Asignatura	Datos del alumno	Fecha
Atacando Máquinas con Metasploit	Apellidos: Paz López	03.01.2021
	Nombre: Angel Ramon	

Índice

Atacando máquinas con Metasploit

Introducción

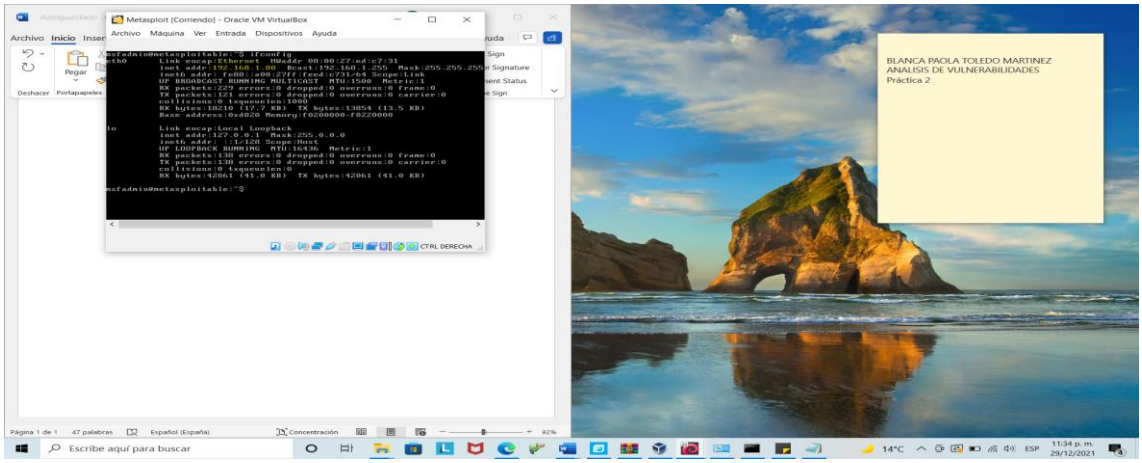
Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades y de seguridad y ayuda en las pruebas de penetración y el desarrollo de firmas para sistemas de detección de intrusos, la versión gratuita es muy potente únicamente con los exploits públicos que contiene, esta herramienta está enfocada a auditores de seguridad y hacker éticos, pero también es utilizada por ciberdelincuentes.

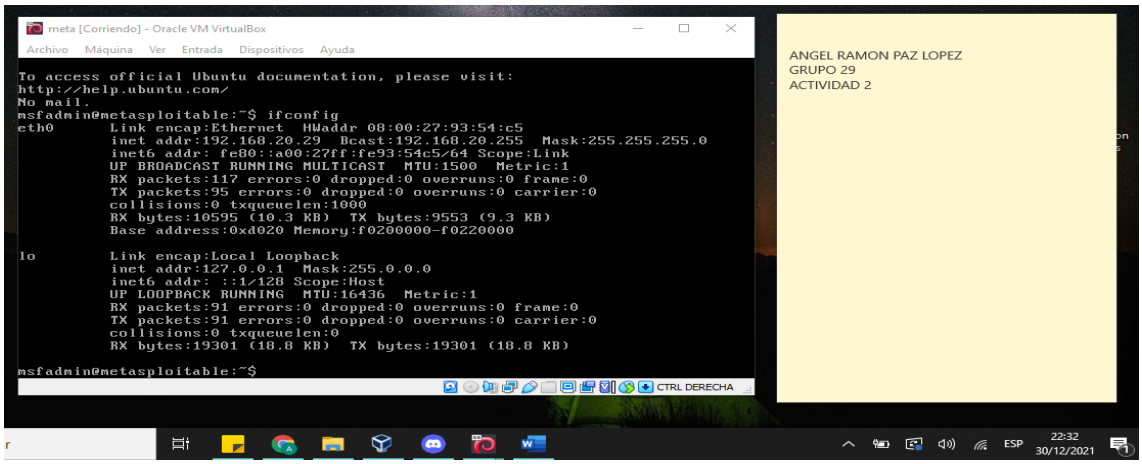
En esta actividad se montó un escenario de auditoria denominado **pentesting**, dentro del cual se utilizan varias herramientas para realizar ataques dentro del ambiente ponderado creado.

