

**Universidad Nacional de la Patagonia San Juan Bosco**

**Licenciatura en Sistemas O.P.C.G.P.I.**



**ARyS**

**TP N.º 2**

**Docentes: Mg. Ing. Ricardo Antonio López  
Lic. Cristian Javier Parise**

**Alumnos: Aguila Maximiliano  
Krmptic Lucas**

# TRABAJO PRACTICO Nº 2

## SECCION 1: FOOTPRINTING

1. ¿Qué es “Footprinting”?; liste distintos medios que se le ocurran que pueden llegar a ser utilizados para averiguar información de modo pasivo.

El Footprinting, también llamado “Reconocimiento”, es la primera etapa que se realiza antes de un ataque.

En ella, el atacante recolecta, reúne y organiza toda la información que puede sobre su víctima.

Su principal fuente es internet, aunque se pueden dar otras fuentes también.

Luego hay que filtrar toda esa información para quedarse con lo más importante (O lo que nos compete a lo que queremos hacer).

Alguna de la información que se busca obtener es:

- \_ Rango de Red y sub-red (Network Range y subnet mask)
- \_ Computadoras activas
- \_ Puertos abiertos y las aplicaciones que están corriendo en ellos
- \_ 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, etc.)
- \_ DNS records

Algunas herramientas de footprinting son:

- Netcraft
- Harvester
- Maltego
- Claves PGP
- Dorks

2. Elija dos organizaciones cualesquiera y utilizando WOHIS y DIG, averigüe toda la información que pueda: servidores de correo, servidores DNS, Servidores WEB, etc. (Consigne aquí al menos 8 datos de cada organización).

## Información del contacto

### Contacto del Registrante

Nombre: Sysadmin Team  
Organización: Stack Exchange, Inc.  
Dirección postal: 110 William St, Piso 28, Nueva York NY 10038 EE. UU.  
Teléfono: +1.2122328280  
Ext:  
Fax:  
Fax Ext:  
Correo electrónico: sysadmin-team@stackoverflow.com

### Contacto de


#### administrador

Nombre: Sysadmin Team  
Organización: Stack Exchange, Inc.  
Dirección postal: 110 William St, Piso 28, Nueva York NY 10038 EE. UU.  
Teléfono: +1.2122328280  
Ext:  
Fax:  
Fax Ext:  
Correo electrónico: sysadmin-team@stackoverflow.com


### Contacto técnico

Nombre: Sysadmin Team  
Organización: Stack Exchange, Inc.  
Dirección postal: 110 William St, Piso 28, Nueva York NY 10038 EE. UU.  
Teléfono: +1.2122328280  
Ext:  
Fax:  
Fax Ext:  
Correo electrónico: sysadmin-team@stackoverflow.com

3. 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). (Consigne aquí al menos 8 datos de la organización).

Título del sitio	Universidad Nacional de la Patagonia San Juan Bosco	Fecha de primera vista	Junio de 1998
Rango del sitio		Lenguaje primario	Español
Descripción	Sitio web de la Universidad Nacional de la Patagonia San Juan Bosco.		
Palabras clave	No presente		
Clasificación de riesgo de Netcraft [FAQ]	7/10 		

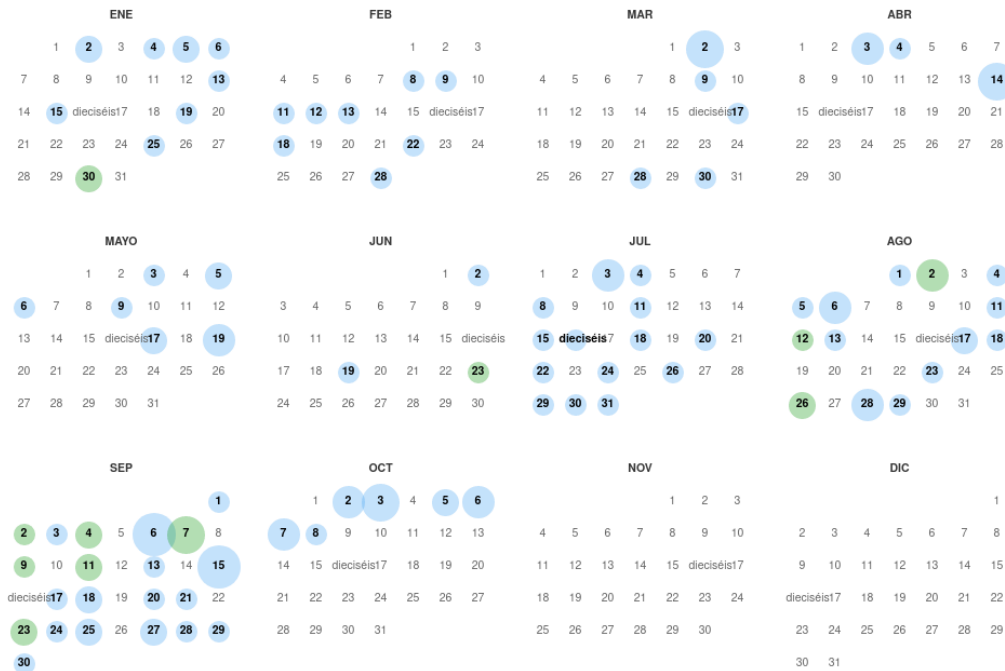
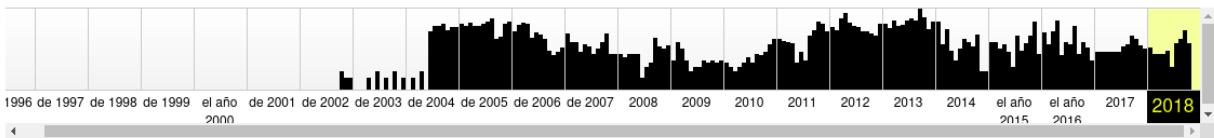
#### Red

Sitio	<a href="http://www.unp.edu.ar">http://www.unp.edu.ar</a>	Propietario de Netblock	<a href="#">Red de Interconexión Universitaria</a>
Dominio	<a href="http://unp.edu.ar">unp.edu.ar</a>	Nombre del servidor	chenque.unp.edu.ar
dirección IP	170.210.88.21 ( <a href="#">VirusTotal</a> )	Administrador de DNS	hostmaster@unp.edu.ar
Dirección IPv6	No presente	DNS inverso	desconocido
Registrador de dominios	desconocido	Organización del servidor de nombres	desconocido
Organización	desconocido	Compañía anfitriona	unp.edu.ar
Dominio de nivel superior	Argentina (.edu.ar)	Extensiones de seguridad DNS	desconocido
País anfitrión	 Arkansas		

4. 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?

