UNCUYO
UNIVERSIDAD NACIONAL DE CUYO

FACULTAD DE INGENIERÍA

Licenciatura en Ciencias de la Computación

Redes de Computadoras
Trabajo práctico Nº7 - Parte A - 2025
Introducción a la seguridad en redes de computadoras

Objetivo

- Distinguir sitios web seguros de no seguros, entender los elementos que hacen seguros a los primeros y las vulnerabilidades de los segundos.
- Analizar distintos tipos de cifrado y certificados SSL empleados en peticiones https en la actualidad.
- 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.

Metodología

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

Aprobación

- Mostrar en clases las actividades 2, 3 y 5 funcionando.
- Elaborar un informe que incluya:
    - Breve explicación de cada actividad (un párrafo es suficiente).
    - Capturas de pantalla de todas las actividades (de la 1 a la 5). Al menos una captura por actividad.
    - Contestar brevemente las preguntas de las actividades 4.1 (ARP spoofing), 4.2 (DoS mediante ping), 4.3 (DoS a servidor NAT), 4,4 (MiTM).

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.

- Sistemas operativos Linux Ubuntu y Linux Kali (ambos disponibles en el laboratorio de la Facultad de Ingeniería. Pueden descargarse libremente desde sus páginas web). Instalados como sistemas operativos nativos (recomendado) o sobre máquinas virtuales con adaptador de red configurado como puente.
- 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.
    - Clonador de sitios web Httrack o Webhttrack (disponible sin costos en repositorios de Ubuntu).
    - Herramientas Nping, Hping3 y Ettercap sobre Linux Kali (recomendado) o Linux Ubuntu (disponible sin costos en repositorios de Linux).
    - Herramienta OpenSSL.
    - Firewall Ufw (instalados por defecto en Linux) y Gufw (disponible sin costos en repositorios de Linux).
    - Navegador web.
    - Servidor web Apache.

Chatbots de IA sugeridos

Para las actividades de este trabajo práctico todos los chatbots sugeridos abajo entregan resultados satisfactorios y precisos, aunque cometen algunos errores (pero pocos).

- ChatGPT de OpenAI (https://openai.com/).
- Grok de xAI (https://grok.com/).
- Gemini de Google (https://gemini.google.com/).
- Meta AI de Meta (accesible a través de Whatsapp).

Actividad 1: Análisis de encriptación y certificados.

Analice los certificados de diferentes páginas web que se indican en el cuestionario Nº7.

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”.

Las páginas web son:

- https://mail.ingenieria.uncuyo.edu.ar/mail/
- https://hb.redlink.com.ar/bna/login.htm
- http://isep.edu.ar/

La información que se pide para cada página web es:

a. Algoritmo de firma del certificado
b. Autoridad de certificación
c. Algoritmo de encriptación de clave simétrica
d. Protocolo de encriptación
e. ¿Podrá un impostor robar sus datos?

Actividad 2: Spoofing web y Phishing.

Clone la página web principal del Banco Patagonia (https://www.bancopatagonia.com.ar/personas/index.php) utilizando la herramienta Webhttrack (Puede instalar la herramienta Webhttrack en Linux Ubuntu con *sudo apt install webhttrack*).

Se pedirá crear un proyecto. Tome nota de la ruta (carpeta) donde se almacenará el proyecto.

Para que la copia no sea demasiado grande y no tome mucho tiempo, vaya a opciones (podría llamarse “definir las opciones” o similar), y configure algunas opciones para limitar la cantidad y tamaño de los archivos a clonar. Entre estas opciones, configure:

- Enlaces->Capturar los ficheros no html próximos: Seleccione No.
- Experto ->Filtro primario->almacenar ficheros html
- Limites->Profundidad máxima: 2
- Limites->Profundidad máxima externa: 1
- Limites->Tamaño máximo otros: 10

Luego comience la captura.

Cuando la captura termine, encontrará el sitio web completo en la carpeta con el nombre del proyecto que indicó al principio. Copie el sitio web en la carpeta de trabajo del servidor Apache. Ingrese y explore la página desde un navegador en la misma computadora, u otra computadora en la misma red LAN (puede utilizar un teléfono celular). (Puede encontrar más información sobre Webhtttrack, incluyendo manuales de uso y foros en https://www.httrack.com/).
Busque el archivo con el código HTML de la página de login (dentro de la carpeta *ebankpersonas*). Cambie el código de manera que cuando el usuario ingrese su nombre de usuario y contraseña y presione la tecla *Ingresar*, se invoquen procedimientos escritos en lenguaje PHP que realicen las siguientes acciones:

1. Almacenen en un archivo el usuario y contraseña ingresadas.
2. El usuario sea direccionado a la página web real de login del Banco Patagonia (de manera que el usuario crea que ha habido un fallo en la conexión de red).