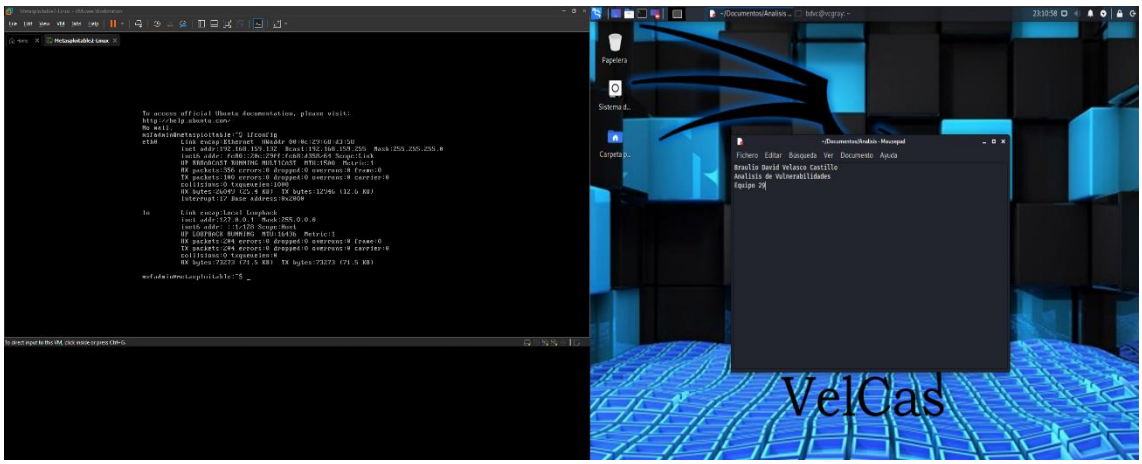
Fingerprint

Se deben de identificar los puertos y las versiones con en el comando **nmap**, para realizar el fingerprint, sobre la maquina Metasploitable, utilizaremos la herramienta Kali Linux como el atacante. Al ser una auditoría interna accedemos a la máquina para obtener la IP.

© Universidad Internacional de La Rioja (UNIR)

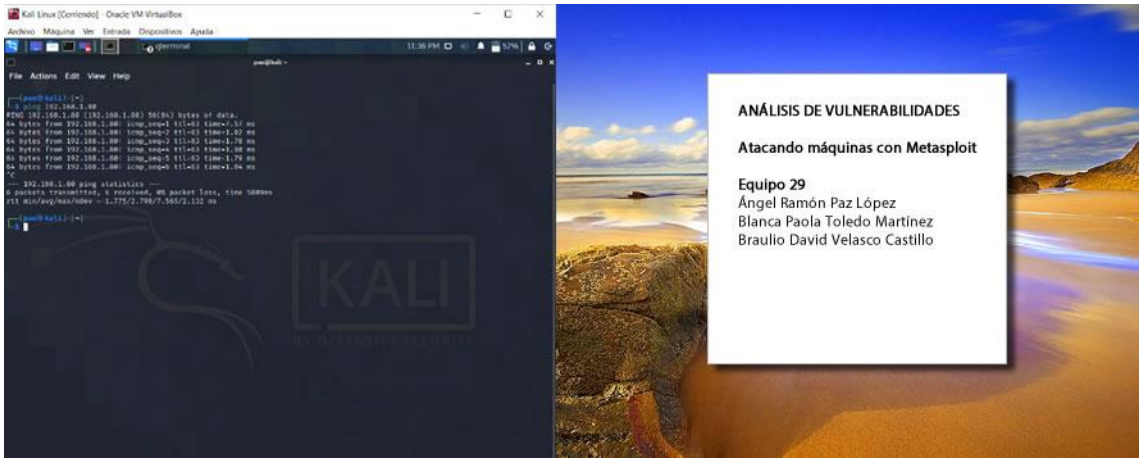






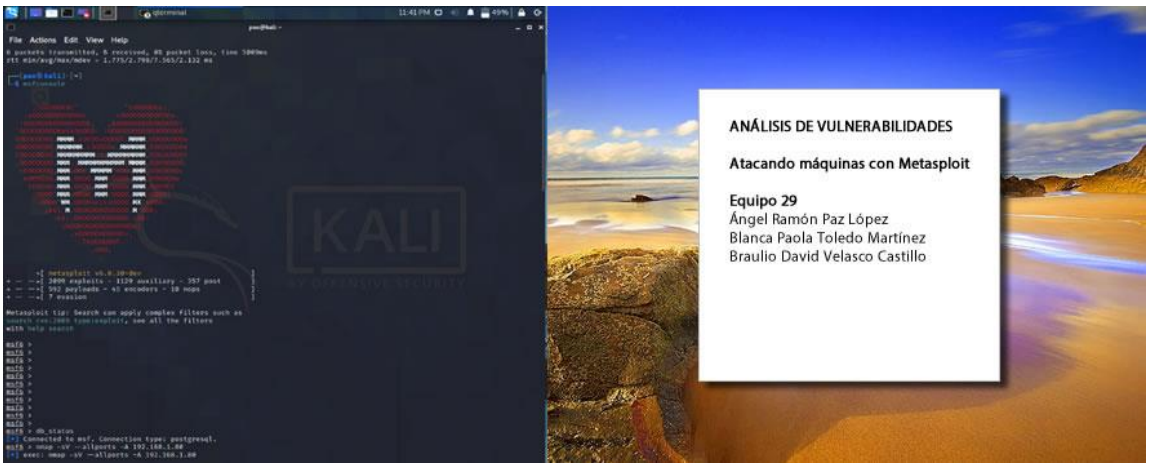
Se realiza ping desde la maquina atacante Kali Linux para corroborar la conexión.

