Redes de Computadoras
Trabajo práctico Nº6 - 2021
Seguridad en redes

Objetivo

- Analizar distintos tipos de cifrado y certificados SSL empleados en peticiones http en la actualidad.
- Distinguir sitios web seguros de no seguros, entender los elementos que hacen seguros a los primeros y las vulnerabilidades de los segundos.
- Desplegar algunos tipos de ataques comunes en el campo de las redes de computadoras con el propósito académico de entender su mecanismo de funcionamiento, sus posibles consecuencias y cómo proteger un equipo ante estos.
- Comprender el funcionamiento de herramientas útiles en auditoría de seguridad en redes como nmap y Linux Kali.

Metodología

Trabajo individual o grupal. 2 estudiantes por grupo máximo.
Tiempo de realización: 2 clases.

Aprobación

- Contestar a través de la plataforma Moodle las preguntas planteadas.

Materiales necesarios

- Idealmente tres computadoras con acceso a Internet, mínimo dos computadoras con acceso a Internet. Una computadora puede ser un teléfono celular con navegador web conectado en la misma red WiFi que su o sus computadoras, o una máquina virtual con su interfaz de red configurada como puente.
- Sistema operativo Linux (altamente recomendado), como sistema operativo nativo o instalado en máquina virtual con adaptador de red tipo puente. También puede utilizarse Windows, pero tendrá funcionalidades limitadas y mayor dificultad para instalar y configurar las herramientas necesarias.
- Herramientas de software (Todas estas herramientas se encuentran disponibles libremente para ser empleadas en entornos Linux. No tienen costo. Se dan instrucciones de instalación y configuración necesarias):
    - Analizador de tráfico de red Wireshark
    - Mapeador de redes nmap

- Herramienta hping3
- Navegadores web, preferentemente Google Chrome, Mozilla Firefox u Opera.
- Servidor web Apache.
- Linux Kali como sistema operativo nativo o en máquina virtual con adaptador de red configurado como puente (se sugiere VirtualBox).

Actividades

Actividad 1: cifrado y certificados.

Analice los certificados de diferentes páginas web que se indican en la plataforma Moodle (Preguntas 1, 2 y 3).

Para buscar información de seguridad y certificados en páginas web siga los siguientes pasos:

- Chrome:
  - Certificados: Clic en el candado (o signo de admiración), luego clic en “La conexión es segura”, luego en “el certificado es válido”.
  - Información de seguridad: Opciones -> Más herramientas -> Herramientas del desarrollador -> Seguridad.
- Firefox:
  - Certificados: Clic en el candado (o el candado tachado), luego en “Conexión segura” (o en “conexión insegura”), luego en “más información”, luego en “seguridad”, luego en “ver certificado”.
  - Información de seguridad: Clic en el candado (o el candado tachado), luego en “Conexión segura” (o en “conexión insegura”), luego en “más información”, luego en “seguridad”.

Actividad 2: Spoofing web.

Ingrese a la página web cuya URL se indicará en clases, siendo la dirección http://[dirección IP]/bancopatagonia. Esta es una página web clonada del Banco Patagonia corriendo en un servidor Apache en la red local de la facultad de Ingeniería. En otra pestaña, ingrese a la página real del Banco Patagonia (https://bancopatagonia.com.ar). Navegue por ambas páginas y compárelas. Conteste las preguntas que se plantean en la plataforma Moodle.

En la página web clonada original (http://[dirección IP]/bancopatagonia) vaya a "Patagonia eBank", escriba un usuario y contraseña y haga clic en "Ingresar". ¿A qué página web es redirigido? (Conteste en la Plataforma Moodle).

Nota: La página web clonada ha sido obtenida con la herramienta **httrack** de Linux Kali, una distribución de Linux preparada para auditorías de seguridad en redes. Puede ingresar a Linux Kali (instalado en las computadoras de la facultad de Ingeniería), instalar la herramienta (sudo apt install httrack) y clonar cualquier página web, para luego cargarla en un servidor Apache.

Actividad 3: Cifrado y certificados.

En el trabajo práctico N°5 implementó una página web sencilla. Analice si su página web es segura.

