



Universidade do Minho  
Escola de Engenharia

# **TECNOLOGIA DE SEGURANÇA**

TP2 – Parte A

*Passive Information Gathering*

Diogo Araújo A78485; Diogo Nogueira A78957

# Conteúdo

1. Contextualização.....	3
2. Passive Information Gathering .....	4
2.1    EDP – Energias de Portugal.....	5
2.1.1.    Análise Informações de Registo de Domínio.....	5
2.1.2.    Análise Página WEB/Procura de Informações Online .....	11
2.1.3.    Estratégias de Segurança .....	13
2.2    TUB – Transportes Urbanos de Braga.....	15
2.2.1.    Análise Informações de Registo de Domínio.....	15
2.2.2.    Análise Página WEB/Procura de Informações Online .....	20
2.2.3.    Estruturas de Segurança .....	23
3. Conclusões e Observações Finais.....	24
4. Referências.....	25

# 1. Contextualização

Quando se fala de *Passive Information Gathering*, automaticamente se assume que se trata do ato de receber/submeter uma ação sem responder ou iniciar uma outra ação em troca disso. Na Tecnologia de Segurança, estamos a falar do processo de adquirir o máximo de conhecimentos possível sem que seja necessário estabelecer um contacto entre o atacante e o “sistema alvo”. Por isso se diz que esta recolha inicial de informação se trata da primeira tarefa que qualquer atacante realiza (ou deve realizar) antes de proceder à concretização do ataque. Recorrendo a um conjunto de ferramentas e técnicas, o atacante tenta obter um leque de informações que deve permitir uma consciencialização daquilo que pode ser beneficiado para se executar o ataque.

Neste processo passivo, o “sistema alvo” não tem qualquer tipo de informe sobre a atividade da recolha em si, dado que não existe um envio de pacote de dados ao servidor de destino - apenas uma navegação típica de qualquer utilizador do *website*. Assim se deduz que esta recolha de informações é limitada para qualquer utilizador comum, o que faz com que todo o processo varie consoante o *website* que se está a “consumir”.

A ideia principal deste guião prático passa então por realizar uma recolha passiva de informações, através de uma análise de processos e técnicas que auxiliam na descoberta deste tipo de informações. Serão ainda incluídos detalhes acerca do significado das mesmas e que eventuais medidas estas “empresas” devem/podem implementar para limitar ou até mesmo eliminar a exposição geral a possíveis ameaças.

Para isso, escolheram-se duas empresas de dimensões distintas para que pudesse ser feita uma pequena comparação final entre ambas, na tentativa de compreender as diferenças de postura adotadas pelos domínios de cada uma destas. Falaremos assim de uma das maiores empresas globais ao nível da energia – **EDP** – e da empresa de Transportes Urbanos de Braga – **TUB**.

## 2. Passive Information Gathering

Qualquer sistema conectado à Internet acaba inevitavelmente por facultar informações internas acerca da sua organização e que podem depois ser utilizadas para formular um ataque perfeitamente direcionado. Dependendo da origem da fuga, estas informações podem estar relacionadas a componentes/equipamentos utilizados na infraestrutura da empresa, nos processos de gerência existentes ou até mesmo na hierarquia de trabalhadores. Isto cria logo uma ideia de alarme, dado que a infraestrutura de uma empresa é a base do funcionamento de qualquer organização e que todas as entidades nela existentes podem representar uma ponte fácil para um ataque bem planeado.

O grande problema nesta fuga de informações é que a maioria se encontra disponível de forma pública na Internet e muitas das vezes em sistemas alheios à empresa em causa. Isto leva a que o acesso seja independente dos recursos da mesma, podendo ser obtido por qualquer utilizador comum. Tendo em conta que estes processos são perfeitamente simples e exequíveis, é apenas necessário recorrer a um conjunto de ferramentas igualmente triviais, criando um planeamento prévio da avaliação de segurança do ataque a realizar.

Conforme ficou perceptível na contextualização inicial, existem várias técnicas e processos disponíveis quando se vai realizar um *Passive Information Gathering*. Neste trabalho prático serão estudadas apenas as mais relevantes, tentando-se com isso compreender o pensamento necessário para se identificar as informações obtidas e avaliar os riscos ao nível da segurança que estas trazem.

## 2.1 EDP – Energias de Portugal

A EDP trata-se de uma empresa global de energia, que existe há mais de 40 anos e se espalha a nível mundial por mais de 15 países e 4 continentes. A sua organização conta com uma vasta gama de funcionários (cerca de 11.500), que atuam no setor da eletricidade e na comercialização de gás.

### 2.1.1. Análise Informações de Registo de Domínio

O registo e a manutenção global de informações acerca dos endereços IP forma todo o registo de serviços da Internet. Sabe-se que os endereços IP são os identificadores dos *hosts* que existem pela rede no geral. Sabe-se também que a cada um destes endereços se encontra associado um nome de domínio, que visa facilitar a memorização/especificação para cada *host*. O endereço IP e o seu nome de domínio consistem assim num duo de especificação importante, servindo como uma espécie de coordenadas a nível internacional.

Esta ideia base é essencial para o estudo em causa, já que para administrar todos estes endereços IP/nomes de domínio, as empresas são normalmente “forçadas” a fornecer detalhes acerca da administração em si, tal como endereços físicos e até mesmo informações técnicas de contacto. Tendo em conta que esse tipo de informações está disponível aos utilizadores comuns, podendo ser requeridas por qualquer um destes, acaba-se por formar o início daquele que é o exercício da recolha passiva de informações.