© Universidad Internacional de La Rioja (UNIR)

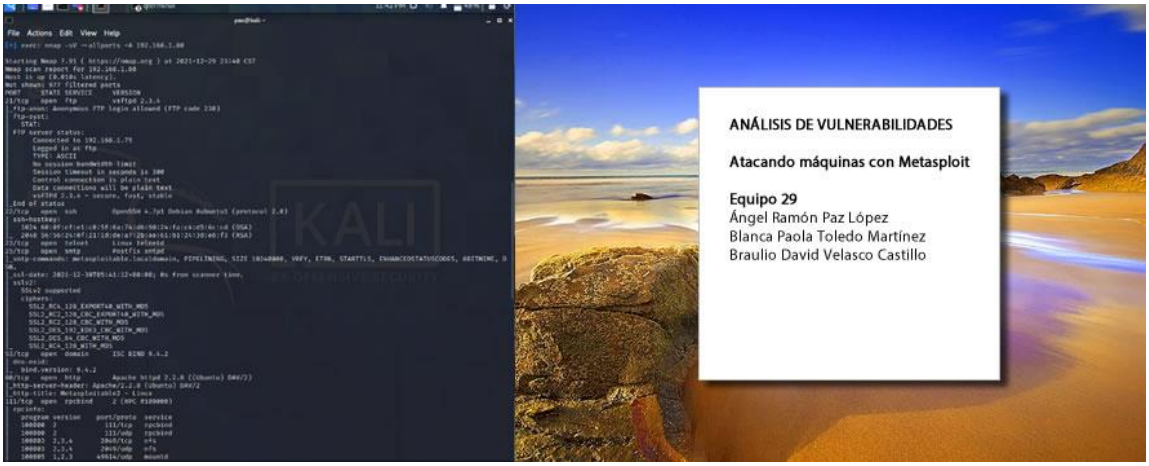


Procedemos a obtener todos los puertos, servicios y versiones que se tienen activos dentro de la máquina victima e inclusive la versión del sistema Operativo, con la utilización de los siguientes comandos:

- db_nmap -A 192.168.1.80
- db_nmap -sV -O 192.168.1.80 -p -65535
- nmap -sV --allports -A 192.168.1.80



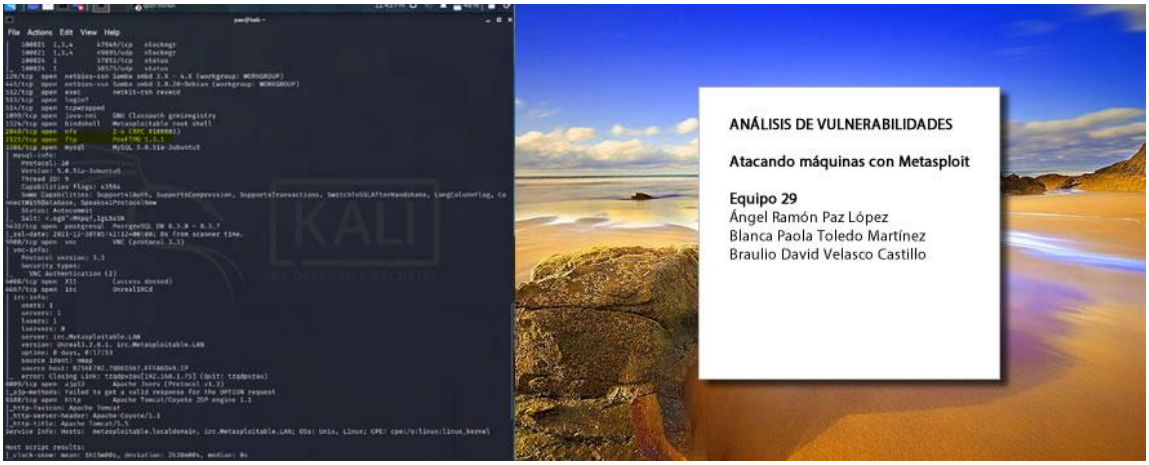
© Universidad Internacional de La Rioja (UNIR)