Para analizar si alguien puede "robar" su usuario y contraseña, ejecute Wireshark y comience una captura de datos. Ingrese a su página web desde otra computadora, ingrese un usuario y contraseña y presione enviar. En Wireshark filtre paquetes del tipo http y por la IP de la máquina cliente y busque peticiones POST. Verifique si puede ver en dichos paquetes el nombre de usuario y contraseña que ingresó.

Agregando certificados:

> Nota: Un certificado debe ser provisto por una autoridad de certificación. Sin embargo, la emisión de los mismos tiene un costo monetario. En este trabajo práctico se utilizará una clave pública y un certificado autofirmado para que el proceso sea sin costo. Para un servidor real debe comprar un certificado a una autoridad de certificación.

Agregue un certificado en su página web. Para ello, siga los siguientes pasos:

Instale openssl para Apache2:

apt-get install apache2 openssl

Habilite los módulos ssl para Apache2:

a2enmod ssl

a2enmod rewrite

Cree un certificado con el el siguiente comando:

mkdir /etc/apache2/certificate

cd /etc/apache2/certificate

openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out mi_certificado.crt -keyout mi_clave.key

Se pedirán ingresar varios datos. Puede ingresar los valores que desee (esos valores aparecerán en el certificado). Cuando se pida el dato COMMON_NAME, debe indicar la IP del servidor.
Los primeros dos comandos crean una carpeta en /etc/apache2/certificate y acceden a dicha carpeta. El tercer comando crea un par clave pública y clave privada y un certificado. Puede cambiar el nombre del certificado y la clave privada al nombre que desee.
Luego, indique a Apache la ubicación del certificado editando el archivo: */etc/apache2/sites-enabled/000-default.conf*, puede usar gedit con:
sudo gedit /etc/apache2/sites-enabled/000-default.conf
En dicho archivo agregue:

```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/apache2/certificate/mi_certificado.crt
        SSLCertificateKeyFile /etc/apache2/certificate/mi_clave.key
</VirtualHost>
```

Por último, reinicie el servidor Apache:
sudo systemctl restart apache2
Intente acceder a su página web escribiendo *https* en lugar de *http*.
Verifique nuevamente si puede leer los datos intercambiados entre cliente y servidor, especialmente el usuario y contraseña.
Nota: Recibirá una advertencia de su navegador indicando que el certificado no es válido. Esto es porque el certificado no está firmado por ninguna autoridad de certificación, sino que está firmado por usted mismo!!. Ignore la advertencia, pues usted generó el certificado.

Actividad 4: ARP spoofing

Nping

La herramienta Nping (se instala por defecto junto con Nnmap tanto el Linux como en Windows) permite generar paquetes de prueba de manera similar a la herramienta ping, pero permite generar paquetes tanto a nivel de capa de enlace, red y transporte, como también permite cambiar el valor de cualquiera de los campos de un paquete (permitiendo por ejemplo, asignar como MAC o IP origen la MAC o IP de cualquier otra máquina). Por ejemplo, algunas opciones de Nping son:

Paquetes ARP: Permite enviar paquetes del tipo ARP (repase protocolo ARP si no lo recuerda).
--arp: Indica que se va a enviar paquetes ARP.
-arp-type <type>: permite enviar un paquete ARP eligiendo el tipo de paquete. Type puede valer ARP (petición ARP), ARP-reply (respuesta ARP) entre otros.
--arp-sender-mac <mac>: permite escribir cualquier valor en el campo dirección MAC de origen (suplantando la MAC de su placa de red con cualquier otra.
--arp-sender-ip <ip>: permite escribir en el campo IP origen cualquier dirección IP.

Paquetes ICMP:
--icmp: Indica que se va a enviar paquetes ICMP (Repase protocolo ICMP si no lo recuerda).

Otras opciones
--count <n>: Indica que se van a enviar n paquetes.
--rate <n>: Indica la cantidad de paquetes por segundo a enviar.

