

Universidade do Minho
Escola de Engenharia

Universidade do Minho
Mestrado Integrado em Engenharia Informática

SSI

Segurança de Sistemas Informáticos **Trabalho Prático 2**

Dezembro 2020

Tânia Filipa Amorim Rocha
A85176

Maria Miguel Albuquerque Regueiras
A85242

Conteúdo

1	Introdução	5
2	Contextualização	6
3	Parte 1 - Coleta Passiva de Informação	6
3.1	Empresa Local - Transportes Urbanos de Braga (TUB)	6
3.1.1	Análise de Informações de Registo de Domínio	6
3.1.2	Análise da Página WEB/Procura de Informações Online	9
3.1.3	Possíveis Estratégias de Segurança	16
3.2	Corporação - Transportes Aéreos Portugueses (TAP)	16
3.2.1	Análise de Informações de Registo de Domínio	17
3.2.2	Análise da Página WEB/Procura de Informações Online	21
3.2.3	Possíveis Estratégias de Segurança	28
3.3	Conclusões - Parte 1	29
4	Parte 2 - Scanning	30
4.1	Contextualização	30
4.2	NMAP	30
4.2.1	Questão 1	30
4.3	Nessus, Snort e Wireshark	37
4.3.1	Questão 2	37
4.3.2	Questão 3	40
4.3.3	Questão 4	42
4.3.4	Questão 5	43
4.4	Conclusões - Parte 2	47
5	Conclusão	48
6	Bibliografia	49

Lista de Figuras

1	Processo <i>Pentest</i>	6
2	Detalhes devolvidos pelo comando whois quando aplicado ao site da TUB	7
3	Detalhes devolvidos pelo site whois.domaintools.com quando aplicado ao site da TUB	8
4	Detalhes devolvidos pelo comando host quando aplicado ao site da TUB	8
5	Detalhes devolvidos pelo comando nslookup quando aplicado ao site da TUB	9
6	Detalhes devolvidos pelo comando dig quando aplicado ao site da TUB	9
7	Página 'contactos' do website da TUB	10
8	Órgãos Sociais do website da TUB e Pesquisa	10
9	<i>WayBackMachine</i> - resultados da procura do site da TUB	11
10	Resultados da procura no site da TUB	12
11	Código fonte do site da TUB	13
12	Código do script angular/socket.js do site da TUB	13
13	Pesquisa da palavra TODO no script directives.js	13
14	Código do script services.js do site da TUB	14
15	Pesquisa pela palavra login no script app.js	15
16	Código do script app.js do site da TUB	15
17	Pesquisa no código pela palavra TODO	16
18	Detalhes devolvidos pelo comando whois quando aplicado ao site da TAP	17
19	Detalhes devolvidos pelo comando whois quando aplicado ao site da TAP	18
20	Detalhes devolvidos pelo site whois.detailtools.com quando aplicado ao site da TAP	19
21	Detalhes devolvidos pelo comando host quando aplicado ao site da TAP	20
22	Detalhes devolvidos pelo comando nslookup quando aplicado ao site da TAP	20
23	Detalhes devolvidos pelo comando dig quando aplicado ao site da TAP	21
24	Página "contactos" do website da TAP	22
25	Página "Administração" do website da TAPAirPortugal	23
26	Curriculum do Presidente da empresa	23
27	Estruturação das .acções da TAP presente no relatório de contas de 2019	24
28	Dados económicos da empresa presentes no relatório de contas de 2019.	24
29	Posição financeira, financiamentos e rendimentos da empresa.	25
30	Capital da empresa	26
31	Atas públicas da empresa	27
32	Página "contactos" deste website	27
33	Candidaturas disponíveis em Outubro de 2019	28
34	Código Fonte do site da TAP	28
35	Output do scan -sS	31
36	Output do scan -sN , -sF, -sX respetivamente.	32
37	Output do scan -sA	33
38	Output do scan -sO	33
39	Output do scan -sV	34
40	Vulnerabilidade CVE-2018-15919 do serviço OpenSSH.	34
41	Vulnerabilidade CVE-2018-8407 do serviço Microsoft Windows RPC.	35
42	Vulnerabilidade CVE-2020-13159 do serviço NetBios.	35
43	Vulnerabilidade CVE-2019-0584 do serviço Windows Server 2008 R2.	36
44	Vulnerabilidade CVE-2017-10784 do serviço WEBrick httpd 1.3.1 (Ruby 2.3.3).	36
45	Vulnerabilidade CVE-2016-6662 do serviço MySQL 5.5.20-log.	37
46	Vulnerabilidade CVE-2020-0655 do serviço Windows Terminal Service.	37
47	Resultados da procura de vulnerabilidades no Metasploitable 3 através do Nessus	38
48	Vulnerabilidades de uma mesma família.	38
49	Vulnerabilidades BlueKeep.	39
50	Vulnerabilidade com nível crítico.	39
51	Tráfego anómalo do tipo Misc activity.	40
52	Tráfego do Wireshark	40
53	Tráfego anómalo do tipo Attempted Denial of Service.	41
54	Vulnerabilidade CVE-2000-0138.	41
55	Tráfego do Wireshark	41
56	Output do Snort correspondentes aos pacotes do tipo UDP.	42

57	Vulnerabilidade CVE-1999-0016.	43
58	Vulnerabilidade Media.	43
59	CVE-2018-8722.	44
60	Instalação da nova versão do Manager Engine Desktop.	44
61	“Família”de vulnerabilidades do mesmo software.	44
62	Vulnerabilidade alta.	45
63	“família”de vulnerabilidades do Elasticserach.	45
64	“família”de vulnerabilidades do Elasticserach.	45
65	Windows Update Desligado.	46
66	Windows Update à procura de Actualizações.	46
67	Actualizações disponíveis.	46
68	Antes de qualquer alteração.	47
69	Depois das alterações.	47

1 Introdução

Este trabalho prático encontra-se enquadrado no programa da Unidade Curricular de Segurança de Sistemas Informáticos e tem como objetivo aprofundar os conhecimentos adquiridos nas aulas sobre a fase de *footprinting* da actividade de *Penetration Testing*, ou seja, *Pentest*. Deste modo, este projecto é dividido em duas partes com o objectivo a separar os métodos passivos e activos de *Footprinting*.

A primeira parte consiste no uso de técnicas para colecta passiva de informação como ferramenta de análise da postura de segurança em sistemas e infraestruturas reais de empresas de grande dimensão e locais.

A segunda parte serão utilizadas técnicas activas para a identificação de vulnerabilidades e fraquezas de um sistemas a partir de um ambiente configurado para o mesmo.

2 Contextualização

Penetration Testing é uma actividade que se baseia numa tentativa autorizada para ganhar acesso a um sistema com objectivo de identificar e recomendar soluções para possíveis vulnerabilidades no mesmo. É também conhecida por *Ethical Hacking*.

Este projeto está focado nas duas fases de *Footprinting* existentes no processo ciclico de *Pentest*.

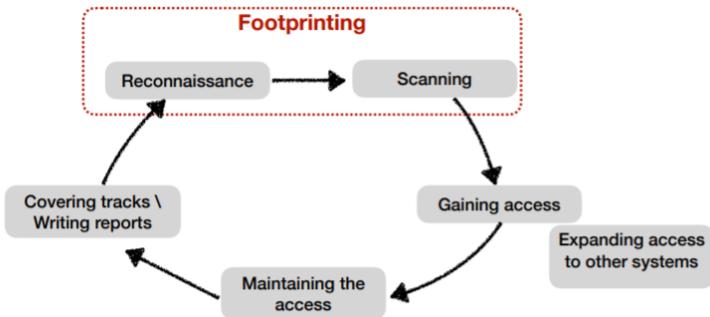


Figura 1: Processo *Pentest*

A ideia principal desta primeira parte deste guia prático passa então por realizar uma recolha passiva ou seja, *Reconnaissance* 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 mas de contexto semelhante para que pudesse ser feita uma pequena comparação final entre ambas, na tentativa de compreender as diferenças de postura adoptadas pelos domínios de cada uma destas. Falaremos assim de uma das maiores empresas nacionais a nível de transportes aéreos – TAP – e da empresa de Transportes Urbanos de Braga – TUB.

3 Parte 1 - Coleta Passiva de Informação

3.1 Empresa Local - Transportes Urbanos de Braga (TUB)

Os Transportes Urbanos de Braga, normalmente designados por TUB, é uma empresa municipal portuguesa, de transporte de passageiros. Tem como principal objectivo servir as populações do concelho de Braga.

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.

Número de trabalhadores desagregado segundo a modalidade de vinculação em 31 de Dezembro de 2019: Contrato de trabalho em funções publicas - 120. Contrato de trabalho ao abrigo do regime geral - 225.

3.1.1 Análise de 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. Esta pesquisa retornou a seguinte informação:

```
(kali㉿kali)-[~]
└─$ whois tub.pt
Domain: tub.pt
Domain Status: Registered
Creation Date: 28/10/2003 00:00:00
Expiration Date: 28/02/2021 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: AlmourolTec - 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:
```

Figura 2: Detalhes devolvidos pelo comando whois quando aplicado ao site da TUB

- 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 28/10/2021;
- Além do nome de quem registou este endereço pode-se obter a informação da localização da empresa em si, especificando a morada e o respectivo 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 AlmourolTec - 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, registrando o seu website;
- É mostrado o email relativo à equipa desta empresa.
- São ainda demonstrados dois name servers juntamente com a informação IP de cada um deles.

Através do website www.whois.domaintools.com é ainda possível obter informação adicional relacionada com o sistema autónomo e o seu identificador ASN, *Autonomous System Number*, registrado. Um sistema autónomo (AS) é um conjunto de redes que se gera como se de um único sistema se tratasse. Esses sistemas em conjunto partilham também de um conjunto de regras em comum (como estratégias de routing). Um ASN único é atribuído a cada AS e este é importante porque identifica esse conjunto

de redes na Internet. O ASN pode ainda ser público (se se incluir na gama 1 a 64511) ou privado (gama 64512 a 65534). A diferença encontra-se no facto de que, se for público, quer dizer que tem conexão a outros sistemas autónomos e troca informação entre eles pela Internet. Pela figura 3, podemos observar que o AS onde este se encontra tem o identificador 24768, significando que é público e tem conectividade a outros sistemas autónomos.

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
IP Location	PT - 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 1 year
Website	
Website Title	T 500 SSL negotiation failed:
Response Code	500

Figura 3: Detalhes devolvidos pelo site whois.domaintools.com quando aplicado ao site da TUB

Adicionalmente, podemos querer detalhes sobre o endereço IP do domínio tub.pt. Existem vários métodos para a procura de informações sobre um determinado endereço:

- *Host* - O comando *host* é um utilitário de pesquisa de DNS , localizando o endereço IP de um nome de domínio. Também realiza pesquisas reversas , localizando o nome de domínio associado a um endereço IP. Através do comando *host* do *website* é possível obter os seguintes detalhes:

```
(kali㉿kali)-[~]
└─$ host tub.pt
tub.pt has address 109.71.45.11
tub.pt mail is handled by 0 tub-pt.mail.protection.outlook.com.
tub.pt mail is handled by 32767 ms51869157.msv1.invalid.
tub.pt mail is handled by 32767 7d28f8b64b2cf2659ac2f010dfe662436ea31a35.msv1.invalid.
```

Figura 4: Detalhes devolvidos pelo comando host quando aplicado ao site da TUB

Passamos então a ter o conhecimento que o endereço do site da TUB é 109.71.45.11.

- *nslookup* - O comando nslookup (Name Server lookup) consulta servidores de nomes (interactivamente ou não) em busca de informações tanto relativas a nomes de domínio como de próprios endereços IP. Este comando devolve também informações semelhantes ao comando *host*:

```
(kali㉿kali)-[~]
└─$ nslookup tub.pt
Server:      192.168.8.1
Address:     192.168.8.1#53

Non-authoritative answer:
Name:   tub.pt
Address: 109.71.45.11
```

Figura 5: Detalhes devolvidos pelo comando nslookup quando aplicado ao site da TUB

Neste caso obtemos uma resposta não-autoritativa, significando que o DNS em questão não conseguiu resolver a query sozinho e teve de questionar outros DNSs até obter a resposta. Ficamos então a saber qual o endereço do servidor do site tub.pt.

- **dig** - dig (Domain Information Groper) é um comando que executa consultas sobre registos de DNS. É muito semelhante aos anteriores e revela algumas informações como o *time to live* (7100) que tipo de registo é (A) e os endereços.

```
(kali㉿kali)-[~]
└─$ dig tub.pt
; <>> DiG 9.16.8-Debian <>> tub.pt
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 57562
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0
;
;; QUESTION SECTION:
;tub.pt.                      IN      A
;
;; ANSWER SECTION:
tub.pt.                       60      IN      A      109.71.45.11
;
;; AUTHORITY SECTION:
tub.pt.          7110    IN      NS      ns1.tub.pt.
tub.pt.          7110    IN      NS      ns2.tub.pt.
;
;; Query time: 4 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Sun Dec 06 17:34:03 EST 2020
;; MSG SIZE  rcvd: 76
```

Figura 6: Detalhes devolvidos pelo comando dig quando aplicado ao site da TUB

3.1.2 Análise da Página WEB/Procura de Informações Online

Visto que uma maioria das empresas hoje em dia tem como requisito ter atividade online, é possível que exista vazamento de informações. Por esta mesma razão, é imprescindível a procura de informações a nível web.

Neste sentido foi feita uma procura no website desta empresa com objectivo de encontrar informações úteis para um futuro planeamento de ataque.