ANÁLISIS DE VULNERABILIDADES

Atacando máquinas con Metasploit

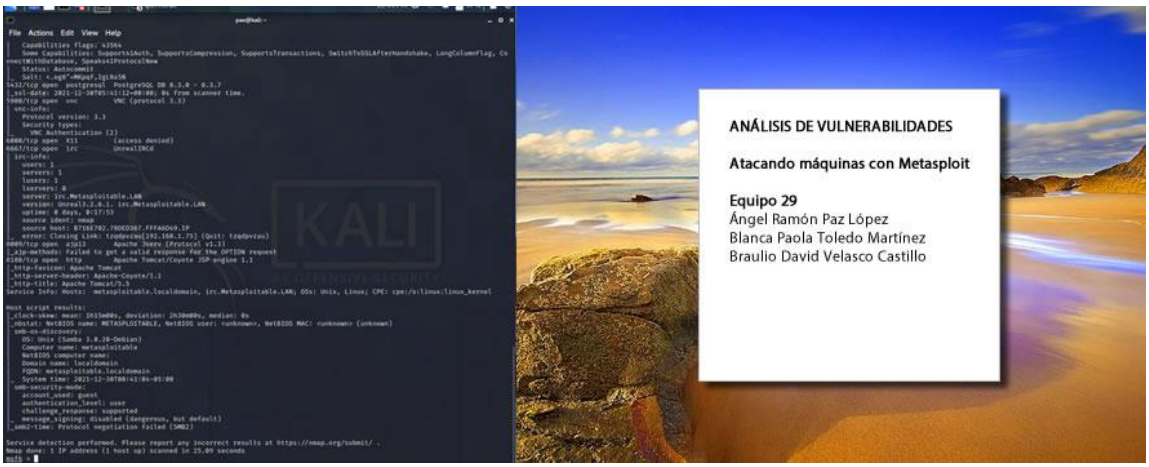
Equipo 29
Ángel Ramón Paz López
Blanca Paola Toledo Martínez
Braulio David Velasco Castillo



ANÁLISIS DE VULNERABILIDADES

Atacando máquinas con Metasploit

Equipo 29
Ángel Ramón Paz López
Blanca Paola Toledo Martínez
Braulio David Velasco Castillo



ANÁLISIS DE VULNERABILIDADES

Atacando máquinas con Metasploit

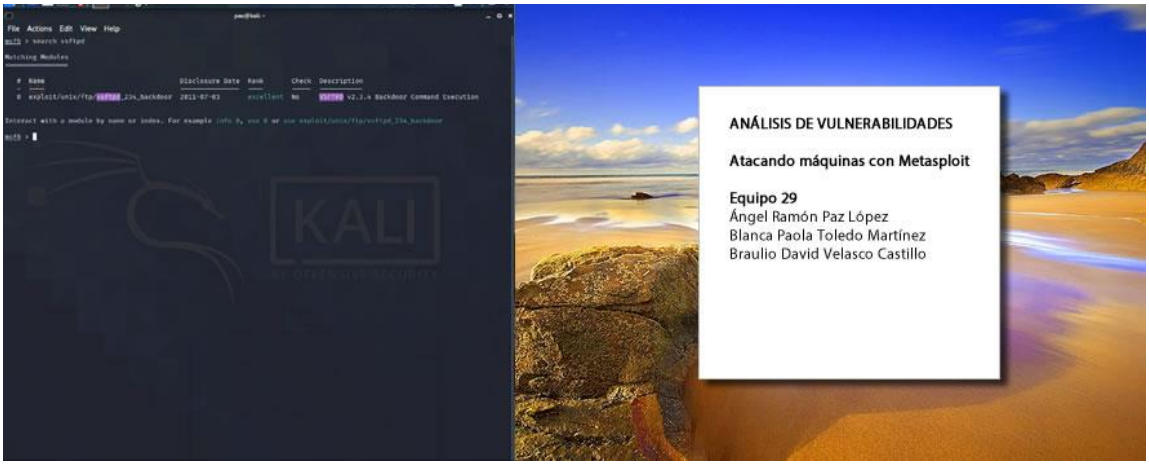
Equipo 29
Ángel Ramón Paz López
Blanca Paola Toledo Martínez
Braulio David Velasco Castillo

