“VIRUS, TROYANOS, Y GUSANOS”

Trabajo Preparatorio N°3

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se tratara temas acerca de Virus, Troyanos y Gusanos que hacen referencias a códigos maliciosos que dañan el sistema de computo y da control a los atacantes identificando así la facilidad con la que dichos programas pueden crearse a partir de librerías disponibles realizado en un entorno aislado y virtualizado.**

***Index Terms*—Aislado, Atacante, Entorno, Gusano, Malicioso, Troyano, Virus.**

I. Introducción

Actualmente existe gran cantidad de herramientas que permiten realizar ataques a diferentes dispositivos; una vez que estas aplicaciones han obtenido acceso al equipo de la víctima, pueden realizar muchas cosas como son descargar archivos, escalar privilegios, utilizar un keylogger o activar cámara de video entre otras muchas posibilidades más.

II. Objetivos

- Identificar la facilidad con la que un programa malicioso podría crearse a partir de librerías y herramientas disponibles.
- Hacer en un entorno aislado y virtualizado una prueba de concepto para la creación de un troyano que permite la conexión remota de un atacante al sistema vulnerado.
- Evidenciar en este entorno el grave impacto que podría tener un ataque de este tipo en la seguridad de la víctima.

III. Cuestionario

A. Revisar el marco teórico para la realización de la práctica.

B. Instale una máquina virtual Windows 7 o 10 en VmWare o VirtualBox.

En la siguiente figura, se presenta la instalación de la máquina virtual solicitada

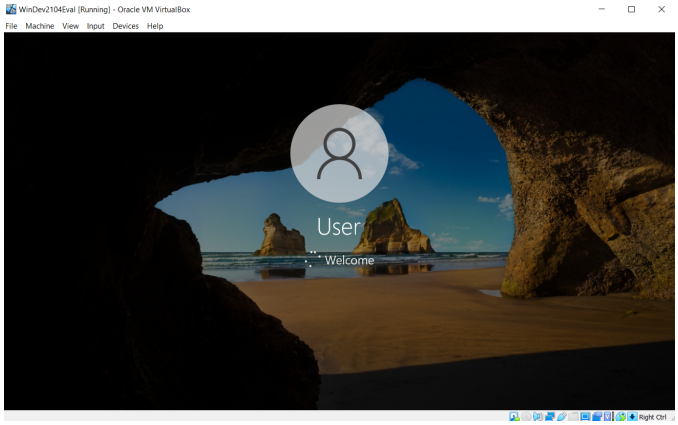

Fig. 1. Windows 10 instalado

C. Que es “conexión reversa” y describir su utilidad para un atacante de la seguridad en red. (máximo una carilla)

La conexión reversa consiste en que el equipo interno a la organización el que inicia la conexión hacia el exterior, para luego pasar el control al sistema externo. La manera que tienen de realizar esto es iniciando la conexión, algo que suele estar más abierto o si quieren permitido en los cortafuegos [1]. La máquina atacante se pondrá en un puerto a la escucha y la máquina víctima se conectará a ella. Estas conexiones tienen un mayor éxito de ser establecidas ya que es la máquina víctima es quien inicia la conexión hacia la máquina atacante y esto evitará un posible bloqueo de la conexión en el firewall del equipo víctima ahora lo que antes era el cliente (nosotros) pasamos a ser un servidor que oímos en un/os puerto/s prefijados a nuestro antojo y seremos nosotros los que atenderemos a las peticiones de conexión de las máquinas infectadas y una vez establecida la conexión ganar el control de la máquina infectada. Lo único que se necesita, pues, es tener bien configurada nuestra red para aceptar conexiones hacia nuestra maquina en el puerto (o rango) especificado y esperar a que nos lleguen las notificaciones de “infección”. La mayoría de firewalls y routers no analizan el trafico saliente, suelen centrarse en el entrante, y esto posibilita que las conexiones del troyano hacia nuestro servidor sean prácticamente efectivas al 100 [2]. Para asegurar la conexión, el atacante puede utilizar una IP fija o un nombre de dominio. La conexión inversa presenta ventajas sobre la indirecta, especialmente al traspasar algunos firewalls, se pueden utilizar en redes situadas detrás de un router sin problemas, no es necesario conocer la dirección IP del servidor. Las formas más comunes de infección son: [3].

- Descarga de programas en redes P2P. Páginas web con contenido ejecutable, como ActiveX o aplicaciones Java.
- Ingeniería social, en la que el pirata o atacante manda el troyano directamente a la víctima por medio de mensajería instantánea (muy común en el tiempo de MSN Messenger).
- Archivos adjuntos en correos electrónicos.
- Como los troyanos se ejecutan y se mantienen ocultos, el usuario podría pasar meses infectado sin darse cuenta, por ello es muy difícil detectarlo y eliminarlo manualmente, por lo que es recomendable tener un antivirus actualizado, además de un firewall.

D. Consultar que es Meterpreter en Metasploit y explique cómo trabaja. (máximo una carilla)

Meterpreter es un playload de ataque de MetaSploit que proporciona una cubierta interactiva de la que un atacante puede explorar la máquina de destino y ejecutar el código [4]. Se implementa utilizando inyección DLL en memoria. Como resultado, Metropeter reside completamente en la memoria y no escribe nada al disco. No se crean nuevos procesos, ya que el medidor se inyecta en el proceso comprometido, desde el cual puede migrar a otros procesos de funcionamiento, como resultado se tiene que el fingerprint de un ataque es muy limitado.

Permite obtener una gran cantidad de información sobre un objetivo comprometido, así como también manipular ciertas características del sistema objetivo [4].

La comunicación entre el interprete Meterpreter y la maquina remota es vía SSL lo que quiere decir que la información intercambiada entre las dos maquinas viaja cifrada, ademas es posible utilizar múltiples canales de ejecución, es decir, múltiples programas ejecutándose en la maquina remota y todos pueden ser manejados desde meterpreter con los comandos “channel” y “execute” [5].

REFERENCES

[1] D. Soler ”Herramientas de acceso remoto por conexión inversa”, Nov. 3,2018.https://www.securityartwork.es/2008/11/03/herramientas-de-acceso-remoto-por-conexion-inversa/(accedido Jun. 23, 2021).

[2] L. Adrian. ”Conexiones directas e inversas con Netcat (nc): Obteniendo shells, transferencia de ficheros, banner grabbing y TCP/UDP Scan”. Jul 6,2020.https://www.zonasystem.com/search/label/Metasploit. (accedio Jun. 23,2021).

[3] ”Troyanos de conexión inversa/directa”. May. 2,2017. https://blogs.masterhacks.net/geek/interesante/troyanos-de-conexion-inversadirecta/. (accedido Jun. 23,2021)

[4] “Básicos 8: knows basic Metasploit · basic Meterpreter (parte. III) – TonyHAT”. https://tonyhat.wordpress.com/2015/08/13/basicos-8-knows-basic-metasploit-%c2%b7-basic-meterpreter-parte-iii/ (accedido jun. 23, 2021).

[5] “Conceptos Basicos de Meterpreter – MetaSploit Framework”, Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW), abr. 26, 2011. https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/ (accedido jun. 23, 2021).