Fundamentos de la Seguridad Informática
Seguridad en Redes

Grupo de Seguridad Informática
Facultad de Ingeniería
Universidad de la República

Propósito

El propósito de las prácticas descritas en este documento es introducir a los participantes en los problemas relacionados con la seguridad en redes. Pondremos en práctica los conceptos de shell reversa, así como utilización de *firewalls* y redes privadas virtuales.

1. Acceso a shell en forma reversa

1.1. Objetivos

Mostrar las posibles debilidades generadas cuando no se utiliza filtrado de paquetes salientes en los firewalls.

Herramientas

- netcat [4]
- Perl [9]
- Servidor Web Apache [2]

1.2. Presentación

Es común encontrar ataques remotos que generan acceso a una shell. En muchas ocasiones el mecanismo utilizado es ejecutar un programa en el equipo atacado, que escucha en un puerto donde atiende una shell. El atacante luego tiene que conectarse a ese puerto para lograr el acceso.

Debido a la proliferación de firewalls, este tipo de ataques queda bastante limitado ya que generalmente se filtran los accesos a puertos no estándar.

Un mecanismo de obtener una shell remota es que sea el equipo víctima el que genere el pedido de conexión hacia afuera. Los firewalls por lo general admiten accesos salientes a puertos estándares (21, 22, 25, 80, etc).

En este laboratorio veremos cómo efectuar la obtención de una shell remota en donde el inicio de la conexión se realiza por parte del equipo atacado. De esa forma, podremos

evadir los firewalls ya que es la red interna atacada el que inicia la conexión a un puerto estándar del equipo atacante.

1.3. Escenario

Máquina atacante con netcat instalado

Máquina víctima con servidor web apache instalado

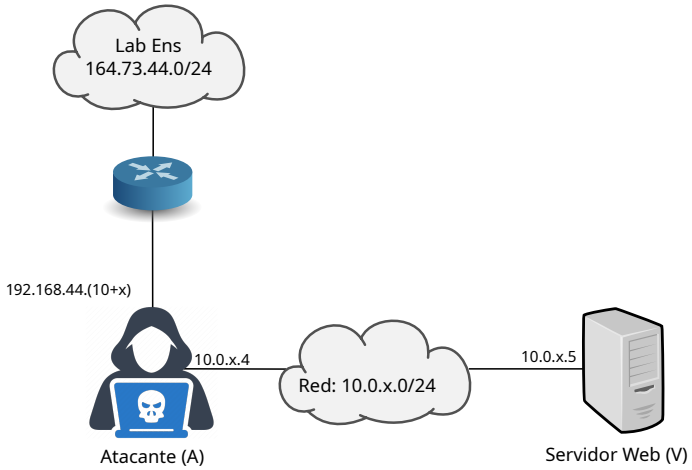

Figura 1: Descripción del Escenario

1.4. Guía de la práctica

La práctica se basará en una vulnerabilidad del `awstats` (https://web.archive.org/web/20101223094755/http://www.securityfocus.com/bid/12543). La vulnerabilidad permite ejecutar comandos remotos con los permisos del usuario que ejecuta el servidor web.

Se sabe que las políticas de firewall permiten que el servidor web pueda establecer conexiones al puerto 80 de cualquier equipo.

Objetivo

Obtener una shell reversa. Esta tarea se realizará en dos etapas:

- Generar un script perl en el equipo remoto que haga la conexión
- Ejecutar el script perl para que se establezca el acceso al servidor

El exploit está disponible en https://web.archive.org/web/20101223094755/http://www.securityfocus.com/bid/12543/exploit.

El script que genera una conexión a un equipo está disponible en el sitio eva del curso.

Entregables

En el directorio `practica1`:

- Archivo que especifique el lugar donde fue instalado el backdoor en el servidor web (el backdoor es el script que permite establecer la conexión reversa).
- Explicación de cómo se ejecuta el backdoor instalado en el servidor Web.

Sugerencias

- Utilizar el comando `netcat` (nc) en la ejecución del backdoor.
- Puede ser de utilidad el comando `wget` para bajar archivos de un sitio Web (puede ser necesario utilizar la opción `--no-proxy`).

Objetivos de aprendizaje

En esta práctica se deberán comprender lo siguientes puntos:

- Investigar qué es una shell reversa y la metodología general utilizada.
- Mecanismo para mitigar la proliferación de estos ataques.
- Utilización de proxies y/o firewalls en el contexto de este problema.

