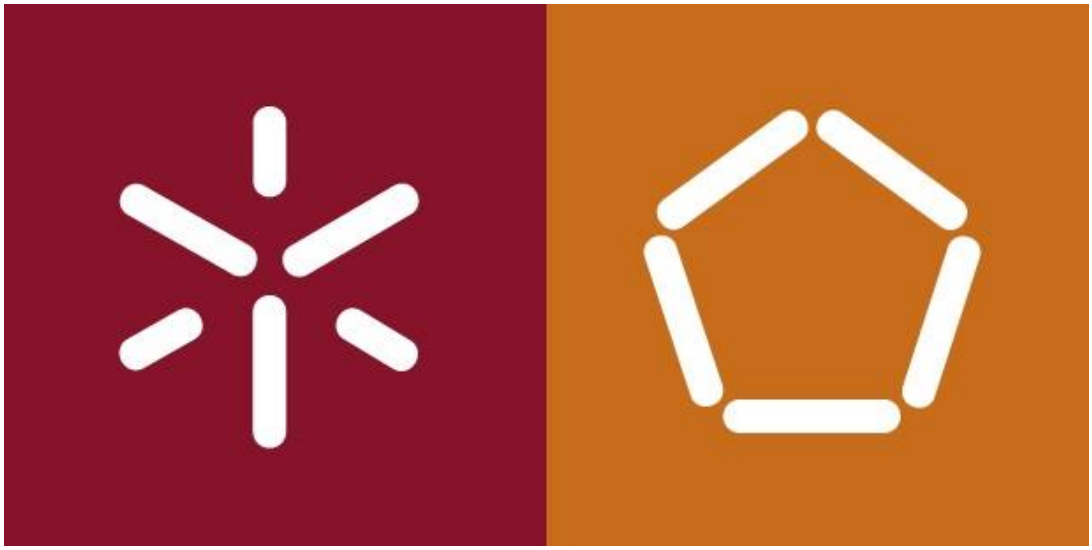
Universidade do Minho



Coleta Passiva de Informações

Mestrado Integrado em Engenharia Informática

Tecnologias de Segurança
1º Semestre , 2018/2019

Grupo 6
A77070 - João Pedro Pereira Alves
A70132 - Nuno André Lopes Leite

Gualtar,Braga
11 de Novembro de 2018

Conteúdo

Lista de Figuras

1 Introdução

A realização deste trabalho prático e escrita deste relatório surge no âmbito da Unidade Curricular de Tecnologias de Segurança, pertencente ao perfil de Criptografia e Segurança de Informação, lecionada no 1º semestre do 4º ano do Mestrado Integrado em Engenharia Informática.

A resolução deste trabalho tem como objetivo a aprendizagem na área da consulta passiva de informações, ou seja nas práticas de coletar informação acerca de uma dada entidade/pessoa com um propósito, o que também pode ser denominado de Engenharia Social.

A realização destas atividades tem como finalidade, neste contexto, obter informação sobre duas empresas escolhidas pelo grupo:

- A *Critical Software*, uma empresa nacional de renome, tanto nacional como internacionalmente;
- A *Ponto25 Informática*, uma empresa local, situada em Braga.

No final, é suposto que sejamos capazes de coletar um volume considerável de informações acerca das empresas e das suas pessoas de interesse, bem como ter a capacidade de comparar a diferença existente em metodologias de segurança com duas empresas que estão em situações opostas (uma é uma empresa muito grande e internacional, a outra é uma empresa local). Além disso, é suposto, no final, sugerir estratégias que permitam combater estas técnicas de coleta de informações.

2 Apresentação de Informações

Nesta secção, serão apresentadas as informações que foram possíveis de ser coletadas sobre as empresas escolhidas e sobre as suas pessoas de interesse. A coleta de informações baseou-se nas pesquisa nos *websites* das empresas, na utilização de utilitários como o *whois* e o *nslookup*, bem como um *website* de geolocalização através do ip de um dado servidor. Além disso, recorremos também às redes sociais, com o intuito de pesquisar as pessoas de interesse, se bem que, esta pesquisa se tornou um bocado infrutífera pelo facto de as pessoas referidas terem pouca informação nas suas redes sociais, ou até não terem conta nessa rede social.