Para esta primeira análise, irá recorrer-se à ferramenta **WHOIS**, que permite um estudo de conhecimentos sobre os domínios e também de endereços IP's através da pesquisa de detalhes sobre a titularidade de ambos.

- **Detalhes sobre o domínio *edp.pt***

Através do recurso de consulta **WHOIS** direcionado para a informação relativa ao domínio em si, podemos obter uma resposta detalhada que permitirá produzir um conjunto de observações inerentes ao processo de recolha passiva de informação.

Falamos de informações que incluem quem registou e administrou o registo do domínio, o local onde o mesmo se encontra registado e ainda contactos relativos a quem efetuou todo este processo.



Estes dados facilitam assim na comunicação com os *owner's* do domínio, criando um bom método para se ligar com problemas que eventualmente surjam.

```
diogoesnog@DESKTOP-OCRRD5H:~$ whois edp.pt
Domain: edp.pt
Domain Status: Registered
Creation Date: 21/03/1997 00:00:00
Expiration Date: 01/06/2020 23:59:10
Owner Name: EDP - ENERGIAS DE PORTUGAL, S.A.
Owner Address: Praça Marquães de Pombal, No.12
Owner Locality: LISBOA
Owner ZipCode: 1250-162
Owner Locality ZipCode: LISBOA
Owner Country Code: PT
Owner Email: dns@edp.pt,gsi.arquitecturas@edp.pt,joao.figueiredo@cms-rpa.com
Admin Name: DMNS - DOMINIOS, S.A.
Admin Address: Parque Multiusos, Area1 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: ns.edp.com.pt | IPv4: 185.58.83.135 and IPv6:
Name Server: ns.edp.pt | IPv4: 185.58.81.135 and IPv6:
edp.pt IN DS 19839 10 2 BC6650AD6255A6A120CA3DD9CEA37666DDB6543D3F86643F5CA84
5DOCB1E046D
edp.pt IN DS 19839 10 1 1BDA413E597B2E4EB179986DE070971495C8262A
```

- O domínio *edp.pt* foi registado pela entidade EDP - Energia de Portugal, S.A, na data de 21/03/1997, devendo ser atualizado na data de 01/06/2020;
- Além do nome da entidade que registou este endereço pode-se ainda extrair a informação da localização da sede em si, especificando-se a morada e respetivo código postal;
- São visíveis três emails que se referem à equipa administrativa da empresa EDP;
- A análise destas informações revela ainda que existe uma entidade administradora responsável pelo serviço de registo/manutenção do domínio, de nome DMNS - Domínios, S.A;
- É possível também obter as informações de morada relativas a esta empresa à qual a EDP recorreu para processar toda a informação, registando o seu *website*;
- São mostrados os emails relativos à equipa desta empresa.

Além destas informações, são mencionados dois *name servers*, juntamente com os seus respetivos endereços IP na versão 4 e 6. Estes *name servers* são os responsáveis para que exista uma ponte viável entre o domínio em si e o servidor onde o *website* se encontra efetivamente alojado.

Recorrendo-se ao *website* [whois.domaintools.com](http://whois.domaintools.com), verifica-se ainda a existência de um *Autonomous System*, através de um *Autonomous System Number (ASN)* registado alguns meses depois de o domínio ter sido oficialmente criado.

Whois Record for Edp.pt		
— Domain Profile		
Registrar Status	taken	
Name Servers	NS.EDP.COM.PT (has 10 domains) NS.EDP.PT (has 0 domains)	↗
Tech Contact	—	
IP Address	195.22.21.202 is hosted on a dedicated server	↗
IP Location	 - Lisboa - Lisbon - Claranet Portugal S.a	
ASN	 AS8426 CLARANET-AS ClaraNET LTD, GB (registered Aug 15, 1997)	
Hosting History	1 change on 2 unique name servers over 4 years	↗
— Website		
Website Title	edp 500 SSL negotiation failed:	↗
Response Code	500	

- Detalhes sobre o endereço IP do domínio *edp.pt*

Os dados **WHOIS** acerca do endereço IP de um determinado domínio fornecem detalhes dos dados administrativos da rede. Veremos através da ferramenta **WHOIS** que estes dados são por norma dados mais internos, na medida em que todos os dados de registo e administração incluem informações relativas aos envolvidos neste processo de registo de endereço(s).

Através do nslookup conseguimos facilmente obter o endereço IP pertencente ao domínio que se está a estudar. Com este endereço em mãos, aplica-se o comando WHOIS para o mesmo, obtendo-se informações complementares às obtidas para o domínio em si.

```
diogoesnog@DESKTOP-OCRRD5H:~$ nslookup edp.pt
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   edp.pt
Address: 195.245.180.99
```

```
diogoesnog@DESKTOP-OCRRD5H:~$ whois 195.245.180.99
% 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 '195.245.180.0 - 195.245.181.255'
% Abuse contact for '195.245.180.0 - 195.245.181.255' is 'abuse@net4b.pt'

inetnum:        195.245.180.0 - 195.245.181.255
netname:        EDINFOR
descr:          EDINFOR - Sistemas Informaticos S.A.
country:        PT
admin-c:        FV1093-RIPE
tech-c:         RA173-RIPE
status:         ASSIGNED PA
mnt-by:         AS9186-MNT
created:        2002-01-15T14:55:35Z
last-modified:  2002-01-15T14:55:35Z
source:         RIPE # Filtered
```

