Politécnico costa atlántica
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

REVISTA GESTIÓN, COMPETITIVIDAD E INNOVACIÓN

Evaluación práctica de los protocolos Telnet y SSH

Practical evaluation of the Telnet and SSH protocols

Mario Luis Avila Pérez *

Isaac Avila Muñoz **

* Ingeniero de Sistemas. Especialista en Pedagogía para el desarrollo del Aprendizaje autónomo. Especialista en Seguridad Informática. Docente Escuela De Ciencias Básicas, Tecnologías e Ingenierías. Universidad Nacional Abierta y a Distancia UNAD, Barranquilla. mavilap@gmail.com

** Universidad Nacional Abierta y a Distancia "UNAD". Colombia. avilaisaac36@gmail.com

Fecha de recepción: 10 de abril de 2021

Fecha de aceptación: 27 de junio de 2021

Citación:

Avila Pérez, M. L., y Avila Muñoz, I. (2021). Evaluación práctica de los protocolos Telnet y SSH. Gestión, Competitividad e innovación(Enero-Junio 2021), 17-29.

RESUMEN

Telnet y ssh son protocolos de acceso que posibilitan la administración de servidores de forma remota, mediante la ejecución de comandos a través de una terminal , cada uno de estos protocolos utiliza un puerto TCP en la capa de aplicación del modelo OSI, en el presente artículo se muestran los resultados de la realización de un experimento sobre estos protocolos para la organización CYBERGOV, como caso de estudio de una empresa ficticia que permite trabajar con temas de criptografía aplicada a la solución de problemas que afectan el entorno, y que son aplicable a cualquier organización del mudo real.

Palabras claves: Protocolo, TCP, IP, telnet, ssh, wireshark.

ABSTRACT

Telnet and ssh are access protocols that allow the administration of servers remotely, by executing commands through a terminal, each of these protocols uses a TCP port in the application layer of the OSI model, in this article The results of conducting an experiment on these protocols for the CYBERGOV organization are shown, as a case study of a fictitious company that allows working with cryptography issues applied to solving problems that affect the environment, and that are applicable to any organization of the real world.

Keywords: Protocol, TCP, IP, telnet, ssh, wireshark.

1. Introducción

Los protocolos telnet y ssh son usados para realizar tareas administrativas en servidores remotos, a través de redes. Estos protocolos cumplen la misma función bajo una arquitectura cliente servidor, sin embargo, tienen diferentes implicaciones a nivel de seguridad. En este estudio se hace uso de cada uno de estos protocolos utilizándolos para conectarse a una máquina remota, para lo cual se configura un banco de pruebas y la instalación y configuración de los servidores de telnet sobre un sistema operativo Linux, así mismo se realiza la instalación de ssh sobre el mismo servidor Linux, con distribución Debian, una vez instaladas estas herramientas, se procede con la realización de test de seguridad, para lo cual se hacen una serie de comprobaciones mediante la configuración de un set de pruebas, para lo cual se utiliza la herramienta wireshark[1]. Estas pruebas arrojan una serie de resultados los cuales permitieron obtener unas conclusiones y recomendaciones, pudiéndose comprobar las fortalezas del protocolo ssh, frente a las debilidades que representa el uso del protocolo telnet.

2. Descripción De Problema

La empresa CYBERGOV viene experimentando una serie de inconvenientes los cuales han ocasionado trastornos en el normal desarrollo de las operaciones de la organización. Una auditoría realizada por un asesor de seguridad ha evidenciado los siguientes hallazgos: se encuentra que en la empresa CYBERGOV aún opera el control de servidores remotos mediante el uso del protocolo de red Telnet lo cual representa un riesgo grave de seguridad,

debido a que se sospecha que telnet tiene serias implicaciones de seguridad, que posibilitan a un atacante obtener el control sobre las máquinas a las que se accede con dicho protocolo.

Por esta razón, se ha desaconsejado el uso de telnet y la adopción del protocolo ssh para la administración remota de las máquinas. Esta situación ha llevado a que se solicite la configuración de un set de pruebas que permitan establecer que tan inseguro es realmente el protocolo telnet frente al protocolo ssh.

