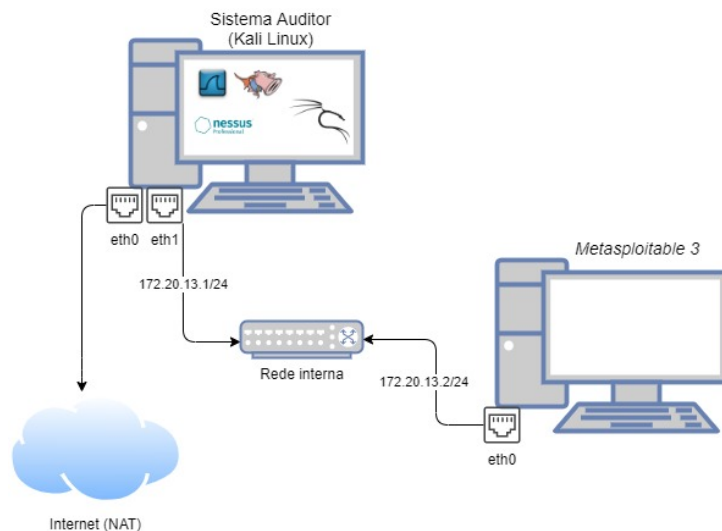


Figura 23: Representação da rede interna

Para uma melhor observação e conclusão dos resultados obtidos por parte do avaliador, devemos referir que a máquina *Metasploitable* escolhida corresponde ao uso dos ficheiros do Github do projeto, e para isso usamos as ferramentas do *Vagrant*.

3.1 Questão 1

Inicialmente, usamos ferramentas que nos permitem tirar algumas informações sobre o sistema *Metasploitable*. A ferramenta *ping* permitiu testar a conexão entre os 2 sistemas, e também permite saber qual o Sistema Operativo do sistema que queremos explorar, através do campo **TTL** (*Time to Live*).

```
(mariolas@kali)~$ sudo hping3 172.20.13.2
HPING 172.20.13.2 (eth1 172.20.13.2): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=172.20.13.2 ttl=128 DF id=2919 sport=0 flags=RA seq=0 win=0 rtt=7.9 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2920 sport=0 flags=RA seq=1 win=0 rtt=7.2 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2921 sport=0 flags=RA seq=2 win=0 rtt=6.3 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2922 sport=0 flags=RA seq=3 win=0 rtt=6.1 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2923 sport=0 flags=RA seq=4 win=0 rtt=6.3 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2924 sport=0 flags=RA seq=5 win=0 rtt=4.9 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2925 sport=0 flags=RA seq=6 win=0 rtt=5.1 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2926 sport=0 flags=RA seq=7 win=0 rtt=4.4 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2927 sport=0 flags=RA seq=8 win=0 rtt=4.1 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2928 sport=0 flags=RA seq=9 win=0 rtt=3.9 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2929 sport=0 flags=RA seq=10 win=0 rtt=3.3 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2930 sport=0 flags=RA seq=11 win=0 rtt=3.1 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2931 sport=0 flags=RA seq=12 win=0 rtt=2.4 ms
len=46 ip=172.20.13.2 ttl=128 DF id=2932 sport=0 flags=RA seq=13 win=0 rtt=1.6 ms
^C
--- 172.20.13.2 hping statistic ---
14 packets transmitted, 14 packets received, 0% packet loss
round-trip min/avg/max = 1.6/4.8/7.9 ms

(mariolas@kali)~$ ping 172.20.13.2
PING 172.20.13.2 (172.20.13.2) 56(84) bytes of data:
64 bytes from 172.20.13.2: icmp_seq=1 ttl=128 time=0.379 ms
64 bytes from 172.20.13.2: icmp_seq=2 ttl=128 time=0.583 ms
64 bytes from 172.20.13.2: icmp_seq=3 ttl=128 time=0.511 ms
64 bytes from 172.20.13.2: icmp_seq=4 ttl=128 time=0.477 ms
64 bytes from 172.20.13.2: icmp_seq=5 ttl=128 time=0.443 ms
64 bytes from 172.20.13.2: icmp_seq=6 ttl=128 time=0.474 ms
64 bytes from 172.20.13.2: icmp_seq=7 ttl=128 time=0.494 ms
64 bytes from 172.20.13.2: icmp_seq=8 ttl=128 time=0.421 ms
64 bytes from 172.20.13.2: icmp_seq=9 ttl=128 time=0.389 ms
^C
--- 172.20.13.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 817ms
rtt min/avg/max/mdev = 0.379/0.463/0.583/0.060 ms
```

Figura 24: *hping* e *ping*

Como o TTL é de 128, podemos assegurar que o Sistema Operativo do *Metasploitable* é *Windows*. A ferramenta *hping* apresenta mais informação sobre os pacotes ICMP transmitidos entre os sistemas, e pode ser facilmente configurável (podemos adicionar vários tipos de *flags*).