2.1 *Critical Software*

A *Critical Software* é uma empresa de software e sistemas de informação portuguesa sediada em coimbra com implantação internacional, especializada em oferecer soluções para serviços críticos, como a indústria aeroespacial, governo, telecomunicações, entre outros.

Fundada em 1998 por Gonçalo Quadros, Diamantino Costa e João Carreira. Dos três fundadores, apenas Diamantino Costa não trabalha atualmente na empresa.

De seguida, enumeraremos as informações encontradas sobre a empresa:

1. **Domínio:** criticalsoftware.com
2. **Endereço:** Parque Industrial de Taveiro, lote 49, 3045-504, Coimbra (Sede, apesar de existirem vários outros locais onde a empresa está instalada, como Porto, Lisboa, Southampton, Califórnia, São Paulo, Maputo, Luanda, etc)
3. **CEO:** Gonçalo Quadros, que é também fundador da empresa;
4. **Responsável pelo domínio:** Make it Simple Consultoria Informática;
5. **Responsável pelos endereços IP's:** Make it Simple Consultoria Informática (figura 2)
6. **Responsável pela página web/setor de tecnologia** João Paulo Macedo Cunha (**CTO** - Chief Technology Officer em Serviços Digitais)
7. **Endereço IP do servidor principal:** 185.63.181.169 (figura 1)
8. **Localização do Servidor Web:** Latitude: 38.7139 Longitude: -9.1394 (Lisboa, perto de Alfama) (figura 2)
9. **Tecnologias utilizadas:** O facto de ser uma empresa muito grande, faz com que use uma enorme variedade de tecnologias, pelo que apresentaremos as principais:
    - Para a Web utilizam ASP.NET, CGI-Perl, HTML, DHTML, AJAX, Javascript, Apache, Tomcat e Jrue;
    - Em Engenharia de Software, utilizam Ada, C, C++, C#, .NET e python;
    - Em Modelação de Software, utilizam UML, SysML e MoDMF;
    - Para bases de dados, utilizam SQL Server, MySQL, Oracle, Sybase, entre outras;
    - Para segurança, utilizam SSL, TLS, LDAP, Kerberos, PKI, CERT, entre outras tecnologias;

- Desenvolvem para e em Windows, MacOs, Linux, Android, iOS, FreeBSD, Solaris, entre outros;

10. Além das informações pedidas, encontrámos também o endereço IP do seu servidor de e-mail: 13.94.118.236 (figura 3)

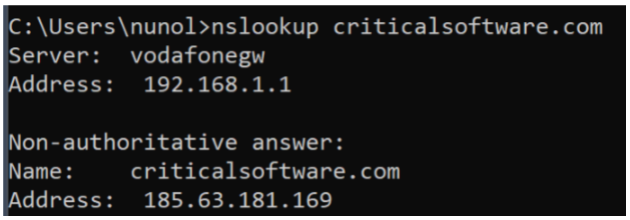
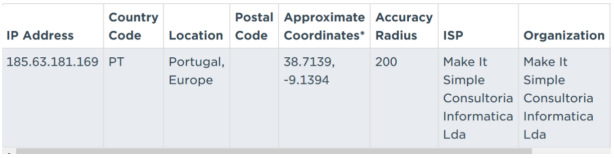


Figura 1: Comando nslookup para descobrir o ip do domínio indicado



IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization
185.63.181.169	PT	Portugal, Europe		38.7139, -9.1394	200	Make It Simple Consultoria Informatica Lda	Make It Simple Consultoria Informatica Lda

Figura 2: Informação de geolocalização e do ISP do servidor principal

MX Lookup for criticalsoftware.com:

Target	IP	Preference value	TTL
mxfilter1.criticalsoftware.com	13.94.118.236	5	1 hrs

Figura 3: Website que permite descobrir o IP do servidor de email

O grupo identificou três pessoas de interesse que figuram, atualmente, nos quadros da empresa, Gonçalo Quadros (CEO) , João Carreira(Chairman) e João Cunha(CTO), que é responsável pelo setor de tecnologia.