2. Firewall

El objetivo principal de esta práctica es de afirmar los conocimientos sobre firewalls.

2.1. Herramientas

Para realizar esta práctica se dispone de `iptables` [1] y Firewall Builder [5].

2.2. Escenario

Equipo con sistema operativo Linux con las herramientas iptables y fwbuilder instaladas.

2.3. Presentación

El comando `iptables` está asociado el firewall de linux y en esencia se puede definir como: "*un conjunto de comandos que permiten decirle al kernel qué hacer con los paquetes que cumplan con ciertas características*". El módulo del kernel asociado a estos comandos es netfilter [1].

Estos módulos están integrados al kernel del sistema operativo desde la versión 2.4. Sus principales características son:

- Stateless packet filtering
- Stateful packet filtering
- NAT

También se puede consultar el libro "Linux Firewalls Second Edition" [10].

Fwbuilder (firewall builder) es una herramienta de configuración y manejo de firewalls. Está compuesta de una interfaz gráfica y un conjunto de compiladores de políticas. Existen compiladores de políticas para varias plataformas, por ejemplo: iptables, ipfilter, cisco PIX y mediante un sistema de plugins se pueden crear nuevos compiladores.

Permite al administrador manejar un conjunto de firewalls de forma centralizada. Además, el lenguaje de alto nivel para escribir las reglas permite una mayor claridad al momento de administrar políticas en organizaciones de mayor porte.

2.4. Guía de la práctica

Generación de reglas para iptables El objetivo de esta práctica es configurar el firewall de una organización de acuerdo a una política dada. El equipo que actúa como firewall tiene 3 tarjetas de red, cuyos números IP son:

- `172.16.42.1` (eth2 DMZ)
- `172.16.43.1` (eth1 interna)
- `172.16.44.1` (eth0 externa - insegura)

Las redes conectadas por el firewall son las siguientes:

DMZ	172.16.42.0/24
Interna	172.16.43.0/24
Insegura	172.16.44.0/24

En la DMZ hay un servidor **multisrv** 172.16.42.2 con los siguientes servicios:

- correo (smtp)
- web
- DNS

El firewall se gestiona desde las máquinas con direcciones 172.16.43.3, 172.16.43.4 y 172.16.43.5.

Utilizando la herramienta fwbuilder, configurar reglas para iptables de forma que se cumpla la siguiente política de acceso:

1. Desde cualquiera de las redes se puede acceder al servidor multisrv, al servicio de correo.
2. Desde cualquiera de las redes se puede acceder al servidor multisrv, al servicio web.
3. Solamente desde la red Interna se puede acceder al servidor multisrv, al servicio DNS.
4. Solamente se permite tráfico DNS hacia la red Insegura desde el servidor DNS.
5. Se permite tráfico ssh desde la red Interna a cualquier lado.
6. Se permite tráfico http desde la red Interna a cualquier lado.
7. El tráfico desde la red Interna y la DMZ es enmascarado con la dirección IP de la tarjeta externa.
8. Solamente está permitido el tráfico ssh hacia el firewall desde las máquinas de gestión.
9. Todo otro tráfico no es permitido.
10. El tráfico descartado se debe registrar.

Entregables:
En el directorio practica2:

- el archivo con la configuración generada por la herramienta (fw-lab3.fwb)
- un archivo de texto con la lista de reglas de iptables generadas y una breve explicación de las reglas que definen la política.

Objetivos de aprendizaje

En esta práctica se deberán comprender lo siguientes puntos:

- Tipos de políticas (restrictivas vs. permisivas).
- Tipos de firewalls (filtrado de paquetes, aplicación, stateless, stateful) [7].
- Generación de reglas de iptables: cadenas, políticas por defecto, reglas con y sin estado, NAT.

3. Red Privada Virtual

Este laboratorio tiene como objetivo experimentar con la creación y configuración de una red privada virtual (VPN).

3.1. Herramientas

OpenVPN (como ejemplo de VPN sobre SSL) [8], OpenSSL [6].

3.2. Escenario

Máquina cliente con OpenVPN instalado (A). Esta es la misma máquina atacante usada en la práctica 1.

Máquina servidor OpenVPN instalado y servicio `echo` para pruebas.