3. Instalación del set de pruebas

Para la realización de este estudio es necesario hacer el ejercicio en un ambiente controlado, para no incurrir en delito por infringir el Artículo 269C: "Interceptación de datos informáticos" de la ley 1273 en Colombia. [2]. Para lograr este propósito se utilizan un sistema virtualizado[3], sobre el cual se hace la instalación de la distribución de Linux Debian 8. Es así como se procede con la descarga de la distribución Linux desde los repositorios de Debian de esa versión, y se procede con su instalación sobre un sistema virtualizado con Oracle VirtualBox. Se descargó en instaló el paquete de virtual box desde la página del fabricante https://www.virtualbox.org/

Se descargó la versión para Linux en paquete y se procedió a la instalación como sistema Huésped., como se aprecia en la figura 1.[4]

Figura 1 Creación de máquina virtual virtualBox. Fuente: El autor.

Se procedió a descargar el el sistema operativo linux Debian en su versión 8.7 desde el sitio https://www.debian.org/News/2017/20170114., una vez descargada la ISO, se procedió a crear la máquina virtual con las siguientes características: Memoria de 1024 Mb, espacio en disco de 10 Gb, dinámico, y el resto de configuraciones básicas. En la figura 2 se muestra la captura de pantalla de la creación de la máquina virtual. [4]

Una vez creada la máquina virtual se procedió a iniciarla pulsando el icono start en la parte superior de la ventana, se seleccionó idioma español, con distribución de teclado para Latinoamérica y se pulsa continuar como se muestra en la Figura. 3. Dando inicio al proceso de partición del disco, el cual se configuró con el asistente del programa de instalación.[5]

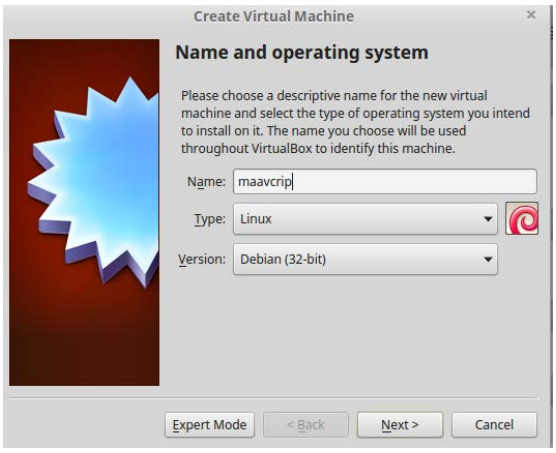

Figura 2 Creación escogencia del S.O Linux Debian. Fuente: El autor.

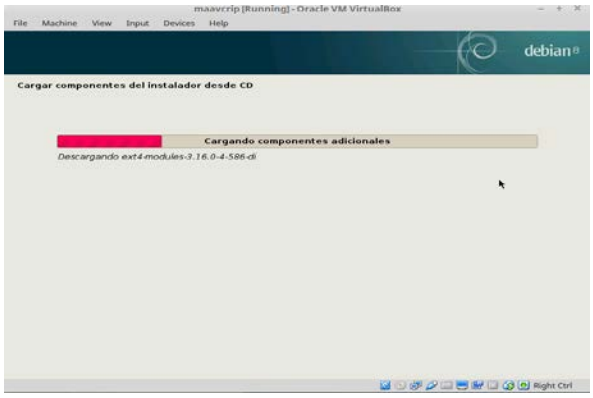

Figura 3 Instalación de S.O Debian en VirtualBox. Fuente: El autor.

Se digitó el nombre de la máquina maavcip como se aprecia en la fig 4, se particionó el disco permitiendo a Debian usar todo el disco virtual.

A partir de este punto el sistema comenzó a descargar los paquetes necesarios desde internet, esto tomó un tiempo de 25 minutos, una vez descargados los paquetes. Se procedió a la instalación de GRUB como gestor de arranque Fig. 5. Y haciendo la confirmación como se describe en la Fig 5.

Una vez se instaló el sistema operativo Debian, se procedió a actualizar el sistema, para que se descarguen las últimas actualizaciones disponibles en los repositorios de Debian.

Se verifica OpenSsl, se actualiza el sistema con la herramienta apt-get.

Una vez que termina la instalación, se procede a iniciar la máquina previamente instalada para la instalación del resto de herramientas necesarias para estos experimentos.

