LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

Redes de Computadoras

Trabajo Práctico 7

Alumnos: Gabriel Lopez Romero, Juan Ignacio Massacesi

Introducción a la seguridad en redes de computadoras

Contents

1 Introducción

Este informe está dirigido a dar detalles sobre las actividades realizadas en este trabajo práctico, orientado a la seguridad en las redes de computadoras, tocando temas como firewall, encriptación, certificados SSL, phishing y otros.

2 Procedimiento

Este trabajo consiste de cinco actividades principales:

2.1 Certificados SSL

Verificar si ciertos sitios web son seguros o no, analizando sus certificados.

2.2 Spoofing web y Phishing

Clonar una página web y simular que estamos modificandola para hacer phishing, guardando credenciales de inicio de sesión a una entidad bancaria.

2.3 Creación de certificados

Generar un certificado para nuestro sitio web de encuestas de equipos de fútbol creado en el TP 6.

2.4 ARP Spoofing, DoS, MITM

Realizar un ataque ARP Spoofing donde un atacante envía mensajes ARP falsos para asociar su dirección MAC con la IP de otro dispositivo.
Realizar un ataque DoS para hacer que una red no esté disponible para sus usuarios, enviando una gran cantidad de tráfico o solicitudes maliciosas.
Realizar un ataque MITM para interceptar la comunicación entre dos maquinas sin que ellas lo sepan.

2.5 Firewall

Hacer experimentos con el firewall, insertando reglas que permitan o bloqueen ciertos comportamientos en la red.

Todos estos incisos fueron llevados a cabo con éxito, cumpliendo con los requerimientos indicados.

3 Resultados

3.1 Actividad 1

En esta actividad, analizamos los certificados SSL de los sitios mencionados en el TP, verificando si estos son seguros o no.

Sitio web	`https://mail.ingenieria.uncuyo.edu.ar/mail/`
Algoritmo de firma	Elliptic Curve
Entidad certificadora	Let's Encrypt
Cifrado simétrico	TLS_AES_256_GCM_SHA384
Protocolo	TLS 1.3
Vulnerable a robo de datos?	No (certificado válido y protocolo actualizado)

Sitio web	`https://hb.redlink.com.ar/bna/login.htm`
Algoritmo de firma	RSA
Entidad certificadora	DigiCert Inc
Cifrado simétrico	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocolo	TLS 1.2
Vulnerable a robo de datos?	No (certificado válido)

Sitio web	`http://isep.edu.ar/`
Algoritmo de firma	N/A
Entidad certificadora	N/A
Cifrado simétrico	N/A
Protocolo	N/A
Vulnerable a robo de datos?	Si (NO tiene certificado SSL)

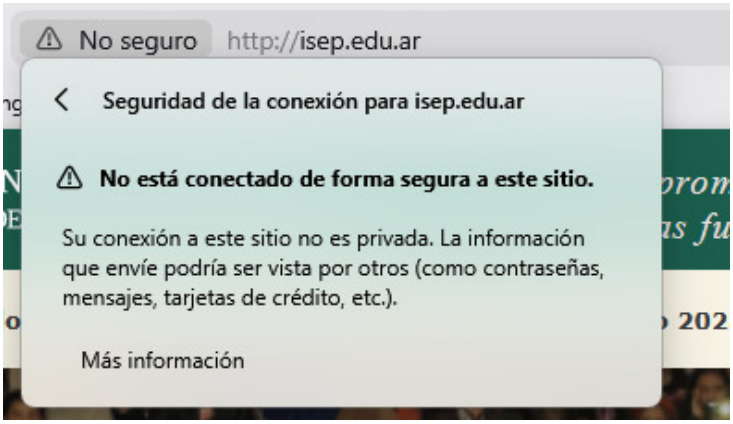

Figure 1: Certificado ausente en la ultima pagina analizada

3.2 Actividad 2

En esta actividad, clonamos el sitio web del Banco Patagonia con el objetivo de modificarla para que al momento de iniciar sesion se redirija al usuario a la página original, simulando un error del sistema, mientras aprovechamos el clon para robar sus credenciales y guardarlas.

