Universidade do Minho
Escola de Engenharia

Trabalho Prático II

Tecnologias de Segurança

Trabalho realizado por:
Filipe Freitas (PG42828)
Maria Barbosa (PG42844)

Dezembro de 2020

Índice

Lista de Figuras

Capítulo 1

Introdução

"The way to be safe is never to feel secure." (Benjamin Franklin)

1.1 Contextualização

Os testes de penetração, tem como principal objetivo detectar e explorar vulnerabilidades num sistema para validar a eficácia dos seus mecanismos de segurança. Permitindo ainda, recomendar soluções para mitigar essas vulnerabilidades. Os testes de penetração, podem ser divididos em cinco fases: **Reconnaissance, Scanning, Gaining access, Maintaining access, Analyze** como mostra a figura 1.1.

Neste trabalho pretende-se aplicar o conhecimento adquirido nas aulas sobre as as duas primeiras fases dos testes de penetração:

- **Reconnaissance.** Corresponde a recolha passiva de informações e de dados do alvo para explorar o ataque.
- **Scanning.** Corresponde a utilização de informações adquiridas durante a fase de reconhecimento para comunicar diretamente com os alvos com a intenção de identificar potenciais ameaças e vulnerabilidades.

1.2 Estrutura do relatório

Este relatório divide-se em quatro partes principais:

- A primeira corresponde a esta introdução e pretende efectuar uma contextualização sobre o tema.

- Na segunda parte, respondemos a parte A deste enunciado, e com a utilização de técnicas de busca passiva procuramos identificar detalhes sobre os sistemas e infra-estrutura de duas empresas.
- A terceira apresenta as respostas a cinco questões da parte B, com recurso a ferramentas de varredura ativa.
- Na última parte é feita uma conclusão, onde se apresenta uma breve síntese do trabalho realizado.

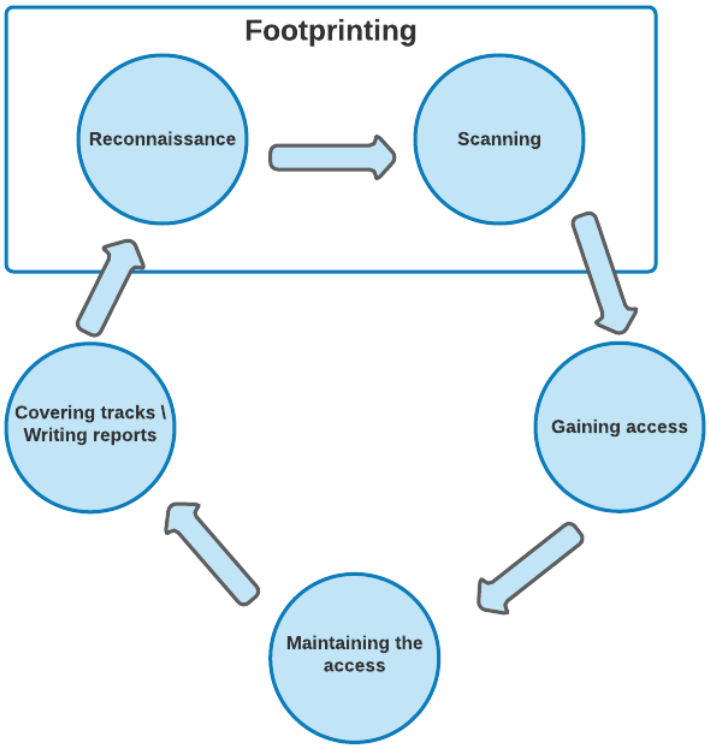

Figura 1.1: Esquema cíclico dos Testes de penetração.

Capítulo 2

Parte A: Reconnaissance

Tal como já foi referido a primeira parte deste trabalho corresponde a recolha passiva de informação sobre duas empresas. Para isso, escolhemos as duas de modo a que apresentem dimensões distintas, permitindo assim perceber a diferença entre as medidas de segurança adoptadas por cada uma delas.