A ferramenta mais útil, que nos permite tirar muita informação dos serviços a correr nas portas, tal como o seu sistema operativo, é a ferramenta de **Port checking**, de nome **nmap**. A flag **-O** permite-nos adquirir informação sobre o Sistema Operativo, e pela imagem abaixo, podemos ver que se trata **Windows 7 SP1**. O campo *Network distance* dá-nos o mesmo que a ferramenta *traceroute*, dá-nos os saltos (*hops*) entre as máquinas.

```

MAC Address: 08:00:27:C9:39:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.51 seconds

```

Figura 25: Informação sobre o Sistema Operativo

A *flag -sV* é a que nos permite tirar maior informação sobre os serviços TCP que estão a correr nas portas do sistema, e as respetivas versões. A identificação das versões dos serviços facilita na exploração de vulnerabilidades e ameaças dentro do sistema. Em baixo, encontra-se a identificação dos serviços e as suas versões.

```

(mariolas@mariolas)-[~]
$ nmap -sV 172.20.13.2/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-18 00:19 WET
Nmap scan report for 172.20.13.1
Host is up (0.00018s latency).
All 1000 scanned ports on 172.20.13.1 are closed

Nmap scan report for 172.20.13.2
Host is up (0.0013s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
22/tcp    open  ssh          OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http         Microsoft IIS httpd 7.5
4848/tcp  open  ssl/appserv-http?
8022/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http         Sun GlassFish Open Source Edition 4.0
8383/tcp  open  ssl/http     Apache httpd
9200/tcp  open  wap-wsp?
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC

```

Figura 26: Informação sobre os serviços TCP e as versões associadas

O uso da *flag -sU* também é bastante útil, pois são relativos aos serviços UDP. O UDP é um protocolo da camada de transporte (*Transport Layer* do *OSI Model*), à semelhança do TCP, porém não nos dá garantia que os pacotes transmitidos cheguem ao destino. Não é orientado à conexão, portanto não possui mecanismos de controlo à conexão, nem possui o *Handshake* inicial típico do TCP. O protocolo UDP costuma ser muito empregado em atividades muito dependentes de tráfego rápido de dados, mesmo que isto custe a perda de pacotes. Por isso, aplicações que encaixam num modelo de pergunta-resposta também são fortes candidatas a usar UDP. No entanto, pode ser necessário implementar algoritmos de *timeouts*, *acks* e, no mínimo, retransmissão.

```

(vagrant@kali)-[~]
$ sudo nmap -sU 172.20.13.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 16:47 EST
Nmap scan report for 172.20.13.2
Host is up (0.00045s latency).
All 1000 scanned ports on 172.20.13.2 are open|filtered
MAC Address: 08:00:27:66:24:0F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.75 seconds

```

Figura 27: Informação sobre os serviços UDP

O *scan* usando esta *flag* não nos permite tirar grande informação sobre os serviços nas portas UDP.

3.1.1 Exploração das portas TCP

Agora segue-se as vulnerabilidades relativos a cada serviço TCP identificado em cima. Esta análise de vulnerabilidades permite o atacante saber se o sistema ainda está exposto a algum *exploit*, portanto esta recolha de informação pública, apesar de ser passiva, é crucial na exploração maliciosa do sistema em causa.

O primeiro serviço identificado relativo à porta **21 TCP**, corresponde a um protocolo, denominado por *File Transfer Protocol (FTP)*, é um método usado para transferir ficheiros, num sistema servidor-cliente. Em baixo, apresenta-se uma vulnerabilidade associado a este serviço.

CVE: CVE-2012-2532

Base Score: 5.0 MEDIUM

Descrição: As versões 7.0 e 7.5 do Microsoft IIS processava comandos não especificados antes do estabelecimento da sessão TLS.

Exploração: Os atacantes conseguiam ter acesso a informação sensível através da leitura das respostas a estes comandos.

A porta **22 TCP** é relativo ao serviço SSH (*Secure Socket Shell*), um protocolo de rede que permite aos *users* aceder e gerir servidores remotamente. A versão deste serviço **OpenSSH** é 7.1, usando o protocolo 2.0.

CVE: CVE-2016-1907

Base Score: 5.3 MEDIUM

Descrição: Vulnerabilidade encontrada numa das funções relativas a um pacote da versão 7.1, protocolo 2, do OpenSSH.

Exploração: Esta vulnerabilidade permite que invasores remotos causem ataques DoS (*Denial of Service*)(leitura fora dos limites e falha do aplicativo) através do tráfego da rede.

Relativamente à porta **80 TCP**, o serviço desta porta é do tipo HTTP. O serviço corresponde a um servidor *Web* criado pela Microsoft para os seus Sistemas Operativos. Este tem nome de *Microsoft IIS (Internet Information Services) httpd*. A versão corrente é a 7.5, portanto agora vamos tentar encontrar uma vulnerabilidade associada.

A vulnerabilidade mais recente publicada no *Website cve.mitre.org* é referente ao ano de 2012.

CVE: CVE-2012-2532

Base Score: 5.0 MEDIUM

Descrição: As versões 7.0 e 7.5 do Microsoft IIS processava comandos não especificados antes do estabelecimento da sessão TLS.

Exploração: Os atacantes conseguiam ter acesso a informação sensível através da leitura das respostas a estes comandos.

Algumas das portas que se seguem referem-se a protocolos e ferramentas de um **Apache Server**. O processo *daemon* do serviço *Apache* na porta **8383 TCP**. O serviço *Apache Tomcat/Coyote JSP engine 1.1* é identificado pela porta **8022 TCP**.