\_\_Esta herramienta es útil para recabar información sobre cómo estaba construida la página en tiempos pasados y para recolectar datos que pudieran haber sido eliminados y que, por ende, no están actualmente disponibles en la página web.

No solamente datos, sino que posibles pasadas vulnerabilidades del sitio.



5. Haciendo fingerprinting de servidores HTTP en forma manual. Usando netcat realice las siguientes pruebas y conteste:

**# nc www.google.com.ar 80**

GET / HTTP/1.1

Host: www.google.com.ar

```
HTTP/1.1 200 OK
Date: Tue, 09 Oct 2018 00:28:41 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2018-10-09-00; expires=Thu, 08-Nov-2018 00:28:41 GMT; path=/; domain=.google.com.ar
Set-Cookie: NID=140=i7k74jOasH2Lw3iG6bxOSQcvMi9ifD5l1eWApMFQvDlJ84xbHSMGVrBr1ObRRJ5HzwE5yQk9jh4cIDVJVRgUz2qbNC_5kNKY1LEdxxbiCkhfNudZ14VDVYj4LMJIQW5C; expires=Wed, 10-Apr-2019 00:28:41 GMT; path=/; domain=.google.com.ar; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

GET /algo\_que\_no\_existe HTTP/1.1

Host: [www.google.com.ar](http://www.google.com.ar)

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1579
Date: Tue, 09 Oct 2018 00:44:44 GMT
```

# nc www.ing.unp.edu.ar 80

GET / HTTP/1.1

Host: [www.ing.unp.edu.ar](http://www.ing.unp.edu.ar)

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 09 Oct 2018 00:39:20 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Accept-Ranges: bytes
```

GET /algo\_que\_no\_existe HTTP/1.1

Host: [www.ing.unp.edu.ar](http://www.ing.unp.edu.ar)

```
HTTP/1.1 404 Not Found
Server: nginx/1.10.3
Date: Tue, 09 Oct 2018 00:42:21 GMT
Content-Type: text/html
Content-Length: 1181
Connection: keep-alive
Last-Modified: Thu, 05 Mar 2009 12:39:22 GMT
ETag: "524-49d-4645e75267280"
Accept-Ranges: bytes
Vary: Accept-Encoding
```

# nc www.microsoft.com 80

GET / HTTP/1.1

Host: [www.microsoft.com](http://www.microsoft.com)

```
HTTP/1.1 200 OK
Server: Apache
ETag: "6082151bd56ea922e1357f5896a90d0a:1425454794"
Last-Modified: Wed, 04 Mar 2015 07:39:54 GMT
Accept-Ranges: bytes
Content-Length: 1020
Content-Type: text/html
Date: Tue, 09 Oct 2018 00:46:28 GMT
Connection: keep-alive
```

GET /algo\_que\_no\_existe HTTP/1.1

Host: [www.microsoft.com](http://www.microsoft.com)

```
HTTP/1.1 404 Not Found
Cache-Control: private
Content-Type: text/html
CorrelationVector: PvajLl3+rUaMmLDe.1.0
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEORIGIN
X-EdgeConnect-Origin-MEX-Latency: 51
Strict-Transport-Security: max-age=31536000
P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo CNT COM INT NAV ONL PHY PRE PUR UNI"
Content-Length: 57433
X-EdgeConnect-Origin-MEX-Latency: 224
Date: Tue, 09 Oct 2018 00:48:49 GMT
Connection: keep-alive
Set-Cookie: MS-CV=PvajLl3+rUaMmLDe.1; domain=.www.microsoft.com; expires=Wed, 10-Oct-2018 00:48:49 GMT; path=/
X-RTag: RT
```

# nc serconex.juschubut.gov.ar 80

GET / HTTP/1.1

Host: serconex.juschubut.gov.ar

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /sys/inicio.aspx
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=oy3uvf5hdccghzu5qljafaxv; path=/; HttpOnly
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 09 Oct 2018 00:55:17 GMT
Content-Length: 133
```

GET /algo\_que\_no\_existe HTTP/1.1

Host: serconex.juschubut.gov.ar

```
HTTP/1.1 200 OK
Cache-Control: private
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=eunqjghwadivv5bp512jhecl; path=/; HttpOnly
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 09 Oct 2018 00:56:37 GMT
```

6. Puede identificar cuales son los productos que se están usando como servidor web en los 4 sitios y las versiones de los mismos mediante las respuestas obtenidas? ¿Cuál es la ultima versión de cada uno de ellos?

\_ Todos los sitios brindan informacion mas o menos especificas que otras.

[www.google.com.ar](http://www.google.com.ar) sobre un GWS

[www.ing.unp.edu.ar](http://www.ing.unp.edu.ar) sobre un Nginx 1.10.3

[www.microsoft.com](http://www.microsoft.com) sobre un Apache

[erconex.juschubut.gov.ar](http://erconex.juschubut.gov.ar) sobre un Microsoft-IIS 1.10

## SECCION 2 : ESCANEEO

1. ¿En qué consiste el escaneo o scanning? Evalúe la facilidad/dificultad de llevar a cabo cada uno de los siguientes tipos de escaneo y el valor de la información obtenida:

El escaneo es un conjunto de técnicas utilizadas para descifrar las características de la red de un sistema. Esto se hace mediante el ping de equipos, determinando rangos de red y escaneando puertos individuales del sistema, entre otras cosas.

### Escaneo de hosts

Es el “destino” al que apuntan los demás tipos de escaneo que se enuncian en este punto. Es decir, el escaneo de puertos se realiza en un host (Típicamente, aunque no sería loco pensar que se podría realizar para VARIOS hosts que estén conectados a un puerto específico, por ejemplo), el escaneo de redes wifi podría desembocar en una identificación de los hosts que están conectadas a las mismas, y el escaneo de los dispositivos bluetooth nos identifican los hosts que están utilizando ese medio para establecer conexiones.

### Escaneo de puertos

El escaneo de puertos puede llegar a tener una dificultad moderada, ya que la técnica a usar correcta dependerá de las características de la comunicación y del estado de la red en sí. Sin embargo, conociendo esto, el proceso es más bien simple y una vez logrado se obtiene la información sobre los puertos y los servicios disponibles, pudiendo a través de ellos encontrar vulnerabilidades en el sistema.

### Escaneo de redes WiFi

No es complicado de hacer, ya que casi todos los sistemas operativos nativamente soportan el escaneo de redes wifi (Con la condición de tener el hardware necesario para hacerlo). Podría llegar a aportar información valiosa si se deseara conocer el tipo de encriptación de alguna red en particular.