1. Primavera - Business Software Solutions - Empresa que se dedica ao desenvolvimento tecnológico de soluções de gestão. Conta com mais 40 mil clientes espalhados por 20 países.
2. Waveform - Empresa que se dedica essencialmente ao desenvolvimento de aplicações para Smartphones e tablets, aplicações e portais web prestando também acessória na construção de estratégias de mobilidade.

Vamos recolher passivamente, para cada uma delas, toda a informação disponível, como o ramo de atuação, existência de filiais, endereços de emails, nomes dos indivíduos que se encontram nos principais cargos. Para isso vamos analisar, entre outras coisas, o domínio, IPs e conteúdo disponível na web.

Um domínio é um nome de fácil memorização e que serve para localizar e identificar o servidor de uma página web. A informação da localização destes servidores está noutro servidor (chamado servidor de nomes) que assegura a indicação do endereço certo para a entrega dos pedidos enviados pelo nosso computador para a Internet. Essa tarefa é operada através da conversão do nome de domínio indicado pelo nosso computador num endereço IP, que identifica a localização dos computadores na Internet [2].

2.1 Primavera - Business Software Solutions

Como foi referido anteriormente a *Primavera Business Software Solutions* é uma tecnológica Portuguesa que se dedica ao desenvolvimento de soluções de gestão. Foi fundada por dois antigos alunos da Uminho, José Dionísio e Jorge Baptista e possui mais de 20 anos de experiência, trabalhando diariamente com mais de 40 mil clientes, distribuídos por 20 países [1].

2.1.1 Procura de informações na Web

Inicialmente, começamos por analisar a página WEB da empresa. Na página principal primaverabss.com, é possível encontrar um conjunto de links para redes sociais, como é o caso do Linkdin(https://www.linkedin.com/company/primaverabss/). Aqui conseguimos obter as seguites informações:

- Descrição da empresa e apresentação das áreas de trabalho;
- Moradas das sedes e filiações ao redor do mundo;

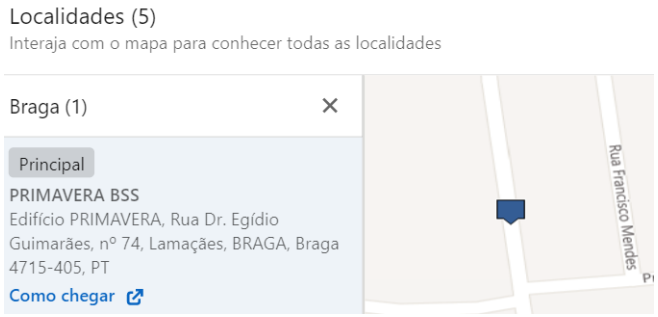

Figura 2.1: Morada da sede de Braga.

- Nomes de 325 funcionários da empresa e respectivas contas linkdin. Para alguns deles é ainda apresentada uma foto, dados pessoais (educação, morada, trabalhos anteriores etc). Estes dados poderão ser usados por exemplo para executar ataques de Engenharia social, onde o hacker pode manipular as vítimas para que executem certas ações ou transmitam informações internas.

