



Universidade do Minho
Escola de Engenharia

Universidade do Minho

TP2-Parte A

Coleta Passiva de Informações

Bruno Rodrigues pg41066

Carlos Alves pg41840

Índice

Introdução	3
Empresa local.....	4
Análise Whois	4
Geo-localização.....	7
Análise da página Web(http://primopecas.pt/).....	8
Empresa grande	10
Análise Whois	10
Address lookup	10
Domain Whois record	10
Network Whois record.....	12
Geo-localização.....	13
Análise da página Web	14
Empresa local vs Empresa Grande	15
Estratégias para ocultar informação relevantes aos mecanismos de busca passiva	16
Conclusão.....	17
Bibliografia.....	18

Introdução

Na unidade curricular de Tecnologia de Segurança foi nos proposto realizar um relatório, onde devemos escolher duas empresas, uma grande corporação e uma empresa local que tivesse minimamente um website, para realizar diversas buscas de informações relativas aos seus domínios e a informações mais pertinentes que conseguíssemos obter.

Neste relatório, iremos apresentar as diferentes posturas adotadas pelas duas empresas, e ainda mostrar as ferramentas usadas para obter tais informações.

O objetivo deste trabalho foca-se principalmente no estudo de coleta passiva de informações utilizando três técnicas:

- Análise de informações de registo do domínio, onde teremos informações diversas sobre o domínio escolhido.
- Análise da página web da empresa.
- E buscas de informações na internet.

Coleta Passiva de Informações

Como o nome indica, coleta passiva de informações nada mais é que o ato de usar diferentes ferramentas e técnicas de modo a obter o máximo de informações possíveis dos sistemas ou empresas, que poderão se tornar um alvo a atacar.

Nesta coleta, a empresa em questão dificilmente saberá das nossas atividades de coleta de informações, pois apenas navegaremos a página web da empresa até encontrar algum tipo de informação relevante. Através da coleta passiva de informações conseguimos reunir diversas informações técnicas, como por exemplo: endereço de IP da empresa, extrair nomes de domínio, subdomínios, identificar os dispositivos e tecnologias usadas por tal empresa. E por último é possível reunir informações sobre os colaboradores que lá trabalham, emails, contactos, que posteriormente pode ser usado para criar um perfil dos funcionários, havendo assim “mais uma porta” por onde possamos entrar.

Empresa local

A empresa local que escolhemos para realizar buscas de informações foi a PRIMOPEÇAS - COMÉRCIO DE PEÇAS E ACESSÓRIOS AUTO, LDA. PRIMOPEÇAS. É uma empresa fundada à mais de 19 anos, de acordo com a Classificação internacional Normalizada Industrial, a atividade desta empresa está focada no desenvolvimento de comércio a retalho de peças e acessórios para veículos, principalmente automóveis.

Análise Whois

https://centralops.net/co/DomainDossier.aspx?addr=primopecas.pt&dom_whois=true&dom_dns=true&traceroute=true&net_whois=true&svc_scan=true

Com a ajuda de uma ferramenta online (referenciado em cima), obtemos informações relativas ao website:

Queried whois.dns.pt with "primopecas.pt"...

#Nome do dominio

Domain: primopecas.pt

Domain Status: Registered

#Data de criação do website

Creation Date: 05/06/2017 13:12:41

#Data de expiração do website

Expiration Date: 04/06/2020 23:59:41

#Informação relativa ao dono do website

#Nome do dono

Owner Name: BSB | SMART & BRIGHT IDEAS, LDA

#Morada relativa ao dono

Owner Address: Rua Conselheiro Januário, nº 65, 3º

Owner Locality: Braga

Owner ZipCode: 4700-383

Owner Locality ZipCode: Braga

Owner Country Code: PT

#Email associado dono do website

Owner Email: adolfoferreira@bsb.pt

#Informações relativas à Entidade Gestora

#Nome da entidade Gestora

Admin Name: AlmouroITec - Servicos de Informatica e Internet Lda

#Morada relativa a entidade Gestora

Admin Address: Estrada Nacional 3 - 9-C

Admin Locality: Constancia

Admin ZipCode: 2250-028

Admin Locality ZipCode: Constancia

Admin Country Code: PT

#Email associado à entidade gestora

Admin Email: registry@buydomain.pt

#Nomes dos servidores

Name Server: a1.bsb.pt | IPv4: 94.46.164.6 and IPv6:

Name Server: a2.bsb.pt | IPv4: 94.46.164.7 and IPv6:

% Information related to '94.46.164.0 - 94.46.164.255'

% Abuse contact for '94.46.164.0 - 94.46.164.255' is 'abuse@ptisp.pt'

inetnum: 94.46.164.0 - 94.46.164.255
netname: PT-ALMOUROLTEC
descr: VIRTUAL PRIVATE SERVERS IP SPACE
country: PT
admin-c: LUIS-RIPE
tech-c: LUIS-RIPE
status: ASSIGNED PA
mnt-by: MNT-ALMOUROLTEC
created: 2017-01-30T15:23:58Z

last-modified: 2017-01-30T15:23:58Z

source: RIPE

person: Luis Inverno

address: Estrada Nacional n3

address: 2250-028 Constancia

address: Portugal

fax-no: +351 249739154

phone: +351 249739099

nic-hdl: LUIS-RIPE

mnt-by: MNT-ALMOUROLTEC

created: 2013-01-22T15:02:18Z

last-modified: 2017-10-30T22:24:12Z

source: RIPE

% Information related to '94.46.160.0/20AS24768'

route: 94.46.160.0/20

descr: ALMOUROLTEC SERVICOS DE INFORMATICA E INTERNET LDA

origin: AS24768

mnt-by: MNT-ALMOUROLTEC

created: 2015-01-29T20:56:30Z

last-modified: 2015-01-29T20:56:30Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.95.1 (ANGUS)

Com isto conseguimos obter informações relativas ao nome do domínio, informações sobre o dono do website, como moradas, e-mails e também informações relativas à entidade gestora do website, como também a data de criação, a data de expiração e nomes dos servidores.

Analisando a informação, descobrimos que o dono do domínio primopecas.pt é a empresa BSB | SMART & BRIGHT IDEAS, LDA, uma empresa de Braga, que se dedica a criação de aplicações web e mobile, como também design de websites. Descobrimos também o e-mail referente à empresa, adolfoferreira@bsb.pt, que está associado ao funcionário/fundador da empresa, Adolfo Ferreira.

Através de uma pesquisa google obtemos:

- O website da empresa:
<https://bsb.pt/>
- A pessoa a quem o email do website está associado:
<https://www.linkedin.com/in/adolfogferreira/>
- Funcionários da empresa:
<https://www.linkedin.com/company/bsb---smart-&-bright-ideas/people/>

A entidade gestora do website é a empresa AlmouroITec - Serviços de Informática e Internet Lda, situada em Constância, Santarém, que se dedica a hospedagem web. Encontra-se também um e-mail associado, registry@buydomain.pt, um numero de telefone, +351 249739099 e um numero de fax, +351 249739154, como também um nome , Luís Inverno, que coincide com o CEO da empresa

Uma pesquisa google obteve os seguintes resultados:

- Website da empresa: <https://ptisp.pt/>
- Dono da empresa: <https://www.linkedin.com/in/luis-inverno-33615614/>
- Funcionários: <https://www.linkedin.com/company/ptisp/people/>

Geo-localização

Retirado de: <https://www.maxmind.com/en/geoip-demo>

A geo-localização faz referência a localização geográfica da empresa do alojamento web.

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
94.46.164.6	PT	Portugal, Europe		38.7139, -9.1394	200	AlmouroITec Servicos De Informatica E Internet Lda	AlmouroITec Servicos De Informatica E Internet Lda		

Websites hospedados no mesmo web server

Retirado de: <https://www.yougetsignal.com/tools/web-sites-on-web-server/>

you get signal

Reverse IP Domain Check

Remote Address

Check

Found 6 domains hosted on the same web server as primopecas.pt (94.46.164.6).

danke.pt
primopecas.pt
www.sanusmedical.pt

eirinhas.com
www.kiomamakeup.com
www.traterme.com

Existem mais seis websites hospedados no mesmo web server.

