Universidade do Minho

Mestrado Integrado em Engenharia Informática

Tecnologia de Segurança

TP2-Parte A: Coleta Passiva de Informações

(Nota importante: O trabalho é para ser realizado nas aulas PL correspondentes.)

1. Objectivos

O principal objectivo deste trabalho é o estudo de Coleta passiva de informações (*Passive Information Gathering*, através das seguintes técnicas: (i) análise de informações de registo do domínio; (ii) análise da página web; e (iii) busca de informações na internet.

Na primeira parte deste estudo é realizada a escolha de um domínio web para análise de informações disponíveis. São analisadas as coleções de páginas web pertencentes ao domínio em busca de informações relevantes para a construção de um documento contendo informações sobre o domínio analisado.

2. Coleta Passiva de Informações

Com o objetivo de obter um conjunto de informações a respeito do domínio em questão é necessário entender como funciona o registro de domínios e IP's na internet. Para aceder a uma página web um utilizador insere o nome do domínio no navegador web (*Chrome, Firefox, Edge, Safari,* etc) e o mesmo deve ser traduzido para um endereço IP de onde está hospedado o Site Web. Esta tradução é efetuada pelo serviço de resolução de nomes (DNS – *Domain Name Service*). Para entender o processo necessário para aceder ao domínio "di.uminho.pt", o mesmo deve ser analisado em partes. O domínio "di.uminho.pt" é composto de três partes: (i) Top-level Domain (TLD) "di.uminho.**pt**" – o domínio de topo, definido pela Internet *Corporation for Assigned Names and Numbers* (ICANN[1].) pode ser genérico (.com, .org, etc.) ou associado a países, como por exemplo ".pt", ".es", ".br"; (ii) *Second-level domain* "di.**uminho**.pt" – o domínio de segundo nível é registrado junto a empresas acreditadas e atribuídas pelo ICANN e que são responsáveis por manter o TLD. Neste caso o domínio é registado junto ao DNS.pt[2] ou a outra empresa acreditada pela ICANN; (iii) *Third-level domain* "**di**.uminho.pt" – é criado pela entidade detentora do domínio "uminho.pt", sendo neste caso a Universidade do Minho. Após a tradução do domínio "di.uminho.pt" em um endereço IP o navegador web realiza a conexão ao servidor onde encontram-se disponíveis os ficheiros web. Para a análise de informações sobre domínios e endereços IP's existe o utilitário *WHOIS* [3] que pesquisa informações sobre a titularidade de domínios e endereços IP's. Existem versões do utilitário para diversos sistemas operativos, ou ainda uma versão online [4] pode ser utilizada. A Figura 1 exibe as informações retornadas pelo utilitário WHOIS no domínio "uminho.pt".

---

[1] https://www.icann.org/resources/pages/welcome-2012-02-25-en

[2] dns.pt

[3] https://whois.icann.org/en/about-whois

[4] https://www.whois.com/whois/

```
Nome de domínio / Domain Name: uminho.pt
Data de registo / Creation Date (dd/mm/yyyy): 29/06/1995
Data de expiração / Expiration Date (dd/mm/yyyy): 03/07/2022
Estado / Status: ACTIVE

Titular / Registrant
   Universidade do Minho
   Campus de Gualtar
   Braga
   4710-057 Braga
   Email: sec@scom.uminho.pt

Entidade Gestora / Billing Contact
   Universidade do Minho
   Email: sec@scom.uminho.pt

Responsável Técnico / Tech Contact
   Universidade do Minho
   Email: sec@scom.uminho.pt

Nameserver Information
   Nameserver: uminho.pt       NS      dns3.uminho.pt.
   Nameserver: uminho.pt       NS      dns.uminho.pt.
   Nameserver: uminho.pt       NS      ns02.fccn.pt.
   Nameserver: uminho.pt       NS      dns2.uminho.pt.
   Nameserver: dns3.uminho.pt. A       193.137.16.65
   Nameserver: dns.uminho.pt.  A       193.137.16.75
   Nameserver: dns3.uminho.pt. AAAA    2001:690:2280:1::65
   Nameserver: dns2.uminho.pt. A       193.137.16.145
```

Figura 1 - Saída do comando WHOIS uminho.pt

Outras informações podem ser obtidas através do uso de ferramentas como: *nslookup, host* para a obtenção do endereço IP responsável pelo servidor[5]. Com posse desta informação é possível obter dados sobre o endereço IP através do WHOIS, ou ainda a localização geográfica através de serviços web[6]. A Figura 2 relaciona o endereço IP com uma base de dados geográfica, e a Figura 3 exibe a saída do WHOIS para o IP 193.136.19.20 (di.uminho.pt).