### Escaneo de dispositivos bluetooth

Tal como se dijo en el inciso anterior, no presenta mayor dificultad si uno tiene el driver necesario instalado en el sistema operativo y el hardware bluetooth. En este caso, la información que aporta no es tan rica como en el caso del escaneo de redes wifi. La única información que aporta es el nombre del dispositivo y el tipo de dispositivo (Que, de todas formas podría llegar a ser útil en la fase de descubrimiento).

2. Indique qué tipo de escaneo (hosts, puertos, vulnerabilidades, WiFi) es posible realizar:

- Sólo manipulando el protocolo ARP
- Sólo manipulando el protocolo ICMP
- Sólo manipulando el protocolo TCP
- Sólo manipulando el protocolo UDP
- Interpretando en forma pasiva tráfico de red (LAN o algún tipo de radiofrecuencias)

Sólo manipulando el protocolo ARP

Se podría realizar escaneos de hosts.

Sólo manipulando el protocolo ICMP

Se podría realizar escaneo de hosts y de puertos.

Sólo manipulando el protocolo TCP

Se podría realizar escaneo de hosts, puertos y vulnerabilidades.

Sólo manipulando el protocolo UDP

Se podría realizar escaneo de hosts y puertos únicamente.

Interpretando en forma pasiva tráfico de red (LAN o algún tipo de radiofrecuencias)

Se podría realizar escaneo de hosts, de puertos y de vulnerabilidades.

3. Para cada uno de los casos anteriores indique si para llevarlo a cabo es necesario estar en la misma red que están los hosts a los que se le está realizando el escaneo.

\_ Para realizar el escaneo manipulando el protocolo ARP y la interpretación pasiva del tráfico de red es necesario estar conectado a la misma red en la que se encuentran los demás hosts. Para las demás opciones no es necesario, ya que se puede especificar el host al que se le quiere enviar el mensaje (Que no necesariamente se encuentra dentro del mismo segmento de red).

## Escaneo de puertos

### a) Escaneo de puertos

El objetivo será realizar los escaneos desde la máquina virtual Kali hacia la máquina real u otra que el instructor pueda poner a disposición. Utilizaremos nmap para realizar escaneos utilizando diferentes técnicas.

Nota: para ver cómo usar nmap con las diferentes técnicas, ver <http://nmap.org/book/man-port-scanning-techniques.html>

Nota : Antes de empezar a realizar las pruebas determine qué puertos de la máquina real están abiertos y cuáles cerrados. Utilice el comando netstat: - Linux ejecute en la consola: netstat -nat (puertos TCP) / netstat -nau (puertos UDP) - En Windows ejecute en la CLI: netstat -na



```

➔ ~ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3389            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.111:51190     64.233.186.188:5228     ESTABLISHED
tcp6       0      0 :::1:5432                :::*                    LISTEN
tcp6       0      0 :::3389                  :::*                    LISTEN
➔ ~

```

```

➔ ~ netstat -nau
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.1.111:49812     64.233.186.189:443     ESTABLISHED
udp        0      0 0.0.0.0:5353            0.0.0.0:*               ESTABLISHED
udp        0      0 192.168.1.111:68        0.0.0.0:*               ESTABLISHED
udp        0      0 192.168.1.111:57472     64.233.190.189:443     ESTABLISHED
udp6       0      0 :::5353                  :::*                    ESTABLISHED
udp6       0      0 :::1:49159               :::1:49159              ESTABLISHED
➔ ~

```

Para realizar un escaneo de puertos TCP use el comando:

***nmap -sV <IP\_destino>***

Para realizar un escaneo de puertos UDP use el comando:

***nmap -sU <IP\_destino> -p <puerto abierto>***

***nmap -sU <IP\_destino> -p <puerto cerrado>***

4. Utilizando la máquina virtual provista por la cátedra, abra una terminal

de root y realice un escaneo de puertos TCP utilizando nmap a la IP local.

***Nmap 127.0.0.1***

```

bruno@kali:~$ nmap 127.0.0.1

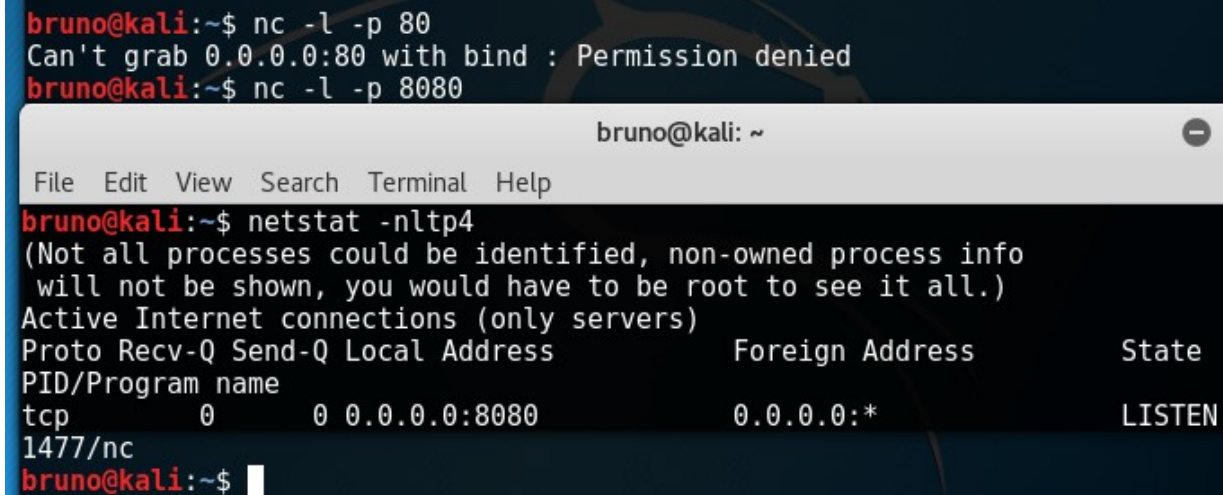
Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-09 15:17 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

```

Compruebe si los puertos detectados son los mismos que están corriendo en la máquina, los cuales puede consultar con el comando:

***netstat -nltp4***

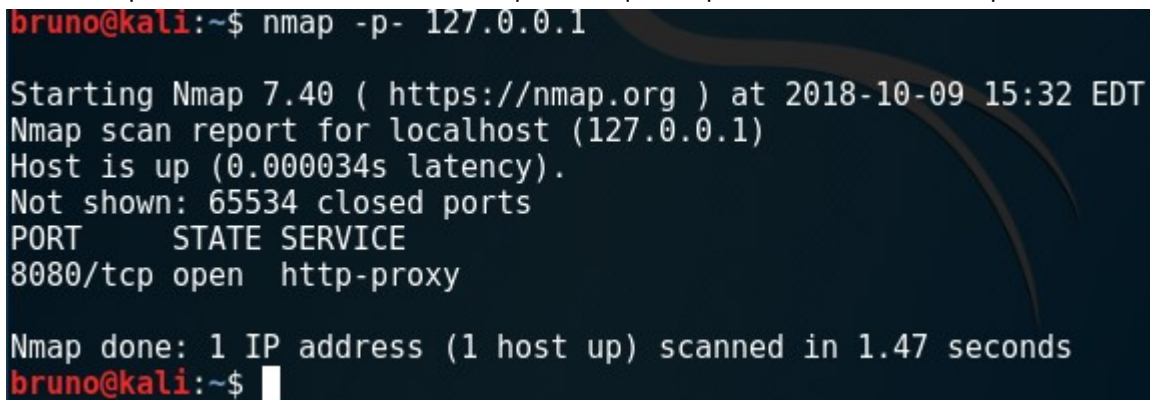
```
bruno@kali:~$ nc -l -p 80
Can't grab 0.0.0.0:80 with bind : Permission denied
bruno@kali:~$ nc -l -p 8080
```



```
bruno@kali:~$ netstat -nltp4
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:8080             0.0.0.0:*               LISTEN
1477/nc
bruno@kali:~$
```

5. En el ejercicio anterior, ¿Se detectaron como abiertos todos los puertos que estaban realmente abiertos? Utilice nmap indicando EXPLICITAMENTE que se requiere que se revisen todos los puertos TCP

```
bruno@kali:~$ nmap -p- 127.0.0.1
```



```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-09 15:32 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000034s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
bruno@kali:~$
```

6. Usando hping3 para realizar escaneo de puertos en forma manual:

- Abra dos terminales de root en ella máquina virtual, una para usar el comando hping3 para escanear como se indica a continuación y la otra para monitorear el tráfico involucrado en el escaneo, con el comando “tcpdump -i lo -n”.
- Escaneo del puerto TCP/80 de la maquina local (localhost)

***hping3 -c 3 -S -p 80 localhost***

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i lo -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
19:57:13.485666 IP 127.0.0.1.2736 > 127.0.0.1.80: Flags [S], seq 1462787338, win 512, length 0  
19:57:13.485680 IP 127.0.0.1.80 > 127.0.0.1.2736: Flags [R.], seq 0, ack 1462787339, win 0, length 0  
19:57:14.505553 IP 127.0.0.1.2737 > 127.0.0.1.80: Flags [S], seq 172038533, win 512, length 0  
19:57:14.505572 IP 127.0.0.1.80 > 127.0.0.1.2737: Flags [R.], seq 0, ack 172038534, win 0, length 0  
19:57:15.505855 IP 127.0.0.1.2738 > 127.0.0.1.80: Flags [S], seq 1978808657, win 512, length 0  
19:57:15.505874 IP 127.0.0.1.80 > 127.0.0.1.2738: Flags [R.], seq 0, ack 1978808658, win 0, length 0  
root@kali:~# hping3 -c 3 -S -p 80 localhost  
HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes  
len=40 ip=127.0.0.1 ttl=64 DF id=17070 sport=80 flags=RA seq=0 win=0 rtt=19.7 ms  
len=40 ip=127.0.0.1 ttl=64 DF id=17255 sport=80 flags=RA seq=1 win=0 rtt=6.2 ms  
len=40 ip=127.0.0.1 ttl=64 DF id=17344 sport=80 flags=RA seq=2 win=0 rtt=5.9 ms  
--- localhost hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 5.9/10.6/19.7 ms  
root@kali:~#
```

– ¿Qué significa la respuesta respecto del estado del puerto  
(abierto/cerrado)?

En los tres paquetes enviados por hping3 se puede ver que los tres se enviaron de 3 puertos diferentes. Y que, al estar cerrado el puerto, les fue devuelto un paquete RST.

Ahora, para una situación en la que el puerto 80 está abierto la salida es la siguiente:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i lo -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:03:10.505564 IP 127.0.0.1.2988 > 127.0.0.1.80: Flags [S], seq 1401160493, win 512, length 0  
20:03:10.505601 IP 127.0.0.1.80 > 127.0.0.1.2988: Flags [S.], seq 506434661, ack 1401160494, win 43690, options  
[mss 65495], length 0  
20:03:10.505614 IP 127.0.0.1.2988 > 127.0.0.1.80: Flags [R], seq 1401160494, win 0, length 0  
20:03:11.506557 IP 127.0.0.1.2989 > 127.0.0.1.80: Flags [S], seq 69482929, win 512, length 0  
20:03:11.506590 IP 127.0.0.1.80 > 127.0.0.1.2989: Flags [S.], seq 1179896494, ack 69482930, win 43690, options [mss 65495], length 0  
20:03:11.506602 IP 127.0.0.1.2989 > 127.0.0.1.80: Flags [R], seq 69482930, win 0, length 0  
20:03:12.507150 IP 127.0.0.1.2990 > 127.0.0.1.80: Flags [S], seq 1610535460, win 512, length 0  
20:03:12.507183 IP 127.0.0.1.80 > 127.0.0.1.2990: Flags [S.], seq 3383167610, ack 1610535461, win 43690, options [mss 65495], length 0  
20:03:12.507196 IP 127.0.0.1.2990 > 127.0.0.1.80: Flags [R], seq 1610535461, win 0, length 0  
root@kali:~# hping3 -c 3 -S -p 80 localhost  
HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes  
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=43690 rtt=1.0 ms  
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=43690 rtt=1.1 ms  
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=43690 rtt=1.0 ms  
--- localhost hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 1.0/1.0/1.1 ms  
root@kali:~#
```