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 respectivos 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
 Latitude: 41°32'24.07"N
 Longitude: 8°26'7.96"W

Administração
 Vogal: tas@tub.pt
 Vogal: sandracerqueira@tub.pt

Departamentos
 Geral: geral@tub.pt
 Aprovisionamento: esteves@tub.pt
 Recursos Humanos: rh@tub.pt
 Comercial: apoiocliente@tub.pt
 Qualidade: qualidade@tub.pt
 Segurança e Higiene no Trabalho: vaniabarbosa@tub.pt
 Formação: antonio.machado@tub.pt
 Exploração: tas@tub.pt



Figura 7: Página 'contactos' do website da TUB

É possível ainda encontrar os nomes e registos pessoais de trabalhadores, administradores e responsáveis através deste website e com pesquisa ter acesso a informações adicionais sobre as mesmas. Por exemplo:

Orgãos Sociais

Conselho de administração:
 Presidente: Miguel Sopas de Melo Bandeira
 Vencimento - Câmara Municipal de Braga
 Vogal: Teotónio Luís Vieira de Andrade dos Santos
 Vencimento: 3.307,38€
 Vogal: Sandra Cristina Leitão Cerqueira
 Vencimento: 3.307,38€

Assembleia Geral:
 Presidente: João Rodrigues

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
 Latitude: 41°32'24.07"N
 Longitude: 8°26'7.96"W

Teotónio Luis Vieira de Andrade dos Santos

pt.kompass.com/empresa-tub-transportes-urbanos-de-... ▾
Empresa Tub - Transportes Urbanos De Braga, Em ... - K...
 20/10/2020 — Administradora. Teotónio Luis Vieira de Andrade dos Santos. Administrador.
 Dr. Margarida Vasconcelos. Diretora Financeira. Sandra Carvalho.

www.ctc-limitalmacavado.com/seminariomobilitade... ▾ PDF
Seminário "Mobilitade, Inovação e Sustentabilidade" - C...
 A sessão foi aberta pelo Eng. Luís Macedo pelo Sr. Presidente do Município de Vila Verde, Dr. António Vieira e ... Teotónio Luis Vieira de Andrade dos Santos.

www.tub.pt/templates/frontoffice/enterprise/pdf... ▾ PDF
Relatório e Contas 2017 - Tub
 31/12/2017 — Vogal Executivo Teotónio Luis Vieira de Andrade dos Santos 14 de novembro de 2017. Vogal Executivo Sandra Cristina Leitão Cerqueira.

www.dps.uminho.pt/uploads/Relatorio-DPS_2015... ▾ PDF
Relatório 2015 - Departamento de Produção e Sistemas
 de Julho com a EEUUM e o DPS, o Vice-Reitor Rui Vieira de Castro afirmou que o convénio com a UTAD for já assinado, por ... Andrade Dias - Presidente da APOGEP, 23 outubro 2015. (9h-13h ... Teotónio Luis Vieira de Andrade dos Santos.

Figura 8: Orgãos Sociais do website da TUB e Pesquisa

Existe também uma página de recrutamento para emprego neste website. No entanto, quando não há necessidade de recrutamento, esta página informa que de momento não apresentam vagas para tal. Esta é uma técnica que ajuda a manter dados sobre a empresa mais seguros porque à primeira vista os protege em grande parte do tempo visto que não expõe requisitos que seriam necessários para informar de que tipo de capacidades estaria à procura em possíveis contratações. No entanto existem métodos para contornar este método de ocultação de dados. Um deles é através do uso de websites como "archive.org" e "WayBackMachine" que permitem visitar a página em questão quando a fase de recrute estaria aberta e obter informações que actualmente não estariam visíveis. Ao procurar pelo website da TUB no "WayBackMachine" aparecem várias opções de datas onde o site é visitável noutras datas que não a actual.

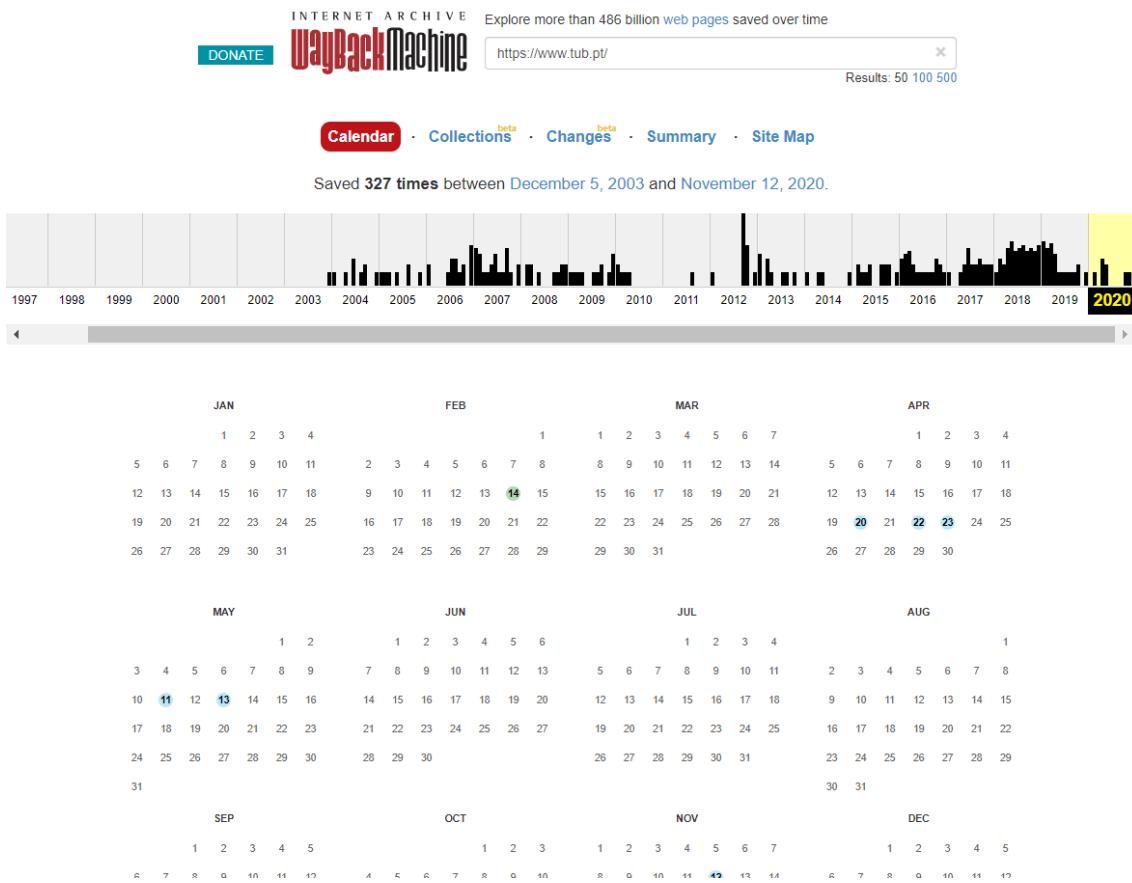


Figura 9: WayBackMachine - resultados da procura do site da TUB

Para além disto, após uma pesquisa no website actual, é possível obter todo o tipo de dados que possam ser úteis desde evoluções de receitas, percursos mais utilizados, número de passageiros que foram transportados, redes, taxas, etc. Aliás, até informação relativa às finanças da empresa são publicas desde volume de negócios, subsídios, estrutura de rendimentos, gastos e outros. Todas estas informações estão disponíveis por ano.

Relatório e Contas

2019:

[PDF RELATÓRIO E CONTAS](#)

2018:

[PDF RELATÓRIO E CONTAS](#)

2017:

[PDF RELATÓRIO E CONTAS](#)

2016:

[PDF RELATÓRIO E CONTAS](#)

2015:

[PDF RELATÓRIO E CONTAS](#)

2014:

[PDF RELATÓRIO E CONTAS](#)

2013:

[PDF RELATÓRIO E CONTAS](#)

Nota curricular Teotónio Andrade dos Santos

Formação:

- Mestrando em Engenharia e Gestão Industrial, Universidade do Minho;
- Licenciado em Engenharia e Gestão Industrial (Pré Bolonha), Universidade Lusíada.

Experiência Profissional:

- Administrador executivo dos Transportes Urbanos de Braga entre 2013 e 2017;
- Foi Diretor de Exploração dos Transportes Urbanos de Braga entre 2002 e 2013;
- Elaborou Estudos de Procura. Elaborou Projectos e implementou varias linhas de transporte urbano de passageiros;
- Responsável pelo Planeamento e Gestão de Operações;
- Coordenou a Reestruturação da Rede regular de transporte colectivo de passageiros;
- Orientou estágios profissionais e curriculares (Universidade do Minho, Faculdade de Ciências da Universidade do Porto, Faculdade Engenharia da Universidade do Porto);
- Técnico superior no Departamento de Exploração dos Transportes Urbanos de Braga entre 2000 e 2001;
- Formador na área de “ Ambiente, Higiene e Segurança ”;

Melhores linhas

Em 12 linhas os TUB transportam 59,71% dos seus passageiros.

Estes números demonstram bem a dimensão do serviço social que é prestado e a coesão territorial que os TUB conseguem fazer.

Ranking	Linha	Designação	P.T.	Peso (%)
1	95	MINHO CENTER - NOVA ARCADIA	1 041 673	8,39%
2	74	CAMÉLIAS - HOSPITAL	993 865	8,01%
3	7	S. MAMEDE D' ESTE - CELEIRÓS	809 900	6,52%
4	87	ESTAÇÃO CF - HOSPITAL	720 146	5,80%
5	2	PONTE DE PRADO - BOM JESUS	713 373	5,75%
6	90	PADIM DA GRAÇA - NOGUEIRÓ	583 854	4,70%
7	24	SEQUEIRA - GUALTAR	541 775	4,36%
8	96	HOTEL DE LAMAÇÃES - E.LECLERC	484 259	3,90%
9	43	ESTAÇÃO CF - UNIVERSIDADE DO MINHO	467 065	3,76%

Figura 10: Resultados da procura no site da TUB

Existe também *disclosure* de salários mensais do conselho de administração e os seus currículos. Tal constitui 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.

Decidiu-se ainda explorar um pouco o código fonte da página para ver se haveria mais informações que à partida estariam escondidas da vista normal do site. Encontrou-se na figura 11 que este estaria organizado da seguinte forma e que os scripts mencionados eram clicáveis sendo possível ler o que estava lá escrito.

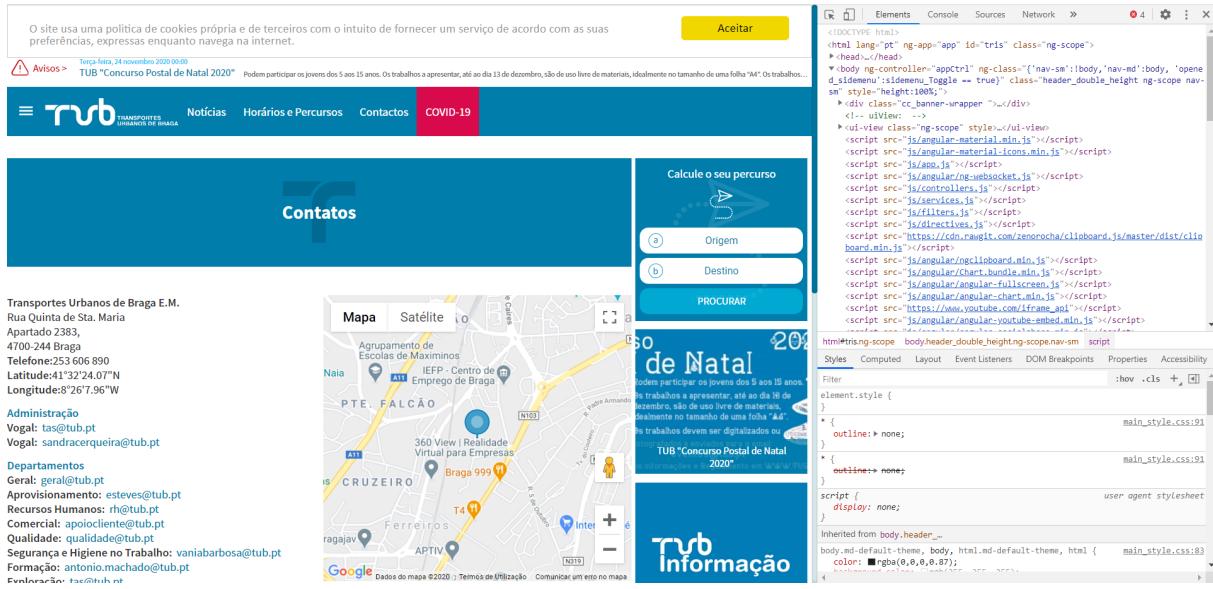


Figura 11: Código fonte do site da TUB

Exploraram-se todos os scripts, sendo a maior parte diretivas para o html e css para o bom funcionamento do site. No entanto, encontraram-se ficheiros que talvez revelem mais informação do que seria necessário. Em particular, os scripts com o nome angular/socket.js, directives.js e app.js.

No primeiro, encontra-se código relativo aos sockets, código este licenciado pelo MIT com o site <http://briantford.com> dado como referência.

```
/*
 * @license
 * angular-socket-io v0.7.0
 * (c) 2014 Brian Ford http://briantford.com
 * License: MIT
 */
```

Figura 12: Código do script angular/socket.js do site da TUB

Saber estas informações à partida não constitui uma grande ameaça, mas um atacante que consiga encontrar vulnerabilidades e código mais fraco pode conseguir tirar partido de tal.

