Módulo 4.2

Redes y Seguridad

Gr. Ing. Informática

J.L. Vázquez Poletti

Objetivo

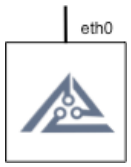
En este módulo aprenderemos sacaremos más rendimiento todavía a la distribución de seguridad **Backtrack**, esta vez escaneando puertos con **nmap** a la vez que nos apoyamos en otras herramientas. Además, aprenderemos el manejo del firewall **iptables**.

IMPORTANTE: Para una mejor comprensión y aprovechamiento del módulo, se debe capturar el tráfico con **wireshark**.

Punto de partida

Entre las habilidades conocidas por los efectivos del Cuerpo de Ingenieros de la Alianza se encuentra el rastreo (escaneo de puertos) y la fortificación (firewall). Su conocimiento es vital para el aprovechamiento máximo de la solución de seguridad instalada en la omniherramienta.

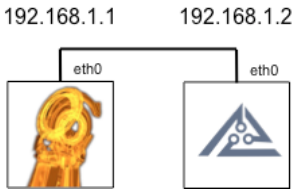
En las siguientes maniobras se enfrentarán ambas habilidades en dos escenarios diversos, uno sencillo y otro más complejo. En ambos se desplegará una máquina objetivo (**RyS-Víctima**) a la que se deberá acceder.



La misma se conecta a la red que se le indique (**Red1**, **Red2**, **Red3** o **Red4**) usando su interfaz **eth0**.

Objetivo 1: Escenario

Este primer escenario cuenta con solamente dos máquinas y servirá para realizar distintos tipos de escaneo de puertos y aplicar las contramedidas necesarias.



El escáner de puertos se ejecutará en **RyS-Backtrack**, mientras que el firewall se configurará en **RyS-Víctima**.

IMPORTANTE: Se deberá configurar la terminal en **RyS-Víctima** para que reconozca el teclado español. Para ello hay que ejecutar como usuario **root**: **loadkeys es**.

Máquinas Virtuales

- RyS-Backtrack (root:toor)
- RyS-Geth01 (ubuntu:reverse)
- RyS-Router1 (ubntu:reverse)
- RyS-Víctima (msfadmin:msfadmin)

Más información

Backtrack: http://www.backtrack-linux.org/

Wireshark: http://www.wireshark.org/

NMap: http://www.nmap.org/

IPTables: http://www.netfilter.org/projects/iptables/

NCat: http://nmap.org/ncat/

ProxyChains: http://proxychains.sourceforge.net/

Objetivo 1: NMAP

El escáner de puertos empleado es **nmap** y éste tiene numerosas opciones. El objetivo será siempre **RyS-Víctima**.

1. Realizar un escaneo con las opciones por defecto.
2. Escanear el rango de puertos 21-25 y 80-139 **en el mismo comando**.
3. Realizar un escaneo **UDP** del mismo rango de puertos de antes.
4. Detectar el sistema operativo del objetivo.
5. Realizar el escaneo completo que incluye detección del sistema operativo, versión de los servicios y trazado de ruta.

Objetivo 1: IPTables

El firewall con **iptables** se configura introduciendo reglas de filtrado que afectan a tres categorías principales llamadas cadenas:

- **INPUT:** paquetes de entrada.
- **OUTPUT:** paquetes de salida.
- **FORWARD:** paquetes que atraviesan la máquina (solo aplicable a routers).

No obstante, se puede definir una política por defecto a través de la opción **-P**, para luego concretar con las siguientes reglas:

- **ACCEPT:** acepta todos los paquetes.
- **DROP:** rechaza todos los paquetes.

De esta manera, la regla más habitual en una máquina segura, rechazar todos los paquetes, se definiría de la siguiente manera:

iptables -P INPUT DROP

iptables -P OUTPUT DROP

A partir de aquí se van añadiendo reglas usando la opción **-A <*CADENA*>** y a continuación se indicando los criterios.