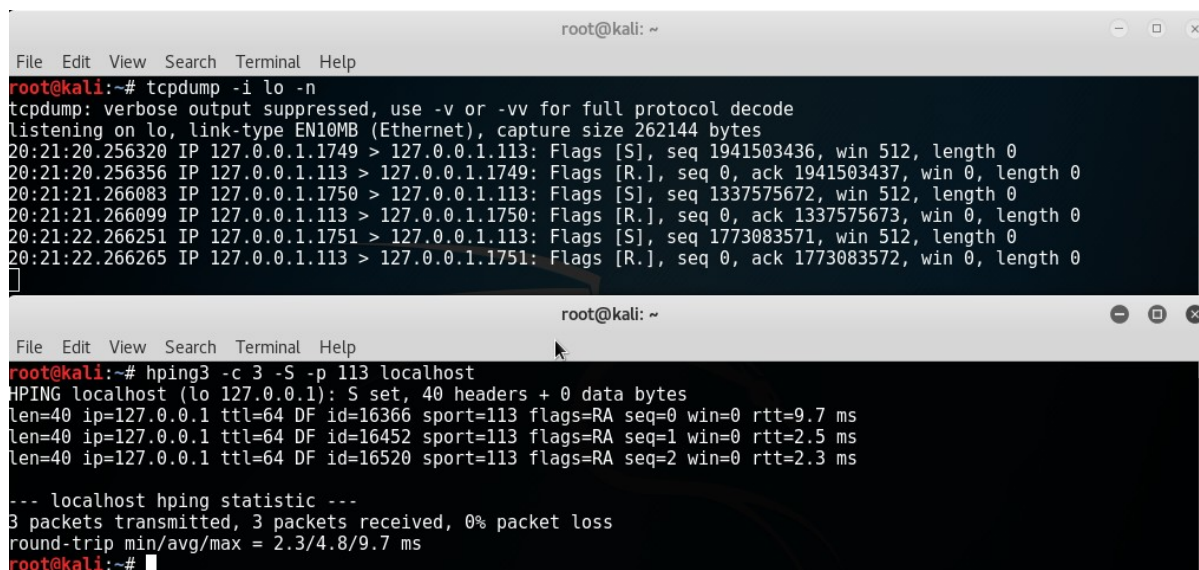
– Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

Se está simulando un escaneo del tipo half-open (SYN scan). El funcionamiento es el siguiente: Se envía un paquete SYN y se evalúa la respuesta. Si fue un SYN+ACK el puerto está abierto, y si fue un RST, está cerrado.

La motivación detrás de este tipo de escaneo es que, al no completarse la conexión, la capa de transporte nunca se entera de ésta.



\_Escaneo del puerto TCP/113 de la máquina local (localhost) **hping3 -c 3 -S -p 113 localhost**



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i lo -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:21:20.256320 IP 127.0.0.1.1749 > 127.0.0.1.113: Flags [S], seq 1941503436, win 512, length 0  
20:21:20.256356 IP 127.0.0.1.113 > 127.0.0.1.1749: Flags [R.], seq 0, ack 1941503437, win 0, length 0  
20:21:21.266083 IP 127.0.0.1.1750 > 127.0.0.1.113: Flags [S], seq 1337575672, win 512, length 0  
20:21:21.266099 IP 127.0.0.1.113 > 127.0.0.1.1750: Flags [R.], seq 0, ack 1337575673, win 0, length 0  
20:21:22.266251 IP 127.0.0.1.1751 > 127.0.0.1.113: Flags [S], seq 1773083571, win 512, length 0  
20:21:22.266265 IP 127.0.0.1.113 > 127.0.0.1.1751: Flags [R.], seq 0, ack 1773083572, win 0, length 0  
root@kali:~#  
  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hping3 -c 3 -S -p 113 localhost  
HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes  
len=40 ip=127.0.0.1 ttl=64 DF id=16366 sport=113 flags=RA seq=0 win=0 rtt=9.7 ms  
len=40 ip=127.0.0.1 ttl=64 DF id=16452 sport=113 flags=RA seq=1 win=0 rtt=2.5 ms  
len=40 ip=127.0.0.1 ttl=64 DF id=16520 sport=113 flags=RA seq=2 win=0 rtt=2.3 ms  
  
--- localhost hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 2.3/4.8/9.7 ms  
root@kali:~#
```

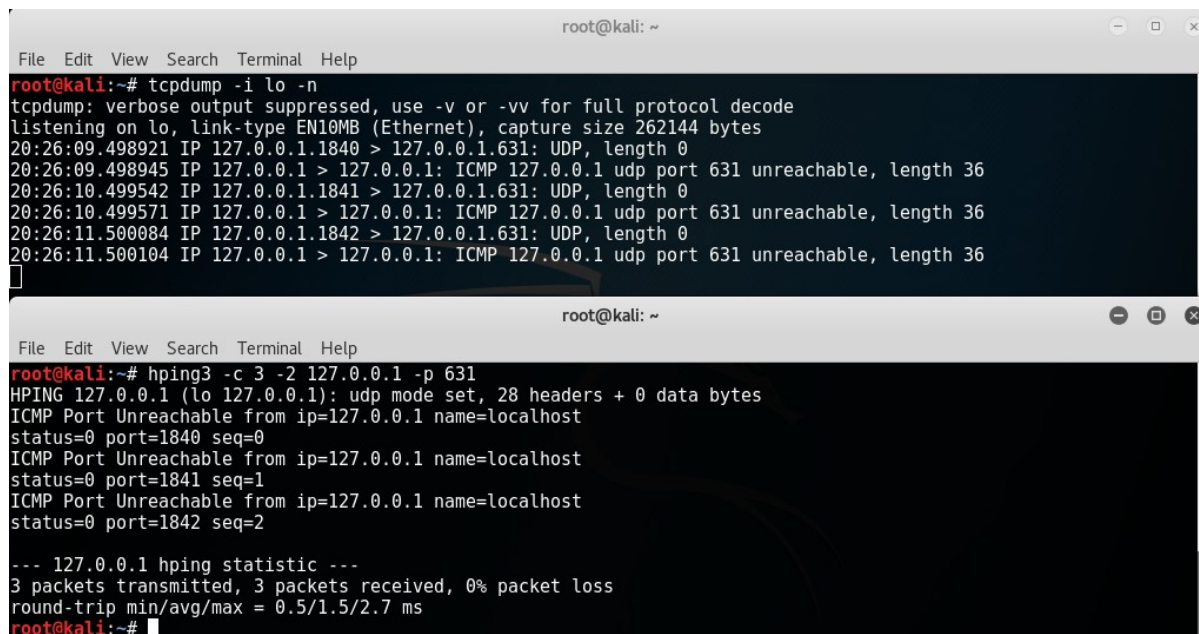
\_¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?

El puerto está cerrado.

\_Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

Es un escaneo de tipo half-open SYN.

Escaneo del puerto UDP/631 de la máquina local (localhost) **hping3 -c 3 -2 127.0.0.1 -p 631**



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i lo -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:26:09.498921 IP 127.0.0.1.1840 > 127.0.0.1.631: UDP, length 0  
20:26:09.498945 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 631 unreachable, length 36  
20:26:10.499542 IP 127.0.0.1.1841 > 127.0.0.1.631: UDP, length 0  
20:26:10.499571 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 631 unreachable, length 36  
20:26:11.500084 IP 127.0.0.1.1842 > 127.0.0.1.631: UDP, length 0  
20:26:11.500104 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 631 unreachable, length 36  
root@kali:~#  
  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hping3 -c 3 -2 127.0.0.1 -p 631  
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 0 data bytes  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1840 seq=0  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1841 seq=1  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1842 seq=2  
  
--- 127.0.0.1 hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 0.5/1.5/2.7 ms  
root@kali:~#
```

\_¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?