De seguida, no script directives.js, encontra-se mais código exposto. Fez-se uma procura por alguns termos comuns nas práticas de programação, nomeadamente a palavra TODO que se refere a uma porção de código inacabada ou por melhorar. Para surpresa do grupo, encontrou-se uma zona que de facto precisaria de ser melhorada como se observa na figura 13. Encontram-se ainda comentários explicativos do código, prática que não deve ser adotada. Comentários devem ser utilizados para documentar e não para explicar porções de código.

```
if (newValue != oldValue) {
    ngModelCtrl.$setViewValue(toUser(newValue));

    // TODO avoid this causing the focus of the input to be lost..
    ngModelCtrl.$render();
}

}, true); // MUST use objectEquality (true) here, for some reason..
```

Figura 13: Pesquisa da palavra TODO no script directives.js

No script services.js, mais uma vez, este apresentava código e como no exemplo anterior, este também apresentava comentários explicativos do código. No entanto, ao analisar melhor o tipo de código, notou-se que este de certa forma estaria a definir os métodos POST, algo que na nossa opinião não deveria estar tão exposto. Os próprios comentários explicam em que tipo de estrutura os dados estão a ser guardados.

```

app.factory('subdomain', ['$location', function ($location) {
    var host = $location.host();
    if (host.indexOf('.') < 0)
        return null;
    else
        return host.split('.')[0];
}]);

app.factory('Server', ['$resource', 'API_SERVER', function($resource, API_SERVER) {
    return $resource(API_SERVER + 'core/request.php', null, {
        'c': {method: 'POST'},
        'r': {method: 'GET'},
        'u': {method: 'PUT'},
        'd': {method: 'DELETE'},
        'ra': {method: 'GET', isArray: true},
        'pdf': {
            method: 'POST',
            responseType: 'arraybuffer',
            transformResponse: function(data, headersGetter) {
                // Stores the ArrayBuffer object in a property called "data"
                return {
                    data: data
                };
            }
        },
        'pdfrotas': {
            method: 'POST',
            url: 'services/gerarhorario.php',
            responseType: 'arraybuffer',
            transformResponse: function(data, headersGetter) {
                // Stores the ArrayBuffer object in a property called "data"
                return {
                    data: data
                };
            }
        },
        'pdfmapa': {
            method: 'POST',
            url: 'services/gerarmapa.php',
            responseType: 'arraybuffer',
            transformResponse: function(data, headersGetter) {
                // Stores the ArrayBuffer object in a property called "data"
                return {
                    data: data
                };
            }
        }
    });
}]);

```

Figura 14: Código do script services.js do site da TUB

Para além disso, pesquisou-se a palavra login, numa tentativa de ver o que podia ser exposto, e este aparece várias vezes. No entanto, mais uma vez, este encontra-se no contexto do código anterior.

```

service dc = function(a, pa, m , p, payload, notoast){
    var obj = refreshinfo();
    var module = obj.module;
    var page = obj.page;
    var deferred = $q.defer();
    var json = {
        module: !m || m != undefined ? m : module,
        page: p || p != undefined ? p : page,
        action: a,
        params: pa
    };

    Server.c(json, payload, function(sucess) {
        if (notoast == false || !notoast){
            showtoastr.toaster(sucess.status, sucess.message);
        }
        deferred.resolve(sucess.result);
    }, function(error) {
        if(error.data.message == "O seu acesso expirou. Por favor autentique-se novamente."){
            $auth.logout();
            $state.go('login');
        }
        else {
            showtoastr.toaster(error.data.status, error.data.message, error.data.title);
        }
        deferred.reject(error.result);
    })
    return deferred.promise;
}

```

Figura 15: Pesquisa pela palavra login no script app.js

Por fim, no script app.js, encontrava-se ainda mais código, mas neste caso observamos a informação que já tínhamos anteriormente, um endereço IP mas neste caso diferente dos outros. Aqui este parece estar a ser associado à variável API_SOCKET indicando que talvez seja este o seu endereço.

```

app.constant('API_SERVER', '/')
app.constant('API_FACEBOOK', 'http://tub.pt/')
app.constant('API_SOCKET', '192.168.1.87:8001')
app.constant('TEMPLATE', 'TUB')

```

Figura 16: Código do script app.js do site da TUB

Mais uma vez, encontrou-se comentários TODO indicando falhas do código.

```

function convertDateStringsToDates(input) {
    // Ignore things that aren't objects.
    if (typeof input !== "object")
        return input;

    for (var key in input) {
        if (!input.hasOwnProperty(key))
            continue;

        var value = input[key];
        var match;
        // Check for string properties which look like dates.
        // TODO: Improve this regex to better match ISO 8601 date strings.
        if (typeof value === "string" && key != 'activity' && key != 'object' && (match = value.match(regexIso8601))) {
            // Assume that Date.parse can parse ISO 8601 strings, or has been shimmed in older browsers to do so.
            var milliseconds = Date.parse(match[0]);
            if (!isNaN(milliseconds)) {
                input[key] = new Date(milliseconds);
            }
        } else if (typeof value === "object" && key != 'activity' && key != 'object') {
            // Recurse into object
            convertDateStringsToDates(value);
        }
    }
}

```

Figura 17: Pesquisa no código pela palavra TODO

3.1.3 Possíveis Estratégias de Segurança

Após a análise do website e procura de informações pelo endereço do site da TUB, do ponto de vista de segurança, existem várias estratégias que podem ajudar a ocultar algumas destas informações. Serão então apresentados os problemas em questão e as respectivas estratégias para os resolver.

Numa primeira instância existem vários problemas a nível web que deveriam ser resolvidos:

- Mensagens de erro na consola da página WEB - Estes erros devem ser corrigidos de modo a não permitir solicitação de conteúdo inexistente ou acesso a informação que não se deva ter acesso.
- Código fonte público - Como observado anteriormente existe uma grande quantidade de partes de código que não deviam estar públicos ao utilizador geral, por isso é recomendado que estes sejam ocultos.
- Comentários em código fonte - Foram encontrados vários comentários que não deviam estar presentes e estes devem ser removidos.
- Informação pessoal dos órgãos sociais - A página ”contactos” do site de TUB expõe demasiada informação sobre os órgãos sociais da Tub que não deviam estar disponibilizados, era recomendado que fossem atribuídos contactos de empresa e removidos endereços e números privados ou qualquer outra informação não relevante. Para além disso, os emails administrativos e de apoio ao cliente muitas vezes tinham o nome da pessoa responsável escritos no endereço email, algo que expõe a identidade.

3.2 Corporação - Transportes Aéreos Portugueses (TAP)

A TAP Air Portugal, MHIH foi criada a 14 de março de 1945, com o nome ”Transportes Aéreos Portugueses” e é a companhia aérea de bandeira portuguesa, com sede em Lisboa e hub no Aeroporto Humberto Delgado, em Lisboa, Portugal. A companhia aérea nacional é membro integrante da Star Alliance. É detida a 72,5% pelo Estado Português, 22,5% por Humberto Pedrosa e 5% pelo grupo de trabalhadores da TAP Air Portugal.

3.2.1 Análise de Informações de Registo de Domínio

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.

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 efectuou este processo todo.

```
(kali㉿kali)-[~]
└─$ whois flytap.com
Domain Name: FLYTAP.COM
Registry Domain ID: 15730316_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2020-12-02T13:12:16Z
Creation Date: 1999-12-21T02:23:25Z
Registry Expiry Date: 2021-12-21T02:23:25Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legal@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1-09.AZURE-DNS.COM
Name Server: NS2-09.AZURE-DNS.NET
Name Server: NS3-09.AZURE-DNS.ORG
Name Server: NS4-09.AZURE-DNS.INFO
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-12-05T22:03:18Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

Figura 18: Detalhes devolvidos pelo comando whois quando aplicado ao site da TAP

```

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: flytap.com
Registry Domain ID: D17392306-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2020-12-02T14:20:21Z
Creation Date: 1999-12-21T00:00:00Z
Registrar Registration Expiration Date: 2021-12-20T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: SA TAP
Registrant Organization: Transportes Aereos Portugueses, S.A.
Registrant Street: Lisbon Airport, Street C, Bld 25
Registrant City: Lisboa
Registrant State/Province:
Registrant Postal Code: 1700-008
Registrant Country: PT
Registrant Phone: +351.218415147
Registrant Fax: +351.218415873
Registrant Email: dnsadmin@tap.pt
Registry Admin ID:
Admin Name: Fernandes Hugo
Admin Organization: TAP Air Portugal
Admin Street: Lisbon Airport, Street C, Bld 19, 3rd Floor, Room 65
Admin City: Lisbon
Admin State/Province:
Admin Postal Code: 1700-008
Admin Country: PT
Admin Phone: +351.218415952
Admin Fax: +351.218415873
Admin Email: dnsadmin@tap.pt
Registry Tech ID:
Tech Name: Fernandes Hugo
Tech Organization: TAP Air Portugal
Tech Street: Lisbon Airport, Street C, Bld 19, 3rd Floor, Room 65
Tech City: Lisbon
Tech State/Province:
Tech Postal Code: 1700-008
Tech Country: PT
Tech Phone: +351.218415952
Tech Fax: +351.218415873
Tech Email: dnsadmin@tap.pt
Name Server: ns1-09.azure-dns.com
Name Server: ns2-09.azure-dns.net
Name Server: ns3-09.azure-dns.org
Name Server: ns4-09.azure-dns.info
DNSSEC: unsigned

```

Figura 19: Detalhes devolvidos pelo comando whois quando aplicido ao site da TAP

Deste output é possível analisar e obter informações sobre os seguintes dados:

- O domínio flytap.com foi registado na data de 21/12/1999, devendo ser actualizado na data de 02/12/2020;
- Além do nome da entidade é possível obter dados de comunicação, localização da empresa, etc.
- São ainda visíveis as informações pessoais dos administradores da empresa. Desta mesma listagem é possível saber a organização responsável, neste caso, TAP Air Portugal.

Além destas informações é possível ainda extrair 4 Name Servers da empresa juntamente com o tipo de endereço aos quais estão alocados. 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 efectivamente alojado.

Outro método de consulta WHOIS é através do website **whois.domaintools.com** que, pesquisando pelo site da TAP são obtidas outras informações como por exemplo ASN isto é, uma *Autonomous System Number*.

Whois Record for FlyTap.com

— Domain Profile

Registrant	SA TAP
Registrant Org	Transportes Aereos Portugueses, S.A.
Registrant Country	pt
Registrar	Eurodns S.A. EuroDNS S.A. IANA ID: 1052 URL: http://www.eurodns.com , http://www.EuroDNS.com Whois Server: whois.eurodns.com legalservices@eurodns.com (p) 35227220150
Registrar Status	clientTransferProhibited
Dates	7,657 days old Created on 1999-12-20 Expires on 2021-12-19 Updated on 2020-12-02
Name Servers	NS1-09.AZURE-DNS.COM (has 312,658 domains) NS2-09.AZURE-DNS.NET (has 573 domains) NS3-09.AZURE-DNS.ORG (has 375 domains) NS4-09.AZURE-DNS.INFO (has 447 domains)
Tech Contact	Fernandes Hugo TAP Air Portugal Lisbon Airport, Street C, Bld 19, 3rd Floor, Room 65, Lisbon, 1700-008, pt dnsadmin@tap.pt (p) 351218415952 (f) 351218415873
IP Address	104.99.81.247 - 2 other sites hosted on this server
IP Location	 - Washington - Seattle - Akamai Technologies Inc.
ASN	 AS16625 AKAMAI-AS, US (registered May 30, 2000)
Domain Status	Registered And Active Website
IP History	86 changes on 86 unique IP addresses over 15 years
Registrar History	4 registrars with 2 drops
Hosting History	6 changes on 6 unique name servers over 14 years

— Website

Website Title	 500 SSL negotiation failed:
Response Code	500

[Whois Record](#) (last updated on 2020-12-06)

Figura 20: Detalhes devolvidos pelo site whois.detailtools.com quando aplicado ao site da TAP

Neste caso, o AS tem base nos Estados Unidos da América, em Washington, Seattle com o ASN 16625 (público).

• Detalhes sobre o endereço IP do domínio flytap.com

Existem vários métodos para a procura de informações sobre um determinado endereço:

- **Host** - Através do comando *host* do *website* é possível obter os seguintes detalhes:

```
(kali㉿kali)-[~]
$ host flytap.com
flytap.com has address 91.198.90.68
flytap.com mail is handled by 10 mx3.tap.pt.
flytap.com mail is handled by 10 mx2.tap.pt.
```

Figura 21: Detalhes devolvidos pelo comando host quando aplicado ao site da TAP

Passamos então a ter o conhecimento que o endereço do site da TAP é 91.198.90.68.

- **nslookup** - Este comando devolve também informações semelhantes ao comando *host*:

```
(kali㉿kali)-[~]
$ nslookup flytap.com
Server:          192.168.8.1
Address:         192.168.8.1#53

Non-authoritative answer:
Name:   flytap.com
Address: 91.198.90.68
```

Figura 22: Detalhes devolvidos pelo comando nslookup quando aplicado ao site da TAP

Nota

É também pertinente ter em consideração de uma situação que ocorreu aquando da procura de detalhes dos endereços da TAP. Devido à utilização do comando nslookup, neste endereço gerou-se uma situação de "quarentena" do IP de onde foi feito o comando, ou seja, qualquer dispositivo que estivesse a usar a rede onde foi feito o comando foi totalmente bloqueado de aceder ao site da TAP. Esta situação pode ser considerada um mecanismo de defesa da empresa para que não existam ataques o que demonstra mecanismos de defesa mais rígidos do que no site da TUB visto que esta situação não se demonstrou.

- **dig** : através do comando dig observamos os 4 name servers (indicados pela flag NS) assim como uma secção adicional sobre 3 dos próprios name servers incluindo os seus endereços.

```
(kali㉿kali)-[~]
$ dig flytap.com

; <>> DiG 9.16.8-Debian <><> flytap.com
; global options: +cmd
; Got answer:
;-->HEADER<-- opcode: QUERY, status: NOERROR, id: 54225
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6

;; QUESTION SECTION:
;flytap.com.           IN      A

;; ANSWER SECTION:
flytap.com.        3209    IN      A      91.198.90.68

;; AUTHORITY SECTION:
flytap.com.        102118   IN      NS     ns4-09.azure-dns.info.
flytap.com.        102118   IN      NS     ns1-09.azure-dns.com.
flytap.com.        102118   IN      NS     ns2-09.azure-dns.net.
flytap.com.        102118   IN      NS     ns3-09.azure-dns.org.

;; ADDITIONAL SECTION:
ns2-09.azure-dns.net. 3335    IN      A      64.4.48.9
ns2-09.azure-dns.net. 3335    IN      AAAA   2620:1ec:8ec::9
ns3-09.azure-dns.org. 137     IN      A      13.107.24.9
ns3-09.azure-dns.org. 137     IN      AAAA   2a01:111:4000 :: 9
ns4-09.azure-dns.info. 3145    IN      A      13.107.160.9
ns4-09.azure-dns.info. 3145    IN      AAAA   2620:1ec:bda::9