Elija dos computadoras. Una computadora será la “víctima”. En otra computadora, ejecute el siguiente comando:
sudo nping --arp --count 1000 -arp-type ARP-reply --rate 100 --arp-sender-mac <Cualquier MAC> --arp-sender-ip <IP del access point o router> <IP atacada>
Intente acceder a Internet desde la IP atacada.
Responda en la plataforma Moodle que acción realiza este comando.

hping3
Utilice preferentemente el sistema operativo Linux Kali, instalado en las computadoras de la facultad de Ingeniería.
También puede instalar la herramienta hping3 en Linux Ubuntu (con sudo apt-get install hping3). Para Windows, descargue desde http://www.hping.org/download.html. No tendrá la misma potencia si no utiliza Linux Kali.
Realice una suplantación de IP origen (IP Spoofing) con el siguiente comando:
hping3 --spoof [ip_a_suplantar] [ip_destino] --icmp --interval u100000
Donde ip_a_suplantar indica la IP que se escribirá en el campo IP fuente.
--icmp indica el tipo de paquetes a enviar. (consulte la ayuda de hping3 para ver más tipos de opciones)
Ip_destino indica la IP a la cual se enviarán paquetes.
--interval u100000 representa el tiempo entre envíos en microsegundos.
Analice con wireshark los paquetes que recibe. Identifique sus IP origen y destino.

Ataque DoS por inundación con hping3

Utilice el siguiente comando

sudo hping3 --flood --icmp --spoof [IP_víctima] [IP_víctima] --interval u1.

Verifique con Wireshark en la máquina víctima que paquetes recibe. Verifique si puede navegar adecuadamente desde la máquina atacada (para impedir que la máquina atacada pueda navegar, puede ser necesario atacar a la máquina víctima desde varias computadoras).

Actividad opcional: Intente atacar la IP de su router o Access Point. ¿Qué resultado obtiene? (no lo intente si otras personas están usando Internet).

Actividad 5: Firewalls

ufw (Uncomplicated Firewall) es una herramienta para configurar por línea de comandos el Firewall incluido en el núcleo de Linux.

Gufw es una herramienta para configurar las reglas de uwf a través de una interfaz gráfica.

Instale ufw y Gufw en una computadora donde posea un servidor web funcionando con:

apt get install ufw (probablemente ya instalado)

apt get install gufw

Ejecute gufw en modo superusuario (desde una consola de comandos, ejecute sudo gufw) y configure como:

Estado: habilitado

Entrante: Denegar

Saliente: Permitir

Verifique si puede entrar a su página web desde otra computadora. Verifique con Wireshark los paquetes que transitan por la red.

Agregue un par de reglas como:

Avanzada

Indique un nombre cualquiera para describir la regla

Política: Permitir

Direccion: Entrante

Interfaz: Todas las interfaces

Registro: Registrar todo

Protocolo: Ambos

A (paquetes entrantes): Indique la IP y puerto al cual permitirá que lleguen paquetes.

Y verifique nuevamente si puede entrar a su página web desde otra computadora.

Agregue una regla para impedir conectarse a alguna IP conocida, por ejemplo, la IP de Facebook. Luego verifique si puede ingresar a la página web bloqueada.

Nota: Gufw no permite configurar todos los comandos de ufw. Para un control mayor del Firewall, debe emplear ufw por línea de comandos.

Anexo 1: Instalación de Linux Kali

Se sugiere instalar Linux Kali como máquina virtual sobre Virtual Box. Linux Kali está disponible como imagen para ser instalada sobre diferentes arquitecturas de procesador ARM o x86 o sobre máquinas virtuales (extensión .iso). También está disponible como sistema operativo virtual para correr máquinas virtuales VirtualBox o VMWare (extensión .ova). La forma más simple de usar es importar a VirtualBox el sistema operativo preinstalado (archivo .ova), pero cualquier método de instalación debería funcionar.

- Puede encontrar imágenes .iso de Linux Kali en https://www.kali.org/downloads/ Deberá instalar la imagen sobre una máquina virtual o sobre una computadora x86 o AMR de la misma manera que instalaría cualquier sistema operativo.
- Puede encontrar el sistema operativo Linux Kali listo para importar para máquinas virtuales VirtualBox o VMWare en https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/ . Para importarlo solo debe hacer doble clic sobre el archivo .ova

Para ambos casos, configure las opciones de red como adaptador puente. Esta opción simulará una interfaz, dándole una IP propia para su máquina virtual Linux Kali, que se comportará como una máquina más de su red. Podrá comunicar su máquina Linux Kali con cualquier otra máquina de la red (incluso la máquina con el sistema operativo huesped), mediante esa IP (pruebe haciendo ping desde su máquina virtual a otras máquinas en su red, o viceversa).