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


3 de octubre de 2018

# Índice

# 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 [2]. Este etapa previa a realizar un ataque, conocida como *fase de reconocimiento*, el atacante intenta encontrar información como [3]:

- 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].

# Referencias

[1] Nikos Danopoulos. *DNS Enumeration Techniques in Linux*. Nov. de 2016. URL: https://resources.infosecinstitute.com/dns-enumeration-techniques-in-linux/.

[2] OpenCampus. *What is Footprinting*. URL: https://www.greycampus.com/opencampus/ethical-hacking/what-is-footprinting.

[3] Victor Torres. *Footprinting (Reconocimiento)*. Mar. de 2012. URL: http://ciberinfosystem.blogspot.com/2012/03/footprinting-reconocimiento.html.