;; Query time: 4 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Sun Dec 06 17:34:24 EST 2020
;; MSG SIZE rcvd: 310
```

Figura 23: Detalhes devolvidos pelo comando dig quando aplicado ao site da TAP

3.2.2 Análise da Página WEB/Procura de Informações Online

De uma maneira semelhante à da empresa anterior foi feita uma pesquisa no *website* da TAP. No entanto, existe um grande constante na quantidade de informação disponível entre as duas empresas. Enquanto que na TUB existiam todo o tipo de informações relativas às pessoas que lá trabalhavam. salário, despesas da empresa, estatísticas etc, no caso da TAP a informação disponível que possa ser considerada útil no possível ataque é quase nula, visto que as poucas páginas adicionais que existem reduzem a sua informação ao mínimo e são utilizados links de apoio por outras redes sociais para prestar contactos:

Contactos

Estamos sempre aqui para o ajudar. Consulte as várias formas de falar connosco.

Fale Connosco

Envie-nos sugestões, elogios ou reclamações. Diga-nos o que podemos fazer para assegurar a melhor experiência de viagem.

[Contacte-nos](#)



Suporte online

Facebook	>
Twitter	>
Skype	>

Telefone

(+351) 211 234 400 >

De 2º a domingo: Das 8h às 24h (WET), hora de Portugal continental

Outros contactos

 TAP Miles&Go  Sede TAP  Corporate  Dept. de Grupos  Carga  Comunicação Corporativa

Contactos **Escreva-nos**

+351 218 415 000

Aeroporto de Lisboa
1704-801 Lisboa
Portugal

Figura 24: Página ”contactos” do website da TAP

No entanto, neste site existe um link que redireciona para um outro *website* que contém as informações sobre a empresa <https://www.tapairportugal.com/pt>. Este tem como objetivo representar a empresa na sua estrutura e composição ao contrário do anterior que visa como campanha publicitária e método de venda de voos a clientes.

Após uma pesquisa neste segundo *website* a quantidade de informação agora encontrada é de quantia significativa e semelhante à da TUB. Foram encontrados os órgãos sociais, relatórios de contas, Atas de assembleias gerais, novos meios de contacto da TAP e outros visíveis a seguir:

TAP, SGPS, S.A.	Assembleia Geral	TAP, S.A.	Portugália
-----------------	------------------	-----------	------------

TAP, SGPS, S.A. - Conselho de Administração



Miguel Frasquilho
PRESIDENTE

Miguel Jorge Reis Antunes Frasquilho (Portugal, 1965) é licenciado em Economia e mestre em Teoria Económica. Com um percurso profissional ligado aos sectores financeiro e académico, é atualmente docente na Universidade Católica Portuguesa.
[Descarregar CV](#)



Ramiro Sequeira
PRESIDENTE DA COMISSÃO EXECUTIVA

Ramiro Sequeira (Portugal, 1981) tem formação em Gestão e diversas certificações Aeronáuticas. O seu percurso profissional está desde sempre ligado ao setor da aviação, contando com mais de 13 anos de experiência internacional em funções de gestão de áreas operacionais, designadamente no grupo IAG.
[Descarregar CV](#)



Alexandra Reis
VOGAL DA COMISSÃO EXECUTIVA

Alexandra Reis (Portugal, 1974), licenciada em Engenharia Eletrónica e Telecomunicações e Executive MBA, tem desempenhado funções de gestão em empresas com um forte cunho tecnológico e operacional, nos setores das Telecomunicações, Energia e Aviação, como por exemplo a Netjets.
[Descarregar CV](#)



Raffael Quintas
VOGAL DA COMISSÃO EXECUTIVA

Raffael Guarita Quintas Alves é formado em Administração de Empresas. O seu percurso profissional está ligado à consultoria, finanças e aviação, tendo desempenhado várias funções na Azul Linhas Aéreas.
[Descarregar CV](#)

Figura 25: Página ”Administração” do website da TAPAirPortugal

PRINCIPAIS ELEMENTOS CURRICULARES E ATIVIDADES PROFISSIONAIS EXERCIDAS

Miguel Frasquilho

Nacionalidade: Portuguesa | Data de nascimento: novembro 1965

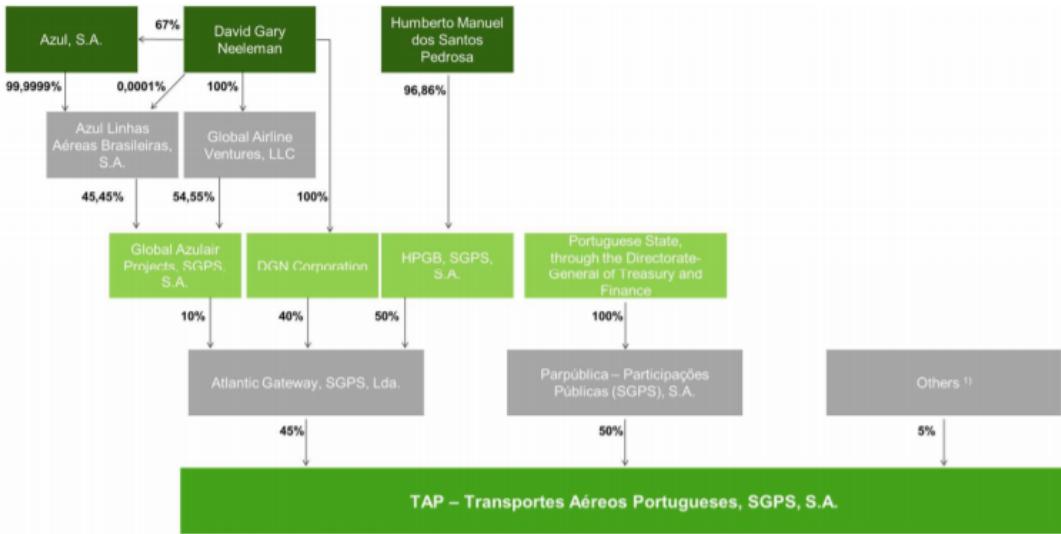
Nomeado Presidente do Conselho da Administração da TAP – Transportes Aéreos Portugueses, SGPS, S.A. em junho de 2017.

Atividade Profissional: Docente na Universidade Católica Portuguesa desde junho 2017 | Presidente do Conselho de Administração da aicep Portugal Global (Agência para o Investimento e o Comércio Externo de Portugal) entre abril de 2014 e abril de 2017 | Deputado à Assembleia da República pelo Partido Social Democrata entre 9 de abril de 2003 e 24 de abril de 2014, tendo sido Vice-Presidente do Grupo Parlamentar do PSD (março 2004 - outubro 2007; outubro 2009 - abril 2014), Presidente da Comissão Parlamentar Permanente de Obras Públicas, Transportes e Comunicações (outubro 2007 - outubro 2009) e Vice-Presidente da Comissão Parlamentar de Acompanhamento das Medidas do Programa de Assistência Financeira a Portugal (junho 2011 - abril de 2014) | Diretor-Coordenador do Departamento Espírito Santo Research (julho 2003 - abril 2014), coordenando o research do Grupo Banco Espírito Santo | Membro da Comissão de Reforma do IRC, cujos trabalhos decorreram entre janeiro e julho de 2013 | Secretário de Estado do Tesouro e das Finanças do XV Governo Constitucional (abril 2002 - abril 2003) | Deputado à Assembleia da República pelo Partido Social Democrata no distrito de Setúbal, como cabeça de lista (março 2002) | Economista Chefe do Grupo Banco Espírito Santo (janeiro 2002 - abril 2002) | Economista Chefe do BES em janeiro de 1998, na sequência do seu ingresso no Banco Espírito Santo como Economista em setembro de 1996 | Docente na Universidade Católica Portuguesa (Faculdade de Ciências Económicas e Empresariais, 1990-2002), no Instituto Superior das Ciências do Trabalho e da Empresa (Centro de Investigação de Mercados e Ativos Financeiros, 1999-2000) e na Universidade Nova de Lisboa (Faculdade de Economia, 1988-1990), tendo lecionado Estatística, Econometria, Matemática, Introdução à Economia, Macroeconomia, Economia Internacional, Economia Industrial, Contas Nacionais e Análise de Ciclos Económicos | Assessor do Gabinete do Secretário de Estado do Comércio no XII Governo Constitucional (1994-1995) | Economista no Conselho Económico e Social (1992-1994) | Economista na empresa FISECO - Serviços Financeiros S.A. (1991-1992).

Outras Atividades: Co-autor do livro “Portugal Agora”, que contém textos de outros 16 autores, sob coordenação de Carlos Sezões e publicado em maio de 2017 | Autor do livro “As Raízes do Mal, a Troika

Figura 26: Currículo do Presidente da empresa

Estrutura Acionista da TAP SGPS



1) Em 10 de abril de 2017, foi lançada uma oferta pública de venda de ações da TAP SGPS reservada a trabalhadores do Grupo TAP (TAP SGPS e outras sociedades do Grupo TAP), no âmbito do processo de reprivatização indireta do capital social da TAP, de acordo com o disposto na Resolução do Conselho de Ministros n.º 42-A/2017, de 23 de março de 2017, na sequência da qual trabalhadores do Grupo TAP adquiriram um total de 75.000 ações representativas de 5% do capital social e dos direitos de voto da TAP SGPS, tendo já parte dessas ações sido alienada a favor de terceiros.

Figura 27: Estruturação das ações da TAP presente no relatório de contas de 2019

2. PRINCIPAIS INDICADORES

Grupo TAP	2019	2018 ⁽¹⁾	Variação		Performance Económico-Financeira
			Abs.	%	
Passageiros ('000)	17.052	15.763	1.289	+8,2%	
RPK (milhões)	42.065	38.048	4.017	+10,6%	
ASK (milhões)	52.527	47.000	5.527	+11,8%	
Load Factor	80,1%	81,0%	-0,9p.p.	-1,1%	
Frota Operacional (Final do período) ⁽²⁾	105	93	12	+12,9%	
Block Hours	409.522	390.544	18.977	+4,9%	
Número de Partidas	136.705	134.718	1.987	+1,5%	
Baga média (km)	1.956	1.874	82	+4,4%	
Yield (€ centavos) ⁽³⁾	6,85	7,08	-0,23	-3,2%	
PRASK (€ centavos) ⁽³⁾	5,49	5,73	-0,24	-4,3%	
CASK (€ centavos) ⁽³⁾	6,19	6,79	-0,60	-8,8%	
CASK ex-fuel ⁽³⁾ (€ centavos)	4,70	5,14	-0,44	-8,6%	
CASK fuel ⁽³⁾ (€ centavos)	1,49	1,64	-0,16	-9,6%	
Pontualidade até 15'	63,9%	58,4%	+5,5p.p.	+9,3%	
Regularidade	99,2%	98,2%	+1,0p.p.	+1,0%	
Quadro do Pessoal Ativo total (Final do período) ⁽⁴⁾	10.952	10.363	589	+5,7%	
Pessoal Ativo - TAP SA	9.006	8.145	861	+10,6%	
Pessoal Ativo - TAP ME Brasil	559	742	-183	-24,7%	
Pessoal Ativo - Outras Empresas	1.387	1.476	-89	-6,0%	
Rendimentos Operacionais (milhões €)	3.345,1	3.250,8	94	+2,9%	
Rendimentos de Passageiros (milhões €)	2.913,9	2.782,3	131,6	+4,7%	
EBITDA (milhões €) ⁽⁵⁾	477,3	211,4	265,9	+125,8%	
Margem EBITDA	14,3%	6,5%	+7,8p.p.	+118,8%	
Resultado Operacional (EBIT) (milhões €)	58,6	-44,0	102,6	s.s.	
Margem EBIT	1,8%	-1,4%	+3,1p.p.	+23,5%	
Resultado líquido atribuível aos acionistas da TAP SGPS (milhões €)	-105,6	-118,0	12,4	s.s.	
Resultado líquido das Empresas do Grupo (milhões €) ⁽⁶⁾	-95,6	-58,1	-37,6	n.m.	
Resultado Líquido TAP, S.A.	5,8	6,0	-0,2	-3,7%	
Resultado Líquido SRH	1,7	1,8	-0,2	-8,2%	
Resultado Líquido TAP/GER	7,1	1,1	6,0	n.m.	
Resultado Líquido Portugal	-14,7	-51,6	36,9	n.m.	
Resultado Líquido Aeropar & TAP ME Brasil					
Performance Económico-Financeira					
Grupo TAP	2019	2018 ⁽¹⁾	Variação		
	EUR milhões		Abs.	%	
Rendimentos operacionais	3.345,1	3.250,8	94,3	+2,9%	
Passagem	2.913,9	2.782,3	131,6	+4,7%	
Mantenção	234,3	280,7	-46,4	-16,5%	
Carga e Correio	137,4	134,7	2,7	+2,0%	
Ganhos e perdas em associadas	1,7	3,7	-2,1	-54,9%	
Outros rendimentos	57,9	49,4	8,5	+17,1%	
Gastos operacionais	3.286,5	3.294,8	-8,3	-0,3%	
Combustível para aeronaves	789,7	798,6	-8,9	-1,1%	
Custos Operacionais de Tráfego	743,2	777,8	-34,6	-4,4%	
Custos com o Pessoal	751,9	702,8	49,1	+7,0%	
Rendas de aeronaves	0,0	177,9	-177,9	s.a.	
Gastos com manutenção de aeronaves	60,8	111,7	-50,9	-45,6%	
Custo dos materiais consumidos	185,2	207,4	-22,2	-10,7%	
Custos comerciais, marketing e comunicação	153,1	186,6	-33,5	-18,0%	
Imparidade de contas a receber, inventários e Provisões	-2,5	9,6	-12,1	s.a.	
Outros gastos	179,7	170,1	9,6	+5,6%	
Reestruturação	6,0	54,5	-48,5	-89,0%	
Outros itens não recorrentes	0,7	20,3	-19,6	-96,6%	
Depreciações, amortizações e perdas por imparidez	418,7	77,5	341,2	+440,2%	
EBIT (Resultado Operacional)	58,6	-44,0	102,6	s.s.	
Margem EBIT	1,8%	-1,4%	+3,1p.p.		
Juros e rendimentos similares obidos	3,2	6,0	-2,8	-46,1%	
Juros e gastos similares suportados	-178,3	-57,9	-120,4	+208,0%	
Diferenças de câmbio líquidas	-22,9	-49,4	26,5	-53,6%	
Resultado antes de Impostos	-139,3	-145,3	6,0	s.a.	
Imposto sobre o rendimento	34,1	28,0	6,1	s.a.	
Resultado líquido do período	-105,2	-117,2	12,0	s.a.	
Resultado líquido atribuível aos acionistas da TAP SGPS	-105,6	-118,0	12,4	s.a.	
EBITDA⁽⁷⁾	477,3	211,4	265,9	+125,8%	
Margem EBITDA	14,3%	6,5%	+7,8p.p.		

Figura 28: Dados económicos da empresa presentes no relatório de contas de 2019.

24 – Rendimentos e ganhos operacionais

Os Rendimentos e ganhos operacionais incorridos durante 2019 e 2018 foram como segue:

	2019				
	Passagens	Mantenção	Carga e Correio	Outros	Total
Receita					
Vendas	-	11.894	-	10.922	22.816
Serviços prestados	2.913.870	222.375	137.393	14.720	3.286.358
Outros rendimentos	-	-	-	32.253	32.253
	2.913.870	234.269	137.393	57.895	3.343.427
	2018				
	Passagens	Mantenção	Carga e Correio	Outros	Total
Receita					
Vendas	-	18.483	-	8.851	27.334
Serviços prestados	2.782.292	262.211	134.684	15.892	3.195.079
Outros rendimentos	-	-	-	24.676	24.676
	2.782.292	280.694	134.684	49.419	3.247.089

Posição Financeira

Grupo TAP	31-dez 2019	1-jan 2019 ⁱⁱ	31-dez 2018 ⁱⁱ
EUR milhões			
Total do Ativo	4.449,8	2.636,6	1.627,5
Ativo Não Corrente	3.381,2	1.904,2	895,1
Ativo Corrente	1.068,5	732,4	732,4
Capital Próprio	-560,8	-507,3	-617,9
Total do Passivo	5.030,6	3.143,9	2.245,4
Passivo Não Corrente	3.340,5	1.622,8	902,1
Passivo Corrente	1.690,0	1.521,1	1.343,3

Financiamentos e Passivos de Locação

Grupo TAP	31-dez 2019	1-jan 2019 ⁱⁱ	31-dez 2018 ⁱⁱ
Divida Financeira ⁱⁱⁱ	1.479,6	888,5	888,5
Emprestimos bancários	401,2	645,8	645,8
Passivos de locação com opção de compra	275,3	132,5	132,5
Empréstimos obrigacionistas	684,3	0,0	0,0
Obrigações Convertíveis	118,8	110,2	110,2
Caixa e equivalentes	435,0	233,2	233,2
Divida Líquida Financeira	1.044,6	655,2	655,2
Passivos de locação sem opção de compra	2.095,7	924,0	0,0

Figura 29: Posição financeira, financiamentos e rendimentos da empresa.

Valores em milhares de Euros	31-dez-18	Impacto da adoção da IFRS 16	01-jan-19
ATIVO			
Ativo não corrente			
Ativos fixos tangíveis	542.551	939.992	1.482.543
Propriedades de investimento	3.228	-	3.228
Goodwill	127.542	-	127.542
Ativos intangíveis	11.323	-	11.323
Participações financeiras	3.322	-	3.322
Outros ativos financeiros	846	-	846
Ativos por impostos diferidos	100.325	-	100.325
Outras contas a receber	105.937	69.117	175.054
	895.074	1.009.109	1.904.183
Ativo corrente			
Inventários	91.152	-	91.152
Outras contas a receber	321.414	-	321.414
Imposto sobre o rendimento a receber	8.464	-	8.464
Outros ativos correntes	64.976	-	64.976
Outros ativos financeiros	13.225	-	13.225
Caixa e seus equivalentes	233.204	-	233.204
	732.435	-	732.435
Total do ativo	1.627.509	1.009.109	2.636.618
CAPITAL PRÓPRIO E PASSIVO			
Capital próprio			
Capital	15.000	-	15.000
Prestações suplementares	224.093	-	224.093
Ouros Instrumentos de capital próprio	36.297	-	36.297
Reservas legais	3.000	-	3.000
Reservas de conversão cambial	(74.495)	-	(74.495)
Reservas de justo valor	(29.132)	-	(29.132)
Ajustamentos em partes de capital	(2.260)	-	(2.260)
Resultados transitados	(670.874)	110.557	(560.317)
Resultado líquido do exercício	(118.039)	-	(118.039)
Total do capital próprio do grupo	(616.410)	110.557	(505.853)
Interesses não controlados	(1.449)	-	(1.449)
Total do capital próprio	(617.859)	110.557	(507.302)
Passivo não corrente			
Provisões	22.381	32.176	54.557
Passivos remunerados	597.054	(102.010)	495.044
Passivo locação com opção de compra	-	102.010	102.010
Empréstimo obrigacionista	110.161	-	110.161
Passivo locação sem opção de compra	-	692.002	692.002
Pensões e outros benefícios pós-emprego	103.523	-	103.523
Passivos por impostos diferidos	19.024	46.261	65.285
Outras contas a pagar	49.960	(49.741)	219
	902.103	720.698	1.622.801
Passivo corrente			
Passivos remunerados	181.236	(30.474)	150.762
Passivo locação com opção de compra	-	30.474	30.474
Passivo locação sem opção de compra	-	232.018	232.018
Outras contas a pagar	665.619	(54.164)	611.455
Imposto sobre o rendimento a pagar	19	-	19
Documentos pendentes de voo	393.466	-	393.466
Outros passivos correntes	102.925	-	102.925
	1.343.265	177.854	1.521.119
Total do passivo	2.245.368	898.552	3.143.920
Total do capital próprio e do passivo	1.627.509	1.009.109	2.636.618

Figura 30: Capital da empresa

Assembleia Geral Anual da TAP, SGPS, S.A. – 30 de junho de 2020: [Convocatória \(PDF 0.15MB, PT\)](#)
Durante os 15 dias anteriores à data da realização da Assembleia, estão disponíveis para consulta de todos os Acionistas, neste sítio da internet, os elementos e informações preparatórios da Assembleia Geral, nos termos e para os efeitos do disposto no Artº 289º do Código das Sociedades Comerciais.

- [TAP SGPS Boletim Voto Assembleia Geral de 30 de junho 2020 \(PDF, 0.13 MB, PT\)](#)
 - [TAP SGPS Modelo de Carta de Representação Pessoas Coletivas Assembleia Geral 30 de junho 2020 \(PDF, 0.24 MB, PT\)](#)
 - [TAP SGPS Modelo de Carta de Representação Pessoas Singulares Assembleia Geral 30 de junho 2020 \(PDF, 0.24 MB, PT\)](#)
 - [Informações Preparatórias da Assembleia Geral 30 de junho 2020 \(PDF, 0.24 MB, PT\)](#)
 - [Proposta CA TAP SGPS Deliberação Ponto Dois da OT - AG de 30 de julho 2020 \(PDF, 0.12 MB, PT\)](#)
 - [Proposta CA TAP SGPS Deliberação Ponto Três da OT - AG de 30 de julho 2020 \(PDF, 0.11 MB, PT\)](#)
 - [Proposta CA TAP SGPS Deliberação Ponto Quatro Art 35 OT - AG de 30 de julho 2020 \(PDF, 0.13 MB, PT\)](#)
 - [Proposta CA TAP SGPS Deliberação Ponto Cinco OT - AG de 30 de julho 2020 \(PDF, 0.10 MB, PT\)](#)
 - [Proposta CA TAP SGPS Deliberação Ponto Seis da OT - AG de 30 de julho 2020 \(PDF, 0.11 MB, PT\)](#)
-

Figura 31: Atas públicas da empresa

Contactos

Encontre aqui o serviço ou departamento da TAP com o qual pretende entrar em contacto.

Sede TAP	Recrutamento TAP	Apoio ao Cliente TAP
+351 218 415 000	Consulte as oportunidades e candidate-se em Recrutamento TAP .	(+351) 211 234 400
Aeroporto de Lisboa 1704-801 Lisboa Portugal		
Comunicação Corporativa	Comunicação e RP / Media	Marketing
+351 218 416 882	corpcom@tap.pt	marketing@tap.pt

Figura 32: Página ”contactos” deste website

Como é observável, existem todo um tipo de informações expostas a público sobre a empresa e os seus órgãos sociais, no entanto em contraste com a TUB, em momento algum foi encontrado contactos, moradas ou qualquer tipo de informação do género sobre a equipa administrativa ou os órgãos sociais. No entanto, ao contrário da TUB, os endereços de email ao apoio ao cliente e administrativos não discriminavam o nome da pessoa responsável por atender a esses pedidos. Algo que protege não só a empresa como os próprios trabalhadores.

Foi ainda encontrado outro *website* pertencente à TAP com o objectivo de recrutamento. No entanto como esta não apresentava qualquer informação devido à inexistência de vagas, através da plataforma *WayBackMachine* é possível navegar por datas nas quais o recrutamento se encontre numa fase aberta:

The screenshot shows a search interface with fields for 'Procurar palavra-chave' and 'Procurar localização', both empty. A green 'Procurar' button is at the bottom right. Below the search bar, there's a section to 'Enviar alertas a cada 7 dias' (Send alerts every 7 days) with a 'Criar alerta' (Create alert) button. The results section shows 5 items:

Título	Localização	Data de Publicação ▼
Curso de Formação - Técnico de Manutenção de Aeronaves	Portugal/Lisboa	22/Oct/2019
Digital Marketing	Portugal/Lisboa	21/Oct/2019
Assistente de Escala e Serviço ao Cliente	Portugal/Lisboa	16/Oct/2019
Assistente de Contact Center	Portugal/Lisboa	30/Set/2019
Técnico de Manutenção de Aeronaves (Ref 2609ME)	Portugal/Lisboa	26/Set/2019

Resultados 1 – 5 de 5

Título	Localização	Data de Publicação ▼
Curso de Formação - Técnico de Manutenção de Aeronaves	Portugal/Lisboa	22/Oct/2019
Digital Marketing	Portugal/Lisboa	21/Oct/2019
Assistente de Escala e Serviço ao Cliente	Portugal/Lisboa	16/Oct/2019
Assistente de Contact Center	Portugal/Lisboa	30/Set/2019
Técnico de Manutenção de Aeronaves (Ref 2609ME)	Portugal/Lisboa	26/Set/2019

Figura 33: Candidaturas disponíveis em Outubro de 2019

Esta situação pode tornar-se muito útil visto que dependendo das propostas de emprego, nas descrições da mesma podem estar incluídas informações da empresa que possa ser útil a um possível ataque.

Analizando o código fonte do site da TAP, este não revela quase nada em comparação com o da TUB. Neste caso, só temos indicações do html e css que dificilmente serão alvo de exploração por parte de um atacante.

The screenshot shows the TAP Portugal website's contact page (tapairportugal.com/pt/contactos). The page includes sections for 'Sede TAP', 'Recrutamento TAP', 'Apóio ao Cliente TAP', 'Comunicação Corporativa', 'Comunicação e RP / Media', and 'Marketing'. The developer tools' Elements tab is open, displaying the HTML structure of the page, including header elements like 'site-header multi-menu', 'site-content', and 'page-area', as well as footer elements and various scripts and styles.

Figura 34: Código Fonte do site da TAP

3.2.3 Possíveis Estratégias de Segurança

Consoante a empresa em estudo, foi feita uma análise de problemas existentes após a pesquisa passiva de vulnerabilidades. Para estes problemas serão apresentados algumas estratégias que visam a correcção e fortificação destas fraquezas. É importante salientar que a nível de FrontEnd e informações WEB existe

uma maior segurança de informação do que no site da TUB daí que algumas estratégias apresentadas na empresa anterior já são consideradas como implementadas.

- Mensagens de erro na consola a nível WEB - Numa análise à consola presente no site da TAP, existem vários erros que se encontram por resolver. Estes devem ser tratados para não criarem aberturas na segurança.

3.3 Conclusões - Parte 1

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. Foi ainda apresentada as varias vulnerabilidades ao nível do código existente.

Quando comparamos esta empresa com a outra analisada, a TAP, observamos uma diferença muito visível a nível da segurança, visto que a TAP tem as suas informações mais restritas e não apresenta vulnerabilidades a nível de código visível o que permite que seja concluído que a TAP tem uma maior segurança da sua informação relativamente à TUB.

Assim, devido aos 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 protecção na divulgação futura.

4 Parte 2 - Scanning

4.1 Contextualização

A ideia base desta parte B do trabalho prático passa por agrupar toda a aprendizagem obtida até então, na tentativa de compreender a importância da mesma na globalidade da segurança da informação.

Na parte anterior sobre colecta Passiva de Informações, pela análise de detalhes divulgados publicamente, vendo até que ponto isso poderia ser útil para um possível início de ataque e terminamos agora na forma mais forte ou agressiva de executar/estudar uma invasão com a colecta activa de Informações.

Esta colecta activa de Informações distingue-se do restante, na medida em que envolve o “contacto” directo com o alvo em causa, algo que vamos comprovar no desenvolver deste relatório.

Para esta coleta de informações foram utilizados ambientes proprios para o efecto contituídos por um sistema alvo, o Sistema Metasploitable 3, e um sistema Auditor com ferramentas necessárias para o efecto.

Ao longo deste relatório serão utilizadas algumas ferramentas bastante conhecidas:

- **NMAP** - Esta ferramente (Network Mapper) explora a rede determinando hosts disponíveis, serviços existentes entre outros.
- **Snort e Nessus** - Ambas as ferramentas permitem obter vulnerabilidades do sistema atacado.
- **Wireshark** - Permite estudar os pacotes que circulam pela rede no decorrer dos scans.

4.2 NMAP

Através de um ambiente de testes devidamente preparado, pretende-se efectuar um scanning activo através de uma Máquina Virtual Kali Linux tendo como alvo de scan a Máquina Virtual Metasploitable 3.

Foi optado por utilizar a ferramenta NMAP visto que o objectivo da questão actual é identificar e detalhar vulnerabilidades e fraquezas para as quais o Sistema Metasploitable 3 está exposto.

4.2.1 Questão 1

Numa primeira instância foi feito uma procura através da ferramenta NMAP que possui várias variantes de procura. Foi optado por fazer vários scans através do NMAP com diferentes flag para além do scan que efectua a pesquisa de serviços, isto porque para além dos serviços, através de outras flags é possível obter outras informações pertinentes sobre o sistema alvo. Os scans efectuados foram os seguintes:

- **nmap -sS (TCP SYN scan)**

Um scan do SYN é a opção de scan padrão e mais popular no que se trata de scan NMAP, isto porque pode ser executado rapidamente, percorrendo milhares de portas por segundo numa rede rápida e não é prejudicado por firewalls mais restritivos. Também é relativamente discreto e furtivo, pois nunca completa as conexões TCP.

Esta técnica costuma ser chamada de scan semi-aberto, porque não abre uma conexão TCP completa. É simplesmente enviado um pacote SYN, como se fosse abrir uma conexão real e então espera por uma resposta. Um sinal em resposta do tipo SYN / ACK indica que a porta está à escuta (aberta), enquanto que um RST é indicativo de que não está à escuta.

Quando foi efectuado este scan no Metasploitable foram obtidos os seguintes resultados remetentes a portas do Metasploitable que se encontram abertas e por isso vulneráveis:

```
└─(kali㉿kali)-[~]
$ sudo nmap -sS 172.20.4.2
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:19 EST
Nmap scan report for 172.20.4.2
Host is up (0.00060s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.00 seconds
```

Figura 35: Output do scan -sS

- **nmap -sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)**

Estes três tipos de scan exploram uma vulnerabilidade subtil no RFC TCP para diferenciar entre portas abertas e fechadas. Geralmente funciona deste modo: “se o estado da porta [destino] estiver FECHADO ... um segmento de resposta que não contenha um RST faz com que um RST seja enviado em resposta.”.

Ao fazer scan de sistemas compatíveis com este texto RFC, qualquer pacote que não contenha bits SYN, RST ou ACK resultará num retorno de RST se a porta estiver fechada e nenhuma resposta se a porta estiver aberta. Desde que nenhum desses três bits esteja incluído, qualquer combinação dos outros três (FIN, PSH e URG) é o suficiente. O Nmap explora isto com três tipos de scan:

- **Null scan (-sN)** - Não define nenhum bit (a flag cabeçalho do TCP é 0)
- **FIN Scan (-sF)** - Define apenas o bit FIN.
- **Xmas scan (-sX)** - Define as flags FIN, PSH e URG, iluminando o pacote como uma árvore de Natal.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sN 172.20.4.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:23 EST
Nmap scan report for 172.20.4.2
Host is up (0.00081s latency).
All 1000 scanned ports on 172.20.4.2 are closed
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.94 seconds

(kali㉿kali)-[~]
└─$ sudo nmap -sF 172.20.4.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:21 EST
Nmap scan report for 172.20.4.2
Host is up (0.00088s latency).
All 1000 scanned ports on 172.20.4.2 are closed
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds

(kali㉿kali)-[~]
└─$ sudo nmap -sX 172.20.4.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:24 EST
Nmap scan report for 172.20.4.2
Host is up (0.00044s latency).
All 1000 scanned ports on 172.20.4.2 are closed
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.13 seconds
```

Figura 36: Output do scan -sN , -sF, -sX respetivamente.

