FOOTPRINTING


GRAY HAT
BLACK HAT
HACKER
GOLDEN HAT
WHITE HAT

Es la técnica utilizada para reunir información sobre sistemas informáticos (objetivo) de entidades u organizaciones. La información es muy útil para proteger contra de intrusiones.

Activa

Cuando se tiene interacción directa con la organización, proceso de auditoría.

Pasiva

Cuando no tenemos interacción con el cliente, los datos que obtenemos es por medio de herramientas de búsquedas para obtener información de página web, ip del sitio, numero de puertos abiertos, etc.

Página web u organizaciones relacionadas (wget del sitio, www.archive.org)

Empleados de la empresa (Ingeniería social)

Motores de búsqueda (Goodady - Google - Droks)

Herramientas de Google (Toolbox)

Análisis de metadatos (Obtenidos mediante imágenes)

Consultas a DNS (dig - fierce)

Reconocimiento IP y puertos (whois - www.ip2location.com - nmap)

Consultas DNS

```
hugo@hugo:/$ dig www.fce.unam.edu.ar

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.fce.unam.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34020
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.fce.unam.edu.ar.           IN      A

;; ANSWER SECTION:
www.fce.unam.edu.ar.    172799  IN      CNAME   sitio-fce.fce.unam.edu.ar.
sitio-fce.fce.unam.edu.ar. 172800 IN    A       170.210.194.143

;; AUTHORITY SECTION:
fce.unam.edu.ar.        13028   IN      NS      ns2.unam.edu.ar.
fce.unam.edu.ar.        13028   IN      NS      ns.unam.edu.ar.
```

Consultas DNS

```
hugo@hugo:/$ dig marandu.com.ar

; <<>> DiG 9.10.3-P4-Ubuntu <<>> marandu.com.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54411
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;marandu.com.ar.                        IN      A

;; ANSWER SECTION:
marandu.com.ar.         3429    IN      A       138.117.79.55

;; AUTHORITY SECTION:
marandu.com.ar.         3291    IN      NS      ns2.marandu.com.ar.
marandu.com.ar.         3291    IN      NS      ns.marandu.com.ar.
```

Consultas DNS

```
sudo ./fierce.pl -dns unam.edu.ar -wordlist host.txt
```

```
Checking for wildcard DNS...
        ** Found 93297203330.unam.edu.ar at 34.234.89.0.
        ** High probability of wildcard DNS.
Now performing 1594 test(s)...
192.100.186.10  www.mupum.unam.edu.ar
192.100.186.11  webs.unam.edu.ar
192.100.186.12  whois.unam.edu.ar
192.100.186.13  webs2.unam.edu.ar
192.100.186.14  facfor.unam.edu.ar
192.100.186.15  acceso.unam.edu.ar
192.100.186.16  conectandofuturo.unam.edu.ar
```

Consultas DNS

```
170.210.197.132 fayd.unam.edu.ar
170.210.197.133 nodal.unam.edu.ar
170.210.197.134 www.mamcyp.unam.edu.ar
170.210.197.135 www.diplomas.unam.edu.ar
170.210.197.136 www.transmedia.unam.edu.ar
170.210.197.140 vicario.unam.edu.ar
170.210.197.144 virtual.fayd.unam.edu.ar
170.210.197.145 zm.unam.edu.ar
170.210.197.150 iguazu.unam.edu.ar
170.210.197.85  am.unam.edu.ar
```

Consultas WHOIS

```
hugo@hugo:~$ whois 192.100.186.10
```

```
inetnum:      192.100.186/23
status:       assigned
aut-num:      AS263235
abuse-c:      PMF2
owner:        Universidad Nacional de Misiones
ownerid:      AR-UNMI-LACNIC
responsible:  Marcelo Puerta
address:      Ruta Nacional, N°12, Km 7 1/2, Villa Lanus
address:      3304 - Posadas - MI
country:      AR
phone:        +54 376 4480200 [280]
```

Consultas WHOIS

```
hugo@hugo:~$ whois 192.100.186.10
```

```
nic-hdl:        PMF2
person:         Puerta Marcelo Fabian
e-mail:         marcelo.puerta@MAIL.UNAM.EDU.AR
address:        [redacted], Av. El Misionesro
address:        3300 - Posadas - Mn
country:        AR
phone:          +54  376154[redacted] [0]
```

Escaneos de puertos con NMAP

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos además posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos.