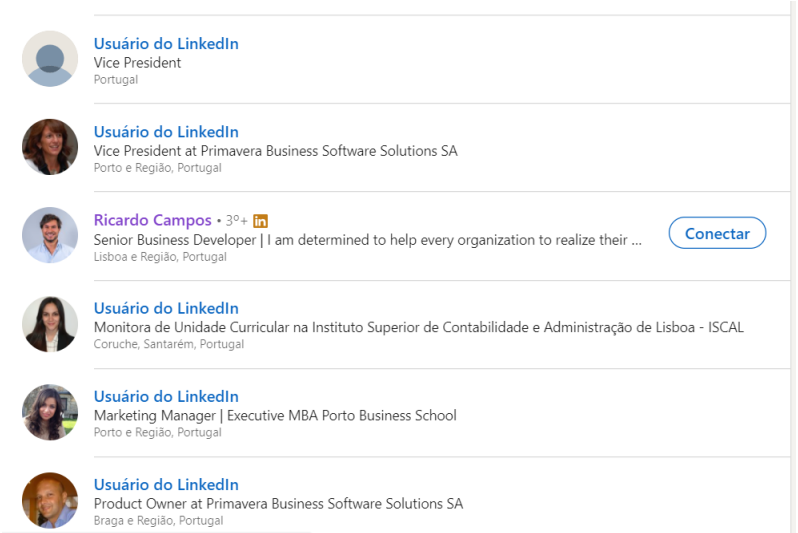

Figura 2.2: Alguns funcionários da empresa.

- Ofertas de emprego. Uma análise, as ofertas existentes, permite concluir quais os principais programas utilizados, permitindo ao atacante prever algumas das suas vulnerabilidades, promovendo uma maior probabilidade de sucesso no ataque. A figura 2.3 apresenta uma dessas ofertas, donde

se pode supor que as bases de dados da empresa são essencialmente SQL, e que certamente alguns dos dados da empresa estão guardados no formato XML e JSON, além de que utilizam as tecnologias: Microsoft C#, Net Framework, TFS.

O que procuramos?
Formação base em Engenharia Informática e/ou similar;
Experiência profissional minima de 5 anos em funções de desenvolvimento com tecnologias Microsoft C#, .Net Framework, .NET Core, Visual Studio, TFS;
Excelentes conhecimentos de Base de Dados (MS SQL Server);
Experiência profissional confirmada com Webservices (REST/SOAP/WSDL), XML, JSON, JavaScript;
Conhecimentos de Web Development (por exemplo: HTML5, Bootstrap, Angular ou semelhante, CSS);
Conhecimentos de Mobile frameworks (por exemplo: Xamarin, Ionics,...) e NoSQL Databases (preferencial);
Experiência prévia no desenvolvimento sobre o ERP PRIMAVERA (preferencial);
Experiência na implementação ou utilização avançada de soluções de gestão (preferencial).

Figura 2.3: Oferta de emprego disponível no linkdin da Primavera.

Além disto, na página Web é possível encontrar um conjunto de contactos telefónicos e emails das várias sedes desta empresa.

Realizando uma análise rápida ao source code da página Web não se encontrou nenhuma informação relevante a cerca da empresa, não existindo conteúdo disponibilizado de forma desprotegida.

2.1.2 Análise do domínio e IP

Recorrendo-se a ferramenta WhoIs, é possível encontrar algumas informações disponíveis sobre o domínio, *primaverabss.com*, como mostram as imagens 2.4 e 2.5.

```
┌──(maria㉿ LAPTOP-9U8LMMFI)-[~]
└─$ whois primaverabss.com
   Domain Name: PRIMAVERABSS.COM
   Registry Domain ID: 339162861_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2020-01-20T05:01:13Z
   Creation Date: 2006-02-08T16:12:19Z
   Registry Expiry Date: 2021-02-08T16:12:19Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: ok https://icann.org/epp#ok
   Name Server: NS1-06.AZURE-DNS.COM
   Name Server: NS2-06.AZURE-DNS.NET
   Name Server: NS3-06.AZURE-DNS.ORG
   Name Server: NS4-06.AZURE-DNS.INFO
   DNSSEC: unsigned
```

Figura 2.4: Output obtido com o comando **whois primaverabss.com**

Da análise do output, observa-se que os dados obtidos apresentam pouca informação relevante sobre o domínio. Aquelas que poderiam ter um maior potencial encontram-se ”mascaradas”, como é o caso

da entidade que efectuou o registo e de e-mails e contactos dos responsáveis. Quer isto dizer que ou não foram publicados detalhes de contacto do proprietário do domínio ou foi dada a instrução de que os mesmo devem permanecer privados.