Gonçalo Quadros é o CEO da empresa que co-fundou em 1998. Licenciou-se em Engenharia Eletrónica, na especialidade de Ciências da computação e, posteriormente, obteu um doutoramento na universidade de Coimbra em 2002. É CEO da empresa desde 2005 (com uma breve interrupção entre 2012 e 2014). Iniciou a sua carreira em 1986, num projeto de sistemas de informação para o banco BES, seguindo-se um período de três anos onde trabalhou para a EDP. Após este período desenvolveu o primeiro sistema de informação para uma fábrica de papel (SOPORCEL). Após o desenvolvimento deste sistema, foi professor nas universidades de Aveiro e Coimbra até 1998, altura em que fundou e integrou a empresa *Critical Software*.

Foi possível encontrar um email associado a esta pessoa:

- goncalo.quadros@criticalsoftware.com

É praticamente inativo em redes sociais, o que dificultou a coleta de informação extra (apenas possui uma conta de *LinkedIn* com pouca informação e uma conta de *Twitter* praticamente não usada).

João Carreira é o *Chairman* e líder da secção de estratégia empresarial. Co-fundou a empresa em 1998. Possui um doutoramento em Ciências da computação pela universidade de Coimbra e um *MBA* em Comercialização de Tecnologia pela Universidade do Texas, de Austin e de Lisboa. Trabalhou na Siemens e na Accenture a partir de 1992 e trabalhou afincadamente na matéria de computação distribuída e tolerância a faltas em Portugal, na Escócia e na Holanda. Em 1998, ao se tornar co-fundador da empresa, assume o cargo de CEO até 2005 (altura em que é substituído por Gonçalo Quadros). A partir de 2005, focou-se na expansão estratégica do grupo Critical, no qual se inclui a empresa que estámos a abordar.

Foi possível encontrar dois emails associados a esta pessoa:

- carreirajoao@gmail.com
- jcarreira@criticalsoftware.com

A pesquisa nas redes sociais de João Carreira, deu a ideia de que seria casado e com filhos, apesar de, mesmo pesquisando nos comentários às suas publicações, ser difícil de afirmar com certeza.

João Paulo Macedo Cunha formou-se na Universidade de Engenharia do Porto (FEUP). Atualmente reside no Porto, tendo já vivido em Braga. Através de pesquisa nas redes sociais, foi possível descobrir que é casado, com filhos.

Foi possível encontrar dois emails associados a esta pessoa:

- joao.macedo.cunha@googlemail.com
- jpcunha@criticalsoftware.com

2.2 *Ponto25 Informática*

A *Ponto25* Informática foi fundada em 1997, por Alexandre Lobo (*CEO*), e tem vindo a desenvolver produtos de *software*, junto das empresas. As soluções desenvolvidas são mais direcionadas para as *PME's*, que necessitam de gestão integrada simples e eficiente, na medida em que tenta responder às principais necessidades do seu mercado.

Agora, iremos enumerar as seguintes informações encontradas sobre a empresa:

1. **Domínio:** ponto25.com
2. **Endereço:** Rua Augusto Veloso, 215. 4705-082, Braga, Portugal
3. ***CEO*:** Alexandre Lobo
4. **Responsável pelo domínio:** Claranet Portugal Telecomunicacoes S.A.
5. **Responsável pelos endereços IP's:** Claranet Portugal Telecomunicacoes S.A.

Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization
PT	Portugal, Europe		38.7139, -9.1394	200	Claranet Portugal Telecomunicacoes S.A.	Claranet Portugal Telecomunicacoes S.A.