Análise da página Web(<http://primopecas.pt/>)

Na realização da análise da página Web da empresa <Primo peças>, fizemos uma busca por todas as abas/menus da página de modo a encontrar informações relevantes para a construção deste relatório.

A página em si, apresenta um pequeno resumo da empresa, onde é possível visualizarmos diversas informações:

- O ano de “nascimento” da empresa, em 2000/07/01;
- O propósito da empresa – o que ela comercializa e para quem;
- O número de funcionário;
- Localização da sede da empresa;
- Quantidade de viaturas comerciais que a empresa tem.



Morada

Rua 25 de Abril n.º 9C, 1.º Dto
4720-332 Ferreiros, Amares
Braga

Num dos “menus” da página podemos encontrar diversos contactos (emails e números de telefones).



Telefone/Telemóvel

Geral: 253 995 282
Geral: 934 151 355



Email

geral@primopecas.pt
agostinhosoares@primopecas.pt
ramiroantunes@primopecas.pt

A partir dos números de telefone não foi possível encontrar grandes informações, ainda tentamos verificar em que nome o número de telemóvel estava associado, na esperança de encontrar o nome de alguma pessoa, mas concluímos que o mesmo se encontrava associado à empresa.

A informação que achamos mais pertinente em toda a página Web da empresa foi os emails que lá se encontram. Esses emails são inicializados pelo nome próprio e apelido de dois colaboradores, que pensamos serem os sócios majoritários(criadores) da empresa. Com estes nomes iniciamos uma busca nas principais ferramentas de busca da internet: as redes sociais (Facebook e ainda **LinkdedIn**).

No **LinkedIn** não foi possível encontrar nenhum dos dois sujeitos, mas no **Facebook** foram encontrados os perfis pessoais desses elementos.

A partir do perfil do colaborador 1 foi praticável a verificação de demasiadas informações pessoais tais como: Data de nascimento, Agregado familiar, quem são os seus funcionários (*em geral são sobrinhos*). E ainda através dele também conseguimos determinar a zona em que reside. Em relação ao perfil do colaborador 2 conseguimos retirar as mesmas e ainda mais informações do que o colaborador 1.

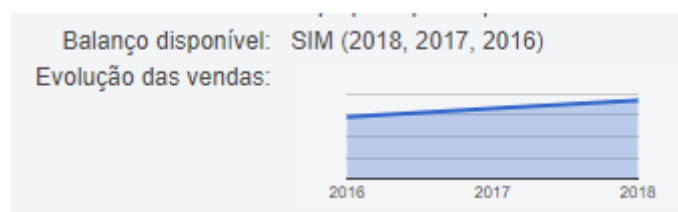
Como a página Web é composta por código HTML, analisamos o código de modo a encontrar algum tipo de informação pertinente, principalmente comentários. Infelizmente não encontramos muita coisa, exceto informação relativa ao input de dados (*var et_pb_custom*) que não entendemos bem se seria alguma falha.

Investigamos também o ficheiro robot.txt, pois geralmente os proprietários dos sites, costumam usar o arquivo *robots.txt* no diretório raiz do próprio site para fornecer instruções aos robôs da Web sobre quais páginas eles pretendem incluir ou excluir durante o processo de rastreamento. Essencialmente se conseguíssemos ver este arquivo, podíamos ver informações que o proprietário do site ocultou do público.

```
User-agent: *  
Disallow: /wp-admin/  
Allow: /wp-admin/admin-ajax.php
```

Além de analisarmos a página web e procurar pelos funcionários/sócios da empresa, fizemos também uma pesquisa no qual conseguimos obter informações relativas à empresa como:

A forma jurídica em que enquadra a empresa, no caso Sociedade por Quotas, por isso que determinamos que os dois sujeitos acima devem ser sócios. Ainda nesta pesquisa, vimos que era relativamente fácil ter acesso e ser possível observar e analisar o balanço financeiro dos últimos 3 anos da empresa coletiva.



Perfis encontrados:

<https://www.facebook.com/agostinho.soares.370> - Fundador

<https://www.facebook.com/ramiro.antunes.501> -Socio

Empresa grande

A grande corporação que escolhemos foi a **PRIMAVERA BUSINESS SOFTWARE SOLUTIONS SA**.