O *Apache Server* é um servidor *Web* livre. O serviço *Apache Jserv* é um protocolo binário que pode funcionar como um *proxy* de pedidos de entrada, de um servidor *Web* para um servidor de aplicações. Por último, o *Apache Tomcat/Coyote* é uma derivação do *Apache Server*, funcionando como um servidor *Web* escrito em *Java*, e o *Coyote* suporta HTTP 1.1 e funciona de suporte ao servidor *Web*.

CVE: CVE-2017-12615

Base Score: 8.1 HIGH

Descrição: Vulnerabilidade encontrada em algumas versões do *Apache Tomcat* em *Windows*.

Exploração: Enquanto corria o *Apache Tomcat* com HTTP PUTs ativo, era possível dar *upload* de um ficheiro *JSP* para o servidor *Web* através de um pedido maliciosamente criado. Este poderia então ser solicitado, e qualquer código nele contido seria executado pelo servidor.

CVE: CVE-2005-2090

Base Score: 4.3 MEDIUM

Descrição: Vulnerabilidade exposta publicamente relativas a versões do *Tomcat 5.0.19 (Coyote/1.1)* e *Tomcat 4.1.24 (Coyote/1.0)*.

Exploração: Permite que invasores, de forma remota, manipulem e comprometam a cache da *web*, ignorem a proteção do *firewall* e conduzam ataques XSS por meio de uma solicitação HTTP. O *Tomcat* encaminha incorretamente a solicitação, fazendo com que o servidor recetor o processe como uma solicitação HTTP separada.

O serviço seguinte identificado referente às portas TCP do sistema, com versão identificada, é um serviço *httpd*, na porta **8080 TCP**, de nome *Sun GlassFish Open Source Edition 4.0*, sendo este um servidor de aplicações *Open Source*.

Relativamente a esta versão *Edition 4.0* não foi encontrada nenhuma vulnerabilidade publicamente exposta. No entanto existe uma vulnerabilidade relacionada com a versão posterior a esta, a *Edition 4.1*, que estava exposta a travessias não autorizadas (**CVE-2017-1000028**).

As portas **49153 TCP** **49154 TCP** correspondem ao serviço **RPC** do *Windows*, este serviço é denominado como *Remote Procedure Call*, sendo este

uma tecnologia de comunicação entre processos que permite a um programa de computador chamar um procedimento em outro espaço de endereçamento.

A vulnerabilidade mais recente encontrada sobre este serviço, dentro do sistema operativo em causa, *Windows 7 SP1*, é relativo ao ano de 2016.

CVE: CVE-2016-0178

Base Score: 8.8 HIGH

Descrição: O *RPC NDR Engine* dentro de vários sistemas operativos, incluindo o que estamos a explorar, administram mal algumas operações.

Exploração: Isto permite que invasores remotos executem código arbitrário por meio de solicitações RPC mal formadas, também conhecido como "Vulnerabilidade de elevação de privilégios do mecanismo de representação de dados de rede RPC".

3.2 Questão 2

3.2.1 Scan de vulnerabilidades no Nessus

Nesta questão, é pedida a utilização de um Scanner de vulnerabilidades, em que no nosso caso escolhemos o Nessus. Assim sendo, utilizamos o Nessus para fazer a varredura ativa ao sistema *Metasploitable 3*, que seguindo as indicações do enunciado, terá o IP 172.20.13.2 .

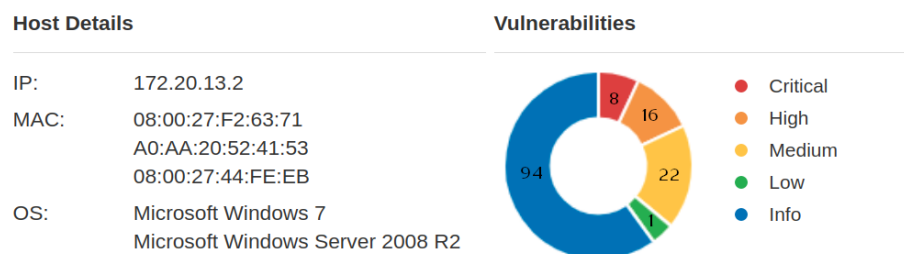


Figura 28: Detalhes do *scan* no Nessus ao sistema Metasploitable 3

As vulnerabilidades encontradas são divididas em 5 categorias:

- **Critical** (8 vulnerabilidades encontradas)
- **High** (16 vulnerabilidades encontradas)
- **Medium** (22 vulnerabilidades encontradas)
- **Low** (1 vulnerabilidades encontradas)
- **Info** (94 vulnerabilidades encontradas)

De forma a que se torne mais legível, iremos colocar aqui uma tabela com as categorias de vulnerabilidades, excluindo as vulnerabilidades da categoria *Info*.

