UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL APLICABLES A UNA RED QUE MITIGUEN EL SECUESTRO DE SESIONES EN EL PROTOCOLO TCP

JIMENEZ PULLA ROSA LISSETTE
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL APLICABLES A UNA RED QUE MITIGUEN EL SECUESTRO DE SESIONES EN EL PROTOCOLO TCP

JIMENEZ PULLA ROSA LISSETTE
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL APLICABLES A UNA RED QUE MITIGUEN EL SECUESTRO DE SESIONES EN EL PROTOCOLO TCP

JIMENEZ PULLA ROSA LISSETTE
INGENIERA DE SISTEMAS

LOJA MORA NANCY MAGALY

MACHALA, 31 DE ENERO DE 2019

MACHALA
31 de enero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado IMPLEMENTACIÓN DE MECANISMOS DE CONTROL APLICABLES A UNA RED QUE MITIGUEN EL SECUESTRO DE SESIONES EN EL PROTOCOLO TCP, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

LOJA MORA NANCY MAGALY
0703410027
TUTOR - ESPECIALISTA 1

JUMBO CASTILLO FREDDY ANIBAL
0704167949
ESPECIALISTA 2

CÁRDENAS VILLAVICENCIO OSCAR EFRÉN
0703935312
ESPECIALISTA 3

Fecha de impresión: viernes 01 de febrero de 2019 - 14:48

Urkund Analysis Result

Analysed Document: JIMENEZ_PULLA_ROSA.pdf (D47095282)
Submitted: 1/22/2019 2:30:00 AM
Submitted By: rljimenez_est@utmachala.edu.ec
Significance: 5 %

Sources included in the report:

PIEDRA PINEDA BÉLGICA VANESSA_PT-010518.pdf (D40244467)
Jorge Castro-Titulacion.pdf (D47087440)

Instances where selected sources appear:

4

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, JIMENEZ PULLA ROSA LISSETTE, en calidad de autora del siguiente trabajo escrito titulado IMPLEMENTACIÓN DE MECANISMOS DE CONTROL APLICABLES A UNA RED QUE MITIGUEN EL SECUESTRO DE SESIONES EN EL PROTOCOLO TCP, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 31 de enero de 2019

JIMENEZ PULLA ROSA LISSETTE
0706603719

DEDICATORIA

Este trabajo está dedicado a Dios y a mis padres que son las personas que más amó, por el sacrificio y esfuerzo que han hecho para que culmine con éxitos la carrera; son quienes me inculcaron la responsabilidad y los deseos de superación.

Srta. Jiménez Pulla Rosa Lissette.

AGRADECIMIENTO

Agradezco a mis padres y hermanas por su apoyo constante, por sus palabras de aliento que me motivan día a día a salir adelante y no darme por vencida ante los problemas que presenten en la vida; a mis docentes por instruirnos con sus conocimientos y habilidades durante todo el proceso de formación académica; a mi tutora la Ing. Nancy Loja por su paciencia y guía permitieron la realización con éxito este trabajo.

.

Srta. Jiménez Pulla Rosa Lissette.

RESUMEN

TCP (Protocolo de Control de Transmisión) es un protocolo seguro que controla que todos los datos transmitidos estén libres de errores y sean recibidos en el mismo orden en que fueron enviados. Si existe una falla en la transmisión de datos emplea mecanismos para que estos sean reenviados y lleguen a su destino.

La problemática de este trabajo se centró en las falencias que tiene el protocolo TCP en el envío de datagramas de una terminal a otra, dado que la información se encuentra desencriptada siendo vulnerable a ataques de suplantación de direcciones IP, el secuestro de sesiones, envenenamiento ARP, entre otros.

Debido a esto, se planteó dos escenarios de simulación de ataques en un entorno virtualizado utilizando las herramientas GNS3 y VirtualBox para emular la creación de host virtuales y el diseño de una red de datos; luego se procedió a utilizar las herramientas Ettercap, Wireshark y netwox para efectuar los ataques de secuestro de sesiones ciego, no ciego y el restablecimiento TCP.

Se implementaron los controles a nivel de host del cliente mediante la modificación de la tabla ARP y a nivel de servidor se configuró los iptables para que elimine los paquetes RST que ingresen en la conexión, evitando con ello el cierre de la sesión. Al implementar los mecanismos de control en la red se evidenció que estos ataques no afectaron su funcionamiento.

Palabras claves: envenenamiento ARP, mecanismos de control, secuestro de sesiones, suplantación de IP, TCP.