Figura 4: Informação de geolocalização e do ISP do servidor principal

6. **Endereço IP do servidor principal:** 188.93.227.87

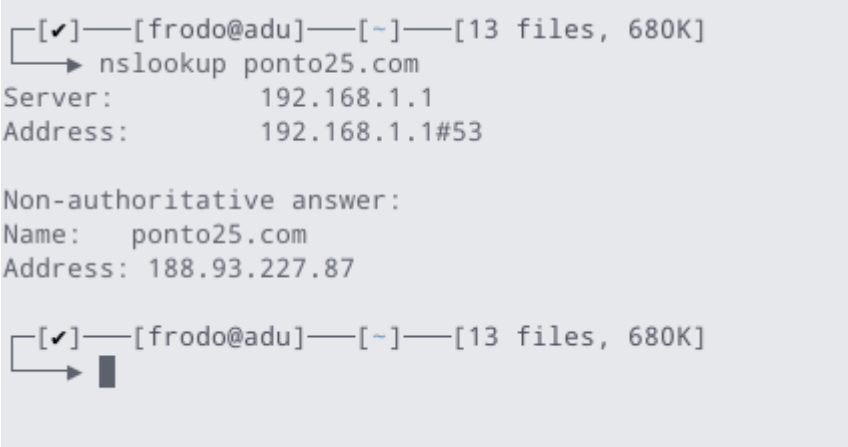


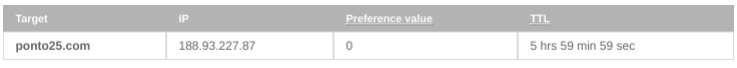
Figura 5: Comando nslookup para descobrir o ip do domínio indicado

7. **Localização do Servidor Web:** Latitude: 38.7139, longitude: -9.1394

8. **Tecnologias Utilizadas:**

   (a) *Windows Azure*
   (b) *HTML*
   (c) *Windows*
   (d) *ASP.NET MVC*
   (e) *Java*
   (f) *C#*
   (g) *Visual C#*
   (h) *SQL Server*
   (i) *.NET*
   (j) *ASP.NET*
   (k) *ASP.NET AJAX*
   (l) *JavaScript*
   (m) *Visual Basic*

9. Finalmente, foi feita a pesquisa do endereço IP do servidor de e-mail, tendo-se obtido o mesmo endereço que o principal.



Target	IP	Preference value	TTL
ponto25.com	188.93.227.87	0	5 hrs 59 min 59 sec

Figura 6: Website que permite descobrir o IP do servidor de email

Para além disto, o grupo encontrou também informações sobre duas pessoas de interesse, sendo estas, Alexandre Lobo (*CEO*) e Vânia Lima (*Marketing Manager*).

Começando pelo Alexandre Lobo, este viveu no Rio de Janeiro, onde iniciou a sua formação académica num setor educacional conhecido como *Estácio*. Um dos maiores e mais respeitados grupos do setor educacional do Brasil, que atua há cerca de 48 anos no segmento do ensino superior. De seguida, mudou-se para Braga, Portugal, onde continuou o seu percurso académico na Universidade do Minho em 1992. Em 1997 fundou então a empresa *Ponto25*, sendo atualmente o *CEO* da mesma. Para além disto, foi também programador/sócio fundador da empresa *Informdisk, ltda*, no Brasil, e programador na empresa ABC Braga Informática, Lda, em Portugal. Finalmente, o sujeito aparenta possuir algumas competências e recomendações, tais como: desenvolvimento de *software*, gestão de projetos e computação em nuvem.

Por último, foi possível ainda descobrir o endereço de e-mail usado por este, nas suas redes sociais, sendo: alexandre.lobo@ponto25.pt.