Sev ▼	Name	Family	Count
MIXED	14 PHP (Multiple Issues)	CGI abuses	14
MIXED	4 Zohocorp Manageengine Des...	CGI abuses	12
MIXED	9 Apache HTTP Server (Multipl...	Web Servers	15
MIXED	7 SNMP (Multiple Issues)	SNMP	7
MIXED	3 Web Server (Multiple Issues)	Web Servers	4
MIXED	5 HTTP (Multiple Issues)	Web Servers	15
MIXED	8 SSL (Multiple Issues)	General	8
MIXED	2 Apache Tomcat (Multiple Issu...	Web Servers	3
MIXED	3 TLS (Multiple Issues)	Service detection	3
MIXED	2 IETF Md5 (Multiple Issues)	General	2
LOW	SSL/TLS Diffie-Hellman Modulus <...	Misc.	1

Figura 29: Categorias das vulnerabilidades excluindo Info.

Além das vulnerabilidades, o Nessus também disponibiliza um conjunto de ações na secção *Remediations*, que irão minimizar ou eliminar as vulnerabilidades expostas anteriormente.

Action	Vulns ▼	Hosts
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities: Upgrade to PHP version 5.3.29 or later.	35	1
Apache 2.2.x < 2.2.34 Multiple Vulnerabilities: Upgrade to Apache version 2.2.34 or later.	25	1
ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check): Upgrade to ManageEngine Desktop Central version 10 build 100479 or later. Alternatively, apply the manual, vendor-supplied workaround.	2	1

Figura 30: Ações sugeridas na secção *Remediations*.

De uma forma geral, os resultados do *scan* no Nessus expôs várias vulnerabilidades em várias categorias, sendo que a categoria com mais exposição é a *CGI abuses*, relacionada com a versão do PHP utilizada, que teve 14 vulnerabilidades associadas (2 critical, 7 high e 5 medium).

3.2.2 Comparação com a Questão 1

Em comparação à Questão 1, podemos identificar uma diferença notória a nível de descoberta de possíveis vulnerabilidades. Na Questão 1, como já referido, fizemos uma recolha de informação sobre o sistema *Metasploitable 3* usando técnicas e ferramentas de *scan* ativa. Este *scan*, ou varredura, consistiu maioritariamente no uso da ferramenta *nmap*, e sendo esta ferramenta um *scanner* de portas, não conseguiu identificar pacotes instalados dentro do Sistema Operativo.

Como podemos ver, a versão PHP utilizada no sistema teve o maior número de vulnerabilidades, com 14. O PHP é uma linguagem de *script* que está associada ao serviço do *Apache*. O uso do *nmap*, apesar de sabermos que existia um serviço *Apache* numa das portas, não permitiu encontrar os pacotes e as versões do PHP associados, para que fosse possível a procura dos CVEs relativos a possíveis vulnerabilidades associadas, portanto considera-se assim, uma grande diferença entre as duas abordagens tomadas nas diferentes questões.

Para além disto, o uso do Nessus facilita bastante na procura de vulnerabilidades porque, por exemplo, os serviços relacionados com o *Apache* associados à varredura de portas TCP (*nmap -sV*) permitiu-nos saber as versões dos serviços, porém as vulnerabilidades, relativas às versões corretas, expostas publicamente são, ou inexistentes, ou difíceis de encontrar.

3.3 Questão 3

Nesta questão, é pedido para avaliar dois eventos identificados como tráfego anômalo, detetado pelo IDS, neste caso o Snort. Tendo em atenção a configuração exposta no enunciado, o Snort gera *logs* mais detalhados com a ativação do *alert_full*. Escolhemos então os seguintes eventos do ficheiro *alert.full*:

3.3.1 Evento 1

```
BAD TRAFFIC

[**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**]
[Classification: Misc activity] [Priority: 3]
12/14-19:21:53.234345 08:00:27:C9:E6:09 ->
08:00:27:F2:63:71 type:0x800 len:0x3C 172.20.13.1:53414
-> 172.20.13.2:0 TCP TTL:64 TOS:0x0 ID:59620 IpLen:20
DgmLen:40 *****S* Seq: 0xD3AFB3B Ack: 0x0 Win: 0x200
TcpLen: 20
```

Este evento foi reportado devido a existir tráfego TCP na **porta 0 TCP**. Normalmente, esta porta é reservada e não tráfego nesta porta é irregular, e pode ser sinal de possível ataque. O Snort classifica este evento como *"Attempted Information Leak"* e dá uma prioridade de 2.

Não há nenhuma vulnerabilidade, nem nenhum CVE associado a este evento porque se trata de um tráfego irregular feito pelo Nessus, ao fazer *port scanning*.

```
(Event)
sensor id: 0      event id: 1      event second: 1607991713      event microsecond: 234345
sig id: 524      gen id: 1      revision: 8      classification: 29
priority: 3      ip source: 172.20.13.1 ip destination: 172.20.13.2
src port: 53414  dest port: 0      protocol: 6      impact_flag: 0 blocked: 0
```

Figura 31: Informação relativa ao evento 1 no ficheiro *snort.alert* .

```
Packet
sensor id: 0      event id: 1      event second: 1607991713
packet second: 1607991713      packet microsecond: 234345
linktype: 1      packet_length: 60
[  0] 08 00 27 F2 63 71 08 00 27 C9 E6 09 08 00 45 00  ..'.cq..'.....E.
[ 16] 00 28 E8 E4 00 00 40 06 1F C0 AC 14 0D 01 AC 14  .(....@.....
[ 32] 0D 02 D0 A6 00 00 0D 3A FB 3B 00 00 00 00 50 02  .....:.;....P.
[ 48] 02 00 62 9A 00 00 00 00 00 00 00 00 00 00 00  ..b.....
```