ABSTRACT

TCP (Transmission Control Protocol) is a secure protocol that controls that all transmitted data are free of errors and are received in the same order in which they were sent. If there is a failure in the transmission of data, it uses mechanisms so that they are forwarded and reach their destination.

The problem of this work focused on the shortcomings of the TCP protocol in the sending of datagrams from one terminal to another, given that the information is decrypted, being vulnerable to attacks of IP address spoofing, session hijacking, ARP poisoning. , among others.

Due to this, two scenarios of simulation of attacks in a virtualized environment were raised using the GNS3 and VirtualBox tools to emulate the creation of virtual hosts and the design of a data network; Then we proceeded to use the Ettercap, Wireshark and Netwox tools to perform blind session seizure attacks, not blind and TCP reset.

The controls were implemented at the client's host level through the modification of the ARP table and at the server level, the iptables were configured to eliminate the RST packets that enter the connection, thereby preventing the session from being closed. By implementing the control mechanisms in the network it was evident that these attacks did not affect its operation.

Keywords: ARP poisoning, control mechanisms, session hijacking, IP spoofing, TCP.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Con el auge de la tecnología y del Internet se han implementado protocolos como el TCP (Protocolo de control de transmisión), el cual permite que los equipos se comuniquen entre sí, por ser compatibles con cualquier sistema operativo que lo utilice. [1]

En las redes TCP los paquetes son enviados de un ordenador a otro envuelven un encabezado IP que contiene la dirección IP, puerto de origen del host emisor y la dirección IP, puerto destino del host receptor. A pesar de que los hosts destino remiten al host de origen, TCP no verifica la dirección IP de origen del paquete. [2]

Por estas falencias en el protocolo TCP, es vulnerable a ataques provocados por terceras personas (atacantes) que intentan hurtar información sensible de los usuarios que se conectan a una aplicación mediante la interrupción de la comunicación, deshabilitando los servicios y provocando graves conflictos en los sistemas que se encuentran manipulando. [3]

La problemática presente en este trabajo es poner a prueba las vulnerabilidades del TCP, a través de un servidor de Telnet instalado en el Sistema operativo Centos 7, teniendo como cliente a Windows 7 y como atacante a Kali Linux; el cual realizó una falsificación de direcciones IP del origen que permitieron efectuar el secuestro de sesiones y el restablecimiento TCP.

Actualmente es indispensable conocer las debilidades que tiene el protocolo TCP en la trasmisión de datos con la finalidad de implementar controles que ayuden a mitigar estos ataques.

Este informe se encuentra detallado de la siguiente manera:

Capítulo 1: Está conformado por la Introducción, el problema, el marco Contextual y el objetivo de la presente investigación.

Capítulo 2: Es la recolección de información científica que ayuda a la fundamentación teórica del Marco teórico.

Capítulo 3: Se encuentra la descripción de los resultados obtenido una vez implementado el ataque y las conclusiones.

1.1. Marco Contextual

Es imprescindible que al momento de diseñar una topología de red se implementen controles y estándares de seguridad que garanticen el envío seguro de paquetes de información entre computadores y aplicaciones, para que no sean afectados por los ataques

de suplantación, secuestro de sesiones y restablecimiento de los paquetes TCP que afecta a la conectividad del servicio.

El secuestro de sesiones se efectúa con un ataque combinado que se encarga de capturar y alterar el tráfico de una red con técnicas de spoofing que hace que se redireccione la conexión hacia el atacante. En seguridad, este tipo de ataque es el que presenta una mayor dificultad para combatirlo.

1.2. Problema

¿Explorar las vulnerabilidades basadas en TCP (Protocolo de control de transmisión), permitirá tomar las mejores decisiones en el diseño e implementación de redes con el menor impacto posible, en caso de que estas vulnerabilidades sean explotadas?

1.3. Objetivo

Implementar mecanismos de control a una red de datos mediante técnicas de seguridad, para la mitigación del secuestro de sesiones en el protocolo TCP.