El puerto está cerrado.

Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

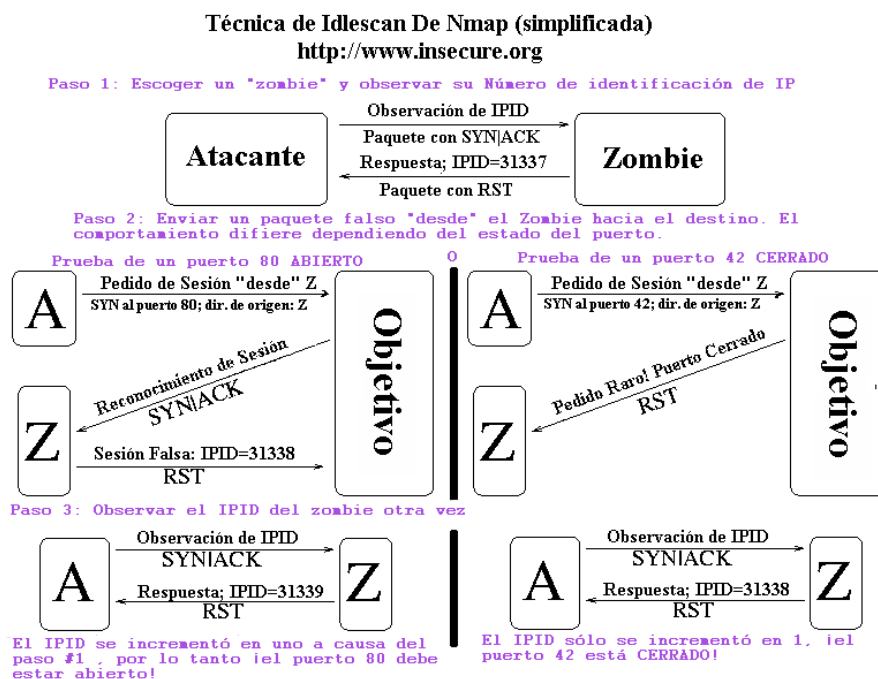
Se está el método de mapeo inverso, en la que se fabrican paquetes ICMP de tipo "Host Unreachable". Dicho método consiste en escanear de manera anónima para conseguir información sobre direcciones IP inactivas que están asociadas a direcciones IP activas.

Escaneo del puerto UDP/53 de la maquina local (localhost) hping3 -c 3 -2 127.0.0.1 -p 53 2

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i lo -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes  
21:03:52.293943 IP 127.0.0.1.1856 > 127.0.0.1.52: UDP, length 0  
21:03:52.293967 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 52 unreachable, length 36  
21:03:53.303867 IP 127.0.0.1.1857 > 127.0.0.1.52: UDP, length 0  
21:03:53.303883 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 52 unreachable, length 36  
21:03:54.304019 IP 127.0.0.1.1858 > 127.0.0.1.52: UDP, length 0  
21:03:54.304035 IP 127.0.0.1 > 127.0.0.1: ICMP 127.0.0.1 udp port 52 unreachable, length 36  
[ ]  
  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hping3 -c 3 -2 127.0.0.1 -p 52  
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 0 data bytes  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1856 seq=0  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1857 seq=1  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=1858 seq=2  
  
--- 127.0.0.1 hping statistic ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 3.7/7.2/10.2 ms  
root@kali:~#
```

## 7. Utilizando IDLE SCAN:

- ¿Qué características debe reunir un host que se pueda utilizar como zombie?



## FOOTPRINTING

9. ¿Cuál es la finalidad de realizar OS fingerprinting? ¿Cómo se lleva a cabo?

La finalidad del OS fingerprinting es la de determinar qué sistema operativo está ejecutando un host mediante el análisis y búsqueda de características únicas de los Sistemas Operativos en el uso de determinados protocolos. El OS fingerprinting se lleva a cabo a través de herramientas que permitan realizar un análisis de banderas, opciones, y datos en los paquetes que responden a determinados protocolos y que un dispositivo envía a la red.

10. Utilice nmap para realizar OS fingerprinting de distintos sistemas operativos. ¿Fue correcto el resultado alcanzado por la herramienta?

Nota: Nmap es una herramienta que además de permitir escanear puertos, implementa diversas técnicas de OS Fingerprinting: <http://nmap.org/book/osdetect.html>.

\_Se le realizó nmap a un celular con android con ip 192.168.1.100

```
➔ ~ sudo nmap -O -sV -p- 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-09 20:15 UTC
Nmap scan report for 192.168.1.100
Host is up (0.011s latency).
All 65535 scanned ports on 192.168.1.100 are closed
MAC Address: D0:77:14:7D:F3:26 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.90 seconds
➔ ~
```

11. ¿Cuál es la finalidad de realizar fingerprinting de servicios? ¿banner grabbing es la forma mas sencillo de realizarlo?

La finalidad del fingerprinting de servicios es la de determinar los servicios corriendo en puertos determinados. Esto además, puede servir para asegurar cualquier duda surgida en el proceso de OS fingerprinting. Banner Grabbing puede ser la forma más sencilla de realizar esto, siempre y cuando la información del banner no esté oculta.

## ENUMERACION

12. ¿Qué es enumeración?

Es el proceso de recopilación de nombres de usuarios, terminales, recursos de red, recursos compartidos y servicios de un sistema.

El objetivo de la enumeración es identificar una cuenta de usuario o del sistema para su potencial uso.

13. ¿Como haría enumeración sobre alguno de los siguientes protocolos y servicios de consulta?

Redes WiFi presentes en la Facultad

Podría realizarse con utilidades provistas por nmap o mediante la herramienta nbtscan.

Dispositivos bluetooth activados

Mediante el uso de un dispositivo con tecnología bluetooth podría realizarse un escaneo y enumeración de los dispositivos cercanos con bluetooth activo.

Recursos presentes en una red windows (servidores / impresoras / shares)

En una red con soporte NetBIOS podría realizarse un escaneo de los recursos disponibles de la red, además de las computadoras conectadas a ella. En una red de estas características, cada dispositivo conectado es identificado con un nombre único.

Información de DNS de algún dominio en particular (usar con responsabilidad)

Podría realizarse con el uso con de las utilidades provistas por la herramienta dnsenum (disponible en Kali Linux).

Realizar enumeración de DNS con Kali

Utilice DNS ENUM para hacer una enumeración del DNS del dominio unp.edu.ar, para ello:

1. Abra la aplicación dnsenum (KALI Linux → Information Gathering → DNS Analysis → dnsenum) y ejecute el comando de la siguiente manera:

`dnsenum unp.edu.ar -f file.txt`