Ainda assim, é possível observar que o domínio *primaverabss.com* foi registado pela *Network Solutions, LLC* a 08/02/2006 e a última actualização ocorreu a 20/01/2020. Além disso, são referidos quatro *name servers*: *ns1-06.azure-dns.com, ns2-06.azure-dns.net, ns3-06.azure-dns.org, ns4-06.azure-dns.info*

```
Domain Name: PRIMAVERABSS.COM
Registry Domain ID: 339162861_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2020-01-20T05:01:48Z
Creation Date: 2006-02-08T16:12:19Z
Registrar Registration Expiration Date: 2021-02-08T16:12:19Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Statutory Masking Enabled
Registrant Name: Statutory Masking Enabled
Registrant Organization: Statutory Masking Enabled
Registrant Street: Statutory Masking Enabled
Registrant City: Statutory Masking Enabled
Registrant State/Province: BR
Registrant Postal Code: Statutory Masking Enabled
Registrant Country: PT
Registrant Phone: Statutory Masking Enabled
Registrant Phone Ext: Statutory Masking Enabled
Registrant Fax: Statutory Masking Enabled
Registrant Fax Ext: Statutory Masking Enabled
Registrant Email: abuse@web.com
Registry Admin ID: Statutory Masking Enabled
Admin Name: Statutory Masking Enabled
Admin Organization: Statutory Masking Enabled
Admin Street: Statutory Masking Enabled
Admin City: Statutory Masking Enabled
Admin State/Province: Statutory Masking Enabled
Admin Postal Code: Statutory Masking Enabled
Admin Country: Statutory Masking Enabled
Admin Phone: Statutory Masking Enabled
Admin Phone Ext: Statutory Masking Enabled
Admin Fax: Statutory Masking Enabled
Admin Fax Ext: Statutory Masking Enabled
Admin Email: abuse@web.com
```

Figura 2.5: Output obtido com o comando **whois primaverabss.com**

Com a ferramenta *nslookup*, descobrimos que o domínio esta alojado no endereço IP **62.28.56.74**

.

```
┌──(maria㉿ LAPTOP-9U8LMMFI)-[~]
└─$ nslookup primaverabss.com
Server:         192.168.121.209
Address:        192.168.121.209#53

Non-authoritative answer:
Name:   primaverabss.com
Address: 62.28.56.74
```

Figura 2.6: Output obtido com o comando **nslookup primaverabss.com**

Aplicou-se o comando *WhoIs* ao IP e obteve-se no terminal o conteúdo exposto nas figuras 2.7 e 2.8. Daqui conseguimos extrair as seguintes informações:

- Os IPs encontram-se no intervalo 62.28.56.64 a 62.28.56.127.
- O Internet Service Provider (ISP) é a empresa PRIMAVERA-NET, que pertence ao grupo PRIMAVERA BUSINESS SOFTWARE SOLUTIONS SA.
- O ISP encontra-se na morada Rua Dr Edigio Guimarães 70 - 74, 4715-248 Braga (Portugal).
- É apresentada uma entidade role que corresponde a MEO-EMPRESARIAL, responsável por gerir os endereços IP (ASN). Encontra-se explicita, uma morada (que corresponde a morada da sede da MEO) e são indicados um conjunto de campos relativos aos administradores cujo o conteúdo não permite extrair informação directa sobre os indivíduos.
- Os endereços IP são geridos pela empresa PTPRMENET - (PT-PRIME - Network service provider).