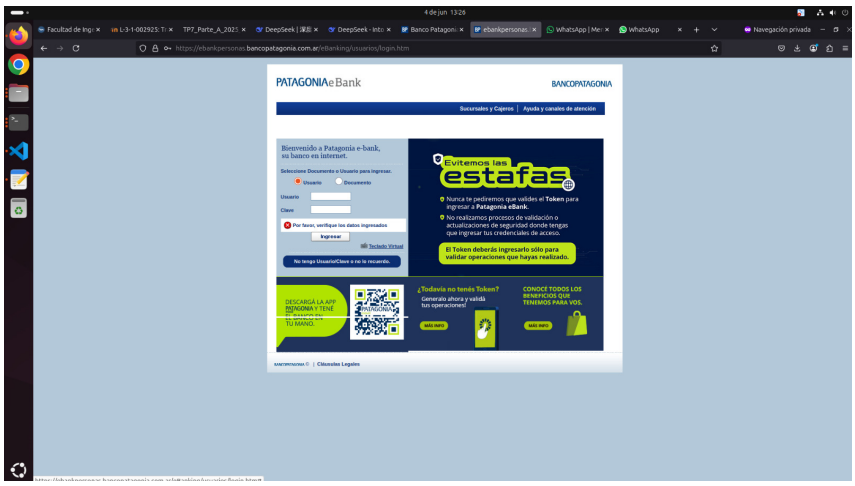

Figure 2: Usuario redirigido a la web original, simulando un error.

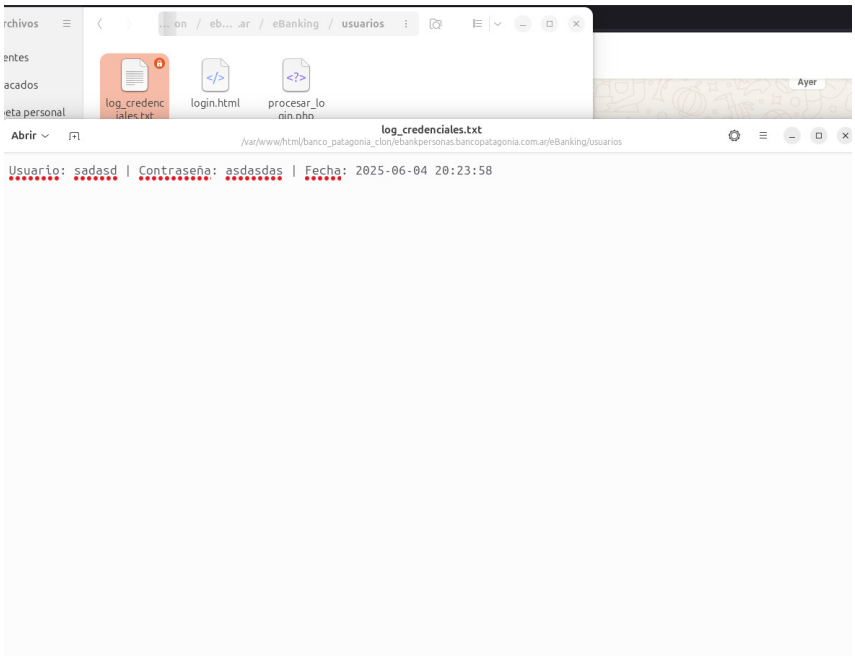

Figure 3: Credenciales guardadas con exito

3.3 Actividad 3

En este inciso, verificamos las vulnerabilidades presentes en el sitio web creado en el TP 6, para luego crear un certificado autofirmado. Este certificado hara que las interacciones cliente-servidor esten encriptadas y no puedan ser interceptadas por Wireshark, como si sucedía antes de generarlo.