- Observa-se que o intervalo de endereços IP se encontra entre 195.245.180.0 e 195.245.181.255. Estes endereços são assim geridos pela Edinet/E3G IP space (referido na parte final acerca da *route*);
- O ISP da empresa Edinfor está alojado em Portugal (PT);
- Os detalhes acerca da morada real do ISP não se encontram descritas;
- O registo de EDINFOR foi modificado a última vez no dia 15/01/2002.



```

person:      Fernando P M Vidiga1
address:     Portugal
phone:       +351-21-3121200
fax-no:      +351-21-3121200
nic-hdl:     FV1093-RIPE
created:     1970-01-01T00:00:00Z
last-modified: 2016-04-05T18:22:45Z
mnt-by:      RIPE-NCC-LOCKED-MNT
source:      RIPE

person:      Ripe ADM
address:     ONITELECOM - Infocomunicacoes S.A.
address:     Av. Fontes Pereira de Melo, 27
address:     1069-447 LISBOA
phone:       +351 211154300
remarks:     *** Please send the Abuse Reports to abuse@net4b.pt ***
nic-hdl:     RA173-RIPE
mnt-by:      AS9186-MNT
created:     2001-12-28T16:16:17Z
last-modified: 2010-10-22T13:56:34Z
source:      RIPE # Filtered

% Information related to '195.245.160.0/19AS9186'

route:       195.245.160.0/19
descr:       Edinet/E3G IP space
origin:      AS9186
mnt-by:      AS9186-MNT
created:     2002-09-13T16:51:22Z
last-modified: 2002-09-13T16:51:22Z
source:      RIPE # Filtered

```

- Verifica-se a divulgação de informação acerca de duas pessoas reais – Fernando P M Vidigal e Ripe ADM;
- Informação acerca do número de telefone para contacto para com este “objeto”;
- No que toca à Ripe ADM, é listada também a sua efetiva morada;
- O mesmo MNTNER é responsável por todos os registos, à exceção da *person* Fernando P M Vidigal.

A partir de todas estas observações, podemos de imediato concluir que o objeto inetnum EDINFOR contém um conjunto de endereços IPv4, alocados e geridos pela Edinet/E3G IP space. Também se identifica o mesmo MNTNER (AS9186-MNT), que se mostra responsável pelos registos de bloqueio da rede em si.

A ideia agora é efetuar uma pesquisa acerca deste MNTNER, tentando analisar melhor as informações nele envolvidas.

```

diogoesnog@DESKTOP-OCRRD5H:~$ whois AS9186-MNT
% 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 'AS9186-MNT'

mntner:        AS9186-MNT
descr:         ONI Maintainer
admin-c:       RA608-RIPE
tech-c:        RA608-RIPE
tech-c:        RA608-RIPE
auth:          MD5-PW # Filtered
auth:          SSO # Filtered
auth:          SSO # Filtered
auth:          SSO # Filtered
mnt-by:        AS9186-MNT
created:       2002-01-15T14:56:08Z
last-modified: 2018-07-02T14:45:23Z
source:        RIPE # Filtered

```

```

role:          RIPE ADMONI
address:       ONITELECOM - Infocomunicacoes S.A.
address:       RUA N3 DA MATINHA, 2 PISO EDIFICIO ALTEJO
address:       AS9186-MNT
address:       1950 - 326 LISBOA
phone:         +351 211154300
remarks:       trouble: *** Please send the Abuse Reports to abuse@net4b.pt
***
admin-c:       CP1386-RIPE
admin-c:       AS32985-RIPE
tech-c:        FMR9-RIPE
nic-hdl:       RA608-RIPE
remarks:       *** Please send the Abuse Reports to abuse@net4b.pt ***
mnt-by:        AS9186-MNT
created:       2002-06-21T11:16:28Z
last-modified: 2017-06-28T22:30:04Z
source:        RIPE # Filtered
abuse-mailbox: abuse@net4b.pt

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

```

- Observamos que existe um conjunto de pessoas envolvidas em manter a *database* em si. O objeto **role** descreve o papel desempenhado por um conjunto de pessoas, descrevendo assim a morada e o número de telemóvel para o **role** em causa;
- Acima desta informação, fica percetível que para alterar qualquer entrada na *database* RIPE é necessária uma autenticação em si, ou seja, qualquer comunicação existente entre as várias pessoas envolvidas no **role**, deve incluir uma *password* (MD5-PW e SSO).

Além de toda esta informação fornecida pelo **WHOIS**, é ainda possível relacionar este endereço IP principal com uma base de dados geográfica, recolhendo detalhes exatos acerca da localização geográfica do ISP.

GeoIP2 City Results								
IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Dom
195.245.180.99	PT	Coimbra, Coimbra, Portugal, Europe	3045-517	40.2053, -8.4204	200	Onitelecom - Infocomunicacoes, S.A.	Onitelecom - Infocomunicacoes, S.A.	

- ISP localizado em Coimbra, com as suas coordenadas aproximadas definidas;
- ISP pertence à organização Onitelecom – Infocomunicacoes, S.A..

### 2.1.2. Análise Página WEB/Procura de Informações Online

Como a maioria das empresas mantém os seus *websites* visíveis a nível *online*, a probabilidade em escapar informações internas torna-se geralmente mais alta. Por essa razão, a análise detalhada do conteúdo da página WEB em si, torna-se muitas das vezes imprescindível para qualquer atacante.

A forma mais eficaz de analisar uma página WEB é criar um espelho do conteúdo local do *website*. Na perspetiva da recolha passiva de informações, este tipo de análise não é propício a ser descoberta e muito menos tomada como uma espécie de ameaça/ataque. A ideia principal com este processo é tentar investigar toda a informação, na tentativa de recolher informes empresarias que podem ser úteis para um futuro planeamento de ataque.