2. DESARROLLO

2.1. Marco teórico

2.1.1. TCP (Protocolo de Control de Transmisión).

Este protocolo funciona a nivel de la capa de transporte, garantizando la comunicación entre hosts, por ello que es muy utilizado por aplicaciones de internet como HTTP y conexiones remotas como Telnet y SSH, dado que se lo considera confiable por la entrega ordenada de la información y por los mecanismos de respuesta que tiene implementado para hacer frente a los fallos mediante el reenvío de los datos.[4], [5]

TCP está diseñado para ser utilizado en conjunto con el protocolo IP que permite el desarrollo de las comunicaciones con cualquier tipo de dispositivo de forma segura, brindando una mayor confiabilidad en la transmisión de datagramas. En la conexión TCP se identifican las tuplas que contienen los datos de la IP y puerto de origen como también del destino, además integra los números de secuencia y de los paquetes que son enviados.[6]

2.1.2. Secuestro de sesiones.

El secuestro de sesiones es el acceso no autorizado de terceras que hurtan las credenciales que poseen los usuarios al hacer uso de los servicios web. A través de herramientas que facilitan la captura del tráfico red al tener información de la ID de sesión o el ID token. [7]

El secuestro de sesión da acceso como un usuario auténtico, atacando a la integridad del servicio.

2.1.2.1. Secuestro de sesiones no ciego.

Este tipo de ataque se da cuando el atacante se encuentra en la misma subred que el servidor. Él tiene acceso a la secuencia y el número de paquetes que son enviados, para poder corromper el DataStream de una conexión ya establecida.[8]

La principal amenaza de la suplantación de identidad es que el atacante puede omitir la autenticación para acceder al servicio.

2.1.2.2. Secuestro de sesiones ciego.

El atacante se encuentra en una subred diferente a la del servidor, en el cual hace uso de las herramientas que permiten obtener los números de secuencia facilitando con ello la captura de los datos a través del envenenamiento ARP.[9]

2.1.2.3. Ataque de reinicio de TCP.

Un ataque de reinicio de TCP consiste en abortar una conexión establecida entre dos hosts.

El atacante aprovecha el modo de configuración que tiene TCP para establecer una conexión a través del enlace de 3 vías, mediante el envío de un número ACK incorrecto al remitente ocasionando el reinicio del segmento y perdiendo la conectividad con el servicio que está utilizando la víctima. [10]

2.1.2.4. Man In the Middle

Es el redireccionamiento del tráfico de red hacia un tercero con la finalidad poder interceptar, modificar o eliminar los paquetes que son enviados a la víctima objetivo. El atacante toma el control del canal de comunicación para poder infligir los principios de seguridad como Integridad, Disponibilidad y Confidencialidad. Este este tipo de ataque la víctima desconoce al atacante, al pensar que está protegida la conexión. [11]

Hay distintas formas de ejecutar el Hombre en el medio como son las siguientes:

- ✓ MITM basado en técnicas suplantación
- ✓ MITM basado en el canal de comunicación en la que se encuentra el atacante
- ✓ MITM basado en la ubicación del atacante.

2.1.3. Herramientas utilizadas para la ejecución del ataque.

2.1.3.1. Ettercap.

Ettercap es una herramienta de código abierto que se puede ejecutar en distintos sistemas operativos como Mac OS, Linux y Solaris. Fue diseñada para interceptar y rastrear la comunicación de una red a través de inyecciones de caracteres; además facilita el filtrado de paquetes y el envenenamiento ARP, posibilitando el análisis de las comunicaciones que hay entre los distintos hosts. [12]

2.1.3.2. Wireshark.

Esta herramienta se denomina como un analizador de protocolo de red o sniffer al permitir la captura y el análisis de los paquetes de una red. Se puede utilizar para examinar los detalles del tráfico que tiene cada protocolo de red para ver las variaciones de nivel que tiene una terminal en el envío de datagramas. La captura de paquetes puede proporcionarle a un administrador de red información suficiente sobre el tiempo de transmisión, la fuente, el destino, el puerto y los datos del encabezado de un segmento. Esta información puede ser útil para evaluar los eventos de seguridad. [13]

2.1.3.3. Nmap.

Esta herramienta sirve para evaluar la seguridad de un sistema informático, permitiendo el

análisis del tráfico de la red a través del escaneo de servicios o puertos que se encuentran habilitados; permitiéndole al atacante extraer información confidencial del cliente. [14]