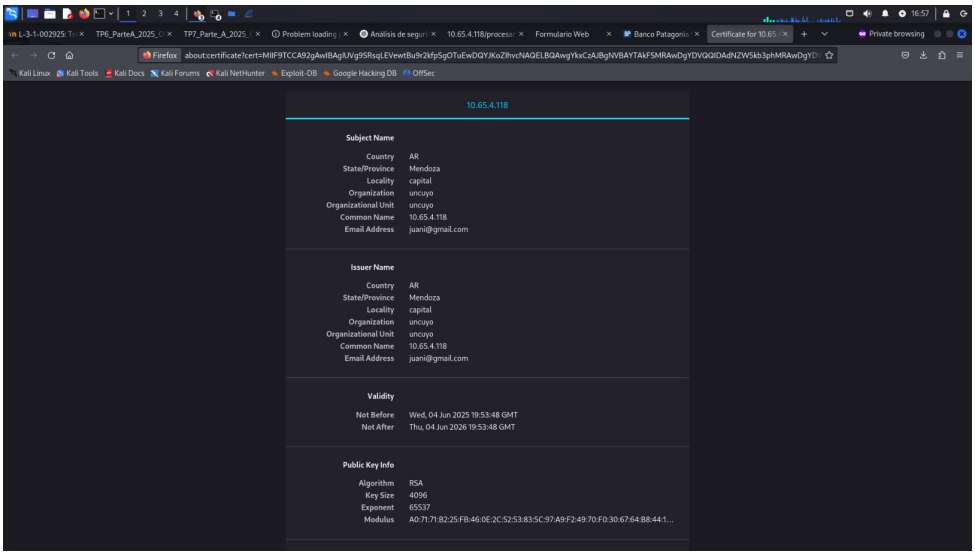

Figure 4: Detalles del certificado SSL generado

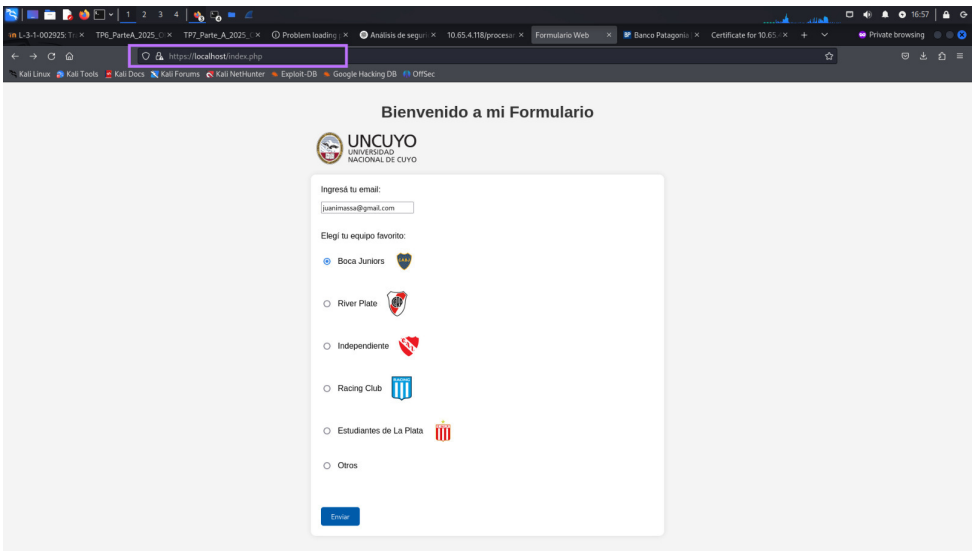

Figure 5: Certificado aplicado correctamente (https)