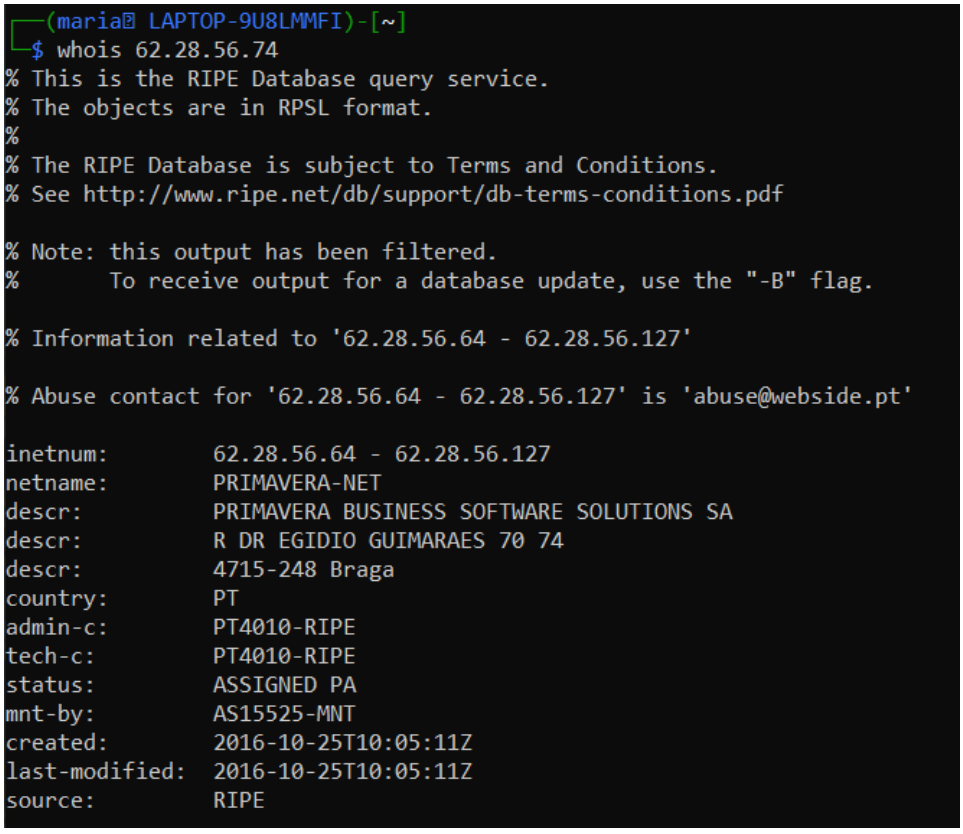

Figura 2.7: Primeira parte do output obtido com o comando **whois 62.28.56.74**

```
role:           MEO-EMPRESARIAL
org:            ORG-PP3-RIPE
address:        Local Internet Registry Management
address:        MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.
address:        Av. Fontes Pereira de Melo, 40 - 3 Bl A
address:        Forum Picoas - 1069-300 Lisboa
address:        Portugal
phone:          +351-215000000
admin-c:        HCR20-RIPE
admin-c:        NPM17-RIPE
admin-c:        DPM37-RIPE
admin-c:        LAS102-RIPE
admin-c:        TPM7-RIPE
tech-c:         RTM15-RIPE
tech-c:         JCO39-RIPE
tech-c:         HAC24-RIPE
tech-c:         HCO6-RIPE
tech-c:         AA2895-RIPE
nic-hdl:        PT4010-RIPE
abuse-mailbox:  abuse@webside.pt
mnt-by:         AS15525-MNT
mnt-by:         TELEPAC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2019-04-18T10:37:02Z
source:         RIPE # Filtered

% Information related to '62.28.0.0/16AS15525'

route:          62.28.0.0/16
descr:          PTPRIMENET
descr:          PT Prime - Network Service Provider
origin:         AS15525
mnt-by:         AS15525-MNT
created:        2006-06-08T12:32:07Z
last-modified:  2006-06-08T12:32:07Z
source:         RIPE

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

Figura 2.8: Segunda parte do output obtido com o comando **whois 62.28.56.74**

2.1.3 Estratégias para fortalecer a Segurança

De um modo geral, a informação que foi possível recolher com estes métodos é pouco relevante não fornecendo acesso a dados que deveriam permanecer confidenciais à empresa.

2.2 Waveform - Tecnologias de informação

A *weveform* é uma empresa bracarense que se destaca no sector da Tecnologia de informação. E tal como foi dito, concentram-se no desenvolvimento de soluções de software capazes de estimular experiências e incentivar o envolvimento dos usuários.

2.2.1 Procura de informações na WEB

Começamos esta análise, pela página web da empresa.

Na secção de contactos, é apresentada a morada do escritório, bem como um contacto telefónico e email.

- O contacto 910 978 750 apresentado na página web pertence a uma pessoa real Luís Leite, como mostra a figura 2.9.

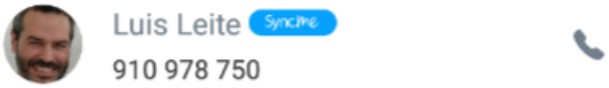

Figura 2.9: Pela aplicação sync.me concluímos que o contacto telefónico pertence a Luís Leite.

- O email apresentado, info@waveform.pt não é pessoal. Diz respeito a uma função geral do site.

A secção Recrutamento, permite obter algumas informações relevantes sobre a área de actuação da empresa, e software utilizado: *HTML, CSS, Javascript, React, Angular, node.JS, Python, PHP, C, .NET Ruby, MySQL, Microsoft Azure e Amazon AWS*.

É também possível encontrar alguns clientes da waveform, como por exemplo: *vodafone, Primavera, trofa Saúde*.