Para isso, foi usada uma extensão via Google Chrome de nome “*Email Extractor*”, que permite fazer um *scan* dos e-mails que existem na página em si, mas que não estão visíveis a olho nu. Aliado a isto, fez-se o *download* da página WEB principal, obtendo-se todo o conteúdo necessário para uma análise fora da rede.

## ▪ Detalhes sobre a Página Principal *edp.pt*

- Não se obtiveram quaisquer emails ocultos;
- A análise do *source-code* referente ao HTML em si não demonstrou código comentado (que é muita das vezes importante neste tipo de análises);
- Ainda no *source-code*, não foi possível encontrar *links* para possíveis arquivos de dados ou qualquer outro conteúdo protegido de forma inadequada;
- Observa-se a existência de *links* para *websites* externos, como o LinkedIn (<https://www.linkedin.com/company/edp>);

Ao entrar no LinkedIn da empresa, algumas informações potencialmente reveladoras podem ser descobertas. Não só um conjunto de localidades da empresa em si, mas também um conjunto de nomes de funcionários da EDP, que encaminham para o perfil LinkedIn destes, podendo tal conteúdo ser usado para posteriores ataques como os *Brute-force Attack* ou até mesmo os conhecidos Ataques de Engenharia Social.

### Localidades


Principal

Av. 24 de Julho  
nº12  
Lisboa, PT

[Como chegar](#) 

Avenida 24 de Julho 12  
Lisbon, Lisbon 1200-480, PT

[Como chegar](#) 

Exibir mais localidades 

### Funcionários na EDP



Vitor Cordeiro



Maria João Gama



Abid Ahmed



Miguel Stilwell d'Andrade  
Executive Board Member at EDP

[Visualizar todos os funcionários](#)

- Detalhes sobre a página de Apoio ao Cliente *edp.pt/particulares/apoio-cliente/contactos/edp.pt*
- Consegue-se obter um email oculto [distribuicao.setgas@galpenergia.com](mailto:distribuicao.setgas@galpenergia.com);
- Em termos de análise de *source-code*, nota-se que o mesmo é visivelmente mais extenso que a Página Principal, dado que se trata de uma página que consiste numa espécie de formulário, sendo necessário existir todas as opções que o Cliente eventualmente escolha;
- Observa-se a existência dos mesmos *links* para *websites* externos encontrados na Página Principal.

É importante ter em conta que esta análise de conteúdo depende do volume de informações apresentados pela EDP. Algo que saltou logo à vista foi a boa prática de código, atendendo ao facto de que o mesmo se encontrava devidamente organizado e documentado consoante os níveis e detalhes necessários para o programador. Em termos de *links* par arquivos de dados ou outro tipo de conteúdos, apenas existiam referências aos ficheiros *javascripts*.

Assim, não houve grande informação exposta a não ser informação acerca da empresa no geral, das suas localizações e parte da sua equipa de trabalhadores.

### 2.1.3. Estratégias de Segurança

No ponto de vista de segurança, existem muitas estratégias que podem ajudar a ocultar informações relevantes aos mecanismos de busca passiva que se tem vindo a estudar. A tabela seguinte será usada para descrever alguma dessas estratégias, consoante a empresa em estudo, dando a entender a necessidade de se implementar tal “funcionalidade”. Estas estratégias são referentes ao estudo no geral, já que algumas pertencem ao domínio em si e outras à página WEB da empresa.

É importante referir que muitas destas estratégias estão já corretamente implementadas pela EDP.

Problema	Estratégia de Resolução
Divulgação de vários objetos <i>person</i> por parte dos registos do ISP	<p>Neste caso, este problema está resolvido, uma vez que se usa um <b>role</b>, com o intuito de divulgar a informação referente a um conjunto de pessoas.</p> <p>Isto diminui muito a fuga de conteúdo importante, dado que os nomes, emails ou números de telemóvel podem ser usados causando um grande impacto nos ataques em si.</p>
Não autenticação para uso da <i>database</i> por parte dos MNTNER	<p>Ao criar-se um mecanismo de autenticação, cria-se uma “porta” necessária para futuros ataques por parte de MNTNER falsos.</p> <p>O uso do esquema MD5-PW é uma boa escolha por si só, dado que se baseia no algoritmo de hash MD5, fornecendo uma forte autenticação. Com ele, garante-se que as informações de autenticação armazenadas na <i>database</i> correspondem a um segredo criptográfico.</p>
Não uso de um sistema de <i>login</i> único	<p>Ao usar-se um <i>Single Sign-On</i> (SSO), existe um maior controle no acesso ao permitir que um <i>user</i> aceda a vários serviços apenas com um <i>login</i>. Este método atenua o risco de acesso a <i>websites</i> de terceiros, uma vez que se evita guardar as <i>passwords</i> ou até mesmo geri-las de forma externa.</p>
Mensagens de erro por parte da página WEB	<p>A ideia é que a empresa simplifique o processo de erro aquando da solicitação de conteúdo inexistente, não indicando quaisquer tipo de dados importantes. No caso da EDP, o <i>user</i> é redirecionado para um página de erro geral a todos os erros, contendo a mensagem “A página que procura está sem energia.”.</p>
Informações acerca dos <i>emails</i>	<p>Deve-se preferencialmente usar um <i>email</i> que diga respeito a uma função de “trabalhadores” no geral, ao invés da divulgação de <i>emails</i> pessoais. Obtivemos o email <a href="mailto:distribuicao.setgas@galpenergia.com">distribuicao.setgas@galpenergia.com</a> que parece corresponder a algo mais geral.</p>
Ficheiro robots.txt	<p>O <i>website</i> da EDP possui o ficheiro “robots.txt”. A ideia é que este ficheiro não seja usado para ocultar informações importantes dado que é um ficheiro disponível publicamente. Neste caso, esse ficheiro não parece conter qualquer secção importante.</p>

## 2.2 TUB – Transportes Urbanos de Braga

A empresa TUB – Transportes Urbanos de Braga tem como objeto social a prestação do serviço de transporte urbano de passageiros no concelho de Braga. A sua missão é oferecer serviços de mobilidade para a região de forma acessível e transparente.