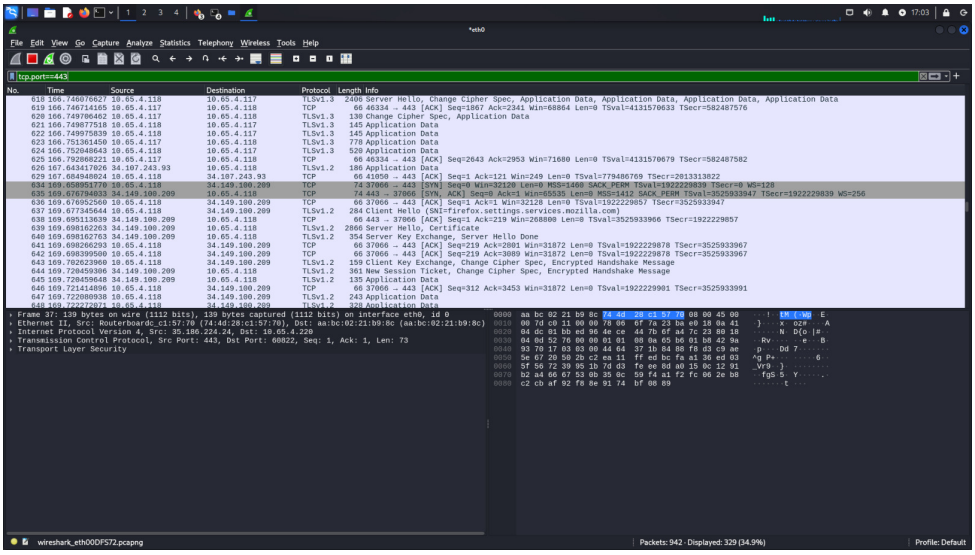

Figure 6: Paquetes encriptados gracias al certificado SSL

3.4 Actividad 4

3.4.1 ARP spoofing con Nping

El comando ejecuta un ataque de ARP Spoofing, en el que se envían 100.000 respuestas ARP falsas a razón de 1000 por segundo. Estas respuestas le indican a la computadora víctima que la dirección IP del gateway está asociada a una dirección MAC falsa (distinta de la real).

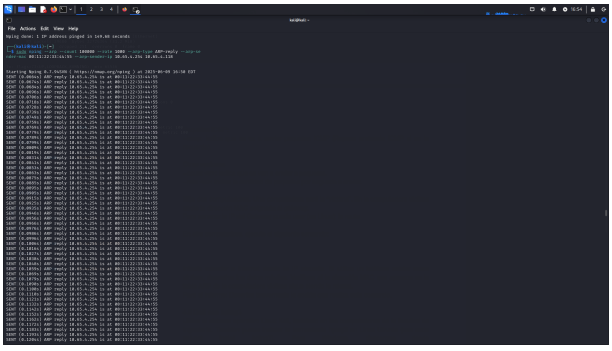

Figure 7: Terminal de la computadora que realiza el ataque ARP Spoofing

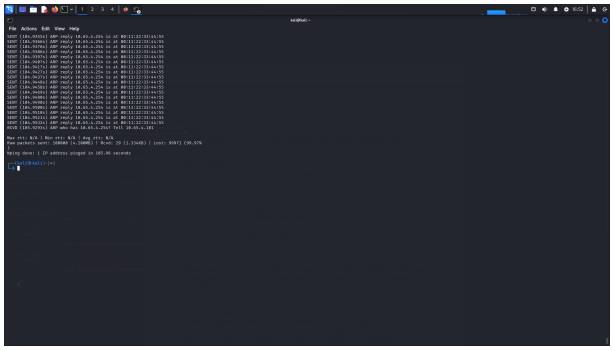

Figure 8: Terminal de la computadora que realiza el ataque ARP Spoofing

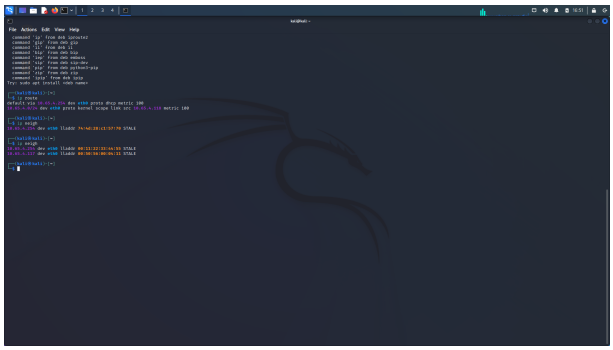

Figure 9: Terminal de la computadora victima (vemos que la dirección MAC cambio de la real a la falsa)

3.4.2 DoS con hping3

Este comando permite simular que los paquetes provienen de otra máquina, enviando mensajes ICMP a gran velocidad. El objetivo es saturar al equipo de destino con tráfico inútil, provocando una sobrecarga de red o del sistema, lo cual puede ralentizar o interrumpir sus servicios normales.