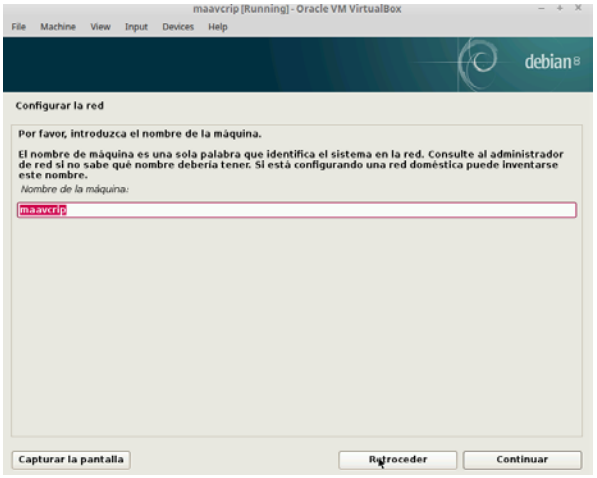

Figura 4 Nombre de la maquina Debian. Fuente: El autor.

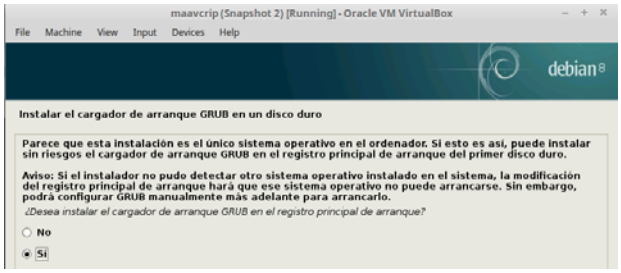

Figura 5 Instalación del cargador GRUB. Fuente: El autor.

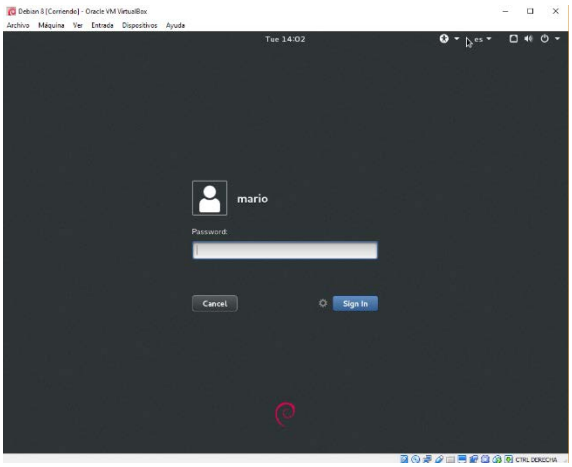

Figura 6. Inicio de debían 8. . Fuente: El autor.

Luego se ingresa a la terminal de la maquina Linux, para ejecutar el comando ifconfig, verificándose que las interfaces de red se encuentran debidamente configuradas y activadas.[6]

```
root@debiano8:/home/mavila# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fe:e5:9e
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fefe:e59e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27869 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13223 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23066612 (21.9 MiB)  TX bytes:802340 (783.5 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31534 (30.7 KiB)  TX bytes:31534 (30.7 KiB)
```

Figura 7. Salida del comando ifconfig. Fuente: El autor.

Instalación de telnet

Para instalar cliente de telnet, se procede a ejecutar el comando apt-get install telnet en la terminal, verificando que este ya se encuentra instalado. Se procedió a la instalación del servidor de telnet, para lo cual se ejecutó el comando apt-get install telnet, como se aprecia en la figura 3.

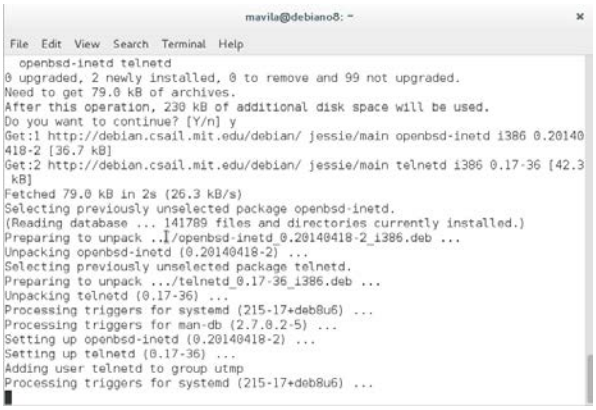

Figura 8. Instalación del servidor telnet. Fuente: El autor.