Figura 32: Informação relativa ao evento 1 no ficheiro *snort.log* .

```

144 34.824904972 172.20.13.1 172.20.13.2 TCP 60 53414 - 0 [SYN] Seq=0 Win=512 Len=0
146 36.808073804 172.20.13.1 172.20.13.2 TCP 60 [TCP Retransmission] 53414 - 0 [SYN] Seq=0 Win=512 Len=0
148 38.960108172 172.20.13.1 172.20.13.2 TCP 60 [TCP Retransmission] 53414 - 0 [SYN] Seq=0 Win=512 Len=0
Frame 144: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0
  Interface id: 0 (eth1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 15, 2020 00:21:53.234345797 WET
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1007991713.234345797 seconds
  [Time delta from previous captured frame: 0.497733366 seconds]
  [Time delta from previous displayed frame: 0.497733366 seconds]
  [Time since reference or first frame: 34.824904972 seconds]
  Frame Number: 144
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: TCP SYN/FIN]
  [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
  Ethernet II, Src: PcsCompu_c9:e6:09 (08:00:27:c9:e6:09), Dst: PcsCompu_f2:63:71 (08:00:27:f2:63:71)
  Internet Protocol Version 4, Src: 172.20.13.1, Dst: 172.20.13.2
  Transmission Control Protocol, Src Port: 53414, Dst Port: 0, Seq: 0, Len: 0
    Source Port: 53414
    Destination Port: 0
    [Stream index: 10]
    [TCP Segment Len: 0]
    Sequence number: 0 (relative sequence number)
    Sequence number (raw): 221969211
    [Next sequence number: 1 (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x002 (SYN)
    Window size value: 512
    [Calculated window size: 512]
    Checksum: 0x629a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  [Timestamps]

```

Figura 33: Informação relativa ao evento 1 no analisador de tráfego *Wireshark*

3.3.2 Evento 2

```

ICMP PING NMAP
[**] [1:469:3] ICMP PING NMAP [**] [Classification:
Attempted Information Leak] [Priority: 2]
12/14-19:22:08.677382 08:00:27:C9:E6:09 ->
08:00:27:F2:63:71 type:0x800 len:0x3C 172.20.13.1
-> 172.20.13.2 ICMP TTL:1 TOS:0x0 ID:47286 IpLen:20
DgmLen:28 Type:8 Code:0 ID:1 Seq:1 ECHO [Xref =>
http://www.whitehats.com/info/IDS162]

```

Neste caso, o Snort detetou que o sistema estava a ser alvo de um *ICMP ping* pelo *nmap*, ou seja, detetou que estava a ser alvo de um *scan* ativo por outro sistema, possivelmente malicioso.

Como o evento anterior, este evento não possui CVE associado pois relata um possível *scan*, e não uma vulnerabilidade do sistema em si.

```

(Event)
sensor id: 0      event id: 4      event second: 1607991728      event microsecond: 677382
sig id: 469      gen id: 1      revision: 3      classification: 4
priority: 2      ip source: 172.20.13.1 ip destination: 172.20.13.2
src port: 8      dest port: 0      protocol: 1      impact_flag: 0 blocked: 0

```

Figura 34: Informação relativa ao evento 2 no ficheiro *snort.alert* .

```

Packet
  sensor id: 0      event id: 4      event second: 1607991728
  packet second: 1607991728      packet microsecond: 677382
  linktype: 1      packet length: 60
[  0] 08 00 27 F2 63 71 08 00 27 C9 E6 09 08 00 45 00 ..'.cq..'.....E.
[ 16] 00 1C B8 B6 00 00 01 01 8E FF AC 14 0D 01 AC 14 .....
[ 32] 0D 02 08 00 F7 FD 00 01 00 01 00 00 00 00 00 .....
[ 48] 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Figura 35: Informação relativa ao evento 2 no ficheiro *snort.log* .