Payload a través del puerto 21

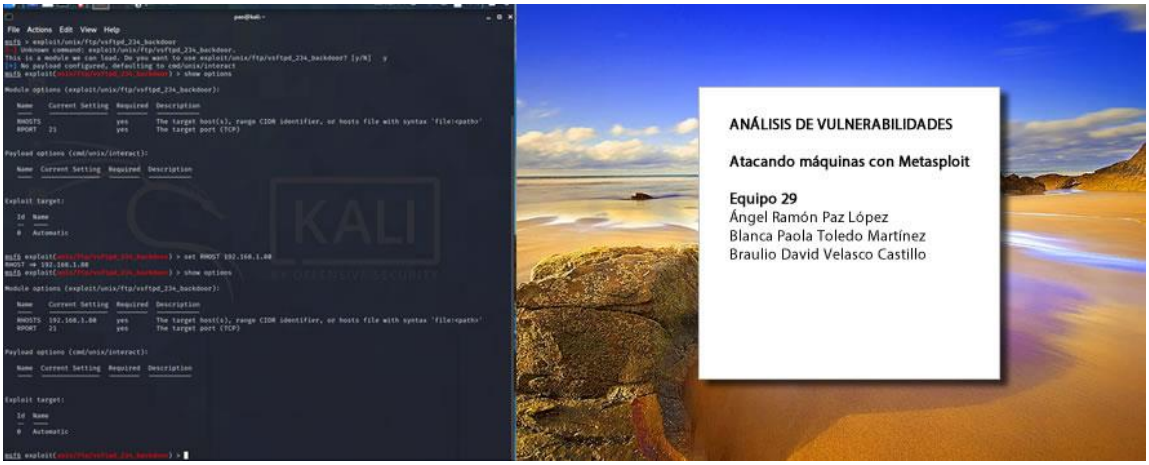
En el ejercicio previo con ayuda del comando **nmap**, nos dimos cuenta de que el puerto 21 se encuentra abierto el que hace referencia al servicio “FTP” en la versión “1.3.1”. Podemos

© Universidad Internacional de La Rioja (UNIR)

encontrar la vulnerabilidad gracias al comando **msfconsole** y buscando con el comando **search vsftpd**.

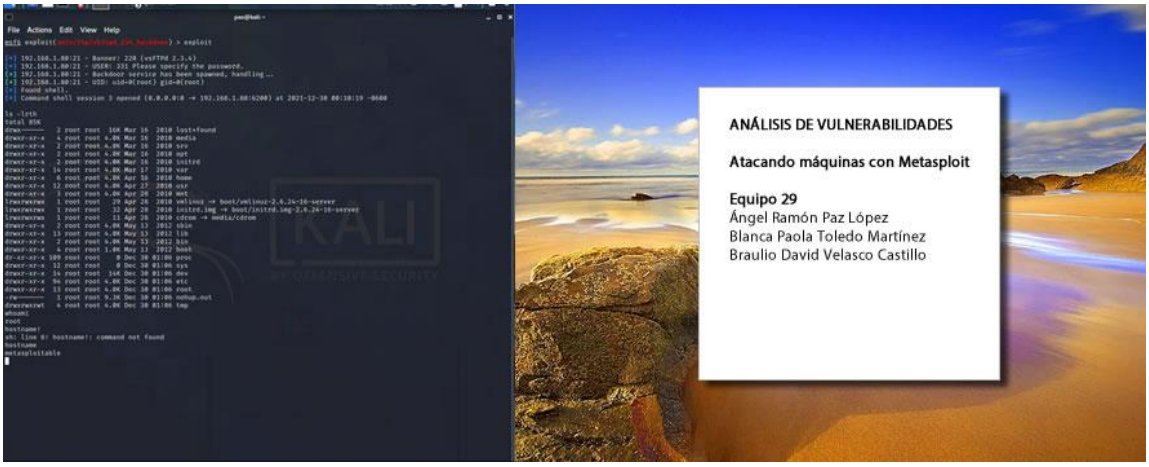


Existe un exploit para la versión “2.3.4” por medio del uso “Backdoor”, el cual vamos a utilizar para aprovecharnos de la vulnerabilidad antes encontrada con el comando exploit/unix/ftp/vsftpd_234_backdoor. Al ingresar al exploit se debe configurar mediante el comando show options y donde nos enlista las configuraciones requeridas para el uso del exploit, donde se configura RHOST, añadiendo la ip de la máquina victima con el comando set RHOST 192.168.1.80.



Una vez terminada con la configuración se debe ejecutar el comando exploit, donde se nos dará acceso a un Shell con usuario root, permitiéndonos acceso total a la maquina victima donde se puede crear, modificar y eliminar archivos, usuarios o directorios.