2.1.3.4. Netwox

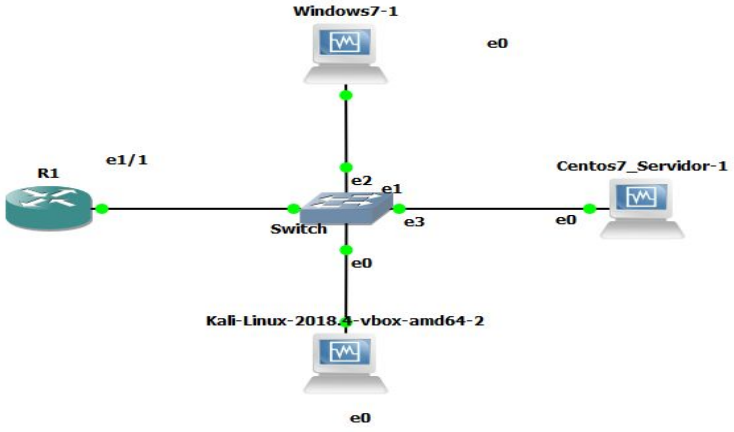
Netwox es una herramienta que permite transmitir paquetes falsificados en una red. Por medio de ella, se pueden enviar paquetes en estado RST que fuerzan el reiniciar de la conexión TCP .[15]

2.2. Solución del problema

2.2.1 Construcción del Escenario Virtual.

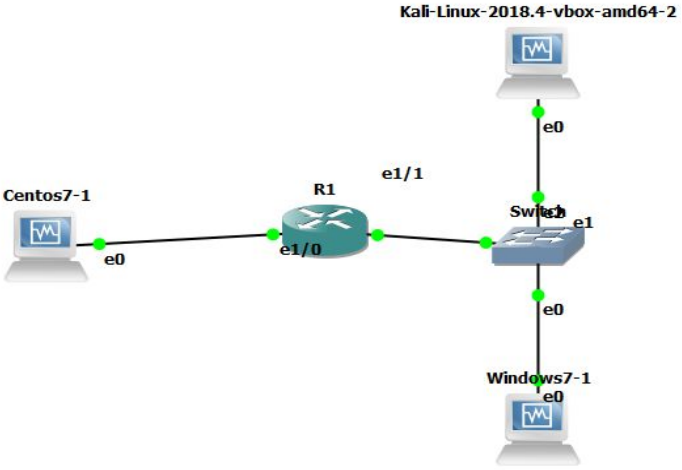
Para poner a prueba las vulnerabilidades de TCP en el secuestro de sesiones se diseñó un escenario virtual utilizando las herramientas GNS3 2.0.3 y VirtualBox 5.2.22 para emular las siguientes topologías de red en los escenarios de la Fig. 1 y Fig. 2.

Figura 1: Escenario #1



Fuente: Elaboración propia

Figura 2: Escenario #2



Fuente: Elaboración propia

Los escenarios están conformados por los elementos que interviene en la topología de red detallados en la Tabla 1.

Tabla 1: Componentes de la topología de red

Equipo	Sistema Operativo	Actividad
Router	Cisco IOS	Enrutamiento de dirección IP que van utilizar los hosts para conectarse a una red
Servidor	Centos7	Servicio de Telnet
Atacante	Kali-Linux	Prueba de penetración en la red.
Víctima	Windows 7	Persona que accede a Telnet

Fuente: Elaboración propia

Para el diseño de la topología de red se elaboró una tabla de direccionamiento IP que va a tener asignado cada equipo de acuerdo a la Tabla 2.

Tabla 2: Configuración de direcciones IP

Equipo	Dirección IP	Máscara de Subred	Puerta de Enlace
R1 – Router	e1/0 192.168.2.17	255.255.255.240	192.168.2.17
	e1/1 192.168.2.1	255.255.255.240	192.168.2.3
Centos7-Servidor	192.168.2.3 192.168.2.21	255.255.255.240	192.168.2.1 192.168.2.17
Windows7-Víctima	192.168.2.18	255.255.255.240	192.168.2.17
Kali-Linux-Atacante	192.168.2.20	255.255.255.240	192.168.2.17

Fuente: Elaboración propia

2.2.2 Desarrollo del ataque de Secuestro de sesiones no ciego.

Para el desarrollo de ataque se utilizó el escenario # 1 que se muestra en la Fig. 1.

En la topología planteada en ese escenario se visualiza que todos los hosts se encuentran en la misma subred, con la cual el atacante emplea la herramienta Ettercap para realizar el hombre en el medio por envenenamiento ARP, que consiste en enviar Sniff por la red como se muestra en la Fig 3.