É ainda apresentado o link para a conta Linkdin da empresa, que revela as seguintes informações:

- A waveform é uma pequena empresa, composta por no máximo dez trabalhadores. Sendo que, 6 possuem conta LinkdIn.
- Os perfis e nomes dos seis funcionários encontram-se restritos.
- O escritório encontra-se localizado no *Centro de Negócios Ideia Atlântico, Cx 025, Braga, Braga 4719-005 Tenões, PT.*

Em seguida, efectuou-se uma analise ao *source code* da página, mas não se encontrou links para acesso a conteúdo desprotegido.

Por ultimo, com uma pesquisa rápida no google por **Luís Leite** (membro identificado através do contacto telefónico) revela o seu perfil Linkdin. Permitindo o acesso ao seu historial de formação (licenciado em Ciências da computação pela Uminho), experiência profissional (antes de fundar weveform trabalhou na Microsoft) entre outros.

2.2.2 Análise do domínio e IP

Com a ferramenta Whois, vamos consultar a informação disponível sobre o domínio, *www.waveform.pt*, cujo conteúdo apresentamos na figura 2.10.

Da análise da figura, sabemos quem registou e administra o domínio, o local de registo e alguns contactos das entidades envolvidas. Apresentamos em seguida as principais conclusões:

- O registo foi criado a 16/09/2011;

```
┌──(maria LAPTOP-9U8LMMFI)-[~]
└─$ whois waveform.pt
Domain: waveform.pt
Domain Status: Registered
Creation Date: 16/09/2011 08:02:46
Expiration Date: 16/09/2021 23:59:46
Owner Name: WAVEFORM - TECNOLOGIAS DE INFORMAÃÃO, LDA
Owner Address: Centro de NegÃ³cios Ideia AtlÃ¢ntico, Caixa 25, s/n
Owner Locality: Braga
Owner ZipCode: 4719-005
Owner Locality ZipCode: Braga
Owner Country Code: PT
Owner Email: info@waveformtec.com
Admin Name: DMNS - DOMINIOS, S.A.
Admin Address: Parque Multiusos, Areal Gordo, Lote 3A
Admin Locality: Faro
Admin ZipCode: 8005-409
Admin Locality ZipCode: Faro
Admin Country Code: PT
Admin Email: dns@dominios.pt,mailmanager@dominios.pt
Name Server: dns2.host-redirect.com | IPv4:  and IPv6:
Name Server: dns1.host-redirect.com | IPv4:  and IPv6:
waveform.pt IN DS 53597 8 1 AE9E4DCDFCC4B92BC45D994C9BB6B5945E4C9A5D
waveform.pt IN DS 53597 8 2 A9FF4EC6C0C29FD9C98368D78045BEC4D6D56F5A59EE0F6A75B871BA54E2CEF6
```

Figura 2.10: Output obtido com o comando **whois waveform.pt**

- O domínio foi registado por *WAVEFORM - TECNOLOGIAS DE INFORMAÇAO, LDA*, cujo a morada é: Centro de Negócios Ideia Atlântico, Cx 025, Braga, Braga 4719-005 Tenões, PT. Além disto é apresentado um email.
- A entidade administrativa é a DMNS - DOMINIOS, S.A., localizada em Faro, para qual são apresentados dois emails *dns@dominios.pt,mailmanager@dominios.pt*.

A ferramenta nslookup, permite saber que o domínio se encontra no endereço IP: **65.52.128.33**.