© Universidad Internacional de La Rioja (UNIR)

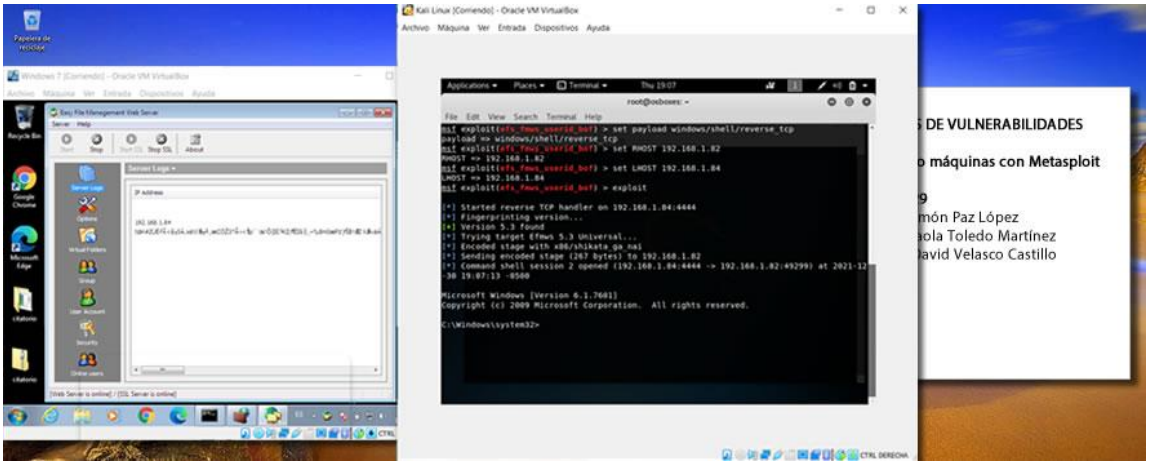


Payload bind and reverse

Un Payload o carga lógica se entiende como un pedazo de código que se ejecuta tras haber logrado un acceso en el sistema y que nos permite poder realizar determinadas acciones (crear, modificar, eliminar, robar archivos). Ofrece el poder trabajar sobre la maquina vulnerada con total libertad.

Existen dos tipos de Payload por método de conexión:

- **Reverse:** El cual consiste en realizar la conexión de la máquina víctima a un servidor creado en la máquina que está ejecutando Metasploit. La víctima se está conectando con nosotros.
    - Reverse: set payload windows/shell/reverse_tcp

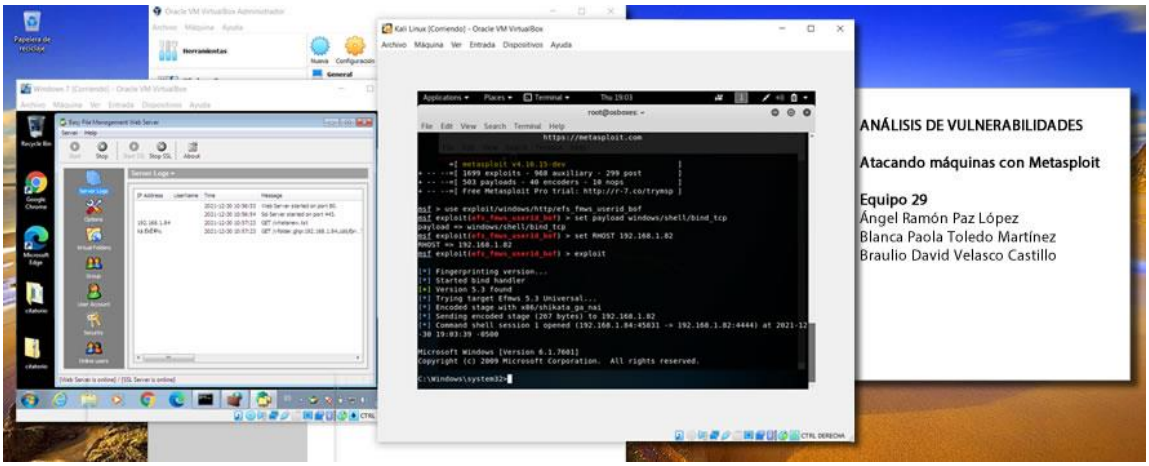


- **Bind:** La conexión se realiza al revés, ahora nosotros nos conectamos a la víctima, este método puede fallar si la víctima realiza un cambio de IP o posee un DHCP activado.

© Universidad Internacional de La Rioja (UNIR)