Uma empresa também da nossa região que se dedica ao desenvolvimento e comercialização de soluções de gestão e plataformas para integração de processos empresariais num mercado global, disponibilizando soluções para diferentes tipos de empresas/organizações (pequenas, medias e grandes organizações). A empresa está presente em sete países, principalmente no continente Africano. Segundo a **cotecPortugal**, *A Primavera BSS encontra-se entre as 500 maiores empresas europeias com maior potencial de crescimento e com maior potencial de crescimento, um ranking promovido pela Growth Plus.*

Decidimos escolher esta corporação devido ao fato de ser “mais” possível encontrar informações pertinentes, do que numa empresa de maior magnitude como Google, Amazon, Altice.

Análise Whois

https://centralops.net/co/DomainDossier.aspx?addr=pt.primaverabss.com&dom_whois=true&dom_dns=true&traceroute=true&net_whois=true&svc_scan=true

Com a ajuda de uma ferramenta online (referenciado em cima), obtemos informações relativas ao website:

Address lookup

canonical name [pt.primaverabss.com](https://centralops.net/co/DomainDossier.aspx?addr=pt.primaverabss.com&dom_whois=true&dom_dns=true&traceroute=true&net_whois=true&svc_scan=true).

aliases

addresses 37.187.199.1

Domain Whois record

Queried whois.internic.net with "dom 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: 2019-09-20T09:42:58Z
Creation Date: 2006-02-08T16:12:19Z
Registry Expiry Date: 2020-02-08T16:12:19Z
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
URL of the ICANN Whois Inaccuracy Complaint Form:
<https://www.icann.org/wicf/>
>>> Last update of whois database: 2019-11-01T19:20:03Z <<<

Queried whois.networksolutions.com with "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: 2019-03-04T16:09:05Z
Creation Date: 2006-02-08T16:12:19Z
Registrar Registration
Expiration Date: 2020-02-08T16:12:19Z
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:
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
Registry Tech ID:
Tech Name: Statutory Masking Enabled
Tech Organization: Statutory Masking Enabled
Tech Street: Statutory Masking Enabled
Tech City: Statutory Masking Enabled
Tech State/Province: Statutory Masking Enabled
Tech Postal Code: Statutory Masking Enabled
Tech Country: Statutory Masking Enabled
Tech Phone: Statutory Masking Enabled
Tech Phone Ext: Statutory Masking Enabled
Tech Fax: Statutory Masking Enabled
Tech Fax Ext: Statutory Masking Enabled
Tech Email: abuse@web.com

```
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
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-11-01T19:20:13Z <<<
```

Network Whois record

Queried whois.ripe.net with "-B 37.187.199.1"...

% Information related to '37.187.199.0 - 37.187.199.255'

% Abuse contact for '37.187.199.0 - 37.187.199.255' is 'abuse@ovh.net'

```
inetnum:        37.187.199.0 - 37.187.199.255
netname:        OVH
descr:          OVH SAS
descr:          VPS Static IP
descr:          http://www.ovh.com
country:        FR
admin-c:        OK217-RIPE
tech-c:         OTC2-RIPE
status:         ASSIGNED PA
notify:         noc@ovh.net
mnt-by:         OVH-MNT
created:        2014-09-23T18:41:15Z
last-modified:  2014-09-23T18:41:15Z
source:         RIPE
```

```
role:           OVH Technical Contact
address:        OVH SAS
address:        2 rue Kellermann
address:        59100 Roubaix
address:        France
e-mail:         noc@ovh.net
admin-c:        OK217-RIPE
tech-c:        GM84-RIPE
tech-c:        SL10162-RIPE
nic-hdl:        OTC2-RIPE
notify:         noc@ovh.net
abuse-mailbox:  abuse@ovh.net
mnt-by:         OVH-MNT
created:        2004-01-28T17:42:29Z
last-modified:  2014-09-05T10:47:15Z
source:         RIPE
```

```
person:         Octave Klabba
address:        OVH SAS
address:        2 rue Kellermann
address:        59100 Roubaix
address:        France
phone:          +33 9 74 53 13 23
e-mail:         noc@ovh.net
nic-hdl:        OK217-RIPE
mnt-by:         OVH-MNT
created:        1970-01-01T00:00:00Z
```

```

last-modified: 2017-10-30T21:44:51Z
source: RIPE

% Information related to '37.187.0.0/16AS16276'

route: 37.187.0.0/16
descr: OVH
origin: AS16276
notify: noc@ovh.net
mnt-by: OVH-MNT
created: 2013-03-22T19:37:35Z
last-modified: 2013-03-22T19:37:35Z
source: RIPE

% This query was served by the RIPE Database Query Service version
1.95.1 (ANGUS)

