Practico 2

Sección 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.

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).

3. Visite el sitio http://www.netcraft.net/ y pruebe la funcionalidad del mismo contra el dominio www.unp.edu.ar. (Consigne aquí al menos 8 datos de la organización).

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. ¿Qué ventajas presenta esta herramienta respecto de otras herramientas de footprinting?

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

GET /algo_que_no_existe HTTP/1.1
Host: www.google.com.ar

# nc www.ing.unp.edu.ar 80
GET / HTTP/1.1
Host: www.ing.unp.edu.ar

GET /algo_que_no_existe HTTP/1.1
Host: www.ing.unp.edu.ar

# nc www.microsoft.com 80
GET / HTTP/1.1
Host: www.microsoft.com
```

```
GET /algo_que_no_existe HTTP/1.1
Host: www.microsoft.com

# nc serconex.juschubut.gov.ar 80
GET / HTTP/1.1
Host: serconex.juschubut.gov.ar

GET /algo_que_no_existe HTTP/1.1
Host: serconex.juschubut.gov.ar
```

NOTA: Puede ejecutar el comando en una linea como el suguiente Ej:

`"GET / HTTP/1.1\nhost: www.ing.unp.edu.ar\n\n\n" | nc www.ing.unp.edu.ar 80`

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? ¿Cúal es la ultima versión de cada uno de ellos?

Sección 2

Escaneo

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:
   - Escaneo de hosts
   - Escaneo de puertos
   - Escaneo de redes WiFi
   - Escaneo de dispositivos bluetooth
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)
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.

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*

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`
   Compruebe si los puertos detectados son los mismos que están corriendo en la máquina, los cuales puede consultar con el comando:
   `netstat -nltp4`

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

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`
     - ¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?
     - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- Escaneo del puerto TCP/113 de la maquina local (localhost)
  `hping3 -c 3 -S -p 113 localhost`
  - ¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?
  - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- Escaneo del puerto UDP/631 de la maquina local (localhost)
  `hping3 -c 3 -2 127.0.0.1 -p 631`
  - ¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?
  - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- Escaneo del puerto UDP/53 de la maquina local (localhost)
  `hping3 -c 3 -2 127.0.0.1 -p 53`
  - ¿Qué significa la respuesta respecto del estado del puerto (abierto/cerrado)?
  - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

7. Utilizando IDLE SCAN:
   - ¿Qué características debe reunir un host que se pueda utilizar como zombie?

   Realice un IDLE SCAN:

   Para el idle escaneo usted necesita utilizar un zombie. Verifique si alguna de las PCs (Kali o la maquina real (windows o linux)) podría llegar a ser usada como zombie (observar el IPID retornado por la estación) con el siguiente comando:

   ```
   hping3 -S -p 80 <IP_destino>
   ```

   En caso de tener un zombie (Z) a su disposición, usted podría escanear un puerto de la estación víctima (V), desde Kali (K) de la siguiente manera:

   IDLE Scan desde (K) de puerto abierto en (V)

   ```
   hping3 -S -p 80 <IP_de_(Z)>
   hping3 -a <IP_de_(Z)> -S -p <puerto_abierto_en_(V)> <IP_de_(V)>
   ```

   IDLE Scan desde (K) de puerto cerrado en (V)

```
hping3 -S -p 80 <IP_de_(Z)>
hping3 -a <IP_de_(Z)> -S -p <puerto_cerrado_en_(V)> <IP_de_(V)>
```

8. ¿Es posible detectar un escaneo de puertos? ¿Cómo? Para cada técnica que se le ocurra, piense alguna manera de realizar el escaneo evitando la detección con la misma.

Fingerprinting

9. ¿Cuál es la finalidad de realizar OS fingerprinting? ¿Cómo se lleva a cabo?
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 tecnicas de OS Fingerprinting: http://nmap.org/book/osdetect.html.

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

Enumeración

12. ¿Qué es enumeración?
13. ¿Como haría enumeración sobre alguno de los siguientes protocolos y servicios de consulta?
    a. Redes WiFi presentes en la Facultad
    b. Dispositivos bluetooth activados
    c. Recursos presentes en una red windows (servidores / impresoras / shares)
    d. Información de DNS de algún dominio en particular (usar con responsabilidad)
    e. 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
```

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 → Explotation Tools → Metasploit → metasploit framework. Deberia aparecer una consola con: **msf >**

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

msf > **search ssh**

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

```
msf > **use scanner/ssh/ssh_login**
```

iv. Para ver las opciones que se pueden configurar:

msf auxiliary(ssh_login) > **show options**

v. Suponiendo que queremos realizar la fuerza bruta sobre la máquina real lacual 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**
```

Verificar nuevamente las opciones configuradas:

```
msf auxiliary(ssh_login) > **show options**
```

Ejecutamos el ataque:

```
msf auxiliary(ssh_login) > **exploit**
```

15. Fuerza bruta SSH con HYDRA Hydra es un cracker de contraseñas con soporte para una gran cantidad de protocolos.
    i. En Kali ir a Applications → KALI Linux → Password Attacks → Online → hydra-gui

ii. Configurar en la pestaña [Target] Suponiendo que queremos realizar la fuerza bruta sobre la máquina real la cual tiene como IP la dirección x.x.x.x
    1. Single Target → x.x.x.x
    2. Port → 22
    3. Protocol → ssh
iii. Configurar en la pestaña [Passwords]
    1. Username → postgrado
    2. Password List → badpasswords
iv. Iniciar el CRACK en la pestaña [Start]
    1. Botón Start

Sección 3

Firewall

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

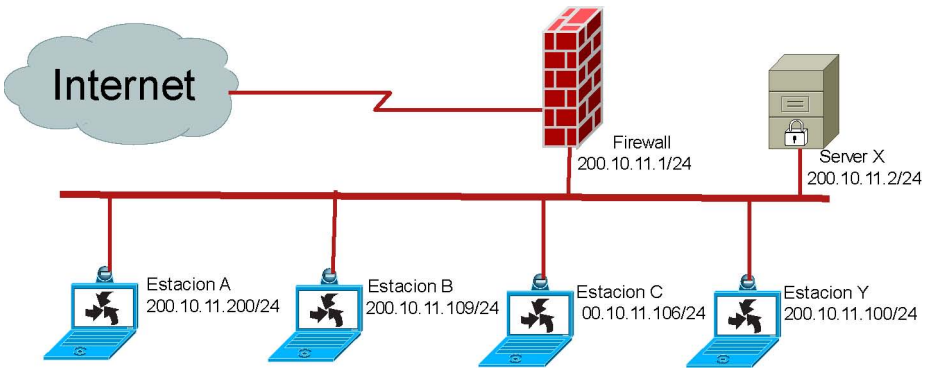

Figure 1: img/ej1_firewall.png

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?

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.

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?

IPTables

A) Topología LAN

Utilizando la herramienta "core" arme una topología como la siguiente:

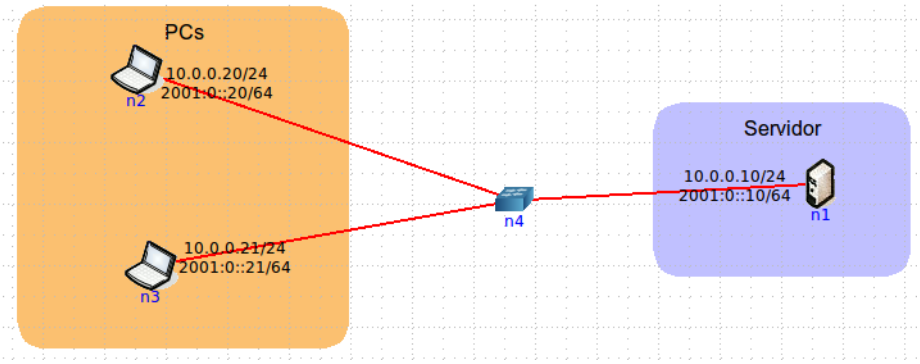

Figure 2: img/iptables_ej1.png

1. Efectué la instalación y:
   a. Verifique la configuración IP tanto de los Clientes como del Servidor con los comandos: `ifconfig` y `netstat -nr`.

b. Verifique los servicios (TCP/UDP) que cada uno ofrece con los comandos: `netstat -natp` y `netstat -naup`. Liste los puertos abiertos.

c. Utilice el comando: `iptables -nL -v` para corroborar el funcionamiento del server.

2. Configure los firewalls según se indique en cada uno de los casos presentados más adelante, cumplimentando para cada uno lo siguiente:
   a) Utilice los comandos: 1) `telnet` o `netcat <ip> <port>`, 2) `nmap -v` y 3) `ping` desde el host, e indique lo que sucede en cada caso.

   b) Utilice el comando: `iptables -nL -v` para corroborar el funcionamiento del server.

   c) Escriba las reglas de firewall (en orden), que fueron necesarias para resolver el problema.

   d) Una vez finalizado, desconfigure lo hecho, de modo que el firewall acepte todo. *Nota: con el comando: `iptables -F` se eliminan todas reglas, salvo las políticas configuradas, y con: `iptables -Z` se reinicializan los contadores a cero.*
   Utilice el comando: `iptables -nL -v` para corroborar el funcionamiento del server.

Casos:

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

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

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

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.*

B. Topología Ruteada

Utilizando la herramienta "core" arme una topología como la de la figura. En esta topología se dispone de cinco equipos, dos clientes, un hub/switch, un router/firewall y un servidor.

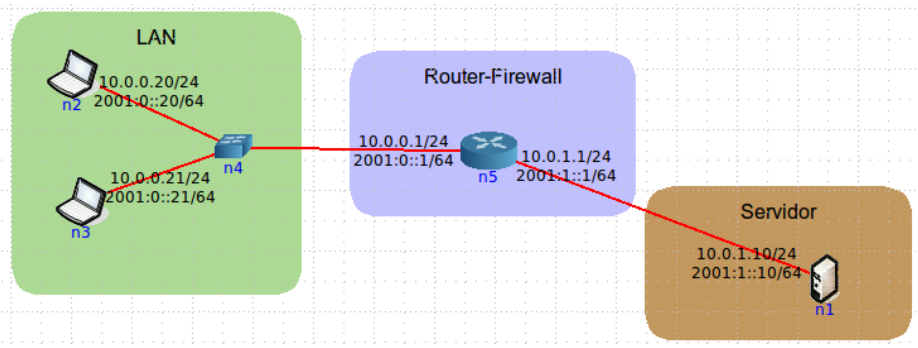

Figure 3: img/iptables_ej2.png

1. Efectué la instalación y:
   a. Verifique la configuración IP tanto del Cliente, del Router/Firewall como del Web Server con los comandos: `ifconfig` y `netstat -nr`.

   b. Verifique los servicios (TCP/UDP) que cada uno ofrece con los comandos: `netstat -natp` y `netstat -naup`. Liste los puertos abiertos.

   c. Utilice el comando: `iptables -nL -v` para corroborar el funcionamiento de los tres equipos.

   d. Utilice el comando: route en el cliente para verificar el router por defecto y efectúe ping a hosts de la red y al Server para evidenciar el ruteo.
2. Verifique que el router/firewall:
   a. Tenga la conmutación de paquetes habilitada. Para ello, visualice el contenido del archivo `/proc/sys/net/ipv4/ip_forward`, con el siguiente comando: `cat /proc/sys/net/ipv4/ip_forward`. (1 = habilitada. 0 = deshabilitada).