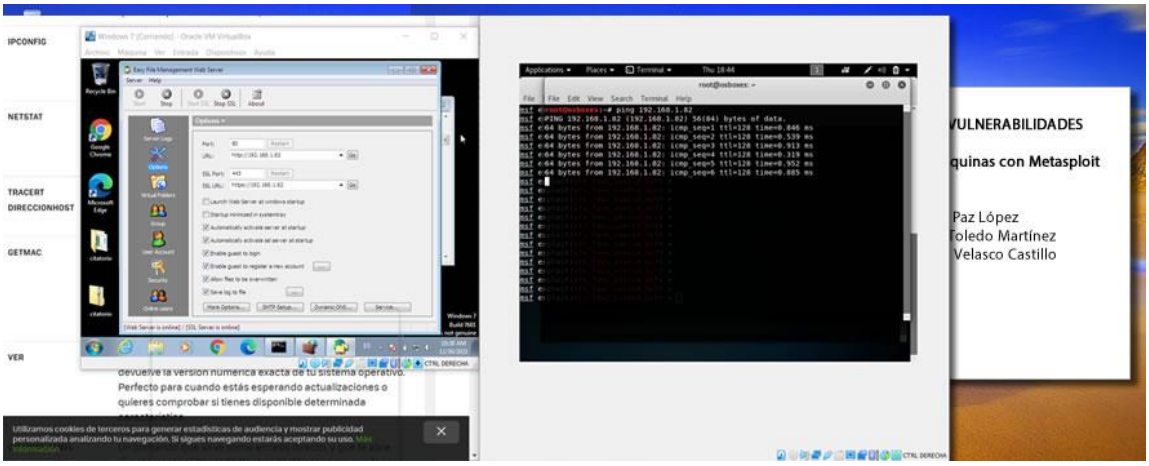
Además, que en la mayoría de los casos las reglas que se encuentran definidas para los Firewall entrantes pueden bloquear el tráfico.

- comando set payload windows/shell/bind_tcp



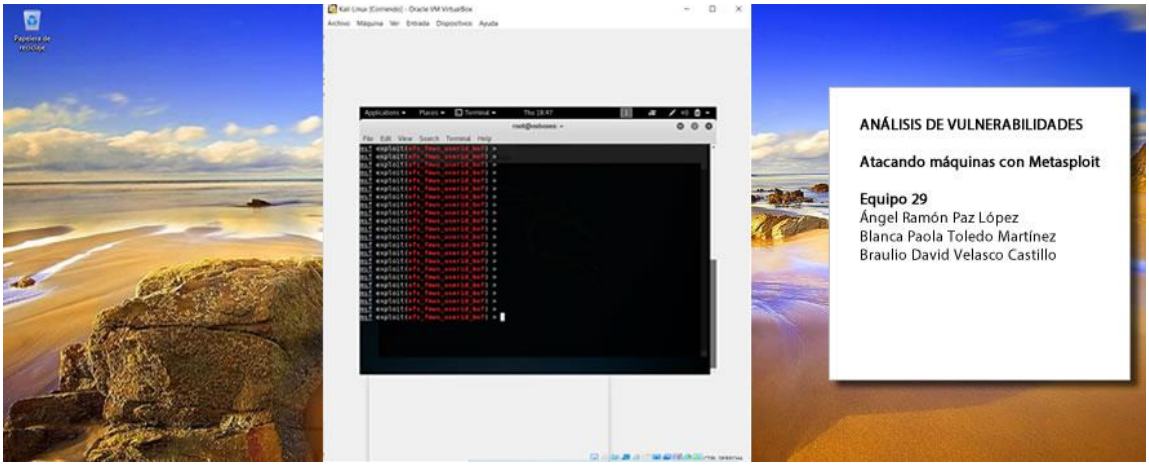
Metasploit y Easy File Management Web Server 5.3

Corroboramos que la maquina Windows 7 y la atacante Kali Linux se encuentren en la misma red y procedemos a la instalación de Easy File Management Web Server para ejecutarlo.

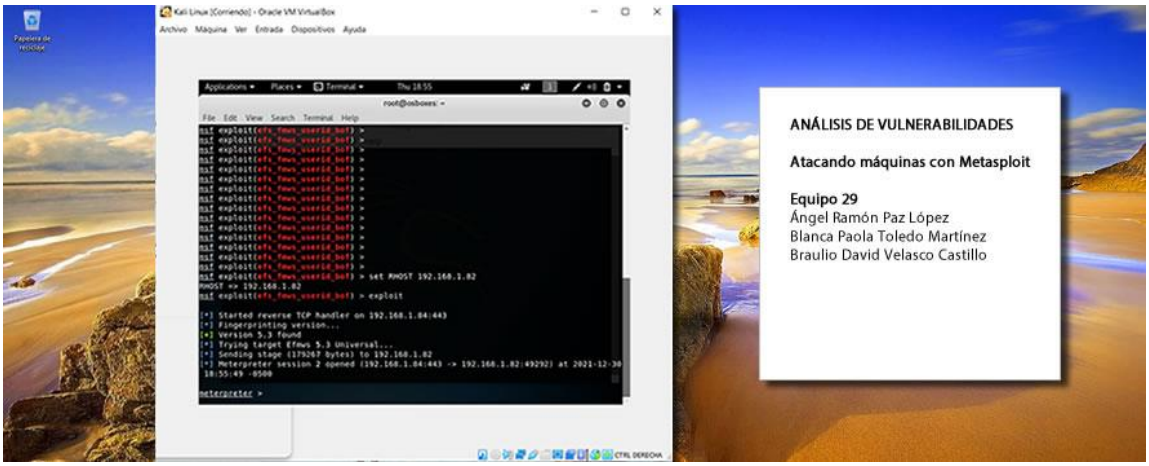


Desde la máquina atacante (Kali Linux) procedemos a ejecutar metasploit con el comando msfconsole y usamos el exploit “use exploit/windows/http/efs_fmws_userid_bof” que se aprovecha de la vulnerabilidad de la aplicación Easy File Management Web Server en sus versiones 4.0 y 5.3.