Instalacion del servidor ssh

En la misma terminal que abierta se procedió a ejecutar al comando apt-get install ssh

En este caso ya previamente tenia instalado este servicio, si hubiese necesidad de configurar algún parámetro, se debe reiniciar el servidor ssh nuevamente, mediante el comando

/etc/init.d/ssh restart

Para probar que el servidor ssh funciona, se puede hacer desde la terminal, en este caso como las pruebas se están haciendo local, hay que utilizar el nombre localhost como nombre de la maquina a la que vamos a conectarnos, y lo haremos con el usuario mario, utilizando el siguiente comando:

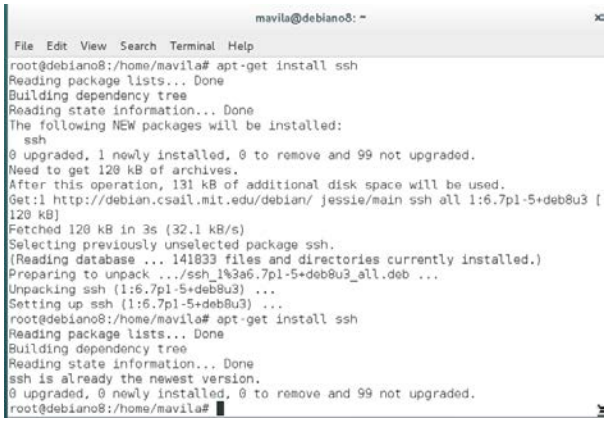

Figura 9. Instalacion de servidor ssh. Fuente: El autor.

ssh mario@localhost, Este comando la primera vez nos va pedir una confirmación del tipo yes/no , al decir yes o “y”, se conecta a la máquina y muestra lo que se aprecia en la figura 10.

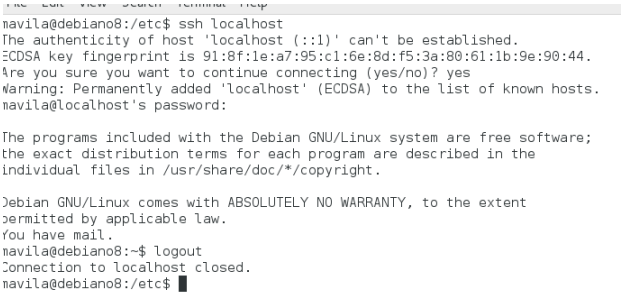

Figura 10. Conexión ssh. Fuente: El autor.

Wireshark.

Como el ejercicio se va a realizar con la misma máquina Debian se procede a la instalación de wireshark, mediante la ejecución del comando apt-get install wireshark como se puede observar en la figura 11.

Se muestra configuración de wireshark-common esto se realiza para manejar permisos separados, donde se crea el grupo de usuarios “wireshark”, para brindar permisos de root a dumpcap.

Una vez el proceso de instalación finaliza, se procede a ejecutarlo desde la terminal, ejecutando el comando wireshark se abre la ventana de wireshark donde se destacan entre otras cosas las interfaces de red de la máquina, como se aprecia en la figura 12.

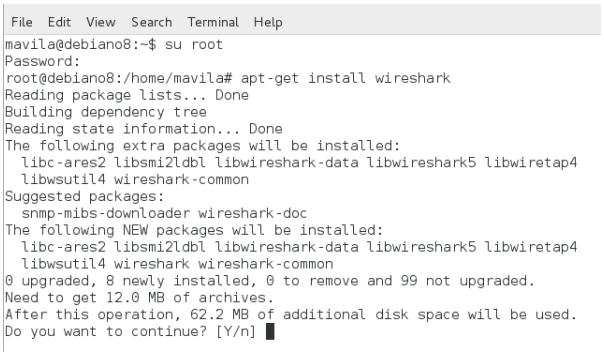

Figura 11. Instalación de wireshark. Fuente: El autor.

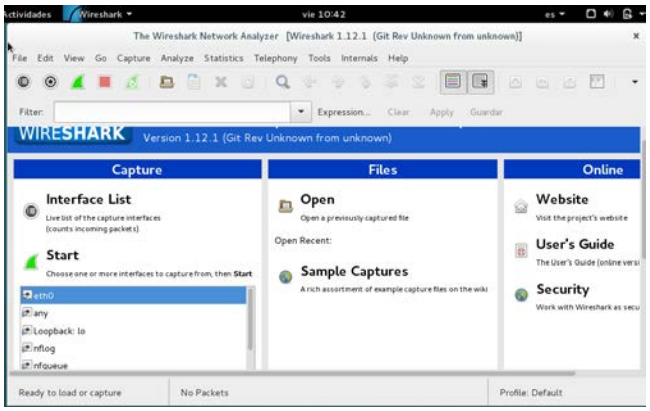

Figura 12. Wireshark Fuente: El autor.

