ADMINISTRACIÓN DE REDES Y SEGURIDAD

TRABAJO PRÁCTICO 2

October 15, 2018

Cátedra:
Lic: Zappellini, Bruno Damian

Integrantes:
Toledo Margalef, Pablo Adrian
UNPSJB - Trelew

Contents

1. FOOTPRINTING

¿Qué es footprinting?

Footprinting , también conocido como `reconocimiento` es una técnica utilizada para recolectar información sobre dispositivos y su entorno. Dentro de los métodos que se pueden utilizar se encuentran:

- Consultas DNS
- Identificación de sistema Operativo (nmap)
- Escaneo de puertos
- Querys de WHOIS
- google hacking

DIG y WHOIS

Se utilizaran las siguientes dos organizaciones

- Administración Federal de Ingresos Públicos
  - `afip.gov.ar`
- IBM
  - `ibm.com`

DIG: es una herramienta para realizar peticiones a servidores de nombres. tomando un nombre de dominio y realizando el lookup correspondiente.

WHOIS: herramienta que busca un nombre de dominio en la base de datos de ls RFC 3912, la base de datos que almacena la correspondencia entre usuarios registrados y nombres de dominio.

Realizamos las consultas utilizando `afip.gov.ar` y listamos los resultados

- name: ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS
- IP (dns lookup): 200.1.116.6
- Fecha de registro: 1997-05-26 00:00:00

- Fecha expiración: 2019-06-25 00:00:00
- Servidor de nombres: ns1.afip.gov.ar (200.1.116.10/32)
- Registrar: nicar

Ahora con `ibm.com`

- name: IBM.COM
- IP (dns lookup): 129.42.38.10
- Fecha de registro: 1986-03-19T05:00:00Z
- Fecha expiración: 2019-03-20T04:00:00Z
- Servidor de nombres: EUR2.AKAM.NET
- Registrar: CSC Corporate Domains, Inc.

NETCRAFT - www.unp.edu.ar

Realizamos la consulta en `netcraft.net` sobre `www.unp.edu.ar` y listamos algunos datos que se muestran allí.

Site title	Universidad Nacional de la Patagonia San Juan Bosco
Date first seen	June 1998
language	Spanish
Description	Sitio web de la Universidad Nacional de la Patagonia San Juan Bosco.
Netcraft Risk Rating	7/10
Netblock Owner	Red de Interconexion Universitaria
Nameserver	chenque.unp.edu.ar
IP address	170.210.88.21 (VirusTotal)
DNS admin	hostmaster@unp.edu.ar
Hosting company	unp.edu.ar
Top Level Domain	Argentina (.edu.ar)
Hosting country	AR

archive.org

Este sitio ofrece, una snapshot del sitio que se busque. Proviendo las cualidades, casi, completas que nos ofrecía. De este modo, si en algún momento se dejó al descubierto alguna información de valor y se realizó la snapshot, ese dato está disponible, por más que se haya cambiado en el sitio real.

Fingerprinting

- **www.google.com.ar**: gws ()
- **www.ing.unp.edu.ar**: nginx/1.10.3
- **www.microsoft.com**: Apache
- **www.google.com.ar**: Microsoft-IIS/10.0

SECCIÓN 2

Scanning

Consiste en la búsqueda exhaustiva de diversas cuestiones a determinado nivel o niveles para encontrar vulnerabilidades.

El **escaneo de hosts** se realiza dentro una subred y permite enumerar los dispositivos que se encuentran conectados a ella. Teniendo como objetivo un equipo en particular, se puede realizar un **escaneo de puertos** de forma tal que se puede saber qué puertos se encuentran abiertos y disponibles para inciar una conexión.

Cuando se cuenta con red de Wi-Fi se puede realizar un **escaneo de redes Wi-Fi** para identificar las redes disponibles y poder hacer algún ataque a alguna en particular. Lo mismo se puede hacer cuando se tiene conectividad por bluetooh, listando los dispositivos disponibles para atacar.

Posibilidad de escaneo

- Sólo manipulando ARP: Escaneo de Hosts. Requiere estar en el mismo segmento de red.
- Sólo manipulando ICMP: Escaneo de puertos y host. No requiere estar en la misma red.

- Sólo manipulando TCP: Escaneo de puertos. No requiere estar en la misma red.
- Sólo manipulando UDP: Escaneo de puertos. No requiere estar en la misma red
- Interpretando tráfico: Escaneo de Wi-Fi, Bluetooth. Hosts y puertos. Se puede estar fuera de la red, en el caso de las radiofrecuencias. Salvo para LAN, ahí es mandatorio estar dentro de alguna red.

Escaneo de puertos

En la máquina virtual provsita por la cátedra, como primera medida, ponemos a funcionar el servicio de ssh, que atiende en el puerto 22 y corremos el comando netstat para verificar la existencia de puertos abiertos.

```
root@kali:~# netstat -nltp4
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1645/sshd
```

Luego, utilizando `nmap` escaneamos por puertos TCP que se encuentren abiertos.

```
root@kali:~# nmap -sV localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-15 18:22 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Como se puede observar, el puerto 22 (propio de ssh) fue detectado por nmap.

Seguidamente, le pedimos a `nmap`, explicitamente, que escanee los 65536 puertos disponibles.

```
root@kali:~# nmap -p0-65535 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-15 18:52 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65535 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

Escaneo manual de puertos

hping3 -c 3 -S -p 80 localhost: en la salida del analizador de protocolos se observa que el host responde con la bandera de `reset`. Indicando que el puerto está cerrado. En este caso se realiza un escaneo de tipo SYN. Ya que sólo se envía un paquete con la bandera `SYN`, imitando el inicio de una conexión.

Bibliography

[1] Wikipedia. *Footprinting*. Oct. 2018. URL: https://en.wikipedia.org/wiki/Footprinting.