Dada a sua natureza pública e que o capital social é pertencente à Câmara Municipal de Braga, esta empresa torna-se um excelente candidato para analisar dados passivos de informação crucial presente no *website* sobre os vários ramos da empresa e informações sensíveis que têm de ser públicas dada a lei de *information disclosure* sobre entidades públicas ser imperativa.

### 2.2.1. Análise Informações de Registo de Domínio

Como falado anteriormente, o registo e a manutenção global dos endereços IP engloba a identificação dos *hosts* que existem pela Internet no geral. Esta combinação entre os nomes de domínio e o seu *host*, ou seja, endereço IP associado torna esta informação imperativa para analisar detalhes da administração da empresa, tal como endereços físicos da mesma ou mesmo informações dos técnicos responsáveis.

Desta forma, na próxima primeira análise iremos recorrer à utilidade **WHOIS**, que permite estudar sobre estes domínios e os seus *hosts* associados através da pesquisa do *ownership* de cada um.

- Detalhes sobre o domínio *tub.pt*

Através da consulta de **WHOIS** direcionado para o domínio obtemos esta resposta detalhada que nos permite observar várias situações de recolha passiva de informação, como quem registou o *website* e quem administra o registo do domínio, o local onde se encontra registado e ainda os contactos relativos a quem efetuou este processo todo.

```
diogoesnog@DESKTOP-OCRRD5H:~$ whois tub.pt
Domain: tub.pt
Domain Status: Registered
Creation Date: 28/10/2003 00:00:00
Expiration Date: 28/02/2020 23:59:00
Owner Name: Tub - Empresa Transportes Urbanos de Braga - E.M.
Owner Address: Quinta Santa Maria - Maximinos
Owner Locality: Braga
Owner ZipCode: 4703-244
Owner Locality ZipCode: Braga
Owner Country Code: PT
Owner Email: geral@tub.pt,webmaster@tub.pt
Admin Name: AlmouroITec - Servicos de Informatica e Internet Lda
Admin Address: Estrada Nacional 3 - 9-C
Admin Locality: Constancia
Admin ZipCode: 2250-028
Admin Locality ZipCode: Constancia
Admin Country Code: PT
Admin Email: registry@buydomain.pt
Name Server: ns1.tub.pt | IPv4: 109.71.45.11 and IPv6:
Name Server: ns2.tub.pt | IPv4: 109.71.45.73 and IPv6:
```



- O domínio *tub.pt* foi registado pela entidade Tub - Empresa Transportes Urbanos de Braga - E.M., na data de 28/10/2003, devendo ser renovado antes da data de 28/02/2020;
- Além do nome de quem registou este endereço pode-se obter a informação da localização da empresa em si, especificando a morada e o respetivo código postal;
- São visíveis também dois emails que se referem à parte geral da TUB e também à parte administrativa do *website* da TUB;
- A análise destas informações revela ainda que existe uma entidade administradora responsável pelo serviço de registo/manutenção do domínio, de nome AlmouroITec - Serviços de Informática e Internet Lda;
- É possível também obter as informações de morada relativas a esta empresa à qual a TUB recorreu para processar toda a informação, registando o seu *website*;
- É mostrado o email relativo à equipa desta empresa.

Para além destas informações, são demonstrados dois *name servers*, juntamente com a informação do IP de cada um deles. Recorrendo-se ao *website* [whois.domaintools.com](http://whois.domaintools.com), verifica-se ainda a existência de um *autonomous system*, através da existência de um *autonomous system number (ASN)* registado alguns anos depois de o domínio ter sido oficialmente criado.



## Whois Record for Tub.pt

### — Domain Profile

Registrar Status	taken
Name Servers	NS1.TUB.PT (has 1 domains) NS2.TUB.PT (has 1 domains)
Tech Contact	—
IP Address	109.71.45.11 is hosted on a dedicated server <span>Reverse IP ↗</span>
IP Location	 - Santarem - Tomar - Almouroltec Servicos De Informatica E Internet Lda
ASN	 AS24768 ALMOUROLTEC, PT (registered Nov 12, 2009)
Hosting History	1 change on 2 unique name servers over 0 year <span>↗</span>

- Detalhes sobre o endereço IP do domínio *tub.pt*

Os dados fornecidos através das ferramentas utilizadas anteriormente dão-nos informações sobre como a rede é gerida internamente. Através da ferramenta *nslookup* conseguimos obter facilmente o endereço IP do *host* pertencente ao domínio da empresa TUB. Fazendo a *query WHOIS* agora ao endereço IP do *host* temos acesso a uma panóplia de informações associadas à base de dados **RIPE** que se consegue retirar algumas informações passivas que contém dados sobre pessoas e empresas associadas.

```
diogoesnog@DESKTOP-OCRRD5H:~$ whois 109.71.45.11
% 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
.
inetnum:        109.71.45.0 - 109.71.45.255
netname:        PT-ALMOUROLTEC
descr:          ALMOUROLTEC - Lda dba PTisp
descr:          *****
descr:          * for abuse or spam complains contact:
descr:          * abuse@ptisp.pt
descr:          *****
country:        PT
admin-c:        LUIS-RIPE
tech-c:         LUIS-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-ALMOUROLTEC
created:        2011-10-05T12:08:28Z
last-modified:  2013-08-10T23:44:52Z
source:         RIPE
```