© Universidad Internacional de La Rioja (UNIR)

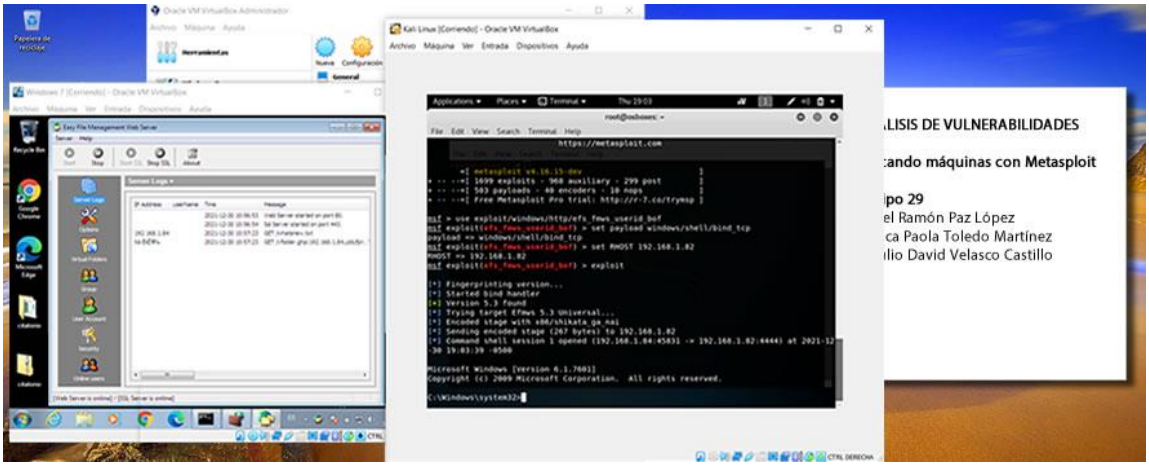


Después procedemos a la configuración del exploit mediante el comando de show options en donde se ingresará por medio del comando set RHOST la ip de la máquina víctima y ejecutar el comando exploit en donde crearemos una sesión meterperer con la víctima.



Ahora procederemos a ejemplificar el mismo exploit con un payload con el comando set payload windows/shell/bind_tcp

© Universidad Internacional de La Rioja (UNIR)



Conclusión

Metasploit es una herramienta de detección de vulnerabilidades de seguridad de código abierto que viene con cientos de vulnerabilidades de software conocidas y se actualiza con frecuencia. Potente marco de pruebas de penetración denominado por la comunidad de seguridad como "puede hackear todo el universo". Ya hay muchos Exploit existentes en Metasploit, proporciona una interfaz de uso externa, de modo que los usuarios pueden apuntar a la máquina de destino sin comprender el principio de la vulnerabilidad y el shellcode.

- Exploit: Se refiere a un ataque realizado por un atacante o probador de penetración utilizando una vulnerabilidad de sistema, aplicación o servicio.
- Payload: Se refiere al código que esperamos que el sistema objetivo ejecute después de ser penetrado por el ataque.

Bibliografía

- https://www.metasploit.com
- http://calebbucker.blogspot.com/2012/12/metasploit-atacando-windows-mediante.html
- https://backtrackacademy.com/articulo/metasploit-atacando-a-windows
- http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson8/
- https://jesusfernandeztoledo.com/instalacion-de-metasploit-en-kali-linux/
- https://docs.rapid7.com/metasploit/

© Universidad Internacional de La Rioja (UNIR)

Tabla de valoración individual.

Indica en la actividad el nombre de todos los componentes del equipo y cumplimenta la siguiente tabla de valoración individual:

- Ángel Ramon Paz López
- Blanca Paola Toledo Martínez
- Braulio David Velasco Castillo

	Sí	**No**	**A veces**
Todos los miembros se han integrado al trabajo del grupo	X		
Todos los miembros participan activamente	X		
Todos los miembros respetan otras ideas aportadas	X		
Todos los miembros participan en la elaboración del informe	X		
Me he preocupado por realizar un trabajo cooperativo con mis compañeros	X		
Señala si consideras que algún aspecto del trabajo en grupo no ha sido adecuado		X	

© Universidad Internacional de La Rioja (UNIR)