```

Com isto conseguimos obter informações relativas ao nome do domínio, morada da empresa, data de criação, a data de expiração e nomes dos servidores, mas ao contrário do que acontece com a primopecas.pt, já não é possível obter informações, como números de telefone, email, nomes relativos a administradores, donos da pagina, entre outros, visto que um mecanismo de segurança está ativo a salvaguardar essas informações, *Data Masking*, que é utilizado para esconder varias informações apresentadas pelo **Whois**. Devido a isso, a recolha de dados fica muito limitada, e torna difícil obter informação útil.

Geo-localização

Retirado de: <https://www.maxmind.com/en/geoip-demo>

A geo-localização faz referência a localização geográfica da empresa do alojamento web

GeoIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
37.187.199.1	FR	France, Europe		48.8582, 2.3387	500	OVH SAS	OVH SAS	ip-37-187-199.eu	

Websites hospedados no mesmo web server


Retirado de: <https://www.yougetsignal.com/tools/web-sites-on-web-server/>

Não existem websites com o mesmo IP

you get signal

Reverse IP Domain Check

Remote Address

 No web sites found.

Análise da página Web

Na realização da análise da página Web da empresa <Primavera BSS>, fizemos uma busca por todas as abas/menus da página de modo a encontrar informações relevantes para a construção deste relatório.

Na sua página é possível encontrar as seguintes informações:

- Ano em que foi fundada;
- Governação Corporativa, principais rostos por trás da gestão/administração da PRIMAVERA BSS;
- Relatório Anual de contas – Valores registados;
- Número de colaboradores;
- Contactos e localização de onde estão sediados;

As informações presentes na página Web da PRIMAVERA BSS são bem mais escassas. Os contactos de telefone são todos números de telefones fixos. Os emails não transparecem quais quer tipo de informação relevantes, seja ela nomes de colaboradores ou outros. A possibilidade de o utilizador comum conseguir colocar inputs é muito reduzida, apenas foi encontrada nos contactos uma zona onde poderíamos colocar lá o nome e informações sobre nós, mas mesmo aqui é necessário seguir certas diretrizes antes de submeter o input.

Através da secção onde é possível observar a governação corporativa da empresa, conseguimos talvez retirar algumas informações que com alguma pesquisa na internet seja possível criar um perfil dos principais rostos da organização.

Depois de alguma pesquisa foram encontrados três perfis de Facebook, mas com pouquíssima informação para traçar um perfil complexo, apenas pequenas informações pessoais foram observadas (familiares, data de nascimento). De seguida fizemos a mesma busca no **LinkedIn**, e foram encontrados novamente os três perfis, complementando com a informação que capturamos da Plataforma **Facebook** não conseguiríamos traçar um perfil. Talvez se fossemos mais “fundo” na pesquisa, percorrendo a formação académica de cada um ou até os cargos executados poderíamos ter informação pertinente para um perfil. Achamos curioso não termos encontrado praticamente nada sobre um dos elementos do grupo de executivos da corporação.

Em geral, as principais figuras da empresa não transparecem muitas informações pertinentes para o publico, deixam mais difícil a análise.

Ainda analisamos o código HTTP da página da corporação, em busca de algum comentário ou descrição, mas não foi possível encontrar nada de relevante para a análise. Ainda assim tentamos investigar o ficheiro robot.txt, como era de se esperar nem foi possível visualizá-lo.

Para concluir, fizemos uma busca em diversos websites, **kompas**, de forma a obter mais informações da empresa. Assim sendo, a PRIMavera BSS foi fundada em 1993, a forma jurídica da mesma é Sociedade Anónima (Ações), tem um capital social de cerca de 2.550.000 euros e tem cerca de 249 funcionários em todo o mundo.