- Consegue-se obter o intervalo de endereços IP *classless* que se encontram entre 109.71.45.0 e 109.71.45.255. Estes endereços são também geridos pela Almouroltec Serviços De Informática e Internet Lda falada anteriormente no seguimento de *autonomous system*;
- O ISP desta empresa está localizado em Portugal (PT);
- Detalhes adicionais sobre a localização não se encontram descritas, dado que também é opcional nesta base de dados **RIPE**;
- O registo da AlmourolTec foi modificado a última vez no dia 8/10/2013.

```

person:      Luís 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 '109.71.45.0/24AS24768'

route:       109.71.45.0/24
descr:       ALMOUROLTEC SERVICOS DE INFORMATICA E INTERNET LDA
origin:      AS24768
mnt-by:      MNT-ALMOUROLTEC
created:     2014-12-30T13:49:29Z
last-modified: 2014-12-30T13:49:29Z
source:      RIPE

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

```

Esta secção secundária da base de dados **RIPE** é a única que contém informações pessoais sobre pessoas. Verifica-se assim a divulgação de uma pessoa chamada Luís Inverno, incluindo a sua morada pormenorizada, número de telefone e também número fax.

Esta informação toda tem algo em comum que é o MNTNER (MNT-ALMOUROLTEC), que se encontra responsável por tudo isto e também pela proteção de alguns dados aqui fornecidos. Desta forma, iremos analisar a informação passiva do mesmo a seguir.

```

diogo@DESKTOP-OCRRD5H:~$ whois -r MNT-ALMOUROLTEC
% 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 'MNT-ALMOUROLTEC'

mntner:        MNT-ALMOUROLTEC
descr:         ALMOUROLTEC SERVICOS DE INFORMATICA E INTERNET LDA
admin-c:       LI90-RIPE
auth:          MD5-PW # Filtered
auth:          SSO # Filtered
mnt-by:        MNT-ALMOUROLTEC
created:       2009-11-11T00:03:08Z
last-modified: 2015-12-04T12:34:14Z
source:        RIPE # Filtered

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

```

Nesta informação fornecida sobre o *maintainer* conseguimos a informação que para alterar algo na base de dados **RIPE** é necessária uma autenticação em si, ou seja, comunicação existente entre as várias pessoas envolvidas deve incluir uma *password* (MD5-PW e SSO).

Além de toda esta informação fornecida pelo **WHOIS**, é ainda possível relacionar este endereço IP principal com uma base de dados geográfica, recolhendo detalhes exatos acerca da localização geográfica do ISP.

GeoIP2 City Results							
IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization
109.71.45.11	PT	Lisbon, Lisbon, Portugal, Europe	1300-229	38.7174, -9.1321	200	Almouroltec Servicos De Informatica E Internet Lda	Almouroltec Servicos De Informatica E Internet Lda

- ISP localizado em Lisboa, Portugal com as suas coordenadas aproximadas definidas aqui;
- ISP pertence à organização Almouroltec – Serviços de Informática e Internet, Lda.

## 2.2.2. Análise Página WEB/Procura de Informações Online

Como a maioria das empresas mantém os seus *websites* visíveis a nível *online*, a probabilidade em escapar informações torna-se uma probabilidade quase certa. Por essa razão, a análise detalhada do conteúdo da página WEB em si, torna-se muitas das vezes imprescindível para qualquer atacante.

Através do espelhamento do conteúdo local do *website*, analisamos para tentar investigar toda a informação, na tentativa de recolher informações empresariais que podem ser úteis para um futuro planeamento de ataque. Para isso, foi usada uma extensão via Google Chrome de nome “*Email Extractor*”, que permite fazer um *scan* dos e-mails que existem na página em si, mas que não estão visíveis a olho nu. Aliado a isto, fez-se o *download* da página WEB principal, obtendo-se todo o conteúdo necessário para uma análise fora da rede.

Ao analisar as páginas *web* da TUB – Transportes Urbanos de Braga analisamos um comportamento contrário ao que aconteceu na empresa EDP tratada anteriormente. Dada a natureza pública da empresa em estudo conseguimos obter um leque de dados propício para um futuro ataque de engenharia social. Ao analisarmos a página inicial da TUB temos acesso detalhado à morada da sede e dos respetivos postos de serviço e também os diversos *emails* da administração e dos vários departamentos associados.

### Transportes Urbanos de Braga E.M.

Rua Quinta de Sta. Maria

Apartado 2383,

4700-244 Braga

Telefone:253 606 890

Fax:253 606 899

Latitude:41°32'24.07"N

Longitude:8°26'7.96"W

### Administração

Vogal: [tas@tub.pt](mailto:tas@tub.pt)

Vogal: [sandracerqueira@tub.pt](mailto:sandracerqueira@tub.pt)

### Departamentos

Geral: [geral@tub.pt](mailto:geral@tub.pt)

Aprovisionamento: [esteves@tub.pt](mailto:esteves@tub.pt)

Recursos Humanos: [mduarte@tub.pt](mailto:mduarte@tub.pt)

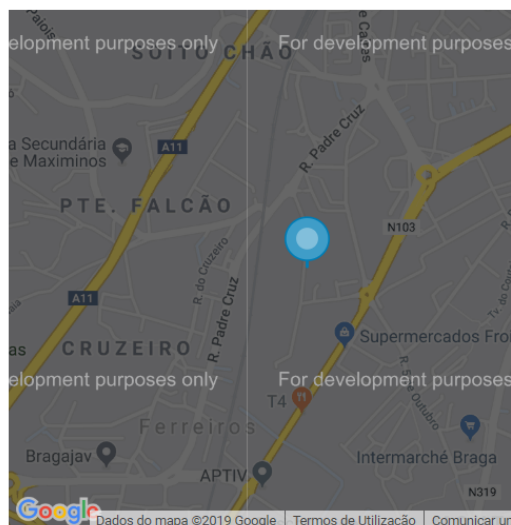
Comercial: [apoiocliente@tub.pt](mailto:apoiocliente@tub.pt)