Algunos de estos criterios son:

- Dirección IP de origen y destino: **-s** y **-d** respectivamente.
- Protocolo: **-p tcp/udp/icmp**.
- Puerto de origen y destino (aplicable a TCP/UDP): **--sport** y **--dport** respectivamente.
- Número de código de mensaje ICMP: **--icmp_type**
- Interfaz de entrada y salida: **-i** y **-o**.
- Estado de la conexión: **-m state --state <*ESTADO*>**, pudiendo estar el *ESTADO* separado por comas.
    - **NEW:** conexiones nuevas.
    - **ESTABLISHED:** conexiones ya establecidas.
    - **RELATED:** paquetes relacionados con conexiones ya existentes.

- **INVALID:** paquetes que no pertenecen a las anteriores categorías.

Y por último hay que indicar la acción a realizar por **iptables** para la regla introducida. Esto se realiza con la opción **-j** seguida de **ACCEPT** o **DROP**.

Las reglas del firewall pueden ser visualizadas con **-L** y pueden ser borradas completamente con **-F**.

NOTA: IPTables no se limita a las opciones vistas aquí. Es más que interesante echarle un vistazo a la documentación existente en Internet para ver todas las posibilidades.

Objetivo 1: NMap Vs. IPTables

A continuación se probarán diversos tipos de escaneo con **nmap** y se mostrará su contramedida mediante **iptables**. La mecánica de este objetivo es la siguiente: realizar el escaneo indicado, aplicar las reglas al firewall, volver a repetir el escaneo para probar su efectividad y por último, eliminar todas las reglas del firewall.

1. Escaneo: **TCP Null**

   Firewall:

   iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

¿En qué consiste este escaneo?

2. Escaneo: **TCP Xmas**

   Firewall:

   iptables -A INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP

¿En qué consiste este escaneo?
¿Es este el único tipo de escaneo TCP Xmas?

3. Escaneo: **TCP FIN**

   Firewall:

   iptables -A INPUT -p tcp --tcp-flags ALL FIN -j DROP

¿En qué consiste este escaneo?

4. Escaneo: **TCP ACK**

   Firewall:

   iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

¿En qué consiste este escaneo?
¿Por qué se usa el modificador "!"?

5. Escaneo: **TCP SYN**

   Firewall:

   iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 4 -j ACCEPT

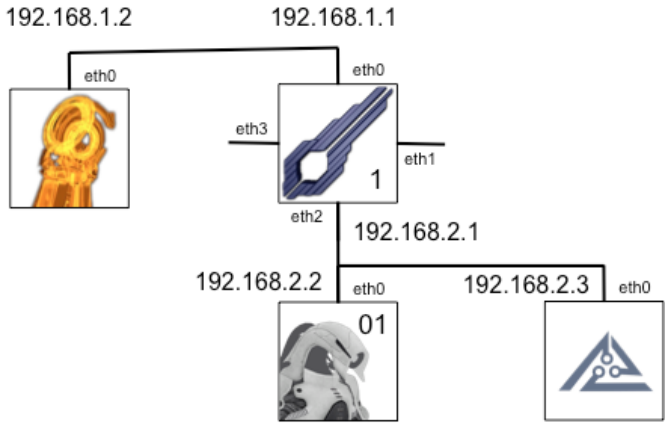
   iptables -A INPUT -p tcp --syn -j DROP

   NOTA: Interrumpir el escaneo tras esperar un tiempo.

¿En qué consiste este escaneo?
¿Cuál es la dificultad a la hora de bloquear este escaneo?
¿Cuál es la respuesta de **nmap** cuando detecta la contramedida de **iptables**?
¿Qué contramedida se podría aplicar a la respuesta de **nmap**?

Objetivo 2: Escenario

En esta ocasión, llegar al objetivo (**RyS-Víctima)** va a ser más difícil, ya que se encuentra protegido por dos niveles de firewall (router y la propia máquina). Además, existe una plataforma Geth en la red interna.



El firewall instalado en **RyS-Router1** tiene las siguientes reglas:

- DROP por defecto en todas las cadenas.
- Permite conexiones omnidireccionales ya establecidas y paquetes relacionados.

- Permite conexiones nuevas SSH (puerto de destino 22) omnidireccionales.
- Permite conexiones nuevas desde la interfaz **eth2** pero no viceversa.

IMPORTANTE: Al ser un router, será necesario rellenar la cadena FORWARD.