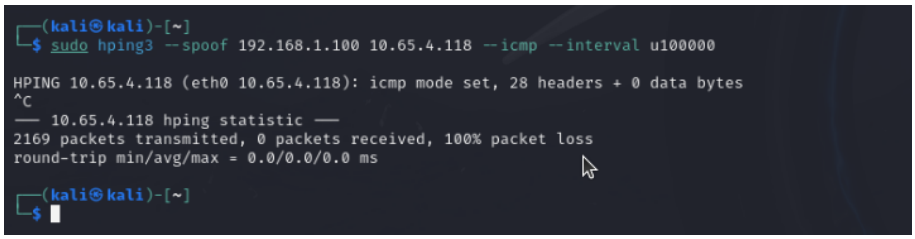

Figure 10: Terminal de la computadora que envia paquetes ICMP, con una IP de origen falsa hacia una IP destino

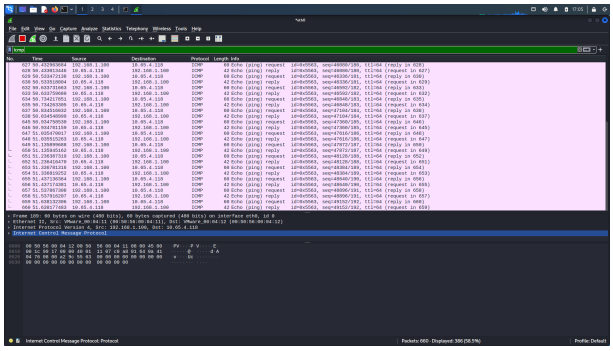

Figure 11: Los paquetes ICMP llegan al equipo víctima con una IP de origen falsa

Ataque DoS por inundación con hping3

Este comando lanza un ataque de Denegación de Servicio (DoS) mediante una inundación de paquetes ICMP, con direcciones IP de origen aleatorias generando una sobrecarga en el sistema de la víctima. La opción –rand-source simula que los paquetes provienen de múltiples orígenes.

Figure 12: Terminal de la computadora que realiza la inundación de paquetes ICMP

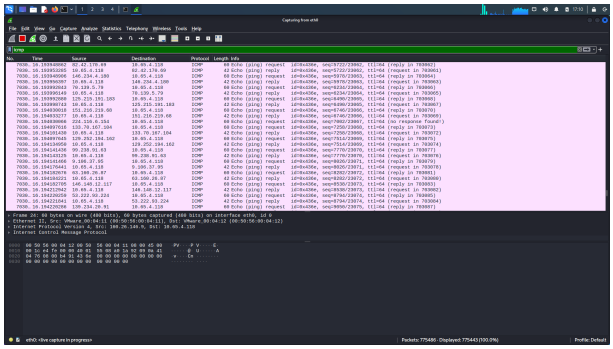

Figure 13: Se observan paquetes ICMP entrantes con diferentes direcciones IP de origen

3.4.3 Ataque DoS a un servidor NAT con hping3

Este comando **sudo hping3 –icmp –flood –rand-source 8.8.8.8** envía una gran cantidad de paquetes ICMP con direcciones IP de origen aleatorias hacia la IP 8.8.8.8.

Dado que las IPs de origen son aleatorias, el servidor NAT trata de crear nuevas entradas en su tabla de conexión para cada paquete, esto puede impedir la salida a Internet de todos los dispositivos conectados a través de él ya que el servidor NAT se verá saturado.

3.4.4 MITM

El comando realizado consiste en falsificar las tablas ARP de dos dispositivos dentro de una misma red. Esto provoca que el tráfico de red entre ambos pase por el equipo atacante. De este modo, es posible capturar información sensible, como contraseñas y mensajes.

