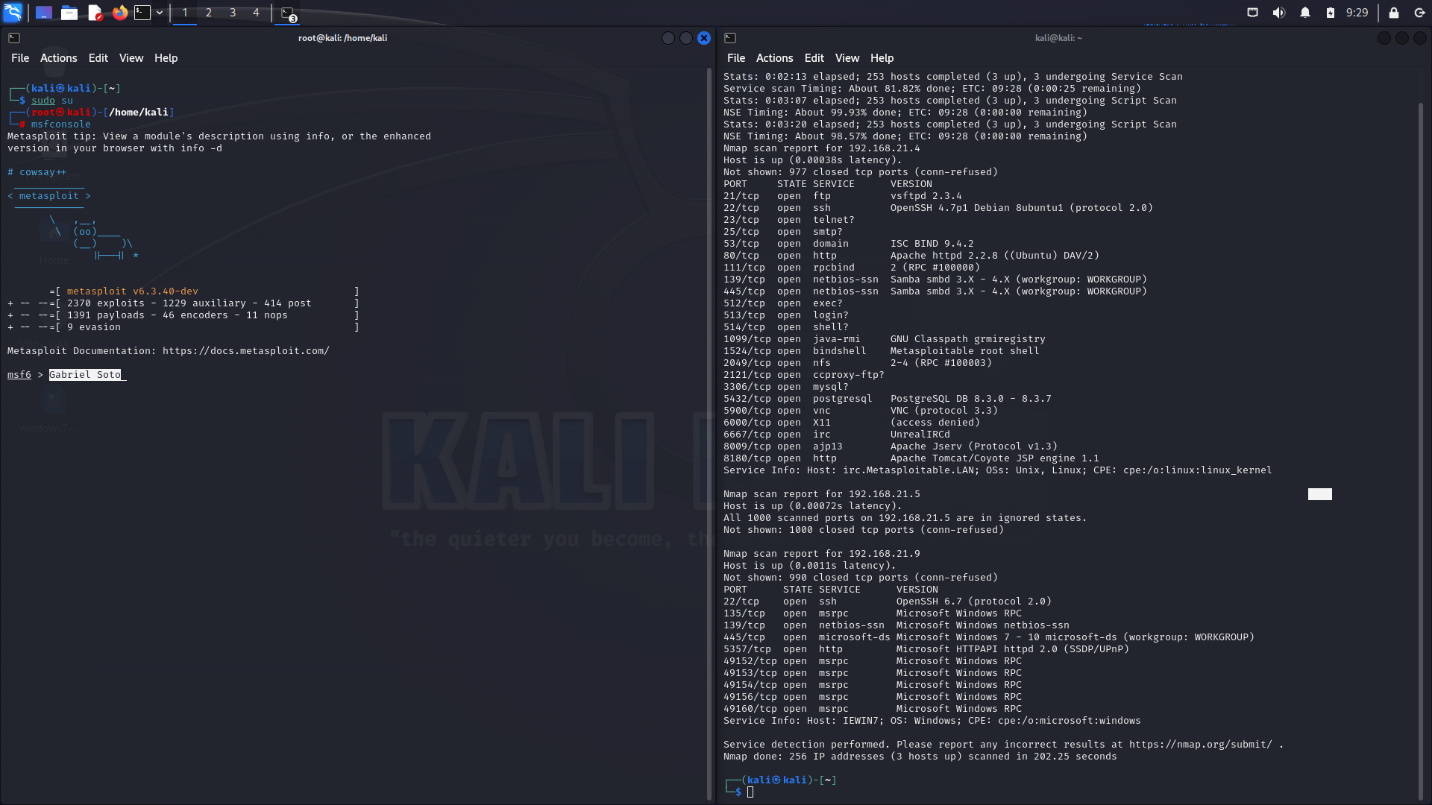
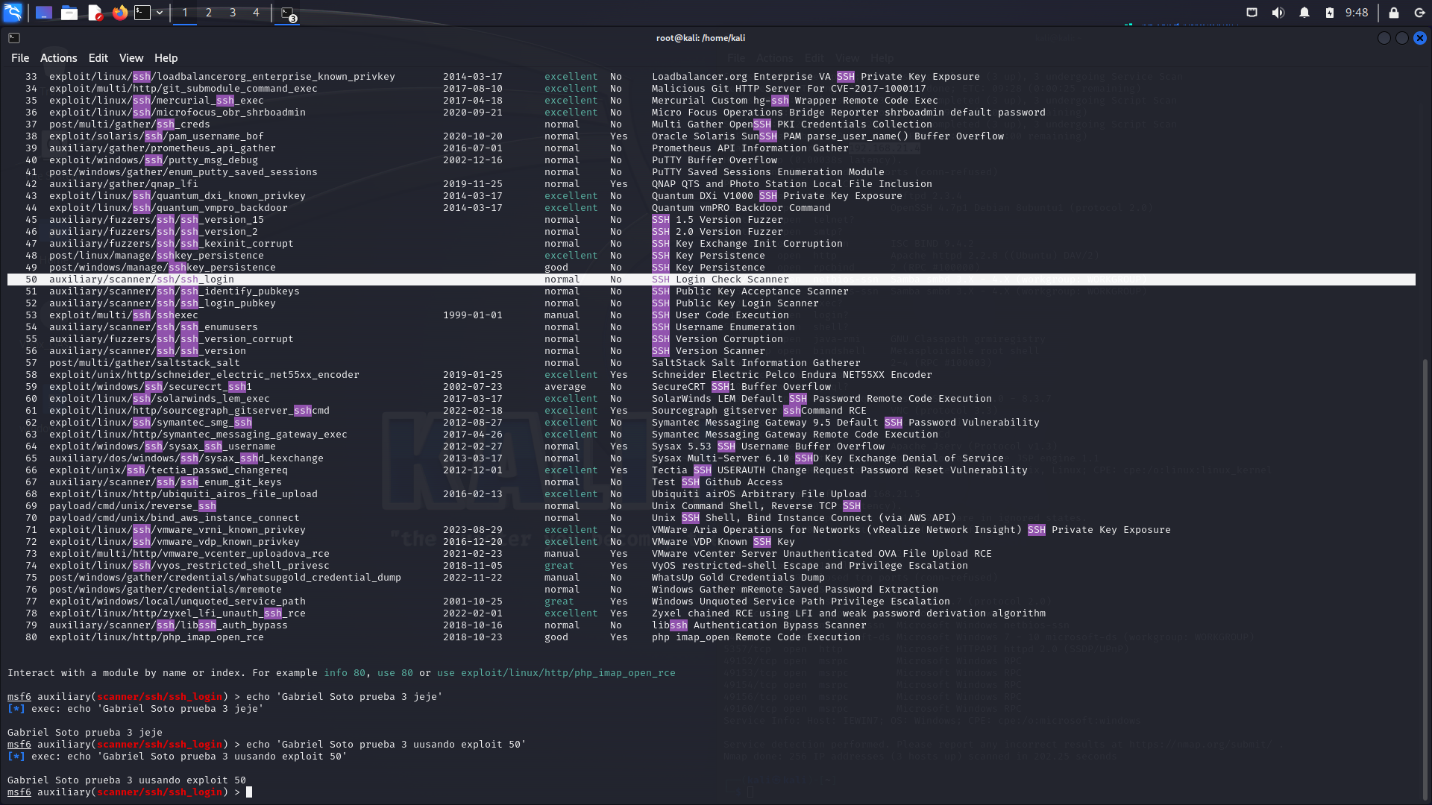
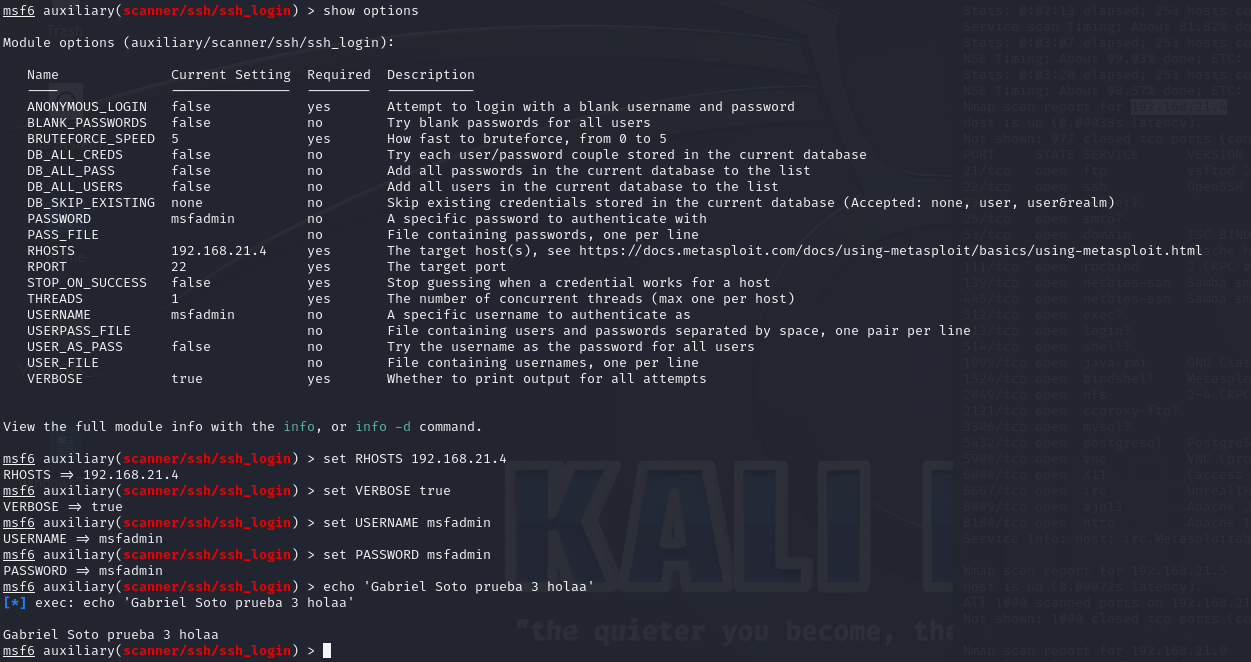