```
bruno@kali: ~  
File Edit View Search Terminal Help  
bruno@kali:~$ dnsenum unp.edu.ar -f file.txt  
dnsenum.pl VERSION:1.2.3  
  
----- unp.edu.ar -----  
  
Host's addresses:  
  
Name Servers:  
  
unpata.unp.edu.ar.      10800   IN      A       170.210.88.3  
chenque.unp.edu.ar.    10800   IN      A       170.210.88.4  
  
Mail (MX) Servers:  
  
pmg.unp.edu.ar.        10800   IN      A       170.210.88.254  
  
Trying Zone Transfers and getting Bind Versions:  
  
Trying Zone Transfer for unp.edu.ar on unpata.unp.edu.ar ...  
unp.edu.ar.            10800   IN      SOA      (                  
unp.edu.ar.            10800   IN      TXT      "v=spf1  
unp.edu.ar.            10800   IN      MX       10  
unp.edu.ar.            10800   IN      NS       unpata.unp.edu.ar.  
unp.edu.ar.            10800   IN      NS       chenque.unp.edu.ar.  
academica.unp.edu.ar.  10800   IN      CNAME    nginx.unp.edu.ar.  
www.academica.unp.edu.ar. 10800   IN      CNAME    nginx.unp.edu.ar.  
aling.unp.edu.ar.      10800   IN      MX       1  
alumnosfcm.unp.edu.ar. 10800   IN      CNAME    nginx.unp.edu.ar.  
alumnosing.unp.edu.ar. 10800   IN      CNAME    nginx.unp.edu.ar.  
www.appsalud.unp.edu.ar. 10800   IN      CNAME    nginx.unp.edu.ar.  
www.apunp.unp.edu.ar.  10800   IN      CNAME    nginx.unp.edu.ar.  
arai-registry.unp.edu.ar. 10800   IN      CNAME    nginx.unp.edu.ar.
```



## Ataques de Fuerza Bruta

### 14. Fuerza bruta SSH con Metasploit

Se utilizará Metasploit para hacer fuerza bruta a servidores SSH.

i. En Kali ir a Applications → Kali Linux → Exploitation Tools → Metasploit

→ metasploit framework. Debería aparecer una consola con: msf >

ii. Sobre la consola metasploit, buscar cosas relacionadas con SSH:

msf > search ssh

```
msf > search SSH
[!] Module database cache not built yet, using slow search

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	normal	Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
auxiliary/fuzzers/ssh/ssh_kexinit_corrupt		normal	SSH Key Exchange Init Corruption
auxiliary/fuzzers/ssh/ssh_version_15		normal	SSH 1.5 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_2		normal	SSH 2.0 Version Fuzzer
auxiliary/fuzzers/ssh/ssh_version_corrupt		normal	SSH Version Corruption
auxiliary/scanner/http/cisco_firepower_login		normal	Cisco Firepower Management Console 6.0 Login
auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	GitLab User Enumeration
auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	Apache Karaf Default Credentials Command Execution
auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal	Cerberus FTP Server SFTP Username Enumeration
auxiliary/scanner/ssh/detect_kippo		normal	Kippo SSH Honeypot Detector
auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	Fortinet SSH Backdoor Scanner
auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	Juniper SSH Backdoor Scanner
auxiliary/scanner/ssh/karaf_login		normal	Apache Karaf Login Utility
auxiliary/scanner/ssh/ssh_enumusers		normal	SSH Username Enumeration
auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	SSH Public Key Acceptance Scanner
auxiliary/scanner/ssh/ssh_login		normal	SSH Login Check Scanner
auxiliary/scanner/ssh/ssh_login_pubkey		normal	SSH Public Key Login Scanner
auxiliary/scanner/ssh/ssh_version		normal	SSH Version Scanner
exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	Apple iOS Default SSH Password Vulnerability

```
msfconsole
```

iii. Sobre la consola metasploit, ejecutar el siguiente comando:

msf > \*\*use scanner/ssh/ssh\_login\*\*

```
msf > use scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) >
```

iv. Para ver las opciones que se pueden configurar:

msf auxiliary(ssh\_login) > show options

```
msf auxiliary(scanner/ssh/ssh_login) > show options
Module options (auxiliary/scanner/ssh/ssh_login):

```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target address range or CIDR identifier
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts



v. Suponiendo que queremos realizar la fuerza bruta sobre la máquina real la cual tiene como IP la dirección x.x.x.x, configurar el host a escanear con:

```
msf auxiliary(ssh_login) > set rhosts x.x.x.x
```

vi. En la carpeta personal del usuario syper, hay un archivo con las 500 claves mas comunes. Las mismas se bajaron de Internet, y serán el diccionario que se usará para realizar el ataque de fuerza bruta.

```
msf auxiliary(ssh_login) > set pass_file badpasswords
```

vii. Indicamos el usuario al que se quiere realizarle la fuerza bruta sea postgrado y que el ataque termine si se llega a tener éxito

```
msf auxiliary(ssh_login) > **set username postgrado**
```

```
msf auxiliary(ssh_login) > **set stop_on_success true**
```

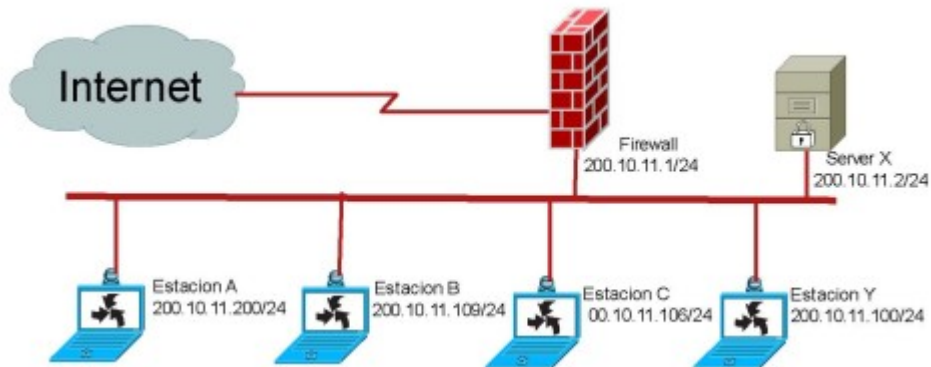
```
msf auxiliary(scanner/ssh/ssh_login) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf auxiliary(scanner/ssh/ssh_login) > set pass_file badpasswords
pass_file => badpasswords
msf auxiliary(scanner/ssh/ssh_login) > set username root
username => root
msf auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(scanner/ssh/ssh_login) >
```

\_ Luego con EXPLOIT se realiza el ataque.