Perfis Encontrados

<https://www.facebook.com/jorge.batista1964> - Co-CEO

<https://www.facebook.com/jose.dionisio.96> - Co-CEO

<https://www.facebook.com/angela.brandao.31> - Vice-Presidente

Empresa local vs Empresa Grande

Diferenças entre as duas.

Uma das diferenças mais obvias encontradas entre as duas é a disponibilização de informação por parte do **Whois**, enquanto que um *query* à **Whois** sobre a **primopecas.pt** retorna-nos múltiplas informações, como o nome do dono do domínio, o nome do administrador, a morada das empresas, números de telefone e email, enquanto que as informações que são obtidas através de um *query* a **Whois** sobre **pt.primaverabss.com** são muito mais escassas. Isto deve-se ao facto que ao contrário da **primopecas.pt**, a **pt.primaverabss.com** tem um mecanismo de segurança ativo que salvaguarda a informações, algumas delas pessoais, como nomes, números de telefone e emails.

As diferenças encontradas entre os websites é as informações por eles transmitidos

Enquanto que a empresa local, a **primopecas.pt**, os emails contêm informações pessoais, como o nome dos sócios da empresa, emails encontrados na **pt.primaverabss.com** são emails gerais, que não transmitem nenhuma informação relativa a funcionários.

Só o facto de os emails da **primopecas.pt** conterem o nome verdadeiro de funcionários da empresa, foi possível, através de uma pesquisa google, obter vários dados pessoais, como também ligações a outros funcionários da empresa.

Estratégias para ocultar informação relevantes aos mecanismos de busca passiva

- Evitar usar nomes verdadeiros no registo de domínio.

Isto permite o uso de ataques de engenharia social, em que pesquisas em redes sociais, como o **Facebook**, ou **Linkedin**, com o nome registado poderá levar a divulgação de mais informação pessoal, ou até para realizar ataques de força bruta. Uma alternativa, será por nomes como “John RIPE” por exemplo.

- Usar uma morada que não seja o escritório principal.
- Usar emails gerais.

O uso de emails que contem os nomes pessoais são desaconselhados, sendo a alternativa usar emails como **admin@companydomain.com**

- Número de telefone para uso único.

Evita *wardialing* ataques.

Conclusão

Neste trabalho analisamos diferentes formas de recolher informações de forma passiva através de ferramentas disponíveis na web. Analisamos informações do domínio, as páginas web de cada empresa, como também realizamos alguma pesquisa usando o *google search* e redes sociais (**Facebook, linkedin**).

Com a realização deste trabalho conseguimos recolher dados associados as empresas-alvo, neste caso, **primopecas.pt**, uma empresa local, do concelho de Amares, Braga, e **pt.primaverabss.com**, uma empresa internacional, com sede em Braga, mas já com escritórios noutros países, com o intuito de estudar de que forma as informações providenciadas nos websites ou nos registos de domínios podem levar de certa forma a exploração da informação e a obtenção de mais detalhes com base nesta.

Com a realização deste trabalho foi possível entender que a divulgação de informação, não importa o quão pequena possa ser, como por exemplo, um email que contenha um nome próprio, pode levar a descoberta de mais informações, que podem levar a uma escalação de informação divulgada. Através da utilização das várias ferramentas utilizadas, que nos permitiram a realização deste trabalho, somos agora capazes de reconhecer e utilizar diferentes ferramentas que nos permitem analisar e recolher informações com base em várias fontes, seja através de um motor de busca, inspeção das informações de registo de domínio, ou a procura através do próprio website.

Bibliografia

eInforma. (s.d.). Empresite. Obtido de Jornaldenegocios:

<https://empresite.jornaldenegocios.pt/PRIMOPECAS-COMERCIO-PECAS-ACESSORIOS-AUTO.html#mod-einforma>

kompass. (23 de Agosto de 2019). Obtido de <https://pt.kompass.com/c/primopecas-comercio-de-pecas-e-acessorios-lda/pt080439/>

Passive Information Gathering, The Analysis of Leaked Network Security Information. Obtido de Gunter Ollmann