```
┌──(maria LAPTOP-9U8LMMFI)-[~]
└─$ nslookup waveform.pt

Server:         192.168.121.209
Address:        192.168.121.209#53

Non-authoritative answer:
Name:   waveform.pt
Address: 65.52.128.33
```

Figura 2.11: Output obtido com o comando **nslookup waveform.pt**

Podemos agora aplicar a ferramenta Whois ao IP. Obtendo o conteúdo das figuras 2.12,2.13 e 2.14.

Concluímos que, IP pertence ao intervalo 65.52.0.0 - 65.55.255.255. O ISP, é gerido pela empresa MICROSOFT-1BLK que pertence a Microsoft Corporation (MSFT), cujo o registo foi actualizado pela última vez em 2013-08-20.

Em relação a organização Microsoft Corporation, não é revelada nenhuma informação relevante.

```
NetRange:       65.52.0.0 - 65.55.255.255
CIDR:           65.52.0.0/14
NetName:        MICROSOFT-1BLK
NetHandle:      NET-65-52-0-0-1
Parent:         NET65 (NET-65-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Microsoft Corporation (MSFT)
RegDate:        2001-02-14
Updated:        2013-08-20
Ref:            https://rdap.arin.net/registry/ip/65.52.0.0
```

Figura 2.12: Primeira parte do output obtido com o comando **whois 65.52.128.33**

```
OrgName:        Microsoft Corporation
OrgId:          MSFT
Address:        One Microsoft Way
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        1998-07-10
Updated:        2017-01-28
```

Figura 2.13: Segunda parte do output obtido com o comando **whois 65.52.128.33**

```
OrgAbuseHandle: MAC74-ARIN
OrgAbuseName:   Microsoft Abuse Contact
OrgAbusePhone:  +1-425-882-8080
OrgAbuseEmail:  abuse@microsoft.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/MAC74-ARIN

OrgTechHandle: MRPD-ARIN
OrgTechName:   Microsoft Routing, Peering, and DNS
OrgTechPhone:  +1-425-882-8080
OrgTechEmail:  IOC@microsoft.com
OrgTechRef:    https://rdap.arin.net/registry/entity/MRPD-ARIN
```

Figura 2.14: Terceira parte do output obtido com o comando **whois 65.52.128.33**

2.2.3 Estratégias para fortalecer a segurança

Poderá usar-se um contacto telefónico geral para a empresa, ao invés da divulgação de contacto pessoal como foi referido anteriormente.

Capítulo 3

Parte B: Scanning

Bibliografia

[1] *DE BRAGA PARA O MUNDO, A PRIMAVERA DA CIDADE*. https://alumni.uminho.pt/pt/news/Paginas/2014/De-Braga-para-o-mundo,-a-PRIMAVERA-da-cidade.aspx. Acedido a 15 de dezembro de 2020.

[2] *O que é um Domínio*. https://www.dns.pt/pt/dominio/o-que-e-um-dominio/. Acedido a 16 de dezembro de 2020.