Tecnologia de Segurança (4º ano de Engenharia Informática)

Trabalho Prático Nº2 Parte A

Relatório de Desenvolvimento

Carla Cruz (a80564)

Adriana Meireles (a82582)

3 de Novembro de 2019

Conteúdo

Capítulo 1

Introdução

Este projecto tem como objectivo principal, o estudo de Coleta Passiva de Informações (Passive Information Gathering), através das seguintes técnicas:

- Análise de informações de registo do domınio;
- Análise da página web;
- Busca de informações na internet.

De modo a efetuar comparações entre as quantidades de informação. decidimos fazer este estudo em duas empresas que diferem bastante na sua dimensão:

- Worten - empresa portuguesa eletrónica de consumo e entretenimento.
- VideoNorte - Centro de cópias.

Capítulo 2

Análise de Técnicas Nas Empresas

2.1 Worten

Worten é uma empresa portuguesa eletrónica de consumo e do entretenimento. Esta empresa pertence à Sonae. A primeira loja Worten foi inaugurada a 12 de março de 1996 em Chaves e tem atualmente mais de 180 lojas em Portugal. Apresentamos uma cronologia que nos mostra a evolução desta empresa com o passar dos anos.

Cronologia

1996	Inauguração da primeira loja, em Chaves.
2001	Lançamento da loja online www.worten.pt.
2002	Liderança de mercado da Worten nos setores dos eletrodomésticos e da eletrónica de consumo.
2004	Apresentação do conceito Worten Mobile como especialista nas telecomunicações móveis.
2004	Criação do conceito Worten mobile como especialista de retalho das telecomunicações móveis.
2006	Lançamento do cartão de crédito Worten, que permite várias modalidades de pagamento, incluindo pagamentos sem juros.
2007	Primeiro rebrand da marca, onde é apresentado um novo logótipo.
2009	Entrada oficial da Worten em Espanha, com a aquisição das lojas Boulanger.
2010	Criação da página oficial da Worten no Facebook.
2013	Lançamento do cartão Worten Resolve, que tem hoje mais de dois milhões de aderentes.
2014	Lançamento do conceito de comunicação "O mundo está cada vez mais Worten", centrado no papel da Worten como marca que leva a tecnologia a todos os portugueses.
2016	Novo rebrand da marca, que dá origem ao logótipo atual e que cria um novo ícone de marca.

Figura 2.1: Cronologia da empresa Worten

2.1.1 Análise do registo de Domınio

Para a realização da análise do registo de Domínio foram utilizadas as ferramentas nslookup, geoip2 e whois. Estas ferramentas são bastante úteis uma vez que podem mostrar dados que nos permitam inferir bastantes

coisas sobre a estrutura informática da empresa em questão.

nslookup

De forma a obter informações sobre os registos de DNS, utilizamos a ferramenta nslookup.

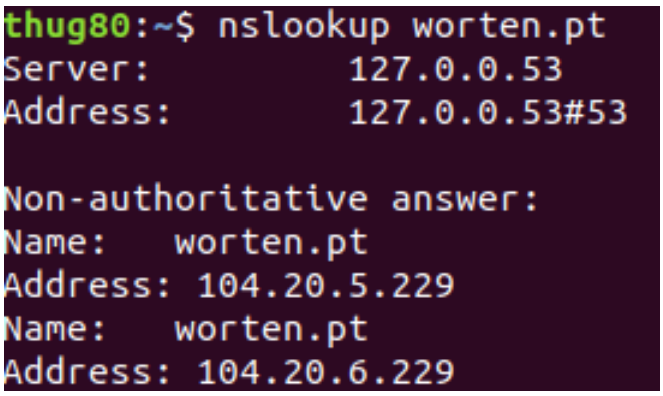


Figura 2.2: Resultado do comando nslookup worten.pt

GeoIP2 City Database Demo

Através da ferramenta utilizada, conseguimos localizar geograficamente o domínio.

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
104.20.6.229	US	United States, North America		37.751, -97.822	1000	Cloudflare	Cloudflare		

Figura 2.3: Resultado da localização Worten

Não é possível aceder à localização exata dos servidores da Worten pois estes estão protegidos por uma reverse-proxy denominada Cloudflare.

WhoIs

Foi realizada uma consulta whois sobre o domínio worten.pt obtendo o seguinte:

Figura 2.4: Resultado de WhoIs de worten.pt

Podemos ver quem é a entidade titular pelo domínio e pela sua gestão. Em relação aos nameservers, decidiram utilizar os serviços da CloudFlare para a prestação do serviço.