Enlace al sitio: https://nmap.org/

Escaneos de puertos con NMAP

Enlace al sitio: https://nmap.org/

Instalación:

Entorno de consola → apt-get install nmap

Entorno gráfico → apt-get install zenmap

Escaneos de puertos con NMAP

Parámetros:

-sT se intenta hacer un barrido de puertos por TCP

-sU se intenta hacer un barrido de puertos por UDP

-sP se intenta hacer un barrido de puertos por ICMP

-sS se usan mensajes de SYN

-sA se usan mensajes de ACK

-sV intenta identificar los servicios por los puertos abiertos

-sO con esta opción se identifica que protocolos de nivel superior a capa tres

Escaneos de puertos con NMAP

Parámetros:

-vv hacer la salida de la herramienta detallada en pantalla

-p se usa para especificar puertos de análisis o rango de puertos

-A Habilita la detección de SO y de versión

-PS realiza un barrido de puertos y enumera aquellos que tiene habilitado el bit SYN

-PA realiza un barrido de puertos y enumera aquellos que tiene habilitado el bit ACK

Escaneos de puertos con NMAP

Estados:

open: el puerto es accesible y hay un demonio escuchando.

closed el puerto es accesible pero no hay un demonio escuchando.

filtered el puerto no es accesible, un firewall filtra el puerto.

Escaneos de puertos con NMAP

Hosts sobre red local

```
hugo@hugo:~$ sudo nmap -sn 10.0.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-15 18:49 -03
Nmap scan report for 10.0.0.2
Host is up (0.0061s latency).
MAC Address: A4:5D:A1:63:B0:40 (ADB Broadband Italia)
Nmap scan report for 10.0.0.4
Host is up (0.038s latency).
MAC Address: 80:58:F8:12:DF:C9 (Unknown)
Nmap scan report for 10.0.0.5
Host is up (0.24s latency).
MAC Address: F0:99:BF:1A:AA:D6 (Apple)
Nmap scan report for 10.0.0.7
Host is up (0.24s latency).
```

Escaneos de puertos con NMAP

```
hugo@hugo:~$ sudo nmap -sS 170.210.194.240

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:37 -03
Nmap scan report for 170.210.194.240
Host is up (0.091s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
```

```
hugo@hugo:~$ sudo nmap -sS www.fce.unam.edu.ar

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:38 -03
Nmap scan report for www.fce.unam.edu.ar (170.210.194.143)
Host is up (0.11s latency).
Other addresses for www.fce.unam.edu.ar (not scanned): 2801:1a8:4::1
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
```

Escaneos de puertos con NMAP

```
hugo@hugo:~$ sudo nmap -PA 170.210.194.240

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:52 -03
Nmap scan report for 170.210.194.240
Host is up (0.18s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
```

```
hugo@hugo:~$ sudo nmap -PA www.fce.unam.edu.ar

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:50 -03
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.55 seconds
```

Escaneos de puertos con NMAP

```
hugo@hugo:~$ sudo nmap -sV 170.210.194.240

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:34 -03
Nmap scan report for 170.210.194.240
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
```

```
hugo@hugo:~$ sudo nmap -sV www.fce.unam.edu.ar

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-16 08:40 -03
Nmap scan report for www.fce.unam.edu.ar (170.210.194.143)
Host is up (0.091s latency).
Other addresses for www.fce.unam.edu.ar (not scanned): 2801:1a8:4::1
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
```

Escaneos de puertos con NMAP

Apache » Http Server » 2.2.22 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.2.22*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-7679	119		Overflow	2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
2	CVE-2017-7668	20			2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

Versión a la fecha: 2.4.35 (released 2018-09-22)

Escaneos de puertos con NMAP

Con parámetro -A

```
Reason: 998 no-responses and 1 admin-prohibited
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 52 Apache httpd 2.2.22 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|specialized|broadband router|media device
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (92%), HP embedded (88%), Crestron 2-Series (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:4 cpe:/h:hp:p2000_g3 cpe:/o:crestron:2_series cpe:/o:linux:l
inux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:3.x
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.13 (92%), Linux 3.10 - 3.19 (90%), Linux 3.18 (90%), Linux 3.2 - 4.0 (90%), HP P2000 G3 NAS de
vice (88%), Crestron XPanel control system (87%), Roku 2 XS media player (Linux 2.6.32) (86%), OpenWrt 12.09-rc1 Attitude Adj
ustment (Linux 3.3 - 3.7) (85%), Linux 3.8 (85%), XBMCbuntu Frodo v12.2 (Linux 3.X) (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.01%E=4%D=10/16%OT=80%CT=%CU=%PV=N%DS=10%DC=T%G=N%TM=5BC5DA93%P=x86_64-pc-linux-gnu)
SEQ(TI=Z%TS=A)
```

Enlace al contenido

HASTA PRONTO!!