- Se procede a ubicar la interfaz local o loopback, que es la interfaz que se quiere olfatear o sniffear, la ubicamos y hacemos clic en start.

- Ahora es necesario ingresar a la maquina Debian con el protocolo telnet, para lo cual se debe ejecutar el comando telnet localhost[6]

- Cuando se realiza la conexión del servidor telnet se solicita el usuario y contraseña.

- En la aplicación wireshark se hace la búsqueda por protocolo TCP telnet y se procede a aplicar ese filtro, como se aprecia en la figura 13.

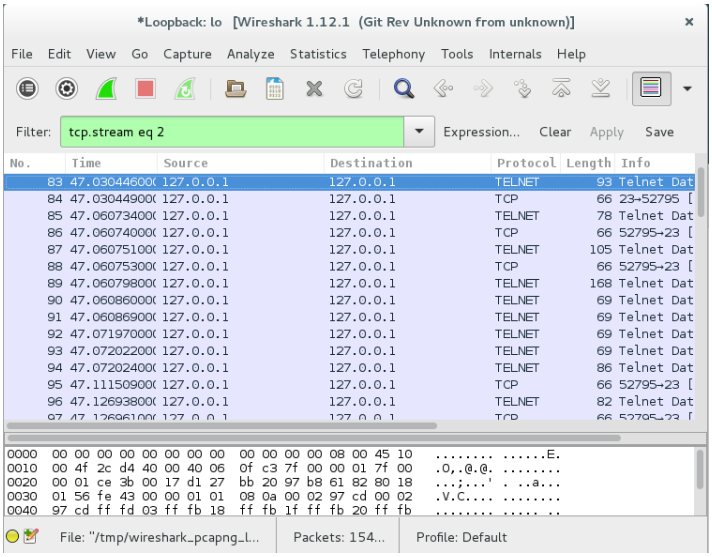

Figura 13. Wireshark captura de tramas. Fuente: El autor.

Al ubicar el registro de telnet es necesario hacer clic derecho y para escoger la opción follow tcp stream, dando como resultado lo que observamos en la figura 14.

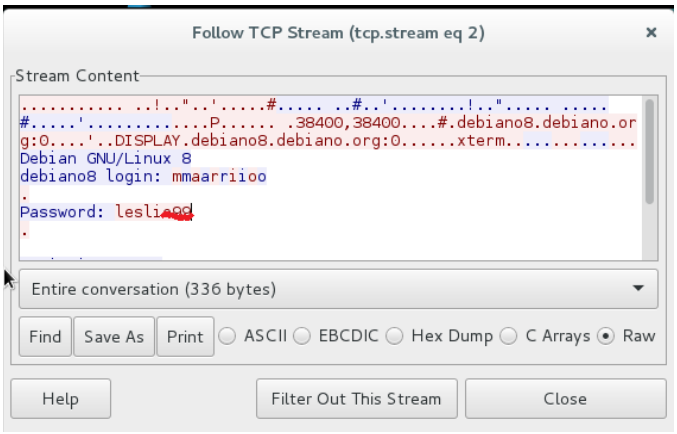

Figura 14. Follow tcp stream de telnet. . Fuente: El autor.

En la figura anterior se puede apreciar claramente el nombre de usuario y contraseña, con lo cual se evidencia que el protocolo telnet los datos se envían sin cifrar.

Ahora lo que se va a hacer es repetir el proceso con el protocolo SSH, para lo cual accedeos nuevamente a la terminal ejecutando el comando ssh mario@localhost, se solicita la contraseña para el usuario mario y ya estamos dentro de la máquina.

Nuevamente se debe acceder a la aplicación wireshark y se aplica el filtro TCP como se hizo con telnet para ubicar tramas de ssh como apreciamos en la figura 15.