No modo padrão de scan, o NMap executa dois tipos de scan:

- Scan de Host – determinação dos hosts disponíveis;
- Scan de Porta – divulgação do estado das portas nos hosts disponíveis

Ao executarmos estes modos de scan, estamos apenas a realizar uma scan de hosts, extraíndo unicamente as informações relativas aos hosts disponíveis que deram resposta ao teste da descoberta do scan efectuado. Basicamente, é o mesmo que fazer ping, confirmando a existência de hosts e os seus respectivos endereços MAC, sem que sejam reveladas as suas portas.

Neste exercício em específico, verifica-se que o resultado do scan para o target 172.20.4.2 (Máquina Virtual Metasploitable 3) devolve o endereço MAC desta mesma máquina.

A principal vantagem destes tipos de scan é que eles podem passar furtivamente por certos firewalls e routers de filtragem de pacotes. Outra vantagem é que esses tipos de scan são um pouco mais furtivos do que até mesmo um scan SYN. No entanto, este caso requer algum cuidado visto a maioria dos produtos IDS modernos poderem ser configurados para os detectar.

• **nmap -sA (TCP ACK scan)**

Este tipo de scan é diferente dos anteriores, pois não determina quais as portas abertas (abertas — filtradas). É usado para mapear conjuntos de regras de firewall, determinando se estas têm estado ou não e quais portas são filtradas. Resultados:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sA 172.20.4.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:20 EST
Nmap scan report for 172.20.4.2
Host is up (0.00060s latency).
All 1000 scanned ports on 172.20.4.2 are unfiltered
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.71 seconds
```

Figura 37: Output do scan -sA

- **nmap -O - Identificação do Sistema Operativo**

Neste caso o nmap não conseguiu dizer com certeza que sistema operativo está a ser usado mas tentou adivinhar algumas hipóteses sendo estas todas versões de Windows, as quais as mais prováveis são o Windows 7 ou 10, no entanto podemos observar que o sistema operativo do Metasploitable se encontra na lista obtida de possíveis sistemas operativos do alvo com 95% de confiança.

```
(kali㉿kali)-[~]
└─$ sudo nmap -O 172.20.4.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 15:25 EST
Nmap scan report for 172.20.4.2
Host is up (0.0011s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 08:00:27:78:89:96 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 7 SP1 (99%), Microsoft Windows 10 1511 (97%), Microsoft Windows 7 SP 0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (97%), Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows 8 (96%), Microsoft Windows 8.1 Update 1 (96%), Microsoft Windows Server 2008 R2 (95%), Microsoft Windows 7 Enterprise SP1 (95%), Microsoft Windows Vista SP1 (95%), Microsoft Windows 7 or Windows Server 2008 R2 (94%)
No exact OS matches for host (test conditions non-ideal).
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 18.63 seconds
```

Figura 38: Output do scan -sO

- **nmap -sV - Identificação de Serviços**

Por fim, um scan que procura serviços que estejam a correr no Metasploitable. Como se pode observar pela figura 39, os serviços que estão a correr nas portas do sistema são vários, alguns dos quais não é reconhecível pelo nmap identificados por "?" à frente do nome ou pelo nome "unknown".

```
(kali㉿kali)-[~] 0.4.2: icmp_seq=3 ttl=128 time=0.462 ms
$ nmap -sV 172.20.4.2 --version-all
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 08:34 EST
Nmap scan report for 172.20.4.2
Host is up (0.00038s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  tms-wbt-server  Microsoft Terminal Service
4848/tcp  open  ssl/appserv-htp?
7676/tcp  open  java-message-service Java Message Service 3.0.1
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http-proxy
8181/tcp  open  ssl/intermapper?
8383/tcp  open  ssl/http         Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?server?
49152/tcp open  msrpc-v-nttp    Microsoft Windows RPC
49153/tcp open  msrpc-kerberos Microsoft Windows RPC
49154/tcp open  msrpc
49155/tcp open  msrpc-item
49158/tcp open  unknown
49163/tcp open  msrpc-proxy
49165/tcp open  msrpc-ssdp

Nmap done at 2020-12-15 08:34 (0.00s)
```

Figura 39: Output do scan -sV

Após a pesquisa destes serviços, podemos analisar as possíveis vulnerabilidades de cada um, no entanto serão apenas mencionadas as mais críticas e recentes dos serviços.

Primeiramente, investigaram-se os serviços todos e pesquisou-se pelas vulnerabilidades de cada. Começando logo pelo OpenSSH na versão 7.1, encontramos uma vulnerabilidade apresentada em 2018 de nível médio de risco como se pode observar pela figura 40. Nesta parece que há um problema na autenticação onde é possível atacantes identificarem utilizadores do sistema remotamente.

CVE-2018-15919 Detail

Current Description

Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 5.3 MEDIUM

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Figura 40: Vulnerabilidade CVE-2018-15919 do serviço OpenSSH.

Encontra-se de seguida o serviço msrpc na porta 135. Pesquisou-se por vulnerabilidades sendo a mais recente a da figura 41. Adicionalmente, apenas pela pesquisa do serviço com a porta 135, encontrou-se uma data de exploits e formas possíveis de explorar este serviço e possivelmente o sistema na sua integridade. Foi surpreendentemente fácil encontrar exploits para vulnerabilidades relacionadas com este serviço. Esta vulnerabilidade diz nos seus detalhes que afeta a versão em

causa do Windows Server 2008 R2 entre outras e esta consiste numa má iniciação de objetos em memória quando o driver "Kernel Remote Procedure Call Provider" está em uso (levando a um ataque de Information Disclosure). Pode ser perigoso ainda que tenha um risco médio.

CVE-2018-8407 Detail

Current Description

An information disclosure vulnerability exists when "Kernel Remote Procedure Call Provider" driver improperly initializes objects in memory, aka "MSRPC Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.

[+View Analysis Description](#)



Figura 41: Vulnerabilidade CVE-2018-8407 do serviço Microsoft Windows RPC.

No caso do serviço NetBios, foram encontradas não só vulnerabilidades recentes como de alto risco, sendo a de mais alto nível (9.8) apresentada de seguida. Na sua descrição menciona que está relacionada com o Artica Proxy o qual tem uma falha que permite a injeção de comandos do sistema operativo em causa por várias vias.

CVE-2020-13159 Detail

Current Description

Artica Proxy before 4.30.000000 Community Edition allows OS command injection via the Netbios name, Server domain name, dhclient_mac, Hostname, or Alias field. NOTE: this may overlap CVE-2020-10818.

[+View Analysis Description](#)



Figura 42: Vulnerabilidade CVE-2020-13159 do serviço NetBios.

Durante a pesquisa realizada pelo grupo, foi realçado inúmeras vezes que a porta 445 pode ser perigosa dependendo do serviço que lá esteja a correr e foram encontrados vários exploits para o serviço SMB (Server Message Block). No nosso caso, observou-se que o serviço que está a correr nesta porta é o Microsoft Windows Server 2008 R2 - 2012 (microsoft-ds). Se pesquisarmos as vulnerabilidades deste serviço encontramos quase 1300 resultados no site NVD e múltiplas de risco elevado. Assim esta porta pode ser um possível ponto de entrada no sistema.

Na figura 43, observamos uma vulnerabilidade de risco alto (7.8) que consiste na possibilidade de execução de código de forma remota uma vez que o Jet Database Engine do Windows tem problemas em gerir objetos em memória. A versão que está a correr no sistema está incluída nas afetadas.

CVE-2019-0584 Detail

Current Description

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583.

[+View Analysis Description](#)

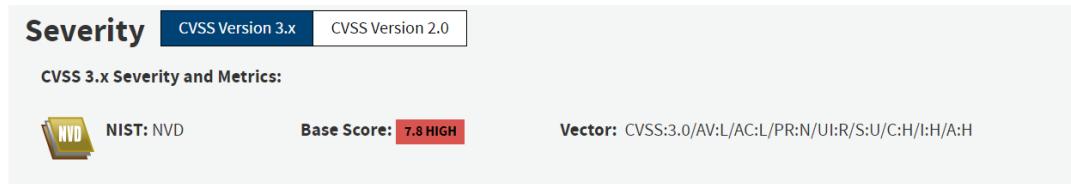


Figura 43: Vulnerabilidade CVE-2019-0584 do serviço Windows Server 2008 R2.

No serviço WEBrick httpd 1.3.1 teve-se em especial atenção a versão do Ruby 2.3.3 (2016) uma vez que muitas das vulnerabilidades apenas afetavam versões mais recentes. Neste caso, encontrou-se uma de 2017 onde atacantes podem, de forma remota e a partir dos seus mecanismos básicos de autenticação, injetar sequências nos logs e possivelmente executar comandos de forma arbitrária via um username falso.

CVE-2017-10784 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The Basic authentication code in WEBrick library in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows remote attackers to inject terminal emulator escape sequences into its log and possibly execute arbitrary commands via a crafted user name.

[+View Analysis Description](#)



Figura 44: Vulnerabilidade CVE-2017-10784 do serviço WEBrick httpd 1.3.1 (Ruby 2.3.3).

Ao pesquisar a versão do serviço seguinte, o MySQL na versão 5.5.20, encontrou-se uma vulnerabilidade de risco alto (9.8) que afeta várias versões incluindo esta. Esta permite utilizadores locais criarem configurações e contornar os mecanismos de proteção ao definir a configuração de general_log_file para a sua configuração. Adicionalmente, esta vulnerabilidade pode levar à elevação de privilégios e a execução arbitrária de código com privilégios de root. Assim, esta vulnerabilidade torna-se muito perigosa, refletindo bem o nível de risco que tem associado.

CVE-2016-6662 Detail

Current Description

Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.

[+View Analysis Description](#)



Figura 45: Vulnerabilidade CVE-2016-6662 do serviço MySQL 5.5.20-log.

De seguida, para o serviço Windows Terminal Service encontraram-se várias vulnerabilidades, e escolheu-se a mais recente na figura 46. Nesta um atacante pode tomar partido de características do clipboard uma vez identificado e executar código arbitrária e remotamente.

CVE-2020-0655 Detail

Current Description

A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Servicesâ Remote Code Execution Vulnerability'.

[+View Analysis Description](#)

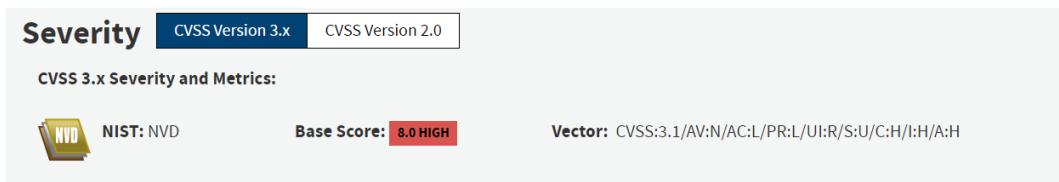


Figura 46: Vulnerabilidade CVE-2020-0655 do serviço Windows Terminal Service.

Para os serviços Java Message Service 301, Apache Jserv, Apache Tomcat não se encontraram vulnerabilidades de alto risco nem recentes que afetassem as versões em causa.

4.3 Nessus, Snort e Wireshark

As ferramentas Nessus, Snort permitem observar vulnerabilidades que caracterizam a Máquina Virtual Metasploitable 3 através de meios gráficos, os níveis de gravidade de cada vulnerabilidade e informações adicionais pertinentes o que permitirá fazer uma comparação de resultados com os métodos de scan activo utilizados na questão anterior.

4.3.1 Questão 2

Numa primeira instância foi efectuado o scan activo da máquina virtual Metasploitable 3 através da ferramenta Nessus em concorrência com o IDS Snort e o Wireshark ativos para ler a atividade durante o scan.

Após o scan efetuado, podemos observar que existe uma grande quantidade de vulnerabilidades e fraquezas que foram expostas através desta ferramenta. Muitas delas com nível crítico de severidade.

Com os resultados obtidos, podemos observar que o número e o detalhe destas vulnerabilidades é bastante maior do que a pesquisa manual feita pelo grupo. Uma ferramenta destas é muito útil pois expõe de uma forma mais extensiva o que pretendemos com esta questão. De facto muitas das vulnerabilidades tinham sido encontradas já na questão anterior. Contudo, a maior parte delas foram só conhecidas após este scan ativo.

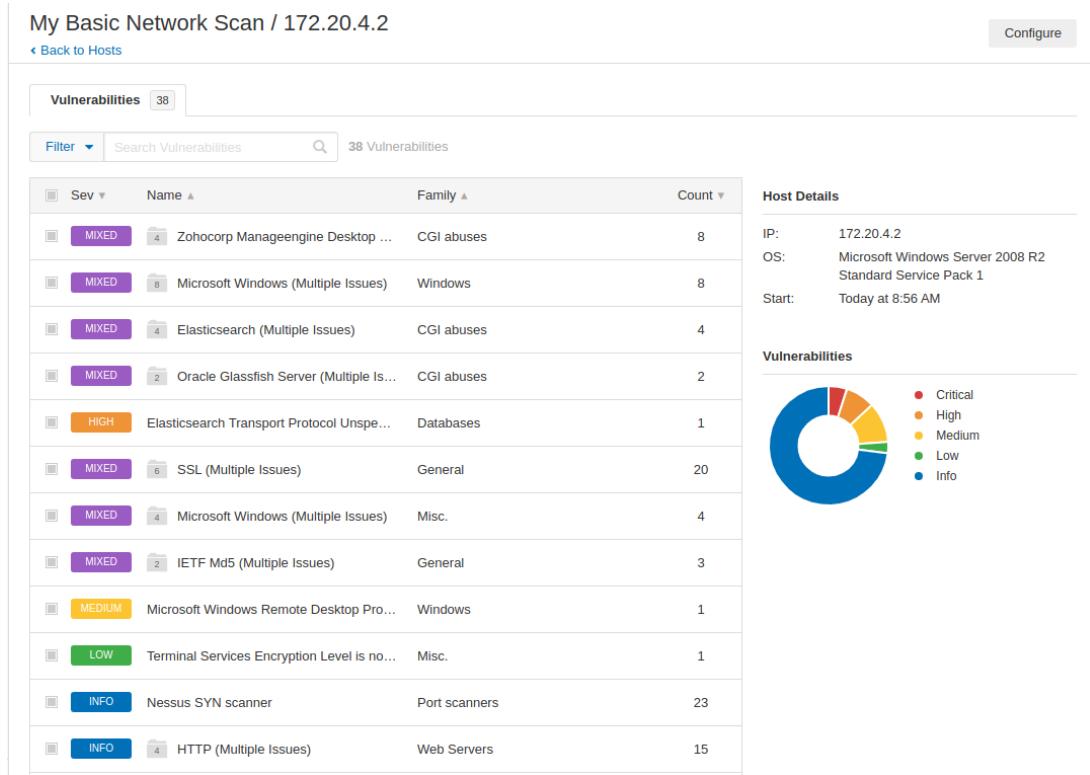


Figura 47: Resultados da procura de vulnerabilidades no Metasploitable 3 através do Nessus

Analizando algumas ”famílias” de vulnerabilidades com a tag *mixed* que agrupa todas as vulnerabilidades numa mesma categoria, podemos observar as mesmas detalhadamente.

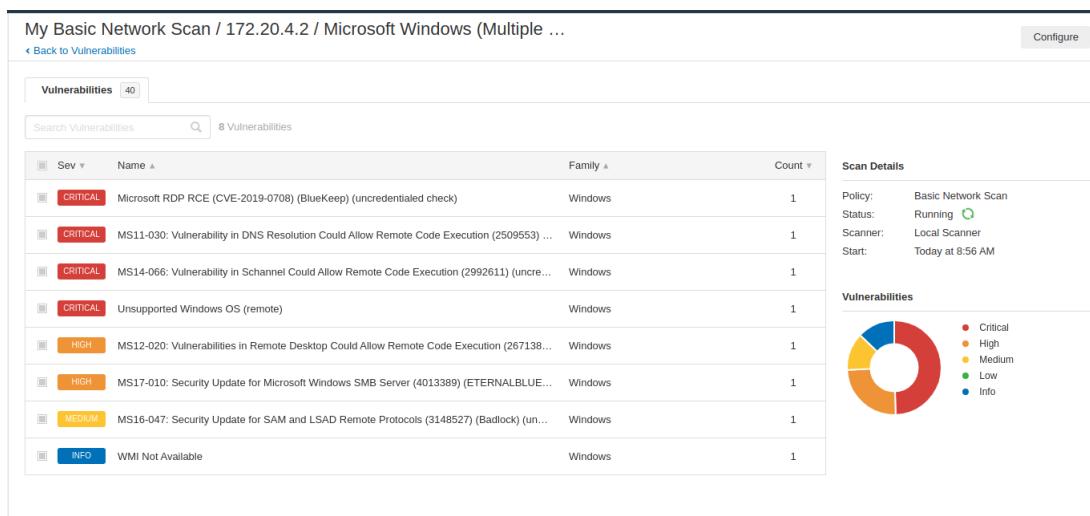


Figura 48: Vulnerabilidades de uma mesma família.

Observamos que há várias vulnerabilidades com risco alto a crítico, e de seguida iremos abordar uma das com nível de severidade mais elevado e de data particularmente recente:

Figura 49: Vulnerabilidades BlueKeep.

BlueKeep é uma vulnerabilidade de segurança descoberta na implementação do Remote Desktop Protocol (RDP) da Microsoft, que permite a execução remota de código. Relatado pela primeira vez em maio de 2019, este exploit está presente em todas as versões do Microsoft Windows sem patch do Windows 2000 ao Windows Server 2008 R2 e Windows 7. A Microsoft lançou um patch de segurança em 14 de maio de 2019. Esta vulnerabilidade recebeu novas actualizações e informações ainda em Agosto de 2020.

Como mencionado anteriormente, o serviço Windows Server 2008 R2 pode ser encontrado a correr na porta 445 e esta versão demonstra esta vulnerabilidade. Esta é facilmente explorada pois existem inúmeros sites e páginas online que explicam como tal pode ser feito. Esta vulnerabilidade expõe o sistema de uma forma muito perigosa e constitui assim um grande risco para este.

Ao efectuar uma pesquisa no site National Vulnerability Database pelo código desta vulnerabilidade, CVE-2019-0708, é de facto afirmado que esta vulnerabilidade tem um base score de 9.8 isto é, nível crítico de severidade, que tem como fonte a *Microsoft Corporation* e que foi modificada a 24 de Agosto de 2020, etc.

Para o caso de uma vulnerabilidade ou exploit mais recente foi encontrada a seguinte:

Figura 50: Vulnerabilidade com nível crítico.

Esta vulnerabilidade encontra-se no software ManageEngine Desktop que se encontra desactualizado.

4.3.2 Questão 3

Durante a análise do tráfego anómalo reconhecido pelo Snort, o grupo identificou alguns tipos de tráfego interessantes, acabando por escolher dois para análise mais detalhada.

Na figura 51, observamos que o snort reconheceu este tráfego como sendo do tipo Misc activity dizendo ainda que se trata de "BAD-TRAFFIC tcp port 0 traffic". Assim, pesquisou-se sobre este tipo de tráfego e analisou-se melhor as componentes deste alerta. Primeiro notou-se que este era proveniente da máquina que estávamos a usar para detetar as vulnerabilidades (neste caso, o Kali com o endereço 172.20.4.1) para o sistema (172.20.4.2). Do que sabemos, é que este tráfego muito provavelmente tem origem nos pedidos que o Nessus está a realizar em background. Se não soubéssemos a sua origem ia ser difícil categorizar estes pacotes como maliciosos ou não. No entanto, é conhecido que a porta 0 é usada às vezes como tentativa de intrusão no sistema. Isto pois pode ser uma tentativa de entrar pela firewall uma vez que muitas vezes as pessoas se esquecem que as portas tcp começam no 0 e não no 1, acabando por não bloquearem a 0 (tornando-a assim um ponto de entrada no sistema). Neste caso, não se conseguiu encontrar o identificador da vulnerabilidade.