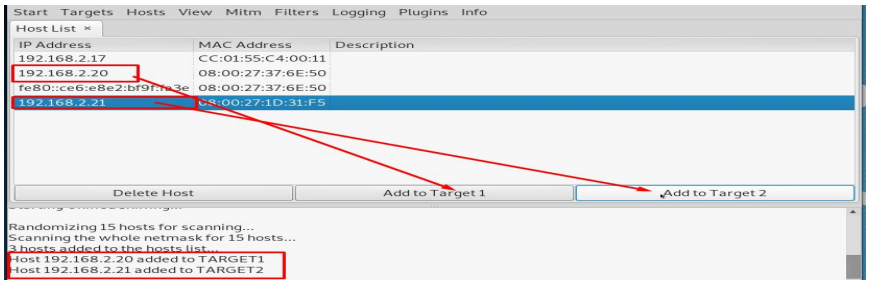
Figura 3: Envío del Sniff a la red

Fuente: Elaboración propia

Luego el atacante procede a escáner los hosts que se encuentra en la red, los enlista, y

selecciona las direcciones IP del servidor de Telnet y del cliente de Windows 7 como se muestra en la Fig. 4.

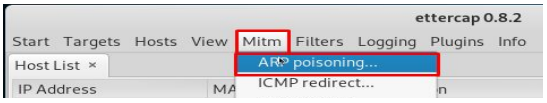
Figura 4: Lista de hosts de la red



Fuente: Elaboración propia

Una vez establecidas las víctimas se procede a ejecutar el ataque de envenenamiento ARP a todas las conexiones, con el objetivo de redireccionar el tráfico de paquetes hacia el atacante como se visualiza en la Fig. 5.

Figura 5: *Ejecución del ataque ARP*



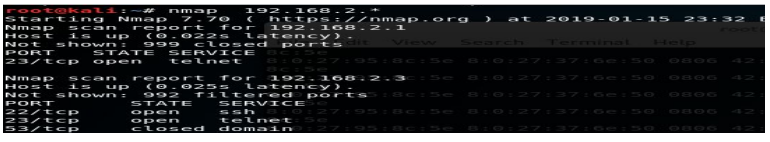
Fuente: Elaboración propia

Con ayuda de Wireshark el atacante captura el tráfico TCP y los paquetes que son enviados al cliente y al servidor de telnet. En ettercap queda capturada la contraseña y el usuario del servidor como se muestra en el Anexo A.

2.2.3 Desarrollo del ataque de Secuestro de sesiones Ciego

Para este ataque se procedió a realizar un escaneo de red global para conocer todas las IP que hay en las distintas interfaces de red como se muestra en la Fig. 6

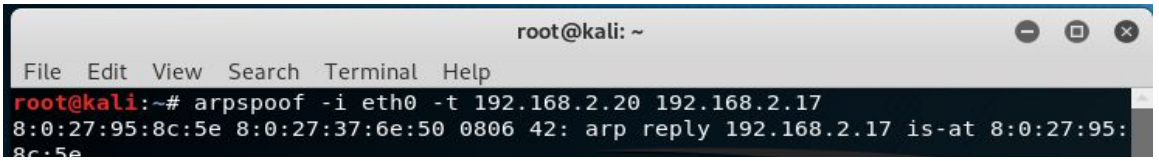
Figura 6: *Escaneo de la red*



Fuente: Elaboración propia

El atacante procede a realizar el envenenamiento ARP a través de la interfaz de red, seleccionando la puerta de enlace y la dirección IP del cliente de Windows 7 como se muestra en la Fig. 7.

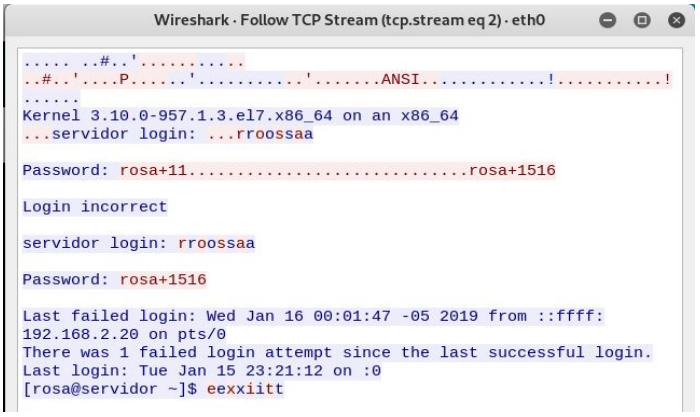
Figura 7: *Envenenamiento ARP*



Fuente: Elaboración propia

El atacante procede a utilizar la herramienta Wireshark para capturar el tráfico de la red y obtener la dirección IP y datos de inicio de sesión del servidor como se muestra en la Fig 8.