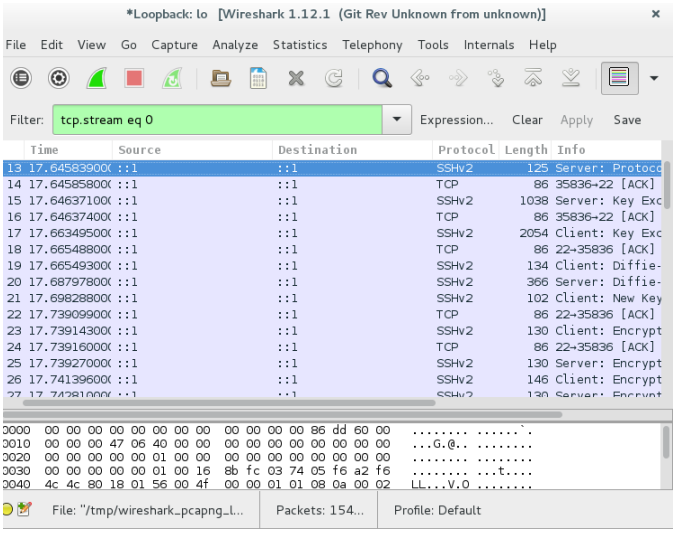

Figura 15. Tramas ssh. Fuente: El autor.

Al ubicar el registro de ssh se debe hacer clic derecho para luego escoger la opción follow tcp stream, dando como resultado lo que observa en la figura 16.

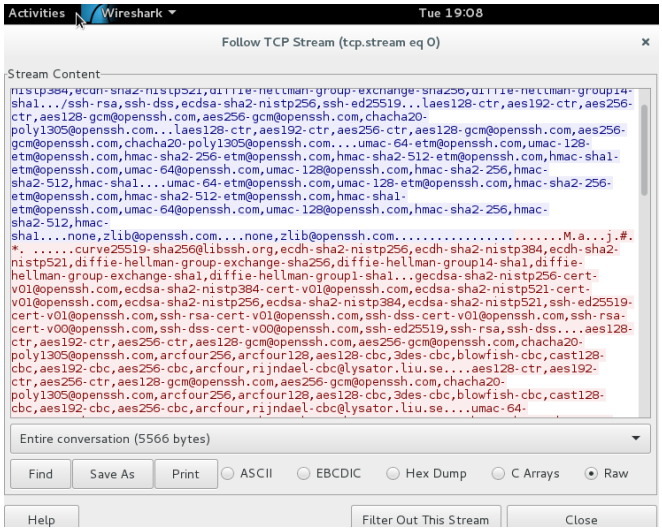

Figura 16. Salida wireshark para SSH. Fuente: El autor.

Como se observa en la figura anterior, los datos están encriptados, lo cual nos brinda la garantía de que no es posible que un atacante acceda al usuario y a la contraseña, si se tiene una contraseña robusta.

4. Resultados

Telnet se deriva del nombre Telecomunication Network y permite a un usuario trabajar en una máquina que físicamente está en otro lugar, como si la máquina estuviera local. SSH (secure Shell) permite operar de manera similar a telnet.[7]

La diferencia entre TELNET y SSH radica en que SSH cifra la información antes de transmitirla y puede emplear mecanismos de autenticación más seguros tal como se comprobó en el ejercicio.

Estos resultados llevan a los siguientes planteamientos:

¿Por qué TELNET es inseguro? ¿Qué se comprueba con el ejercicio anterior?

Ya se mencionó que SSH funciona de manera similar a telnet, pero telnet transmite información a la red sin cifrar, lo que hace al protocolo realmente vulnerable. bastando solamente la interceptación de la comunicación para acceder a la información que está legible. Como lo pudimos comprobar en este ejercicio en que cuando se usa telnet, la información viaja a través de la red sin cifrar.

Por otro lado, ssh es un protocolo más seguro debido a que la información viaja a través de la red cifrada. Esta característica de ssh permite transmitir archivos, simular sesiones FTP cifradas, gestionar claves RSA para no tener que escribir claves al conectar dispositivos.

5. Recomendaciones.

Como recomendación para este ejercicio se recomiendan poner en prácticas las siguientes políticas con el objetivo de minimizar el riesgo de ocurrencia relacionado con la vulneración de la seguridad de la información en la organización CYBERGOV, las cuales se deben socializar has convertirlas en parte de la cultura organizacional.