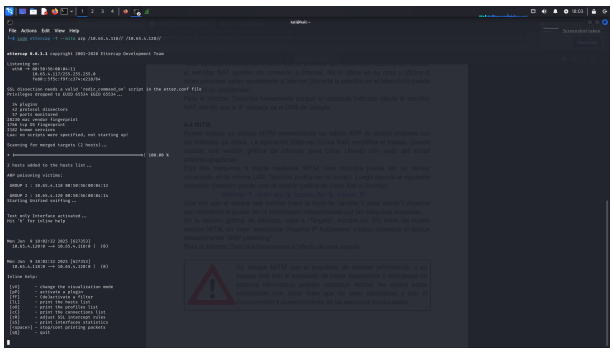

Figure 14: Terminal de computadora que realiza el ataque MITM

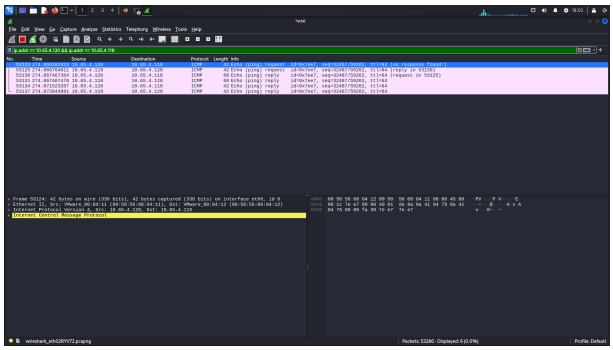

Figure 15: Tráfico de paquetes entre las víctimas

3.5 Actividad 5

Finalmente, en esta actividad, experimentamos con gufw, una aplicación para configurar el firewall de Linux gráficamente. Verificamos que, al activar el firewall, es imposible acceder desde otro dispositivo a la web generada en la Actividad 2, como también conectarse al equipo mediante SSH. Aplicando ciertas reglas, más especificamente, generando excepciones a ciertos puertos (80, 22, 443) para que se pueda acceder mediante ellos.