Posto isto, foi tudo o que conseguimos encontrar sobre Alexandre Lobo, através dos seus perfis públicos do *LinkedIn* e *Facebook*, e também de algumas notícias online. Segue-se então Vânia Lima, que foi porta-voz, juntamente com Alexandre Lobo, numa entrevista recente sobre a empresa.

Vânia Lima, atualmente *Marketing Manager* na empresa *Ponto25*, iniciou o seu percurso académico no ensino superior no Instituto Politécnico de Bragança, onde tirou a licenciatura em Marketing, em 2013. Continuou o seu percurso no *Factory Braga* na área do Marketing Digital, até 2016. Começou a trabalhar na *Ponto25* em 2014, depois de ter alguma experiência com várias empresas como *freelancer*.

Por último, isto foi tudo o que conseguimos encontrar sobre estas duas personalidades de interesse, consoante todo o tipo de informações públicas que estes disponibilizaram.

3 Reflexão sobre estratégias para ocultar informação

Uma primeira estratégia, que se pode aplicar para ocultar informação relevante dos mecanismos de busca passiva, é a utilização de um mecanismo tipo "***proxy***", ou seja, fazer com que exista uma informação intermédia entre a informação verdadeira e a pessoa que tenta descobrir a mesma. Desta forma, essa informação intermédia seria a que iria ser apresentada à pessoa que fez o pedido (*whois* por exemplo), sendo informação que não faz sentido para a mesma, visto que a única informação relevante é a forma como irá ser ligada à informação verdadeira.

Uma segunda estratégia seria ser seletivo em relação à informação que uma empresa transmite para fora, principalmente no seu *website*, podendo, por exemplo, ocultar a secção de tecnologias utilizadas para que não seja possível mapear o tipo de serviços que a empresa utiliza. Isto iria fazer com que apenas candidatos a uma oferta de emprego da empresa soubessem qual a tecnologia em que iriam trabalhar e, sendo assim, não resolveria completamente o problema, mas certamente dificultava a coleta dessa informação, visto que seria necessário investigar várias ofertas de emprego, para ter acesso a todas ou maior parte das tecnologias utilizadas.

Por outro lado, como foi possível verificar, é possível obter uma série de informações irrelevantes, da perspetiva de segurança, somente a partir do ISP. Isto porque, sempre que possível devem ser usados nomes e informações de contacto genéricas.

Vimos também que as *queries* sobre os recursos DNS, fornecem bastante informação ao atacante, de uma forma muito prática. Por isso, os servidores DNS têm que ser cuidadosamente implementados, de modo a não disponibilizar mais informação do que a que é suposto.

4 Conclusão

A realização deste trabalho prático permitiu-nos ganhar sensibilidade para a facilidade com que se consegue obter informação sobre uma empresa e as suas pessoas de interesse, que é uma parte vital no ciclo de realização de um ataque. É notório que, cada vez mais, devem ser aplicadas diferentes e mais fortes estratégias e mecanismos no sentido de combater estas técnicas de Engenharia Social.

Mesmo assim, de hoje em dia, a coleta de informação sobre uma dada empresa que já aplique algum mecanismo para esconder a sua informação, já não é tão fácil, o que, de certa forma, nos dificultou a tarefa de coletar informações sobre as empresas que escolhemos, visto que, apesar de algumas informações serem de fácil acesso, outras requerem muita pesquisa cruzada, ou seja, ir retirando informação intermédia sucessivamente que permita chegar a um ponto onde a informação que queremos é encontrada, como por exemplo, a partir do perfil do *LinkedIn*, coletar o *link* do mesmo, pesquisá-lo num *website* de busca de emails através desse link, obter o email e com o email pesquisar em redes sociais, para coletar informação adicional.

Concluindo, na nossa ótica, o relatório que apresentámos contém bastante informação de qualidade, apesar de que, não conseguimos encontrar toda a informação interessante, como seriam os números de telemóvel das pessoas de interesse por exemplo, que mesmo com pesquisas em redes sociais, em websites pessoais e em motores de busca, não nos foi possível coletar.