```

# 157 50.267941695 172.20.13.1 172.20.13.2 ICMP 60 Echo (ping) request id=0x0001, seq=1/256, ttl=1 (no response)
# Frame 157: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0
  Interface id: 0 (eth1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 15, 2020 00:22:08.677382430 WET
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1607991728.677382430 seconds
  [Time delta from previous captured frame: 0.711622848 seconds]
  [Time delta from previous displayed frame: 12.056437287 seconds]
  [Time since reference or first frame: 50.267941695 seconds]
  Frame Number: 157
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
  Ethernet II, Src: PcsCompu_c9:e6:09 (08:00:27:c9:e6:09), Dst: PcsCompu_f2:63:71 (08:00:27:f2:63:71)
  Internet Protocol Version 4, Src: 172.20.13.1, Dst: 172.20.13.2
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7fd [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
  [No response seen]
  [Expert Info (Warning/Sequence): No response seen to ICMP request]
  [No response seen to ICMP request]
  [Severity level: Warning]
  [Group: Sequence]

```

Figura 36: Informação relativa ao evento 2 no analisador de tráfego *Wireshark*

3.4 Questão 4

Os eventos apresentados na Questão anterior, correspondem a este tipo de eventos que não têm vulnerabilidades correspondentes. Numa tentativa de explicar o nosso ponto de vista, segue-se uma pequena contextualização dos conceitos de IDS e *Scanner* de Vulnerabilidades.

Os **Sistemas de Detecção de Intrusão (IDS)** monitorizam tráfego suspeito, tentando identificar a presença de atividades intrusivas. Isto engloba todos os processos utilizados na descoberta de utilizações não autorizadas de dispositivos de rede ou de computadores. Isto é feito através de um software projetado especificamente para tal propósito. O Snort, o IDS que utilizamos, faz a análise de tráfego em tempo real dentro de uma rede, e assim identifica potenciais ataques ou anormalidades.

Um **Scanner de Vulnerabilidades** é um *software* que, dado um determinado alvo, seja ele um *software*, um computador ou um dispositivo de rede, irá analisá-lo em busca de vulnerabilidades existentes. O *Scanner* irá, sistematicamente, testar o alvo em busca de pontos vulneráveis a ataques. O Nessus testa cada porta de um computador, determina qual serviço dessa porta e, em

seguida, testa esse serviço para garantir que não há vulnerabilidades que possam ser usadas por um *hacker* num ataque malicioso.

A combinação dos dois em cima referidos funciona como, o *Scanner* enviará pacotes a portas específicas de modo a identificar os serviços nas correspondentes portas do Sistema Alvo, funcionando como um *port scanner* mas mais complexo. O IDS captura estes pacotes que identificam o tráfego nessas portas. Para além disso também retorna eventos com vulnerabilidades associadas.

Portanto, sendo que o Snort está à escuta na ligação entre as duas máquinas, à espera de pacotes e de tráfego suspeito, é de esperar que retorne informação que não tem qualquer vulnerabilidade associada, porque captura os pacotes usados pelo *port scanning* do Nessus. Um exemplo disso, é o **Evento 1** em cima referido, onde o Snort avisa sobre tráfego suspeito numa das portas TCP (neste caso, foi na **porta 0** que, como explicado em cima, se trata de uma porta reservada).

3.5 Questão 5

Nesta questão, resolvemos corrigir vulnerabilidades associadas ao PHP, visto que está no ponto mais crítico reportado pelo Scanner de Vulnerabilidades, isto porque conta com um total de 14 vulnerabilidades, sendo essas compostas por 2 Critical, 7 High e 5 Medium. Olhando para a sugestão do Nessus, uma das remediations é *Upgrade to PHP version 5.3.29 or later*. No entanto, antes de prosseguir para a solução, temos de encontrar onde está o problema.

Sev ▼	Name ▲	Family ▲	Count
CRITICAL	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities	CGI abuses	1
CRITICAL	PHP Unsupported Version Detection	CGI abuses	1
HIGH	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.13 CGI Query String Code Execution	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities	CGI abuses	1
HIGH	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	PHP < 5.3.11 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	PHP < 7.3.24 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass	CGI abuses	1

Figura 37: Vulnerabilidades associadas ao PHP 5.3.10

Observando os *Program Files* e *Program Files x86*, não há indícios de nenhuma instalação do PHP.

















Name ^	Date modified	Type
 7-Zip	11/30/2020 10:00 AM	File folder
 Apache Software Foundation	11/30/2020 9:38 AM	File folder
 Common Files	7/13/2009 8:20 PM	File folder
 elasticsearch-1.1.1	11/30/2020 9:59 AM	File folder
 Internet Explorer	11/20/2010 7:33 PM	File folder
 Java	11/30/2020 9:38 AM	File folder
 jenkins	11/30/2020 9:40 AM	File folder
 jmx	11/30/2020 9:42 AM	File folder
 OpenSSH	11/30/2020 9:25 AM	File folder
 Orade	11/30/2020 10:00 AM	File folder
 Rails_Server	11/30/2020 9:50 AM	File folder
 Reference Assemblies	11/30/2020 9:30 AM	File folder
 Windows Mail	11/20/2010 7:33 PM	File folder
 Windows NT	7/13/2009 10:37 PM	File folder
 WindowsPowerShell	11/30/2020 9:26 AM	File folder
 wordpress	11/30/2020 9:41 AM	File folder

Figura 38: Programas em Program Files.









Name ^	Date modified	Type
 Common Files	11/30/2020 9:34 AM	File folder
 Internet Explorer	11/20/2010 7:33 PM	File folder
 Java	11/30/2020 9:33 AM	File folder