El firewall instalado en **RyS-Víctima** tiene las siguientes reglas:

- DROP por defecto en todas las cadenas.
- Permite conexiones omnidireccionales ya establecidas y paquetes relacionados.
- Solo permite conexiones nuevas desde **RyS-Geth01**.

Además, esta es la información con las que contamos para realizar nuestro ataque:

- Se sabe que **RyS-Víctima** está en la red **192.168.2.0**.
- Se sabe que el resto de máquinas son las mismas plataformas cuyas comunicaciones se interceptaron en el anterior módulo.
- Como resultado de una incursión anterior en la que se infectó una máquina (ahora inexistente) de la red de **RyS-Víctima** con el rootkit **Jynx**, el firewall de **RyS-Router1** permite conexiones entrantes desde la interfaz **eth0** (**añadir las reglas oportunas**).

Éstas son algunas de las pruebas que se pueden realizar para verificar la configuración del escenario:

1. No se puede hacer **ping** desde **RyS-Backtrack** al resto de máquinas pero sí viceversa.
2. Solo se puede hacer **ping** a **RyS-Victima** desde **RyS-Geth01**.
3. Se puede hacer **ssh** desde **RyS-Backtrack** a **RyS-Router1** y **RyS-Geth01**.

Objetivo 2: Escaneo desde el exterior

Usaremos nuevamente **nmap** desde **RyS-Backtrack**:

1. Escanear todo el rango de IPs de la red **192.168.2.0** usando la opción de escaneo TCP SYN.

¿Cuál es el resultado? ¿Por qué?

2. Realizar nuevamente el escaneo añadiendo la opción **-Pn**.

¿Cuál es el resultado?
¿Para qué sirve esta opción?

3. Es el momento de utilizar la vulnerabilidad dejada en **RyS-Router1** por la anterior incursión. Realizar el escaneo indicando que el puerto de origen sea el **42**.

¿Qué máquinas son las encontradas? ¿Por qué?

A este punto, está claro que desde la red actual no se podrá acceder a la máquina objetivo. Por otro lado, se ha descubierto una de las máquinas cuyo usuario y contraseña por **telnet** y **ftp** (se obviará el **ssh**) se habían descubierto en el módulo anterior.

Objetivo 2: Escaneo a través de proxy

El objetivo es lanzar un servidor proxy http en **RyS-Geth01** para que pueda ser usado como punto de salto en el escaneo a **RyS-Víctima**. Para ello se empleará **ncat** (la versión mejorada de **netcat**) para desplegar el servidor proxy y **proxychains** para usarlo.

1. Conectarse al servicio **telnet** de **RyS-Geth01** usando **ncat**. Hay que indicar el puerto de origen correcto para poder saltar el firewall.
2. Ya dentro de **RyS-**Geth01 y como usuario **root**:
    a. Apagar el servicio ssh con el comando **service ssh stop**.
    b. Arrancar un servidor proxy de tipo **http** en el puerto **22** con **ncat**.

¿Por qué hay que apagar el servidor ssh?

En **RyS-BackTrack**:

1. Editar **/etc/proxychains.conf**. Eliminar la última entrada para cambiarla por:

    ```
    http  192.168.2.2 22
    ```

2. Ejecutar **proxychains** seguido de **nmap** indicando las siguientes opciones:
    a. Objetivo: **RyS-Víctima**.
    b. Tipo de escaneo: TCP Connect().
    c. No hacer ping.

¿Por qué esta vez no ha sido necesario indicar el puerto de origen en el escaneo?

Como se ha encontrado el puerto 80 abierto, revelando un servidor web, se procederá a conectarse a él usando un navegador.

1. Arrancar **firefox**.
2. Abrir la IP de **RyS-**Víctima.

¿Qué sucede?

3. Ir a **Preferences->Advanced->Network**.
4. En **Settings…**, indicar que se quiere introducir la configuración del proxy de forma manual.
5. Introducir la IP de **RyS-Geth01** y el puerto donde está escuchando el servidor proxy. Indicar que se usará esta configuración para todos los protocolos.
6. Darle a **OK** y volver a probar el acceso a **RyS-Geth01**.