Figura 8: *Captura de paquetes*



Fuente: Elaboración propia

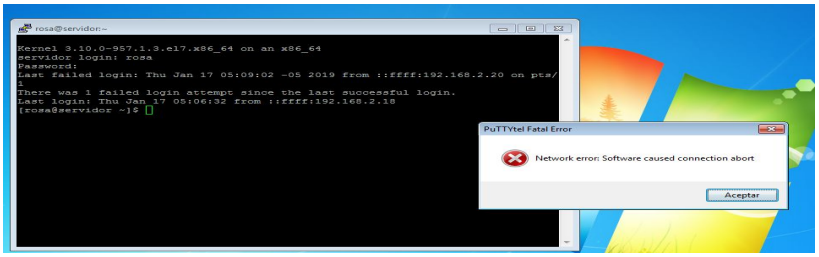
2.2.4 Desarrollo del ataque de Restablecimiento TCP

El ataque de restablecimiento de TCP consiste en terminar una conexión remota ya establecida, deshabilitando el servicio. El atacante para ejecutar la falsificación de un paquete RST procede a ejecutar la sentencia netwox, la cual provoca el restablecimiento del TCP como se muestra en la Fig 9 y Fig 10.

Figura 9: *Sentencia para el Reinicio del TCP*

Fuente: Elaboración propia

Figura 10: *Reinicio del TCP*



Fuente: Elaboración propia

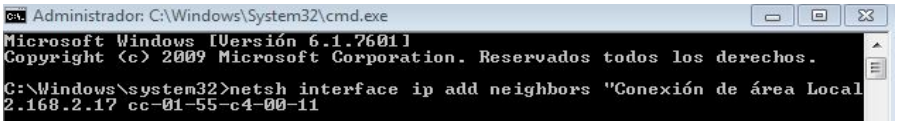
2.2.5 Implementación de Mecanismos de control

2.2.5.1 Mecanismos de control para el Secuestro de sesiones ciego, no ciego.

En los escenarios propuestos, se detectó vulnerabilidades en el protocolo TCP, por ello se procede a implementar controles que ayuden mitigar las falencias que surgieron al momento de ejecutar el ataque de Hombre en el medio con envenenamiento ARP, comprometiendo los principios de la seguridad informática como son: la disponibilidad, integridad y confidencialidad de los usuarios que acceden al servidor de Telnet.

Con base a ello, se propone el manejo de direcciones IP y MAC de forma estática en la tabla ARP que maneja el cliente en Windows, evitando las suplantaciones de las mismas como se visualiza en la Fig 11.

Figura 11: *Asignar ip estatica en los clientes*



Fuente: Elaboración propia

2.2.5.2 *Mecanismos de control para el ataque de Restablecimiento TCP*

Se hace una configuración en los iptables del Servidor para que elimine los paquetes RST del tráfico de red cada dos segundo como se muestra en la Fig. 12, evitando el restablecimiento TCP.

Figura 12: *Configuración de iptables*

Fuente: Elaboración propia

2.2.6 Resultados

El desarrollo de la investigación dio a conocer las vulnerabilidades existentes en el protocolo TCP, que dan inicio a la propagación de amenazas como la suplantación de direcciones IP que proporciona la realización de diversos tipos de perpetraciones como: el ataque ciego, no ciego y el restablecimiento de la conexión que afectan a la red de dato. Por lo tanto, se realizó dos tipos de controles a través de la configuración estática de direcciones IP en los hosts que pertenecen a los clientes logrando con ello mitigar el spoofing, además se realizó una configuración en los iptables del servidor para que elimine los paquetes RST que ingresen en el tráfico red, logrando con ello contrarrestar el restablecimiento TCP.

3. CONCLUSIONES

- Se realizó una investigación exhaustiva de las principales vulnerabilidades que afectan al protocolo TCP, basándose en el número de paquetes que envía de una terminal a otra sin verificar el host de origen que recibe; esto ayudó, a realizar el diseño de las topologías de red.

- Los escenarios propuestos en el presente trabajo fueron diseñados en un ambiente virtualizado con la ayuda de las herramientas GNS3 y VirtualBox para emular los ataques de secuestro de sesiones y de reinicio del protocolo TCP.

- Se implementaron mecanismos de control que ayudaron a mitigar las falencias del protocolo TCP en los ataques del secuestro de sesión ciego, no ciego y de Reinicio del TCP.

- Ettercap y Wireshark son herramientas indispensables a la hora de hacer pruebas de penetración al servidor de Telnet, al detectar las fallas que presenta en la comunicación con otras terminales.