 Microsoft.NET	11/30/2020 9:21 AM	File folder
 Reference Assemblies	11/30/2020 9:30 AM	File folder
 Windows Mail	11/20/2010 7:33 PM	File folder
 Windows NT	7/13/2009 10:37 PM	File folder
 WindowsPowerShell	11/30/2020 9:26 AM	File folder

Figura 39: Programas em Program Files x86.

Após alguma pesquisa, encontramos uma pasta relativa ao WAMP (Windows, Apache, MySQL, PHP). Isto trata-se de uma *solution stack* que permite desenvolver e instalar software de faça uso do Apache, MySQL e PHP. Permite utilizar diferentes versões de software referido anteriormente, e no caso da máquina virtual do Windows Server 2008 que estávamos a utilizar, estavam em utilização o PHP 5.3.10, Apache 2.2.21 e MySQL 5.0.8. Podemos verificar que

realmente estas são as versões a serem utilizadas, por exemplo, acedendo ao serviço *phpMyAdmin* (app instalada no WAMP):



Figura 40: Informação das versões de software no phpMyAdmin.

Além disso, estavam também instalados as seguintes aplicações no WAMP:

- phpMyAdmin 3.4.10.1
- SQLbuddy 1.3.3
- WebGrind 1.0

Portanto, agora que temos a origem do nosso PHP, podemos então pensar numa forma de o atualizar. Decidimos seguir a *remediation* exposta no Nessus, e vamos atualizar a versão do PHP para 5.3.29. Visto que esta máquina virtual está restringida à rede privada virtual imposta, utilizamos a ligação existente criada pela máquina virtual de *development* associada (ub1404), que foi criada juntamente com a máquina virtual alvo, seguindo os passos de instalação exposto na documentação oficial do *Metasploitable 3*, pelo Vagrant. Portanto, o procedimento passou por fazer download dos ficheiros relativos à versão 5.3.29 do PHP para Windows, que já é uma *unsupported version*. Posteriormente, usando Secure Copy (scp), o ficheiro zip foi copiado para a diretoria partilhada `/var/www/html`. Por fim, foi feito *unpack* dos ficheiros, e copiados os ficheiros de configuração relativos ao WAMP para a nova versão do PHP, de modo a que a nova versão ficasse configurada corretamente. Por fim, eliminamos a versão antiga, para que esta não fosse detetada pelo Nessus. Acedendo novamente ao phpMyAdmin, verificamos realmente que já temos a nova versão do PHP instalada corretamente.



Figura 41: Informação das versões de software no phpMyAdmin após atualização do PHP.

Agora que temos a versão atualizada do PHP para 5.3.29, iremos fazer uma nova análise com o Scanner de vulnerabilidades Nessus.

Sev ▼	Name ▲	Family ▲	Count ▼
MIXED	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	12
MIXED	PHP (Multiple Issues)	CGI abuses	2
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	15
MIXED	SNMP (Multiple Issues)	SNMP	7
MIXED	Web Server (Multiple Issues)	Web Servers	4
MIXED	HTTP (Multiple Issues)	Web Servers	15
MIXED	SSL (Multiple Issues)	General	8
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	TLS (Multiple Issues)	Service detection	3
MIXED	IETF Md5 (Multiple Issues)	General	2
LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1

Figura 42: Scan após atualização do PHP para 5.3.29

Comparando com o scan inicial (Figura 29) a única diferença são as vulnerabilidades do PHP, que passaram de 14 para 2, sendo uma 1 critical e 1 medium.

Sev ▼	Name ▲	Family ▲	Count ▼
CRITICAL	PHP Unsupported Version Detection	CGI abuses	1
MEDIUM	PHP < 7.3.24 Multiple Vulnerabilities	CGI abuses	1

Figura 43: Vulnerabilidades associadas ao PHP 5.3.29

A vulnerabilidade *critical* só será resolvida quando o PHP for atualizado para uma versão com suporte atualmente, ou seja, 7.3 ou superior. A outra vulnerabilidade não é especificada, a descrição apenas expõe ser afetada a algumas vulnerabilidades, corrigidas na versão 7.3.24 e posteriores. Portanto, ao atualizar o PHP da versão 5.3.10 para 5.3.29, retiramos 1 vulnerabilidade Critical, 7 vulnerabilidades High (todas) e 4 vulnerabilidades Medium. Este é o máximo de vulnerabilidades de conseguimos retirar atualizando apenas a versão do PHP, pois versões posteriores do PHP 7 têm dependências que fazem com que sejam necessárias mais alterações.

No entanto, quisermos ir mais além e tentar retirar por completo as vulnerabilidades associadas ao PHP. Para isso, tivemos de expandir o alcance das alterações, visto que a última versão do PHP, 8.0.0, é incompatível com algum do software que tínhamos disponível, nomeadamente o Apache (necessita da versão 2.4 ou superior, e estava em uso a versão 2.2.21), e da versão do VC (Visual C++, que para o PHP 5.3.x necessita da versão 9 e para o PHP 8.0.0 necessita da versão 16). Portanto, seguimos uma abordagem semelhante à referida anteriormente, fazer download dos ficheiros necessários e fazer a passagem com o auxílio da máquina virtual de desenvolvimento. Após alguma configuração e alterações, conseguimos com que ficassem as versões mais recentes em prática, mas devido a alguma falta de configuração, as aplicações disponíveis no WAMP necessitam de uma migração para a nova versão do Apache, visto que as configurações entre as versões 2.2 e 2.4 são ligeiramente diferentes. De qualquer das formas, como esse não era o foco deste trabalho, apenas ficamos por deixar o Apache e PHP funcionais, sem dar demasiada importância às configurações das aplicações no WAMP.

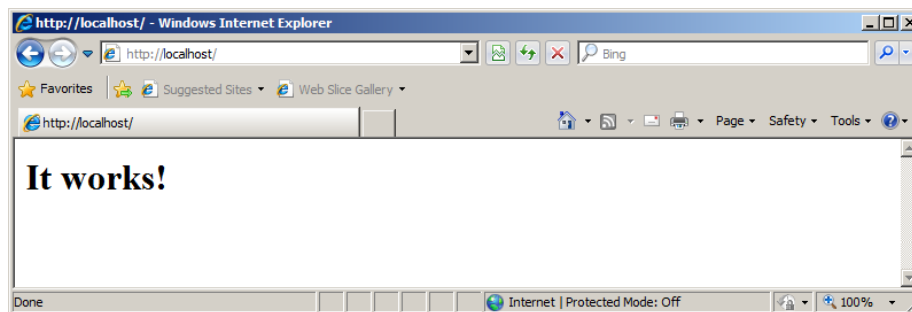


Figura 44: Apache 2.4.46 em funcionamento com PHP 8.0.0

Portanto, acabamos por deixar em funcionamento no WAMP as últimas versões do PHP e Apache (8.0.0 e 2.4.46, respetivamente).