2.1.2 Análise da página web

Após a fase de análise do registo de domínio, avançamos para uma fase de procura de informação disponível na Internet. Procuramos no site da empresa, artigos e redes sociais.
Esta empresa é bastante conhecida e conceituada, contudo, a informação sobre os responsáveis é escassa. Através da leitura de artigos e notícias, constatamos que é uma empresa detida pela Sonae e que a sua CEO é a gestora Cláudia Azevedo. O CEO do ramo em que a Worten se enquadra é o Miguel Mota Freitas. Conseguimos através de notícias encontrar algumas informações sobre a mulher que representa a Sonae e que tem uma relação familiar com um dos ex-representantes. Quando ao Miguel Freitas não encontramos nada em concreto. Iremos apresentar de seguida, todas as informações obtidas.
A nível de redes sociais, a rede social mais visitada é o LinkedIn dado que é uma rede ligada direcionada para os negócios e tem bastantes informações sobre os seus trabalhadores e está em constante atualização. Não encontramos propriamente o perfil de nenhum elemento da administração, apenas de colaboradores e informáticos.

2.1.3 Busca de informações na internet

Através das técnicas utilizadas e informação obtida, apresentamos os seguintes quadros.

2.1.4 Resultados

Domínios

Item	Dados	Descrição
Nome da Empresa	Worten	Worten é uma empresa portuguesa de eletrónica de consumo e do entretenimento
Domínio	PT	worten.pt
Endereço da empresa	Rua João Mendonça, 529,Senhora da Hora,4464-511, Matosinhos	Telefone:800100102
CEO ou Gestor principal	Miguel Mota Freitas	linkedin.com/in/andrepimentaribeiro
Responsável pelo domínio	Worten Equipamentos para o lar SA	
Responsável pelos endereços IP's	Cloud Flare	
Responsável pela página Web ou setor de Tecnologia	Serafim Pinto	linkedin.com/in/miguel-mota-freitas-37916b7/
Endereço IP do Servidor Principal	104.20.6.229/104.20.6.229	
Localização do Servidor Web	Phoenix (EUA)	
Tipo de tecnologias utilizadas pela empresa	SQlServer,Unix,Linux, Java,Remedy,.NET.	

CEO

Item	Dados	Descrição
Nome	Miguel Mota Freitas	
Endereço	Não encontrado	
Estado Civil	Casado	
Telemóvel	Não encontrado	
Currículo	Não encontrado	
Resumo da pessoa	Miguel Mota Freitas entrou na Sonae aos 19 anos. Cresceu no grupo liderando atualmente também o Iberian Sports Retail Group que junta a Sport Zone e a JD Sports Casado e pai de três filhos este economista de 48 anos,é apontado como um dos gestores de confiança de Paulo Azevedo	

2.2 VideoNorte

2.2.1 Análise do registo de Domınio

nslookup

Para se obter informações sobre os registos de DNS foi utilizado o nslookup.

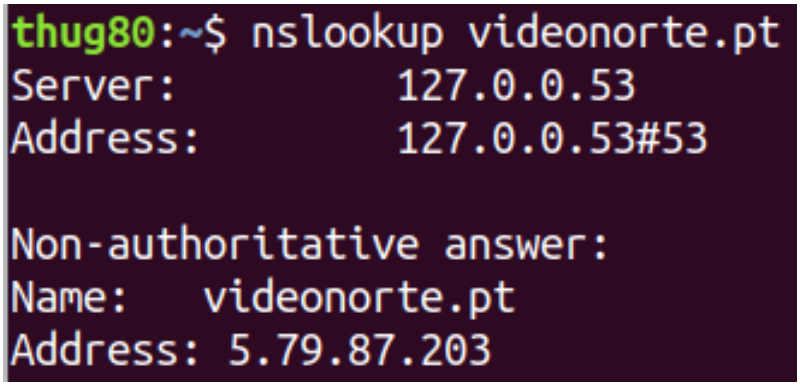


Figura 2.5: Resultado do comando nslookup videonorte.pt

GeoIP2 City Database Demo

Localiza geograficamente o domínio da VideoNorte.

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain
5.79.87.203	NL	Netherlands, Europe		52.3824, 4.8995	100	LeaseWeb Netherlands B.V.	LeaseWeb Netherlands B.V.	leaseweb.com

Figura 2.6: Análise do endereço IP através de uma ferramenta de Geolocalização

WhoIs

Após uma consulta whois sobre o domínio videonorte.pt obtivemos as seguintes informações:

WHOIS videonorte.pt

Domínio	videonorte.pt
Data de Submissão	2016-05-17
Data de Expiração	2023-05-16
Estado	Registered
Titular	Confidencial Contactar Titular
Entidade Gestora	DMNS - DOMINIOS, S.A. DMNS - DOMINIOS, S.A., Parque Multiusos, Areal Gordo, Lote 3A, Faro, 8005-409 Faro, PT dns@dominios.pt; mailmanager@dominios.pt
Informação do Nameserver	ns7.host-servers.net ns8.host-servers.net