BIBLIOGRAFÍA

[1] S. Bishop *et al.*, “Engineering with Logic: Rigorous Test Oracle Specification and Validation for TCP/IP and the Sockets API,” *J. ACM*, vol. 66, no. 1, pp. 1–77, Dec. 2018.

[2] N. Arumugam, “A Novel Method for Detecting and Preventing IP Spoofing Attack in Data Network,” *Int. J. Adv. Sci. Res.*, vol. 3, no. 8, pp. 2456-0774, 2018.

[3] A. Pandey and J. R. Saini, “Attacks & Defense Mechanisms for TCP/ IP Based Protocols,” *Int. J. Eng. Innov. Res.*, vol. 3, no. 1, pp. 17–23, 2014.

[4] S. Gangane, V. Kakade, and A. Professor, “Base of the Networking Protocol-TCP/IP Its Design and Security Aspects,” *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO*, vol. 3, no. 2320–9801, pp. 3712–3718, 2015.

[5] H. M A Hijawi and M. M.N.Hamarsheh, “Performance Analysis of Multi-Path TCP Network,” *Int. J. Comput. Networks Commun.*, vol. 8, no. 2, pp. 145–157, 2016.

[6] A. Quach, Z. Wang, and Z. Qian, “Investigation of the 2016 Linux TCP Stack Vulnerability at Scale,” *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 1, no. 1, pp. 1–19, Jun. 2017.

[7] A. M. Alotaibi, B. Fahaad Alrashidi, S. Naz, and Z. Parveen, “Security issues in Protocols of TCP/IP Model at Layers Level,” *Int. J. Comput. Networks Commun. Secur.*, vol. 5, no. 5, pp. 96–104, 2017.

[8] S. Sahni and P. Jagtap, “A Survey of Defence Mechanisms against IP Spoofing,” *Iarjset*, vol. 4, no. 7, pp. 20–27, 2017.

[9] K. Shyamala and S. Visalakshi, “Mitigating IP Spoofing to Enhance Security in Multi-Agent based e-Learning Environment,” *Indian J. Sci. Technol.*, vol. 8, no. 17, pp. 1–5, Aug. 2015.

[10] N. Hubballi and J. Santini, “Detecting TCP ACK storm attack: a state transition modelling approach,” *IET Networks*, vol. 7, no. 6, pp. 429–434, Nov. 2018.

[11] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[12] B. Pingle, A. Mairaj, and A. Y. Javaid, “Real World Man in the Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use,” in *IEEE International Conference on Electro/Information Technology (EIT)*, 2018, pp. 0192–0197.

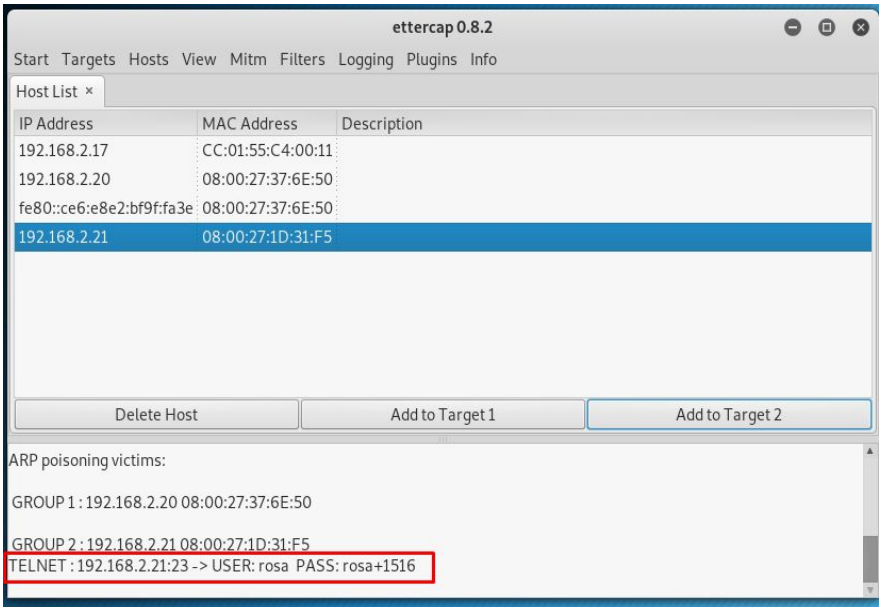
[13] A. Y. El Sheikh, “Evaluation of the capabilities of Wireshark as Network intrusion system,” *J. Glob. Res. Comput. Sci.*, vol. 9, no. 8, pp. 01–08, Sep. 2018.