- Se recomienda el uso de contraseñas seguras con mínimo 8 caracteres que convine minúsculas Mayúsculas y números como mínimo.
- Cambio periódico de claves.
- Evitar que los usuarios comunes trabajen con el perfil de administrador del equipo para evitar que instalen software de dudosa procedencia
- Evitar la instalación de software no licenciado.
- Instalar una arquitectura de llave publica para cifrar la comunicación crítica de la organización.
- Evitar el uso de telnet para comunicaciones remotas
- Fomentar el uso de SSH para conexiones remotas.
- Realizar copias de seguridad periódicas
- Mostrar las extensiones ocultas de los archivos, para evitar archivos ramsonware
- Instalar las actualizaciones de software periódicamente
- Instalar una herramienta de prevención de software mal intencionado
- Fomentar la utilización de solo correos institucionales, divulgando campañas de no reenvío de cadenas de correo.
- Fomentar la disminución de la utilización de memorias extraíbles.
- Cronogramas de mantenimientos preventivos

- Al ser infectados por ramsonware de ninguna manera se debe pagar ya que al realizar dicho pago estamos financiando estos ataques y la mayoría de las veces no se recupera la información.
- Si se detecta un equipo infectado, este se debe colocar en cuarentena, con la finalidad de prevenir que la infección se propague.

Conclusiones

Se logró configurar un set de pruebas mediante la instalación del sistema operativo Linux Debian, virtualizado con Oracle Virtualbox, en el cual se pudieron instalar las herramientas necesarias para los experimentos de ethical hacking.

Se logró probar la seguridad del protocolo telnet mediante la herramienta wireshark olfateando el tráfico de red generado en la interfaz de red, loque permite concluir que el uso de telnet no es recomendable para la organización y por lo tanto inmediatamente deben ser suspendidos este tipo de servicios para conexión remota, de manera definitiva.

Mediante la realización de este estudio se pudo comprobar la seguridad del protocolo ssh al ataque de análisis de tráfico en la red con la herramienta wireshark. Este ejercicio permitió concluir que SSH provee una conexión segura cifrada por lo cual no hay necesidad de seguir usando telnet en la organización.

Los resultados producto de la realización de este ejercicio, han permitido evaluar de manera práctica los protocolos telnet y ssh en un set de pruebas controlado que posibilitó la identificación de vulnerabilidades en el protocolo telnet debido a que la información enviada a través de la red no va encriptada, a diferencia del protocolo ssh, el cual usa encriptación para el envío de la información a la red.

La experimentación con set de pruebas controlados permitió obtener resultados importantes en esta investigación que evidenció las debilidades del protocolo telnet, y también evidenció las fortalezas del protocolo ssh, frete a un potencial ataque de alfabeto de tráfico en la red, como el que se realizó en este ejercicio.

Referencias

[1] “Practical Packet Analysis: using Wireshark to solve real-world network problems,” Netw. Secur., vol. 2011, no. 8, p. 4, 2011, doi: 10.1016/s1353-4858(11)70082-4.

[2] “LEY 1273 DE 2009,” 2009. Accessed: Dec. 05, 2021. [Online]. Available: moz-extension://79636ef4-ca92-4dbe-9c2a-95d4691b35dd/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.enticconfio.gov.co%2Fimages%2Fstories%2Fnormatividad%2FLey_1273_de_2009%2520.pdf.

[3] P. Li, “Selecting and using virtualization solutions: our experiences with VMware and VirtualBox,” J. Comput. Sci. Coll., vol. 25, no. 3, pp. 11–17, 2010, Accessed: Dec. 05, 2021. [Online]. Available: https://www.researchgate.net/publication/234778887.

[4] M. L. Avila Pérez, “Diseño de un sistema de detección de intrusos en la red de la UNAD sede Puerto Colombia.,” Universidad Nacional Abierta y a Distancia UNAD, Jul.

2018. Accessed: Dec. 05, 2021. [Online]. Available: http://repository.unad.edu.co/handle/10596/19906.

[5] M. L. Avila, “Implementación de un IDS,” Gestión Competitividad e Innovación vol 8, 2020. https://pca.edu.co/editorial/revistas/index.php/gci/article/view/91 (accessed Dec. 05, 2021).

[6] M. Baser, E. Y. Guven, and M. A. Aydin, “SSH and Telnet Protocols Attack Analysis Using Honeypot Technique : * Analysis of SSH AND TELNET Honeypot,” Oct. 2021, pp. 806–811, doi: 10.1109/ubmk52708.2021.9558948.

[7] B. Rhodes and J. Goerzen, “CHAPTER 16 Telnet and SSH,” in Foundations of Python Network Programming, Apress, 2010, pp. 263–290.