Es posible que necesite descargar la página de login con Webhtttrack de forma separada a la descarga del resto del sitio web.
Por simplicidad, suponga que los usuarios siempre ingresan seleccionando “usuario” y nunca por “documento”.

Nota 1: No se pide reenviar el nombre de usuario y clave ingresados por el usuario a la página web real del Banco Patagonia, se pide solo direccionar la página real simulando una falla de comunicación. Si desea reenviar los datos ingresados por el usuario a la página web real, de modo de construir una aplicación completa de phishing, puede utilizar una de varias opciones:

- Dentro del código PHP, luego de almacenar los datos de usuario y contraseña, reenviar los datos a una página web PHP que contenga los mismos campos para ingresar usuario y contraseña del formulario de la página web real (estos campos deben tener los mismos nombres que en la página web real), de modo que los datos ingresados por el usuario se peguen en estos campos. Luego, enviar el formulario desde una función de JavaScript que se ejecute al inicio.
- Utilizar la extensión cURL para PHP que permite enviar datos utilizando los métodos GET o POST desde código PHP. Probablemente necesite instalar la extensión cURL (sudo apt install libcurl3-dev php-curl).
- Utilizar la función de JavaScript formLogin.submit(); que tiene el mismo efecto que apretar el botón “enviar” en un formulario HTML (donde formLogin es el id del formulario HTML). Puede utilizar una página web intermedia cuyo único propósito sea recibir los datos ingresados por el cliente para almacenarlos (mediante procedimientos PHP), y luego invocar la función indicada al cargar la página web intermedia (estudie el evento onload en la etiqueta body).

Nota 2: Visite la sección “Aviso y que no hacer” de los creadores de Wehttrack (https://www.httrack.com/html/abuse.html). Preste atención a la advertencia:

- Do not steal private information
  - Do not grab emails
  - Do not grab private information

Este ejercicio práctico, con fines educativos, simula ataques de phishing para comprender y contrarrestar sus mecanismos. Se recuerda que el phishing constituye un delito bajo la figura de Estafa Informática en Argentina, independientemente del uso posterior o no de los datos obtenidos. No realice esta actividad con otros fines que no sean educativos y con el conocimiento y consentimiento de las personas involucradas.

Actividad 3: Creando certificados.

En el trabajo práctico N°6 parte A implementó una página web sencilla. Analice si su página web encripta información.
Para analizar si alguien puede “robar” información, ejecute Wireshark y comience una captura de datos. Ingrese a su página web desde otra computadora (puede ser un teléfono celular), ingrese datos 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 la información enviada.

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 un certificado autofirmado para que el proceso sea sin costo. Para un servidor real debe comprar un certificado a una autoridad de certificación.

1 - Agregue un certificado en su página web. Para ello, siga los siguientes pasos:
Instale openssl para Apache2:
sudo apt install apache2 openssl

2 - Habilite los módulos ssl para Apache2:

sudo a2enmod ssl

sudo a2enmod rewrite

3 - Reinicie el servidor Apache:

sudo systemctl restart apache2

4 - Cree una carpeta donde almacenar las claves y certificados (puede ser cualquiera menos /var/www/html/ ya que dicha carpeta es la carpeta de acceso público de Apache):

5 - Cree un par clave pública y clave privada con Openssl:

sudo openssl genrsa -out mi_clave.key 4096

(el archivo mi_clave.key contendrá sus claves públicas y privadas. Puede nombrar a dicho archivo como desee, conservando la extensión .key).

6 - Cree un certificado autofirmado con:

sudo openssl req -new -x509 -key mi_clave.key -sha256 -days 365 -out mi_certificado.crt

(en archivo mi_certificado.crt contiene el certificado. Puede nombrarlo como desee, conservando la extensión .crt o .pem)

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.

7 - Verifique que Apache esté escuchando solicitudes en el puerto 443 (puerto por defecto para solicitudes https). Para ello, verifique que el archivo */etc/apache2/ports.conf* contenga las siguiente líneas:

```
<IfModule ssl_module>
        Listen 443
</IfModule>
```

(Repasar Unidad 5 y Trabajo Práctico Nº6 si no recuerda estos conceptos)

8 - Configure Apache para indicarle la ubicación del certificado editando el archivo de configuración de Apache: */etc/apache2/sites-enabled/000-default.conf*, puede usar:

sudo gnome-text-editor /etc/apache2/sites-enabled/000-default.conf

(Repasar Unidad 5 y Trabajo Práctico Nº6 si no recuerda estos conceptos)

(Nota: gnome-text-editor es el editor de texto por defecto de Ubuntu 24.04.1. Puede usar cualquier editor de textos)