```
[**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic []
[Classification: Misc activity] [Priority: 3]
12/19-17:49:05.550360 172.20.4.1:23636 -> 172.20.4.2:0
TCP TTL:64 TOS:0x0 ID:55445 IpLen:20 DgmLen:40
*****S* Seq: 0x1FE5DE21 Ack: 0x0 Win: 0x200 TcpLen: 20

[**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic []
[Classification: Misc activity] [Priority: 3]
12/19-17:49:05.550942 172.20.4.2:0 -> 172.20.4.1:23636
TCP TTL:128 TOS:0x0 ID:11558 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0x1FE5DE22 Win: 0x0 TcpLen: 20
```

Figura 51: Tráfego anómalo do tipo Misc activity.

O tráfego captura através do Wireshark foi o seguinte:

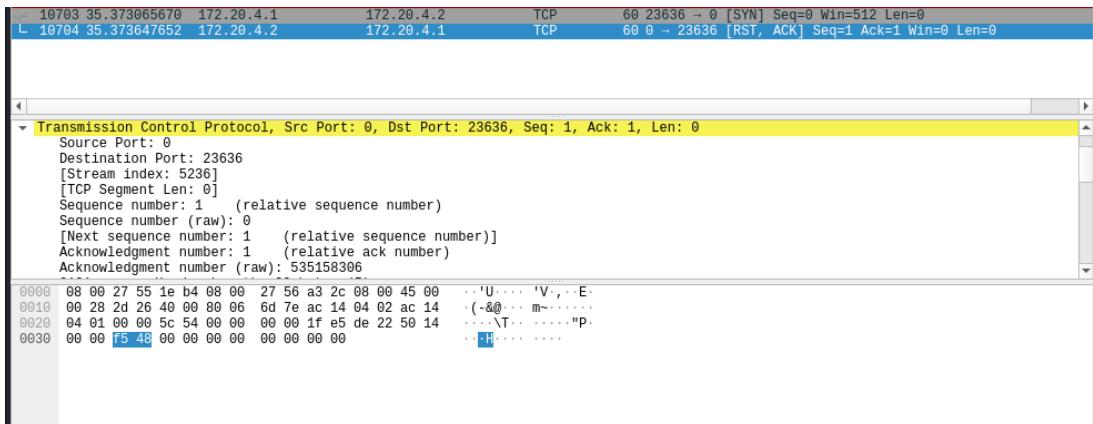


Figura 52: Trafego do Wireshark .

Na figura 53, encontrou-se outro tipo de tráfego anómalo, desta vez categorizado como sendo Attempted Denial of Service. Neste caso, o sistema Kali tentou enviar pacotes para a porta 15104 do sistema em causa e após uma pesquisa sobre o mstream, descobriu-se que este é um software que se encontra na máquina em causa que permite a execução de ataques do tipo Denial of Service na própria máquina.

```

[**] [1:249:8] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/19-17:48:33.925796 172.20.4.1:4932 -> 172.20.4.2:15104
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
*****S* Seq: 0x8E9D6D96 Ack: 0x0 Win: 0x1000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138]
[Xref => http://www.whitehats.com/info/IDS111]

```

Figura 53: Tráfego anómalo do tipo Attempted Denial of Service.

Este tem como identificador de vulnerabilidade CVE-2000-0138 e podemos ver os seus detalhes na figura seguinte:

CVE-2000-0138 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed, such as (1) Trinoo, (2) Tribe Flood Network (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, or (6) shaft.

[View Analysis Description](#)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: N/A

NVD score not yet provided.

Figura 54: Vulnerabilidade CVE-2000-0138.

Foi também capturado o tráfego no wireshark durante este alerta que é o seguinte:

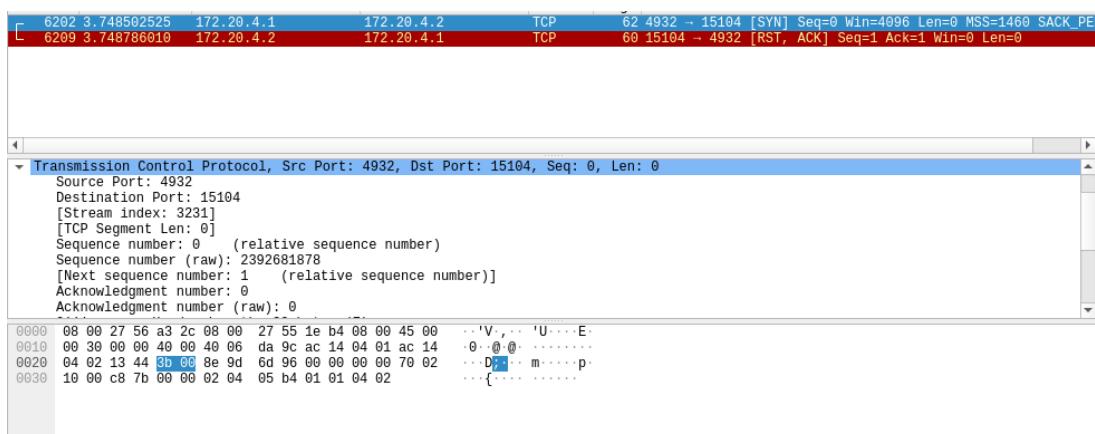


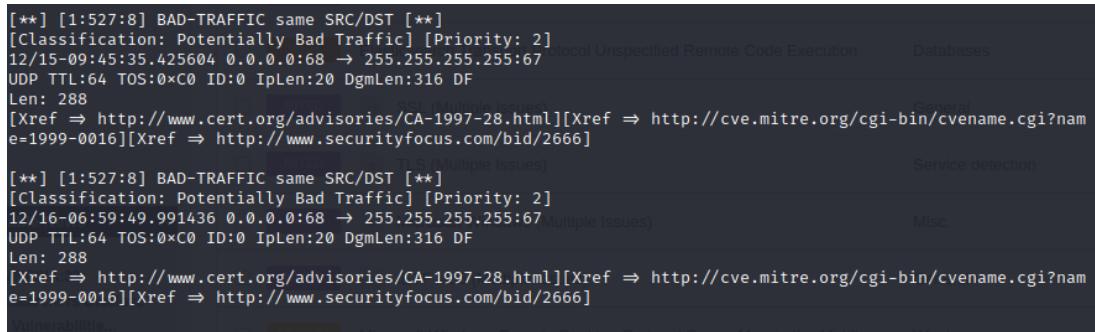
Figura 55: Trafego do Wireshark .

4.3.3 Questão 4

A ferramenta Snort é poderosa e útil no que toca à detecção de ataques ao sistema. Esta ferramenta tem como base a observação dos pacotes que circulam na rede, fazendo comparações de acordo com regras internas próprias gerando alertas caso o pacote cumpra estas ditas regras.

Esta questão passa essencialmente por entender certas diferenças no funcionamento desta ferramenta com a ferramenta de scan usada anteriormente, o Nessus, e de que forma isto leva a que sejam geradas notificações do IDS Snort que não possuem em si uma vulnerabilidade no sistema de scan usado até agora.

A partir da visualização do ficheiro *alert.full* podemos observar que existem pacotes fora do padrão habitual de vulnerabilidades:



The screenshot shows the Snort output window with two entries. The first entry is for a UDP broadcast packet at 12/15-09:45:35.425604, originating from 0.0.0.0:68 to 255.255.255.255:67. It is classified as 'Potentially Bad Traffic' with priority 2. The second entry is for a similar UDP broadcast packet at 12/16-06:59:49.991436, also from 0.0.0.0:68 to 255.255.255.255:67. Both entries mention CVE-1999-0016 and point to various URLs for advisories and references. The interface includes tabs for 'Databases', 'Service detection', and 'Misc.'.