Figura 2.7: Resultado de whois videonorte

Resultados

Item	Dados	Descrição
Nome da Empresa	VideoNorte	
Domínio	videonorte.pt	https://www.dns.pt/pt
Endereço da Empresa	R.Nova da Santa Cruz nº49/47,4710-409 R. São Sebastião, nº120, 3810-187 Aveiro	Endereço da Loja de Braga Endereço da Loja de Aveiro
CEO ou Gestor Principal	Hugo Olival Florbela Pais	Gerente da Loja de Braga Gerente da Loja de Aveiro
Responsável pelo domínio	DMNS-DOMINIOS,S.A	https://www.dominios.pt/
Responsável pelos endereços IP's	DMNS-DOMINIOS,S.A	
Responsável pela página Web ou setor da Tecnologia	DMNS-DOMINIOS,S.A	
Endereço Ip do Servidor principal	5.79.87.203	https://ping.eu/nslookup/
Localização do Servidor Web	Portugal	
Tipo de tecnologias utilizadas pelas empresa(página Web,Funcionários)	Domínio gerido por terceiro Página web	Dominio-https://www.dominios.pt/ Página - https://www.videonorte.pt/

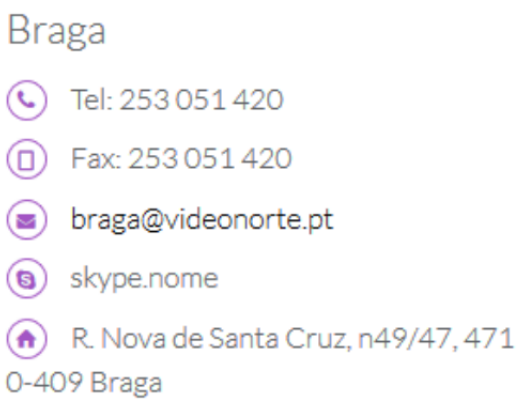
2.2.2 Análise da página web

Esta forma de pesquisa resulta da procura de informações relevantes para nós, consultando a página web da empresa em questão.

Na página web da VideoNorte encontramos informações dos contactos e endereços das lojas.

Para além disso ainda encontramos números de telemóvel e e-mails associados a cada loja específica da empresa.

De seguida, encontram-se representadas essas informações:



2.2.3 Busca de informações na internet

Neste secção iremos apresentar os dados que conseguimos obter através de pesquisas em redes sociais como o Facebook e pesquisas dos elementos no Google. Focamos a nossa pesquisa às pessoas de maior cargo dentro das empresas escolhidas, tentando tirar o maior número de informações destes.

Item	Dados	Descrição
Nome	Hugo Olival	Gerente Video Norte- Centro de Copias
Endereço	Braga, Portugal De Funchal	Vive atualmente em Braga mas é natural do Funchal
Estado Civil	Casado	Casado com Tania Pereira
Telemóvel		
Currículo	Diretor Departamento Ciêntifico - Nebaum Estudou Biologia Aplicada - UM Estuda Mestrado em Bioquímica Aplicada - UM Estudou no Liceu jaime Moniz Formação Pedagógica de Formadores em Twofold Academia de Formação Trabalhou como Delegado Comercial na empresa Barclaycard Monitoria na empresa Associação de Desenvolvimento Comunitário do Funchal- ADCF Gerente da VideoNorte Braga	
Resumo da pessoa	Nascimento Estudos Carreira Vida Pessoal	Nasceu em 29 de Maio de 1990 no Funchal. Estudou no Liceu Jaime Moniz a partir de 2005. Conheceu a sua atual mulher em 2007. Conclui o estudo em 2008, começou a trabalhar na empresa CityBank. Em 2010 começou a trabalhar em Associação de Desenvolvimento Comunitário do Funchal e na empresa Barclaycard. Fez voluntariado em 2012, começou a trabalhar em Nebaum e a estudar na Universidade do Minho, mudou-se para Gualtar,Braga. Acabou o curso em 2015 e começou o mestrado nesse mesmo ano.

2.3 Estratégias de ocultação de informação

Consideramos algumas estratégias de modo a não tornar disponível as informações pessoais a pessoas desconhecidas facilmente. Essas estratégias são as seguintes:

- Utilização do serviço *WHOIS privacy* que esconde informações pessoais tais como a contactos telefónicos, morada, email etc que ficam quando uma pessoa se regista num domínio Top Level ;
- Uma determinada empresa criar uma política restrita de privacidade que impeça os seus trabalhadores de partilharem informações de foro pessoal.

- Empresas deveriam implementar programas de treino de modo a manter todos os seu colaboradores informados acerca de termos como *Identity fishing*,*Password choice*, *Safe Browsing* e *Backup procedures.*

Capítulo 3

Conclusão

Com a realização do trabalho percebemos de que forma é possível fazer a pesquisa sobre uma certa empresa e que tipo de informação se encontra disponível na Internet. Isto é importante a ter em conta pois quanto mais informação tivermos sobre uma empresa mais direcionado e legítimo poderá ser realizado um ataque.
Concluimos que, com base nas empresas escolhidas, as informações encontradas da empresa maior foram poucas em relação à empresa de pequena dimensão. Isto prova a preocupação das grandes empresas em aumentar os recursos para manter a empresa segura.
Por fim, achamos que este trabalho foi bastante enriquecedor dado que trabalhamos com ferramentas novas e realizamos uma pesquisa bastante aprofundada de empresas que nos permitiu fazer um balanço de como se pode melhorar a segurança (ocultação da informação).