Qualidade: [qualidade@tub.pt](mailto:qualidade@tub.pt)

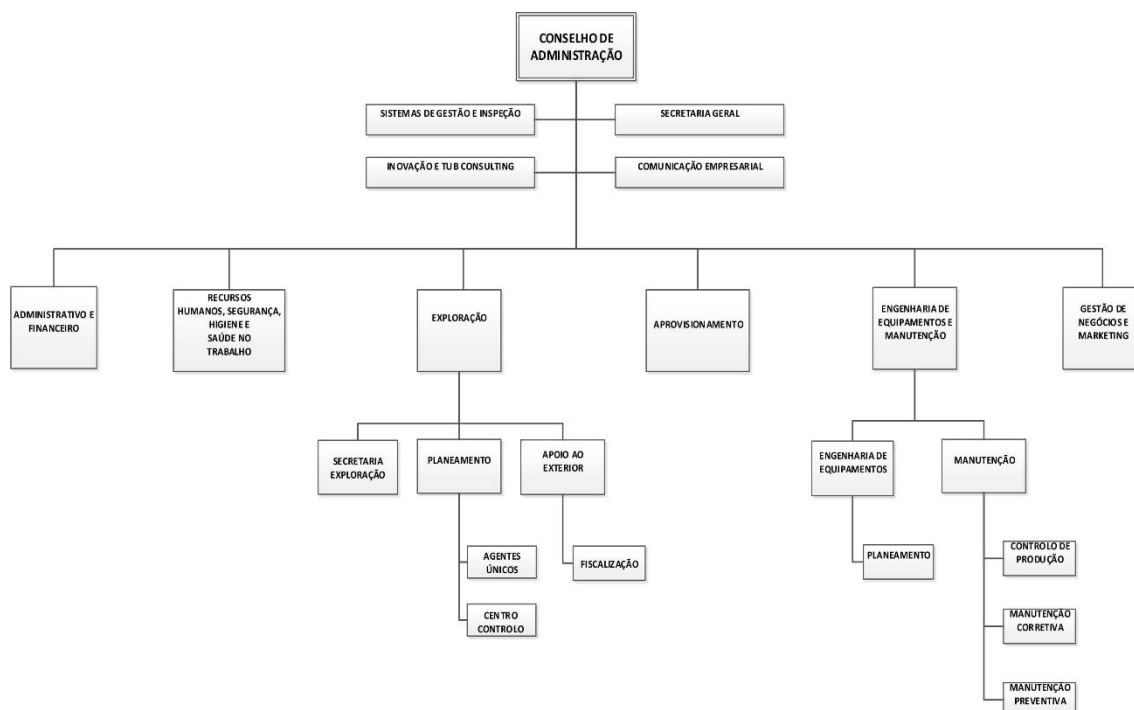
Segurança e Higiene no Trabalho: [vaniabarbosa@tub.pt](mailto:vaniabarbosa@tub.pt)

Formação: [antonio.machado@tub.pt](mailto:antonio.machado@tub.pt)

Exploração: [tas@tub.pt](mailto:tas@tub.pt)



Ao analisar com cuidado o resto das informações fornecidas consegue-se também obter dados como o organograma da empresa, tendo assim um *insight* sobre o funcionamento da empresa e as várias secções que operam a mesma.



Foi através duma análise do *sitemap* escondido que também se teve acesso a uma página de teor estatístico sobre vários indicadores sobre a empresa e o seu funcionamento, como o número de veículos, linhas, paragens, agentes únicos, passageiros transportados e mais informações como visto na figura abaixo.

	2013	2014	2015	2016	2017
Nº De Linhas	70	70	72	73	74
Paragens	1758	1756	1794	1816	1830
Nº De Viaturas	121	119	163	152	142
Km De Rede	294,43	295,69	297,67	300,47	300,53
Freguesias Servidas	37	37	37	37	37
Kms Percorridos	5.198.033	5.319.636	5.491.429	5.803.995	5.822.195
Total Efetivos	315	322	326	324	340
Agentes Únicos	197	208	216	215	233
Passageiros Transportados	10.249.960	10.351.857	10.796.640	11.168.196	11.659.855

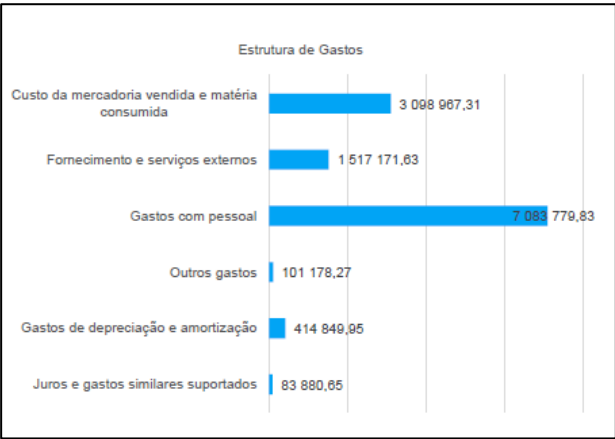
Foi através duma análise mais profunda ao *source code* da página que se encontrou numa pasta *frontoffice* toda uma panóplia de informações referentes às contas e economia da empresa incluindo valores reais do último ano civil.