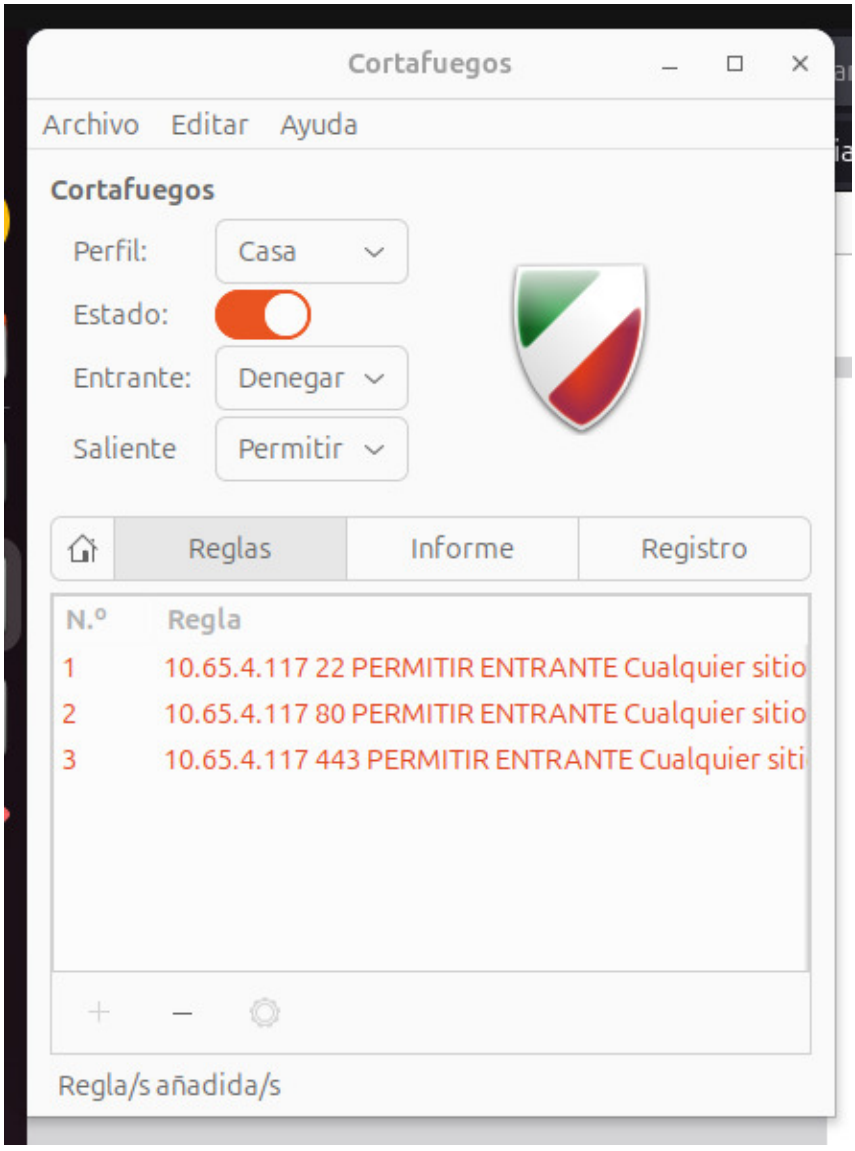

Figure 16: Firewall activado con reglas establecidas, permitiendo comunicación mediante los puertos 80, 22 y 443

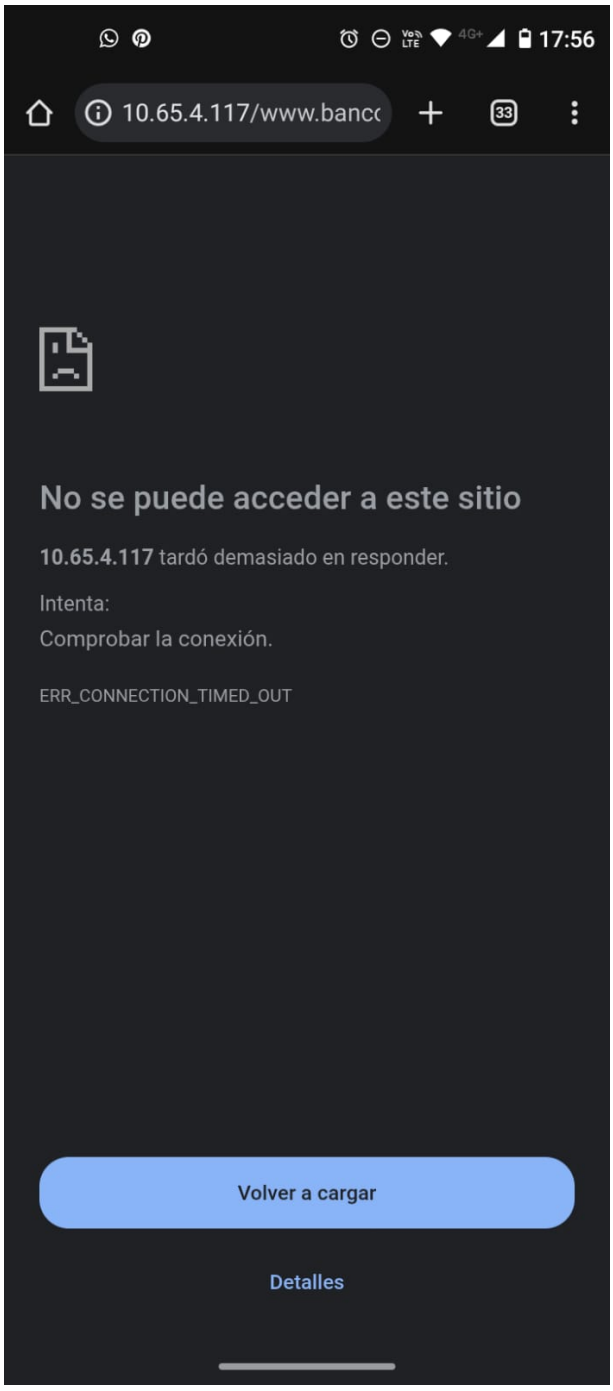

Figure 17: Conexión rechazada al intentar acceder a la web de la Actividad 2 con firewall activado (sin reglas)