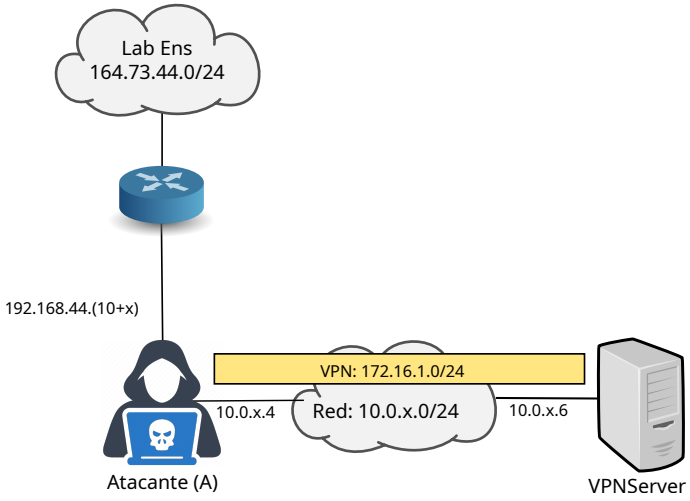

Figura 2: Descripción del Escenario

3.3. Presentación

OpenVPN es una herramienta que permite la creación de redes privadas virtuales. Utiliza el protocolo SSL/TLS y soporta diferentes métodos de autenticación, como ser certificados, clave compartida y smart cards.

En este laboratorio crearemos una VPN entre dos equipos; uno actuará como servidor y el otro como cliente. Utilizaremos certificados para la autenticación del cliente y el servidor. Para ello se ha generado una autoridad certificadora (CA), y se firmaron los certificados del cliente y el servidor. El cliente autenticará el certificado del servidor y el servidor el certificado del cliente. Primero se verificará si el certificado fue firmado por dicha CA y posteriormente el contenido del certificado, como ser el `common name` o el tipo.

3.4. Guía de la práctica

- Acceder por SSH al servidor VPN con usuario `vpnserver` y contraseña `vpnserver`.
- En el eva del curso se encuentra el archivo fsi.zip, que contiene los certificados de la CA y las claves del cliente y del servidor.
- Utilizando estos archivos, configurar el servidor y cliente para establecer una VPN entre ambos.

Entregables En el directorio practica3:

- Los archivos de configuración de OpenVPN, en el cliente y en el servidor, con una breve descripción de las opciones.
- Un archivo de texto describiendo el mecanismo utilizado para verificar que el tráfico dentro de la VPN se transmite cifrado. Sugerencia: utilice el servicio echo.

Objetivos de aprendizaje

En esta práctica se deberán comprender lo siguientes puntos

- Modos de autenticación de OpenVPN.
- SSL VPN vs. IPSec VPN
- Arquitectura de VPNs [3]

Forma de Entrega

Se debe entregar el archivo `entrega3.tar.gz` conteniendo lo solicitado en cada práctica.

La entrega se realizará a través del EVA.

Referencias

[1] Netfilter core team. Netfilter, iptables - command line program to configure packet filtering ruleset. http://www.netfilter.org/projects/iptables/index.html.

[2] The Apache Foundation. Apache web server. http://httpd.apache.org.

[3] Sheila Frankel, Paul Hoffman, Angela Orebaugh, and Richard Park. Guide to ssl vpns. NIST special publication 800-113, revised, National Institute of Standards and Technology (NIST), Jul 2008. See http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf.

[4] Giovanni Giacobbi. The gnu netcat project. http://netcat.sourceforge.net/.

[5] Firewall Builder Project. Firewall builder. https://github.com/fwbuilder/fwbuilder.

[6] The OpenSSL Project. Openssl, secure sockets layer and transport layer security. http://www.openssl.org.

[7] Karen Scarfone and Paul Hoffman. Guidelines on firewalls and firewall policy. NIST special publication 800-41, revised, National Institute of Standards and Technology (NIST), Sep 2009. See http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf.

[8] OpenVPN Technologies. Openvpn solutions, ssl vpn solution. http://www.openvpn.net/.

[9] Larry Wall. The perl programming language. http://www.perl.org.

[10] R.L. Ziegler and C.B. Constantine. *Linux Firewalls*. CampusPress référence. New Riders, 2002. http://books.google.com.uy/books?id=rIWkyUYBsCwC.