Conseguindo informações variadas como mostrado nas figuras ao lado desde informações sobre o total de compras de cada tipo, como passes ou bilhetes a bordo e também nas credenciais. Noutra secção também se descobriu a estruturação dos gastos demonstrando que a empresa gasta mais com o pessoal do que com qualquer outra parte combinada.

Com todas estas informações existia também *disclosure* de salários mensais do conselho de administração e os seus currículos. Isto forneceu uma situação complicada porque são imensas informações tanto internas como externas da empresa, tornando relutante a opinião de que se tudo isto deve ser de tão fácil ou de acesso livre sem qualquer tipo de *login* adicional ou autenticação.

Estrutura dos títulos (*)			
Vendas	2017	2018	Varição
Passes	3 629 310,15	3 657 523,70	0,78%
Pré-comprados	976 640,95	998 662,80	2,25%
Bilhetes de Bordo	1 458 932,35	1 547 821,85	6,09%
Bilhetes turístico	4 299,00	4 620,85	7,49%
Cultura	0	1000,00	100%
Credenciais	13 369,66	13 875,71	3,79%
Total	6 082 552,11	6 223 504,91	2,32

(\*) estes valores incluem IVA à taxa legal.



**Conselho de administração:**

**Presidente:**Firmino José Rodrigues Marques

Vencimento (Câmara Municipal de Braga): 3.453,25€

**Vogal:**Teotónio Luís Vieira de Andrade dos Santos

Vencimento: 3.307,38€

**Vogal:**Sandra Cristina Leitão Cerqueira

Vencimento: 3.307,38€

**Assembleia Geral:**

**Presidente:**Miguel Sopas de Melo Bandeira

**Fiscal Único:**

Sociedade de Revisores Oficiais de Contas

Gaspar Castro, Romeu Silva & Associados – S.R.O.C., Ldª

**Sede:**

Rua Quinta de Santa Maria - Maximinos

Apartado 2383

4700-244 Braga

### 2.2.3. Estruturas de Segurança

No ponto de vista de segurança, existem muitas estratégias que podem ajudar a ocultar informações relevantes aos mecanismos de busca passiva que se tem vindo a estudar. A tabela será usada para descrever alguma dessas estratégias dando a entender a necessidade de se implementar tal “funcionalidade”. Estas estratégias são referentes ao estudo no geral, já que algumas pertencem ao domínio em si e outras à página WEB da empresa.

Problema	Estratégia de Resolução
Divulgação de vários objetos <i>person</i> por parte dos registos do ISP	Isto diminui muito a fuga de conteúdo importante, dado que os nomes, emails ou números de telemóvel podem ser usados causando um grande impacto nos ataques em si.
Mensagens de erro por parte da página WEB	A ideia é que a empresa simplifique o processo de erro aquando da solicitação de conteúdo inexistente, não indicando quaisquer tipo de dados importantes. No caso da TUB, o <i>user</i> é redirecionado para a página inicial de novo.
Informações acerca dos <i>emails</i>	Deve-se preferencialmente usar um <i>email</i> que diga respeito a uma função de “trabalhadores” no geral, ao invés da divulgação de <i>emails</i> pessoais como foi discutido anteriormente.
Ficheiro robots.txt	O <i>website</i> da TUB não possui o ficheiro “robots.txt”. A ideia é que este ficheiro não seja usado para ocultar informações importantes dado que é um ficheiro disponível publicamente.

### **3. Conclusões e Observações Finais**

O processo de *Passive Information Gathering* é um estágio importantíssimo em qualquer exercício de teste de “caixa preta”, dado que consiste em aprender do zero, o máximo de informações existentes em relação à empresa que se pretende atacar. Esta aprendizagem é a base para que se crie uma avaliação de segurança completa e precisa e que permita aos atacantes o uso da informação recolhida para coordenar/planear ataques mais avançados.

Neste trabalho prático em especial, foi feita uma recolha passiva para duas empresas, uma mais local e outra com uma dimensão visivelmente superior, com o propósito de comparar ambas, dando assim a entender que algumas empresas menores podem ter um cuidado mais limitado para um público alvo também ele inferior. Vimos que no caso da TUB, existe uma página WEB dedicada exclusivamente a informação do foro institucional, onde existe uma grande série de detalhes, que acaba até por incluir o vencimento do conselho administrativo da empresa. Entre outros, alguns destes detalhes podem ser obrigatórios por parte da empresa, mas nada impede de se ter um trato especial pelos documentos que se cria e posteriormente se disponibiliza online.

Este trabalho prático serve também para demonstrar a necessidade da prática do exercício de recolha por parte da própria empresa, dado que ao fazer isso por conta própria ou por meio de terceiros de confiança, a empresa consegue prevenir possíveis erros de divulgação, prevenindo futuros ataques.

A importância das técnicas de recolha passiva de informações, tanto no entendimento do significado das técnicas de análise quanto no tipo de informação disponível, está por isso a aumentar de forma significativa. Assim, com os aumentos substanciais do número de ferramentas de análise capazes de realizar vários graus de análise, torna-se imperativo por parte das empresas identificar as informações divulgada, tomando medidas rápidas e eficazes para uma proteção na divulgação futura.



## 4.Referências

- Moronwi, J. (s.d.). *Footprinting: Passive Information Gathering*. Obtido de <https://netseedblog.com/security/footprinting-passive-information-gathering/>
- Obbayi, L. (s.d.). *Ethical Hacking: Passive Information Gathering With Maltego*. Obtido de INFOSEC: <https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/passive-intelligence-gathering/>