En dicho archivo agregue al final:

```
<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 /ruta al certificado/certificado.crt
SSLCertificateKeyFile /ruta al archivo con las claves/mi_clave.key
</VirtualHost>

9 - 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.

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, DoS, MITM

Se sugiere realizar las siguientes actividades utilizando el sistema operativo Linux Kali (En el laboratorio de la Facultad de Ingeniería, puede exportar el mismo desde el arranque de VMWare).

4.1 ARP spoofing con 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). Utilice la herramienta Linux Kali para esta actividad (Puede instalar Nping en Linux Ubuntu, pero no tendrá la misma potencia). La forma de uso es:

nping [tipo de paquete] [opciones] {IP a la cual se envía el paquete}

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 la computadora víctima anote la dirección MAC asignada al gateway.
Para conocer la IP del Gateway puede usar (en Linux): ip route

En otra computadora, ejecute el siguiente comando:
sudo nping --arp --count 100000 -arp-type ARP-reply --rate 1000 --arp-sender-mac <Cualquier MAC, menos la del gateway> --arp-sender-ip <IP del gateway> <IP victima>
Intente acceder a Internet desde la IP atacada. Si utiliza un teléfono celular como víctima, desactive los datos móviles. Verifique si la dirección MAC que aparece en la tabla ARP de la computadora víctima sigue siendo la misma.
Para el informe: Describa brevemente la acción que realiza este comando.

4.2 DoS con hping3
Utilice 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
Para realizar un ataque DoS, utilice el siguiente comando:
sudo hping3 --icmp --flood --rand-source [IP_víctima]

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).
Para el informe: Describa brevemente la acción realizada por el comando indicado.

4.3 Ataque DoS a un servidor NAT con hping3

El siguiente comando puede afectar la performance de un servidor NAT, incluso sacarlo de servicio.

```
sudo hping3 --icmp --flood --rand-source  8.8.8.8
```

Nota: ejecutar el comando anterior puede provocar que todas las máquinas que utilizan el servidor NAT queden sin conexión a Internet. No lo utilice en su casa u oficina si otras personas están accediendo a Internet (durante la práctica en el laboratorio puede utilizarlo sin problemas).
Para el informe: Describa brevemente porqué el comando indicado afecta al servidor NAT, siendo que la IP atacada es el DNS de Google.

4.4 MITM

Puede realizar un ataque MITM envenenando las tablas ARP de ambas víctimas con los métodos ya vistos. La aplicación Ettercap (Linux Kali) simplifica el trabajo. (puede instalar una versión gráfica de ettercap para Linux Ubuntu con *sudo apt install ettercap-graphical*).
Elija dos máquinas a atacar mediante MITM (una máquina puede ser un celular conectado en la misma LAN. También podría ser el router). Luego ejecute el siguiente comando (también puede usar la versión gráfica de Linux Kali o Ubuntu):

```
ettercap -T --mitm arp /ip_equipo_A// /ip_equipo_B//
```

Una vez que el ataque sea exitoso (verá la leyenda “apriete h para ayuda”) visualice con Wireshark si puede ver la información intercambiada por las máquinas atacadas.
En la versión gráfica de ettercap, vaya a “Targets”, escriba las IPs entre las cuales realizar MITM, en “view” seleccione “Resolve IP Addresses” y luego comience el ataque seleccionando “ARP poisoning”.
Para el informe: Describa brevemente el efecto de este ataque.

Un ataque MITM con el propósito de obtener información o un ataque DoS con el propósito de hacer inaccesible o entorpecer un sistema informático pueden constituir delitos. No realice estas actividades con otros fines que no sean educativos y con el conocimiento y consentimiento de las personas involucradas.

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 y verifique si puede conectarse con ssh (no debería poder acceder). 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. Habilite los puertos 80,443,22.
Verifique nuevamente si puede entrar a su página web desde otra computadora y verifique si puede conectarse con ssh (si debería poder acceder).
Agregue una regla para impedir conectarse a alguna IP conocida, por ejemplo, la IP de frm.utn.edu.ar. Luego verifique si puede ingresar a la página web bloqueada.
Nota: Es posible que una DNS tenga varias IPs asociadas. Debe bloquear todas para impedir el acceso a la página web que desea bloquear.
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 sobre Virtual Box

En los laboratorios de informática de la Facultad de Ingeniería dispone de una versión de Linux Kali para instalar como sistema nativo.

Para trabajar sobe su computadora, 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 o .dvi).

Puede encontrar imágenes de Linux Kali en https://www.kali.org/get-kali/#kali-virtual-machines

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 huésped), mediante esa IP (pruebe haciendo ping desde su máquina virtual a otras máquinas en su red, o viceversa).