   Para cambiar dicho valor, utilice los comandos:
   `echo 1 > /proc/sys/net/ipv4/ip_forward`
   `echo 0 > /proc/sys/net/ipv4/ip_forward`

   b. Verifique con los comandos, `ping` y `tcpdump`, en el cliente y en el Servidor respectivamente, cuando modifica la mencionada opción en el router/firewall.

c. Aplique al router/firewall la política: FORWARD DROP y verifique en el Cliente que sucede con los pings enviados al Servidor.

3. Configure los firewalls según se indique en cada uno de los casos presentados más adelante, cumplimentando para cada uno lo siguiente:
   a. Utilice los comandos: 1) `telnet` o `netcat/nc <ip><port>`, 2) `nmap -v` y 3) `ping` desde el host, e indique lo que sucede en cada caso.

   b. Utilice el comando: `iptables -nL -v` para corroborar el funcionamiento del server.

   c. Escriba las reglas de firewall (en orden), que fueron necesarias para resolver el problema.

   d. Una vez finalizado, desconfigure lo hecho, de modo que el firewall acepte todo. _Nota: con el comando `iptables -F` se eliminan todas reglas, salvo las políticas configuradas, y con: `iptables -Z` se reinicializan los contadores a cero. Utilice el comando `iptables -nL -v` para corroborar el funcionamiento del server.

Casos :

1. Ejecute el siguiente script en el Servidor para simular distintos servicios: `# ncat -l 21 -k & ncat -l 25 -k & ncat -l 80 -k &  ncat -l 443 -k &`

2. Verifique los servicios (TCP/UDP) que brinda el servidor con los comandos `netstat -nat` y `netstat -nau`

3. Configure el firewall del router-firewall, utilizando una política restrictiva y las características de STATEFUL del firewall, de modo que:
   a. Se permita únicamente el acceso desde la LAN a los servicios: FTP, SSH y HTTP que corren en el Servidor.
   b. Además de las comunicaciones permitidas anteriormente ninguna otra comunicación hacia el router-firewall debe permitirse, ya sea desde la LAN como desde el Servidor.
   c. Desde el firewall se deben poder iniciar conexiones SSH y HTTPS al Servidor.
   d. Desde el servidor se debe permitir el acceso al servicio SSH de las PCs de la LAN.

4. Configure el firewall con una política restrictiva y sin estados, de modo que se permita únicamente el acceso desde el cliente al servidor, a los servicios: FTP, SSH y HTTP.
   Tenga en cuenta que ninguna otra comunicación hacia el firewall debe ser permitida, ya sea desde el cliente como desde el Servidor. Además, desde

el firewall se deben poder iniciar conexiones SSH al Servidor.

5. Idem punto anterior pero con una política permisiva. Queda a su entender si usara estados en la configuración de las reglas.
6. Configuración Hogareña: Suponga que el cliente es una PC de una red hogareña y el router/firewall es el gateway de ésta. Además suponga que el servidor es un Web Server en Internet. Configure el firewall de modo de permitir que el cliente pueda realizar cualquier tipo de conexión hacia Internet pero desde Internet no se puedan ingresar comunicaciones hacia las PCs de la red hogareña (el cliente).
7. ¿Qué es mas ventajoso, usar estados (stateful) o no usar estados (stateless)? ¿porqué?

Forma y condiciones de entrega

Condicinoes de aprobación para el trabajo de entrega:
* En grupos de 2 integrantes como máximo.
* Se realiza evaluación global del trabajo y evaluación individual dónde deberá demostrar conocimiento sobre el tópico del trabajo de entrega y sobre los enunciados anteriores. Tenga en cuenta que pueden incluirse temas tratados en clase.
* El trabajo deberá ser enviado a través del aula virtual.
* La fecha límite de entrega es el 05/10/2018.