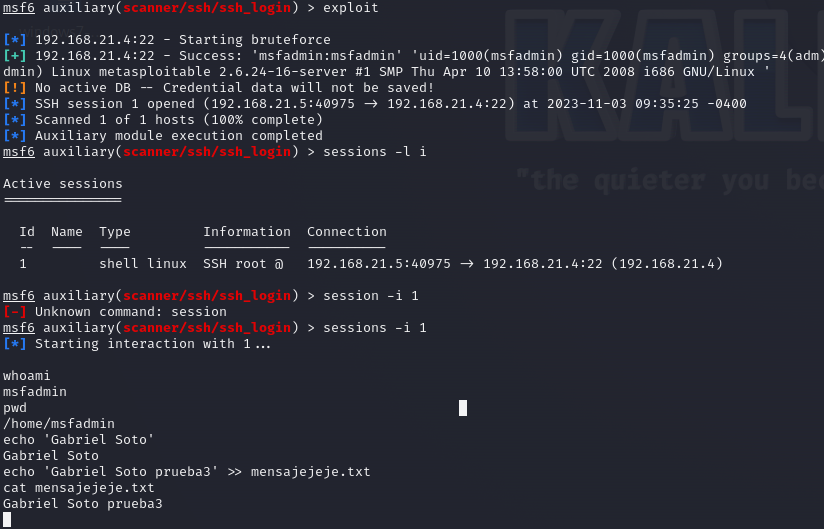
Evidencias prueba 3 Seguridad en Sistemas computacionales