```
C:\wamp\bin\php\php8.0.0>php.exe -v
PHP 8.0.0 (cli) (built: Nov 24 2020 22:04:36) < ZTS Visual C++ 2019 x86 >
Copyright (c) The PHP Group
Zend Engine v4.0.0-dev, Copyright (c) Zend Technologies
```

Figura 45: Última versão do PHP instalada

```
C:\wamp\bin\apache\Apache2.4.46\bin>httpd.exe -v
Server version: Apache/2.4.46 (Win32)
Apache Lounge OS16 Server built: Dec 9 2020 12:37:29
```

Figura 46: Última versão do Apache instalada

Para concluir, fizemos um último scan de vulnerabilidades as diferenças entre PHP 5.3.29 e PHP 8.0.0 (e dependências associadas).

<input type="checkbox"/> Sev ▾	Name ▲	Family ▲	Count ▾
<input type="checkbox"/> MIXED 4	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	12
<input type="checkbox"/> MIXED 7	SNMP (Multiple Issues)	SNMP	7
<input type="checkbox"/> MIXED 3	Web Server (Multiple Issues)	Web Servers	3
<input type="checkbox"/> MIXED 5	HTTP (Multiple Issues)	Web Servers	16
<input type="checkbox"/> MIXED 8	SSL (Multiple Issues)	General	8
<input type="checkbox"/> MIXED 2	Apache Tomcat (Multiple Issues)	Web Servers	3
<input type="checkbox"/> MIXED 3	TLS (Multiple Issues)	Service detection	3
<input type="checkbox"/> MIXED 2	IETF Md5 (Multiple Issues)	General	2
<input type="checkbox"/> LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1

Figura 47: Scan de vulnerabilidades após atualizações para as versões mais recentes

Portanto, podemos então observar que as vulnerabilidades restantes do PHP e as vulnerabilidades do Apache HTTP Server desapareceram (comparando com a Figura 43). Portanto, contamos então com uma eliminação de todas as 14 vulnerabilidades associadas ao PHP (2 Critical, 7 High e 5 Medium), e como consequência da atualização do PHP, com a eliminação de todas as 8 vulnerabilidades do Apache (2 High e 6 Medium).

4 Conclusões

Dado como terminado o segundo trabalho prático da Unidade Curricular de Segurança de Sistemas Informáticos, podemos agora passar às conclusões e observações finais, bem como as dificuldades apresentadas no desenvolver deste trabalho prático.

Na parte A do trabalho, relativa ao processo de varredura passiva, não houve muitas dificuldades, apenas tivemos que aplicar ferramentas, previamente estudadas na aula, de forma a expor informação pública da infra-estrutura explorada. Conseguimos obter informações como *emails* privados, servidores DNS autoritativos dos domínios, e alguma informação relativo a colaboradores das empresas, no entanto, achamos que a postura de segurança de ambas as empresas é forte.

A parte B do trabalho, relativa ao processo de varredura ativa, trouxe dificuldades de configuração da máquina *Metasploitable*. Inicialmente, o grupo optou por fazer separadamente esta varredura ao sistema, para comparar os resultados obtidos no *Scanner* de Vulnerabilidades e no IDS. No entanto, por falha de comunicação, notamos que a máquina proveniente do ficheiro *.ova* e a máquina proveniente do *Vagrant file*, são de versões diferentes, e a primeira mencionada tem muitos mais serviços nas portas TCP do que na segunda, portanto tanto os resultados do **nmap**, como do **Nessus** eram completamente diferentes. Posteriormente, optamos por usar os ficheiros *Vagrant* do Github, como referido anteriormente. Notamos também que a máquina *Metasploitable*, devido à falta de licença *Windows*, ia constantemente abaixo, dificultando o processo de varredura. Tirando estas dificuldades, o processo de configuração e de resposta às questões foi bastante acessível.

Em suma, concluímos que a realização deste trabalho prático permitiu-nos consolidar os conhecimentos estudados nas aulas da disciplina, relativamente aos conceitos de *Footprinting* e *Penetration Testing*.