[14] N. Rocío *et al.*, “Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas,” *Rev. Publicando*, no. 102, pp. 462–473, 2017.

[15] J. Gao, Y. Xiao, S. Rao, and F. Shalini, “Security tests and attack experimentations of ProtoGENI,” *Int. J. Secur. Networks*, vol. 10, no. 3, p. 151, 2015.

ANEXOS

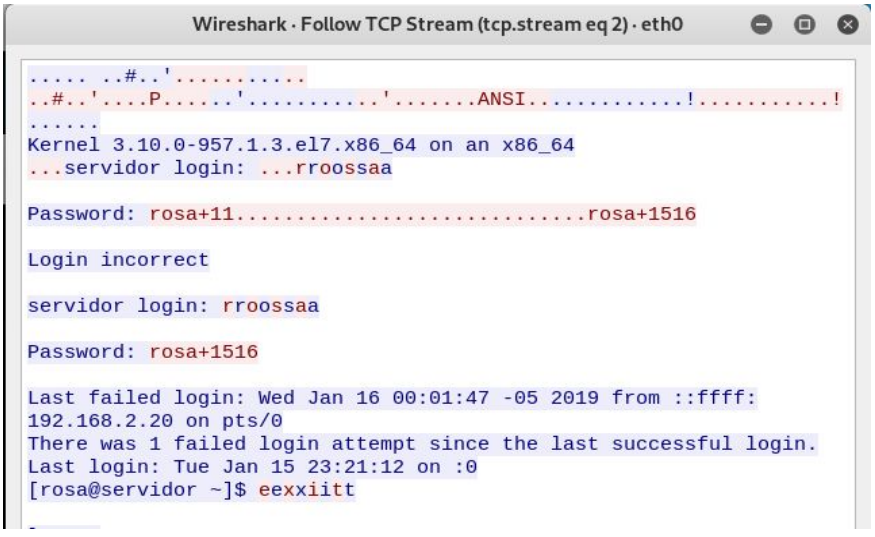
Anexo A. *Resultados del secuestro de sesión no ciego*



Fuente: Elaboración propia

En el Anexo A. se evidencia que el ataque fue exitoso, al obtener las credenciales del servidor.

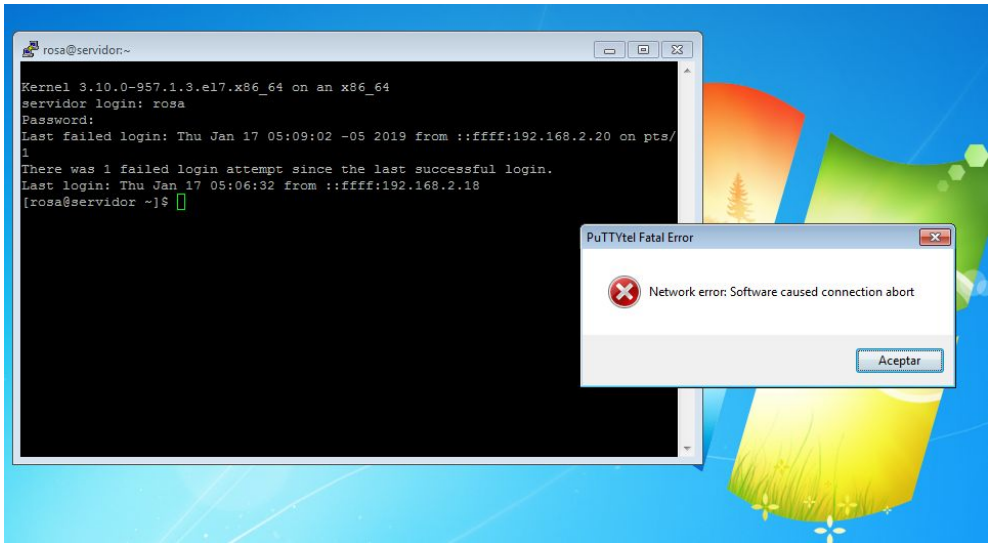
Anexo B. *Resultados del secuestro de sesión ciego*



Fuente: Elaboración propia

En el Anexo B. se visualiza la captura de la información obtenida en Wireshark, al encontrar las credenciales del servidor

Anexo C. *Ejecución del Reinicio TCP*



Fuente: Elaboración propia

En el Anexo C. se evidencia que el ataque de reinicio TCP fue éxito, al bloquear la conexión al cliente de Windows 7.