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization
193.136.19.20	PT	Braga, Braga, Portugal, Europe	4700-000	41.5503, -8.4201	200	Fundacao para a Ciencia e a Tecnologia, I.P.	Universidade do Minho

Figura 2 - Análise do endereço IP através de uma ferramenta de Geolocalização.

[5] http://ping.eu/nslookup/

[6] https://www.maxmind.com/en/geoip-demo

```
% Information related to '193.136.16.0 - 193.136.19.255'

% Abuse contact for '193.136.16.0 - 193.136.19.255' is
'report@csirt.uminho.pt'

inetnum:        193.136.16.0 - 193.136.19.255
netname:        PTUMGUA-1
descr:          Universidade do Minho
descr:          Centro de Informatica
descr:          Campus de Gualtar
descr:          Braga
country:        PT
geoloc:         41.550541 -8.426542
admin-c:        RCUD2-RIPE
tech-c:         RCUD2-RIPE
status:         ASSIGNED PA
org:            ORG-UDM20-RIPE
remarks:        SERVIP-UMINHO
mnt-by:         AS1930-MNT
mnt-lower:      AS1930-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2017-03-27T12:19:22Z
source:         RIPE

organisation:   ORG-UDM20-RIPE
org-name:       Universidade do Minho
org-type:       OTHER
address:        Campus de Gualtar
address:        4710-057 Braga
address:        PORTUGAL
phone:          +351 253604020
fax-no:         +351 253604021
admin-c:        RCUD2-RIPE
tech-c:         RCUD2-RIPE
mnt-by:         AS1930-MNT
mnt-ref:        AS1930-MNT
abuse-c:        CUDM3-RIPE
abuse-mailbox:  report@csirt.uminho.pt
created:        2014-01-20T18:29:59Z
last-modified:  2017-07-29T11:04:41Z
source:         RIPE # Filtered

role:           RCTS Contacts Universidade do Minho
address:        Universidade do Minho
address:        Campus de Gualtar
address:        4710-057 Braga
address:        PORTUGAL
abuse-mailbox:  report@csirt.uminho.pt
admin-c:        PVC8-RIPE
tech-c:         PVC8-RIPE
tech-c:         JMG41-RIPE
tech-c:         PAG10-RIPE
tech-c:         UAC8-RIPE
nic-hdl:        RCUD2-RIPE
mnt-by:         AS1930-MNT
created:        2015-04-25T22:10:25Z
last-modified:  2017-07-29T11:05:40Z
```

Figura 3 - Saída do comando WHOIS no endereço IP 193.136.19.20

Para a análise da página web um navegador deve ser utilizado para efetuar a busca de informações que podem ser relevantes na construção do relatório. No *link* "Não Docentes" do domínio *di.uminho.pt* podemos analisar as informações de quem é a equipa técnica responsável pelo departamento, conforme mostra a Figura 4.

Figura 4 - Reprodução do Link: http://di.uminho.pt/nao_docentes.html

As duas etapas anteriores devem resultar em informações de responsáveis pelos domínios, IP's e página Web, tornando assim possível a realização de consultas em ferramentas de buscas na Internet. Alguns dessas ferramentas são: *Google, Facebook, LinkedIn,* páginas Web de divulgação de empregos, etc.

Atividade:

Escolha duas empresas (uma grande corporação e um negócio local) para realizar buscas de informações que levem ao footprint dos seus domínios na Internet. Identifique e descreva as estratégias usadas, assim como as possíveis diferenças de postura adotadas pelos domínios estudados. Enriqueça a sua análise apontando estratégias destinadas a ocultar informações relevantes aos mecanismos de busca passiva

Bibliografia

Hacking Exposed 7- Stuart McClure, Joel Scambray, and George Kurtz Default Book Series. 2012.
The Social Engineer's Playbook : A Practical Guide to Pretexting. Jeremiah Talamantes. Hexcode Publishing; 1 edition, 2014.