## Sección 3

### Firewall

A. Dada la siguiente topología y conociendo la siguiente información:



Se trata de la red de una organización, la cual tiene direccionamiento IP público.

El firewall de la organización es del tipo sin estados y solamente debería permitir:

- a) acceso desde Internet al servidor X al servicio WEB , de modo que los usuarios desde Internet puedan navegar por la página WEB de la organización.
- b) acceso desde Internet al servidor X al servicio HTTPS , de modo que los usuarios desde Internet puedan navegar en forma segura por la página WEB de la organización.

Por esta razón, la tabla FORWARD del firewall quedó configurada de la siguiente manera:

Orden	Protocolo	IP Origen	Port Origen	IP Destino	Port Destino	Acción
1	TCP	ALL	ALL	200.10.11.2	80	Aceptar
2	ALL	ALL	ALL	ALL	ALL	Denegar

Responda:

1. ¿Qué tipo de política de firewall se implementó?

Utiliza una política RESTRICTIVA.

2. ¿Son suficientes estas reglas?: En caso de que no la considere suficiente para resolver el objetivo planteado, indique qué reglas agregaría y en qué orden las pondría.

Falta una regla que pertenece al paquete que "vuelve". Se incorporaría en la posición 2 para que la regla política restrictiva no la anule y sería de la siguiente forma:

ORDEN	PROTOCOLO	IP Origen	PORT Origen	IP Dest.	PORT Dest.	Accion
1	0	0	0	0	80	0
2	0	0	80	0	0	0
3	TCP	ALL	ALL	200.10.11.2	443	ACEPTAR
4	TCP	200.10.11.2	443	ALL	ALL	ACEPTAR
5	ALL	ALL	0	ALL	0	DENEGAR

*iptables -A FORWARD -p tcp -s 200.10.11.2 --dport 80 -j ACCEPT*

*iptables -A FORWARD -p tcp -d 200.10.11.2 --dport 443 -j ACCEPT*

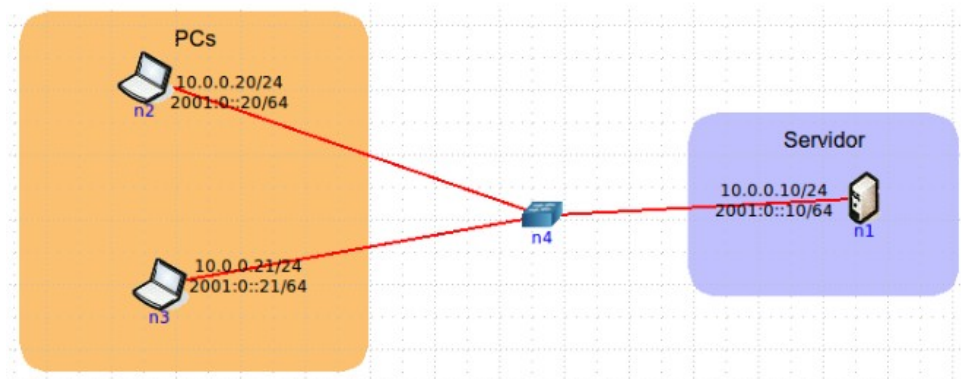
*iptables -A FORWARD -p tcp -s 200.10.11.2 --dport 443 -j ACCEPT*

3. Si además, ahora se quiere que la “Estación Y: 200.10.11.100” pueda hacer ping a www.google.com para ver los tiempos de respuesta ¿cómo modificaría las reglas del firewall?

ORDEN	PROTOCOLO	IP Origen	PORT Origen	IP Dest.	PORT Dest.	Accion
1	0	0	0	0	80	0
2	0	0	80	0	0	0
3	TCP	ALL	ALL	200.10.11.2	443	ACEPTAR
4	TCP	200.10.11.2	443	ALL	ALL	ACEPTAR
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0

*iptables -A FORWARD -p ICMP -s 200.10.11.100 -d 172.217.28.195 -j ACCEPT*

*iptables -A FORWARD -p ICMP -s 172.217.28.195 -d 200.10.11.100 -j ACCEPT*



2. Configure los firewalls según se indique en cada uno de los casos presentados más adelante, cumplimentando para cada uno lo siguiente:

Casos:

1. Configure el firewall del Servidor Web para aceptar solamente conexiones al puerto 80 utilizando una política restrictiva.

La política restrictiva nos dice que: Todo lo que no está expresamente permitido, está prohibido. Entonces, la acción inicial será de definir una política que descarte todo lo que no esté permitido y, seguidamente, agregar una regla que permita el caso que deseamos. Esto es:

***iptables -F*** → Para borrar toda la configuración del firewall para volver a configurarlo de nuevo

***iptables -P INPUT DROP***

***iptables -A INPUT -d 10.0.0.10 -p tcp --dport 80 -j ACCEPT***

2. Configure el firewall del Servidor Web para aceptar solamente conexiones al puerto 80 utilizando una política permisiva. Nota: puede resultar conveniente utilizar estados.

La política permisiva nos dice que: Todo lo que no está expresamente prohibido, está permitido. Inicialmente se flushan todas las reglas y definimos una política de aceptación en la tabla de entrada.

Seguidamente, se define la regla que acepte conexiones nuevas al puerto 80 (NEW) y que acepte a hosts que ya hubieran estado conectados (RELATED) o que ya estuvieran conectados (ESTABLISHED), utilizando reglas de firewall stateful.

***iptables -F***

***iptables -A INPUT -d 10.0.0.10 -p tcp --dport 80 -m state --state NEW -j ACCEPT***

***iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT***

3. Configure el firewall del Servidor Web para redireccionar toda petición al puerto TCP 8080 al puerto TCP 80 del mismo equipo.

***iptables -A PREROUTING -t nat -d 10.0.0.10 -p tcp --dport 8080 -j REDIRECT --to-port 80***

4. Configure el firewall del Cliente de modo que, para cualquiera de los puntos anteriores, el mismo pueda establecer hacia el Servidor cualquier tipo de comunicación (siempre y cuando el Servidor se lo permita), pero sin permitir que el Web Server pueda iniciar comunicaciones nuevas hacia él.

Nota: debe utilizar estados para resolver este ejercicio.

Tomando a n1 como cliente, la configuración es la siguiente:

***iptables -I INPUT -s 10.0.0.10 -d 10.0.0.20 -m state --state NEW -j DROP***

***iptables -I INPUT -s 10.0.0.10 -d 10.0.0.20 -m state --state RELATED,ESTABLISHED -j ACCEPT***

De esta forma, todas las comunicaciones salientes son aceptadas y todas las entrantes son aceptadas, salvo por las conexiones nuevas desde el host n1 (política permisiva).