

UNPSJB

LICENCIATURA EN SISTEMAS OPGCPI

ADMINISTRACIÓN DE REDES Y SEGURIDAD

---

## Trabajo Práctico 2

**Footprinting - Fingerprinting - Escaneo - Enumeración - Firewall**

---

Cátedra

Lic. Bruno Damián Zappellini

Integrantes:

Luciano Serruya Aloisi

4 de octubre de 2018



## Índice

<b>1. <i>Footprinting</i></b>	<b>2</b>
<b>2. <i>Fingerprinting</i></b>	<b>5</b>

# 1. *Footprinting*

El término *Footprinting* se refiere al proceso de recolectar la mayor cantidad de información posible sobre un sistema objetivo con el fin de encontrar formas de penetrarlo [3]. Este etapa previa a realizar un ataque, conocida como *fase de reconocimiento*, el atacante intenta encontrar información como [4]:

- Rango de Red y sub-red (*Network Range* y *subnet mask*)
- Acertar máquinas o computadoras activas
- Puertos abiertos y las aplicaciones que están corriendo en ellos
- Detectar versiones de sistemas operativos
- Nombres de Dominios (*Domain Names*)
- Bloques de Red (*Network Blocks*)
- Direcciones IP específicas
- País y ciudad donde se encuentran los servidores
- Información de contacto (números telefónicos, emails)
- *DNS records*

Mucha de la información antes mencionada, como Domain Names, algunas direcciones IP, país, ciudad, e información de contacto puede ser conseguida consultando a las bases de datos de *whois*. Esto se realiza justamente con el comando *whois* y el nombre del *dominio* al cual se quiere consultar. Por ejemplo, si se desea conocer información sobre el dominio *facebook.com*, se debe realizar la siguiente invocación a *whois*:

```
1 whois facebook.com
```

Además del comando *whois*, que recupera información detallada sobre el dominio consultado (quién es su dueño, fecha de registro, fecha de expiración, entre otros), otras herramientas para hacer consultas a DNS son los comandos *nslookup* y *dig*. Para hacer *enumeración de DNS* (obtener todos los subdominios registrados bajo un dominio) existen herramientas como *fierce*, *dnsrecon*, o *dnsenum* [1].

*Elija dos organizaciones cualesquiera y utilizando WHOIS y DIG, averigüe toda la información que pueda: servidores de correo, servidores DNS, Servidores WEB, etc*

Dentro del directorio “assets” se incluye un *script* nombrado “footprinting.sh”, el cual recibe un nombre de dominio y realiza varias consultas con los comando dig y whois. A continuación se incluye un ejemplo de ejecución con el dominio *github.com* y las partes más importantes de su salida

```
1    bash footprinting.sh github.com
2
3    >>>
4
5    *** dig -t NS +short github.com ***
6    ns3.p16.dynect.net.
7    ns1.p16.dynect.net.
8    ns4.p16.dynect.net.
9    ns-520.awsdns-01.net.
10   ns-1283.awsdns-32.org.
11   ns2.p16.dynect.net.
12   ns-1707.awsdns-21.co.uk.
13   ns-421.awsdns-52.com.
14
15   *** dig -t MX +short github.com ***
16   1 ASPMX.L.GOOGLE.com.
17   5 ALT1.ASPMX.L.GOOGLE.com.
18   5 ALT2.ASPMX.L.GOOGLE.com.
19   10 ALT3.ASPMX.L.GOOGLE.com.
20   10 ALT4.ASPMX.L.GOOGLE.com.
21
22   *** dig -t SOA +short github.com ***
23   ns1.p16.dynect.net. hostmaster.github.com. 1538412644
24   3600 600 604800 60
25
26   *** whois github.com ***
27   Domain Name: GITHUB.COM
28   Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
```

```
28 Registrar WHOIS Server: whois.markmonitor.com
29 Registrar URL: http://www.markmonitor.com
30 Updated Date: 2017-06-26T16:02:39Z
31 Creation Date: 2007-10-09T18:20:50Z
32 Registry Expiry Date: 2020-10-09T18:20:50Z
33 .
34 .
35 .
```

Visite el sitio <http://www.netcraft.net/> y pruebe la funcionalidad del mismo contra el dominio [www.unp.edu.ar](http://www.unp.edu.ar)

Algunos de los datos que indica sitio [www.netcraft.com](http://www.netcraft.com) sobre el dominio de la UNP son los siguientes:

- Título del sitio: *Universidad Nacional de la Patagonia San Juan Bosco*
- Visto por primera vez en *Junio de 1998*
- Lenguaje primario *español*
- Puntaje de 7 sobre 10 en *Netcraft Risk Rating*<sup>1</sup>
- Dominio *unp.edu.ar*
- Dirección IPv4 *170.210.88.21*
- Nameserver *chenque.unp.edu.ar*
- Administrador de DNS *hostmaster@unp.edu.ar*

Visite el sitio <http://www.archive.org/web/web.php> y pruebe la funcionalidad del mismo contra el sitio web de la UNP: [www.unp.edu.ar](http://www.unp.edu.ar). ¿Qué ventajas presenta esta herramienta respecto de otras herramientas de footprinting?

---

<sup>1</sup>Aunque algunos sitios tengan contenido no malicioso, *Netcraft Extension* puede asignar un valor alto de riesgo porque está siendo servido bajo un dominio recientemente agregado a la base de datos de *Netcraft*, porque el sitio nunca fue visto en la *Netcraft Web Server Survey*, o porque la red que sirve el sitio ha servido sitios fraudulentos en el pasado. Distintos factores son tomados en cuenta [2]

A diferencia de herramientas como *dig* y *whois*, el sitio *www.archive.org* se dedica a visitar sitios web y tomarles un *snapshot* de su estado actual. Al hacerle una consulta sobre algún sitio en particular, muestra los distintos cambios por los cuales ha pasado, pudiendo ver versiones anteriores. También brinda herramientas para visualizar la cantidad de archivos tipo MIME con los cuales ha contado el sitio (ya sean imágenes, hojas de estilo, archivos con código Javascript, y demás). Por último, recolecta y muestra las distintas *URLs* que publica el sitio, con los recursos a los cuales se pueden acceder a través de la *URL*.

## 2. *Fingerprinting*

- El sitio *www.google.com* utiliza como servidor web *Google Web Server (GWS)*, pero no se puede saber por las cabeceras HTTP de la respuesta qué versión de servidor usa
- El sitio *www.ing.unp.edu.ar* indica que está usando la versión 1.10.3 del servidor web *NginX*
- El sitio *www.microsoft.com* utiliza como servidor web *Apache*, pero no se puede saber por las cabeceras HTTP de la respuesta qué versión de servidor usa
- El sitio *serconex.juschubut.gov.ar* utiliza un servidor web *Microsoft-IIS*, versión 10.0

## Referencias

- [1] Nikos Danopoulos. *DNS Enumeration Techniques in Linux*. Nov. de 2016. URL: <https://resources.infosecinstitute.com/dns-enumeration-techniques-in-linux/>.
- [2] Netcraft LTD. *How does the Risk Rating work?* 2018. URL: <https://toolbar.netcraft.com/help/faq/index.html#riskrating>.
- [3] OpenCampus. *What is Footprinting*. URL: <https://www.greycampus.com/opencampus/ethical-hacking/what-is-footprinting>.
- [4] Victor Torres. *Footprinting (Reconocimiento)*. Mar. de 2012. URL: <http://ciberinfosystem.blogspot.com/2012/03/footprinting-reconocimiento.html>.