```
[[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
12/15-09:45:35.425604 0.0.0.0:68 → 255.255.255.255:67 Protocol Unspecified Remote Code Execution
Databases
Len: 288
[Xref ⇒ http://www.cert.org/advisories/CA-1997-28.html][Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref ⇒ http://www.securityfocus.com/bid/2666]

[[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
12/16-06:59:49.991436 0.0.0.0:68 → 255.255.255.255:67 Multiple Issues)
Service detection
Len: 288
[Xref ⇒ http://www.cert.org/advisories/CA-1997-28.html][Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref ⇒ http://www.securityfocus.com/bid/2666]

Misc.
```

Figura 56: Output do Snort correspondentes aos pacotes do tipo UDP.

Analizando estes dois pacotes que são semelhantes, podemos observar que é enviado um pacote em modo *broadcast* por parte do localhost. Tal permite concluir que este alerta não se trata de um vulnerabilidade por parte do sistemas de scan mas sim de um alerta que ocorre quando o *host* está a tentar conectar-se a uma rede. Para isso, precisa de enviar pacotes UDP como forma de requisição, ou seja, um situação de reconhecimento de rede e de máquinas existentes.

Para além disso, a partir deste tráfego anómalo conseguimos observar links que nos levam ao site do cve e consequentemente a uma vulnerabilidade CVE-1999-0016. A vulnerabilidade denomina-se por "Land IP denial of service" (local area network denial) e podemos verificar que foi tratada como anómala pelo Snort na figura 56. Isto demonstra claramente que houve uma resposta ao ataque feito pelo Nessus e que devolveu tanto o userid, como o root.

Sem pesquisar pelo identificador da vulnerabilidade podemos assumir coisas sobre ela. Primeiramente, este tráfego não deve ser encontrado em nenhuma rede uma vez que diz que tem a mesma origem e destino. Esta vulnerabilidade com o ID de CVE-1999-0016 atinge a Layer 4 do protocolo IP e tira partido de uma propriedade chamada de "loopback". Esta propriedade é comum observar-se em routers como forma de manipular rotas e gerir tráfego, conceito bastante presente na engenharia de tráfego no geral. Este é iniciado pelo envio de um pacote adulterado do tipo SYN onde os endereços IP de origem e da porta de destino são iguais aos da própria máquina da vítima. Quando um pacote desse tipo é recebido, um loop infinito é iniciado e o sistema vê os seus recursos a serem consumidos, levando à interrupção do funcionamento normal deste. Esta vulnerabilidade foi reportada como sendo mais efetiva nos sistemas da Microsoft e pode resultar na descoberta de uma rota de ataque a um computador por parte de um atacante.

CVE-1999-0016 Detail

Current Description

Land IP denial of service.

[+ View Analysis Description](#)

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
 NIST: NVD	Base Score: N/A	NVD score not yet provided.

Figura 57: Vulnerabilidade CVE-1999-0016.

No entanto, o que pode causar isto, na opinião do grupo, são várias coisas. Pode apenas ser um protocolo que esteja a lançar estes pedidos sem qualquer má intenção, ou pode ser algo externo ao sistema que esteja a tentar aceder por alguma das portas. Assim, é incerto o que está a causar isto mas parece ser inofensivo.

4.3.4 Questão 5

Para esta questão foram escolhidas três vulnerabilidades de diferentes graus de severidades através do Nessus, para tentar efectuar a sua resolução e eliminar as fraquezas que estas forneciam.

Primeiramente foi escolhida uma de nível médio. Após uma analise nas escolhas possíveis foi escolhida a seguinte:

MEDIUM	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities	Plugin Details								
Description The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities. Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.		Severity: Medium ID: 108752 Version: 1.6 Type: remote Family: CGI abuses Published: March 30, 2018 Modified: November 8, 2019								
Solution Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.		Risk Information Risk Factor: Medium CVSS v3.0 Base Score: 6.1 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/ /UI:R/S:C/C:L/I:L/A:N CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/ /RL:O/RC:C CVSS v3.0 Temporal Score: 5.3 CVSS Base Score: 4.3 CVSS Temporal Score: 3.2 CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N CVSS Temporal Vector: CVSS2#E:URL:O/RC:C								
Output <table border="1"><thead><tr><th>Port</th><th>Hosts</th></tr></thead><tbody><tr><td>8022 /tcp /www</td><td>172.20.4.2</td></tr></tbody></table> <table border="1"><thead><tr><th>Port</th><th>Hosts</th></tr></thead><tbody><tr><td>8383 /tcp /www</td><td>172.20.4.2</td></tr></tbody></table>		Port	Hosts	8022 /tcp /www	172.20.4.2	Port	Hosts	8383 /tcp /www	172.20.4.2	Vulnerability Information CPE: cpe:/a:zohocorp:manageengine_desktop_central Exploit Ease: No known exploits are available Patch Pub Date: March 21, 2016 Vulnerability Pub Date: March 21, 2016
Port	Hosts									
8022 /tcp /www	172.20.4.2									
Port	Hosts									
8383 /tcp /www	172.20.4.2									

Figura 58: Vulnerabilidade Media.

Esta vulnerabilidade, CVE-2018-8722, é causada pelo software Manager Engine Desktop que se encontra numa versão desactualizada. Um método de resolução fácil e eficaz é a actualização do software tal como sugere o Nessus.

Pode ser confirmada o base score no site CVE:



Figura 59: CVE-2018-8722.

Foi então efectuado o download de uma instalação recente e instalado no Metasploitable:

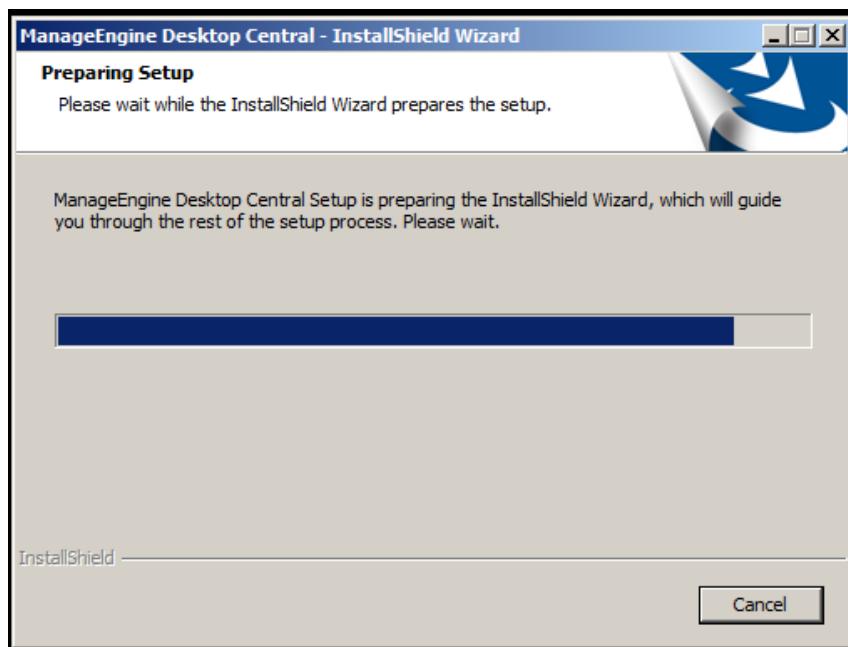


Figura 60: Instalação da nova versão do Manager Engine Desktop.

Após a instalação voltou a ser feita um scan ao Metasploitable com o Nessas para verificar se alguma vulnerabilidade foi eliminada. Reparou-se então que não apenas uma, mas pelo menos 4 vulnerabilidades tinham sido eliminadas. Após uma análise e comparação com os resultados de scans anteriores reparou-se que existiam varias vulnerabilidades de níveis diferente que eram geradas pelo mesmo software que se encontrava desactualizado:

Vulnerabilities 48					
Search Vulnerabilities 4 Vulnerabilities					
Sev	Name	Family	Count		
CRITICAL	ManageEngine Desktop ...	CGI abuses	2	<input type="radio"/>	<input type="checkbox"/>
CRITICAL	ManageEngine Desktop ...	CGI abuses	2	<input type="radio"/>	<input type="checkbox"/>
MEDIUM	ManageEngine Desktop ...	CGI abuses	2	<input type="radio"/>	<input type="checkbox"/>
INFO	ManageEngine Desktop ...	CGI abuses	2	<input type="radio"/>	<input type="checkbox"/>

Figura 61: ”Família” de vulnerabilidades do mesmo software.

Como vulnerabilidade de nível alto foi escolhida a seguinte:

Description
Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system.

Solution
Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port

See Also
<http://www.nessus.org/u?c6b6cf1a>

Output

URL : http://172.20.4.2:9200/
Installed version : 1.1.1
Fixed version : 1.6.1

Hosts

9200 / tcp / elasticsearch... 172.20.4.2
--

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/R:LO/R:C
CVSS v3.0 Temporal Score: 8.5
CVSS Base Score: 7.5
CVSS Temporal Score: 5.5
CVSS Vector: CVSS:3.0/AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Vector: CVSS:3.0/E:U/RL:O/R:C

Figura 62: Vulnerabilidade alta.

Esta vulnerabilidade, CVE-2015-5377, nesta versão do software Elasticsearch pode permitir a um atacante remoto executar código arbitrário no sistema. É causado por um erro no protocolo de transporte. Como o Nessus apresenta, para resolver esta vulnerabilidade é apenas necessário actualizar o software. Após a sua actualização as vulnerabilidades correspondentes a este programa desapareceram, que eram pelo menos 3 incluindo a seguinte "família":

Sev	Name	Family	Count	Actions
HIGH	Elasticsearch ESA-2015-06	CGI abuses	1	
INFO	Elasticsearch Detection	CGI abuses	1	

Figura 63: "família" de vulnerabilidades do Elasticserach.

Por fim, escolhendo uma vulnerabilidade de nível critico, foi optada pela:

Description
The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Solution
Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

See Also
<http://www.nessus.org/u?64e97902>

Output

No output recorded.

Hosts

3389 / tcp / msrdp 172.20.4.2

Figura 64: "família" de vulnerabilidades do Elasticserach.

Esta vulnerabilidade tem como solução, o download de patches actualizados ou a actualização do windows através do Windows update. Foi então por esse último caminho que foram efectuados alguns passos para levar a cabo a actualização do sistema operativo do Metasploitable, que após análise reparou-se que estava com as actualizações automáticas desactivadas:

Windows Update

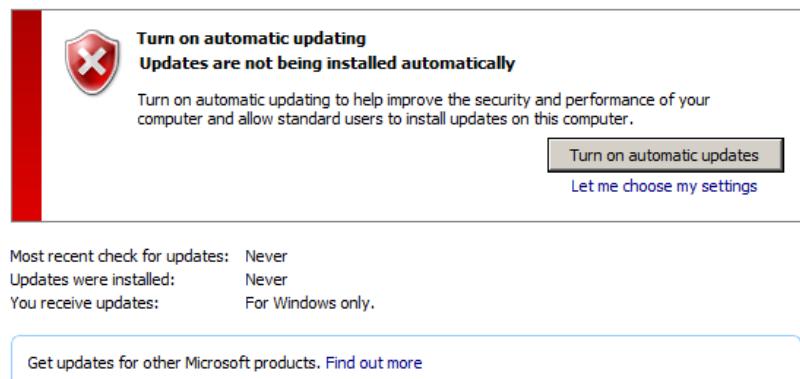


Figura 65: Windows Update Desligado.

Foram então activadas as actualizações automáticas e o windows procedeu à procura das mesma que estivessem disponíveis:

Windows Update

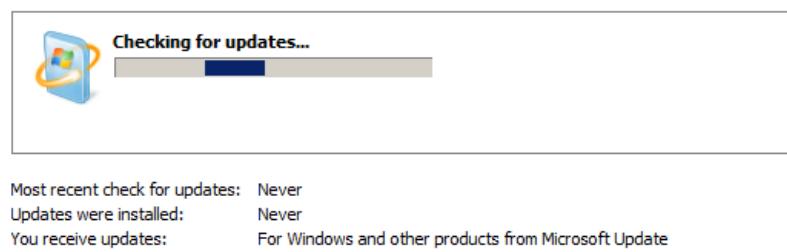


Figura 66: Windows Update à procura de Actualizações.

Tal como era esperado foram encontradas variadas actualizações disponíveis:

Windows Update

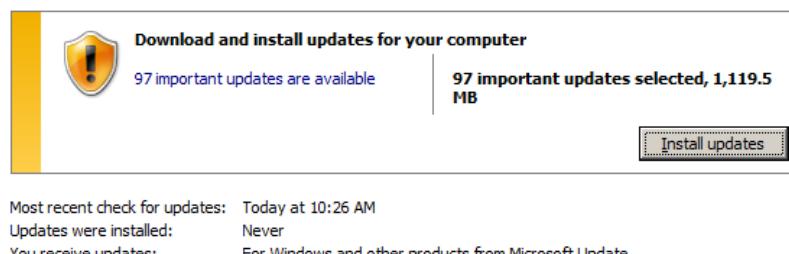


Figura 67: Actualizações disponíveis.

Por fim podemos então comparar a diferença na quantidade de vulnerabilidades que foram eliminadas. Deve se tomar em conta que este número reduziu bastante devido à actualização do sistema operativo:



Figura 68: Antes de qualquer alteração.

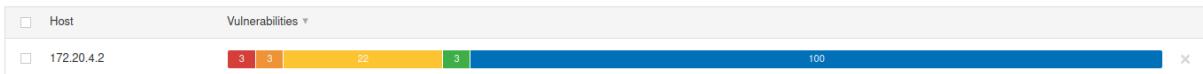


Figura 69: Depois das alterações.

4.4 Conclusões - Parte 2

Com o ambiente de testes totalmente preparado, o objectivo principal passou por detectar vulnerabilidades, a nível dos serviços obtidos por ferramentas como o NMAP, Nessus, etc existentes na Máquina Virtual Metasploitable 3.

Foi entendida a importância de se usar paralelamente o IDS Snort e Wireshark com a análise da lista de vulnerabilidades através do Nessus. Isto porque através deles descobrimos detalhes dos serviços a correr nas várias portas e com essa informação podemos interpretar melhor como/onde poderíamos insistir/pesquisar para corrigir certas vulnerabilidades e através de um estudo dos resultados das mesmas e acabamos assim por perceber que existem pacotes no output do Snort que depois não correspondem a qualquer vulnerabilidade no sistema de scan Nessus/OpenVAS.

5 Conclusão

Este relatório consiste em duas partes principais. Na primeira entendeu-se como é que grandes e médias empresas podem ter as suas informações expostas e a facilidade com que se consegue acessá-las. Para além disso, foi uma boa forma de o grupo por em prática não só as capacidades aprendidas ao longo das aulas como também por à prova a nossa intuição e julgamento crítico.

A segunda parte envolveu uma componente mais técnica usando ferramentas mais poderosas e passando a uma análise mais intrusiva de um sistema. Com esta, aprendeu-se como identificar mais vulnerabilidades específicas ao sistema em causa e como usar isso para resolver os seus problemas inerentes.

Em suma, o grupo considerou este trabalho prático uma boa maneira de testar os nossos conhecimentos de uma forma mais exaustiva e mais aplicada à vida real e a casos reais.

6 Bibliografia

<https://www.flytap.com/pt-pt/>
<https://www.tub.pt/>
<https://www.tapairportugal.com/pt/>
<https://www.recrutamento.tap.pt/>
<https://sectools.org/>
<https://nvd.nist.gov/vuln/detail/CVE-2019-0708>
<https://www.securityfocus.com/bid/2666/info>
<https://nvd.nist.gov/vuln/detail/CVE-1999-0016>