## Gabriel Soto - SEGURIDAD EN SISTEMAS COMPUTACIONALES\_021D

## Profesor Daniel Montero

## Punto 1

1. Hacemos un escaneo de puertos para verificar el puerto, servicio y ip de la víctima que queremos atacar.
2. Ejecutamos una búsqueda haciendo uso del comando ‘search ssh’, la que nos listara todos los exploits relacionados con el termino ssh. Usaremos el exploit llamado ‘ssh\_login’ que está en el índice 50
3. Llenamos con los parámetros indicados en la foto, serian RHOSTS para atacar la ip de la víctima, verbose True para ver con mas detalle lo que está haciendo el exploit, y user y password con msfadmin para poder entrar mediante fuerza bruta, sin embargo, este parámetro puede ser usado también con un diccionario de credenciales. 
4. Para finalizar ejecutaremos el exploit, en caso de que se haya ejecutado correctamente, nos hará una sesión nueva. Listaremos la sesión y nos conectaremos mediante el comando ’sessions -i {índice de la sesión}
5. Para validar que hemos hecho todo bien, ejecutamos los comandos ‘whoami’ Y ‘pwd’. O también pudimos haber ejecutado ‘uname -a’ con un ‘ifconfig’ para asegurarnos aún mas que estamos conectados en la maquina víctima.

## Punto 2

1. Primero, debemos tener en consideración que este ataque solamente funciona en máquinas Windows de 64, Y fijarnos que estemos dentro de la misma red Nat. Seguido de esto, nos preocuparemos de que la maquina victima tenga las actualizaciones de seguridad desactivadas con el script proporcionado en el pdf enviado por el profesor, desactivaremos el firewall de Windows y Windows update

A screenshot of a computer

Description automatically generated

1. En caso de que no sepamos o estemos medios perdidos de que ataque queremos utilizar, usaremos la herramienta de Nessus Essentials para hacer un escaneo básico a la máquina que queremos atacar, en conjunto de nmap, Nessus para saber cuáles son sus vulnerabilidades y Nmap para saber sus puertos abiertos

A screenshot of a computer

Description automatically generated

1. Una vez identificada las vulnerabilidades, ip y los puertos abiertos de nuestra maquina victima (192.168.21.10:445) Procederemos a usar msfconsole en super user para poder ejecutar nuestro ataque con la vulnerabilidad **MS17\_010 eternal blue**

A screenshot of a computer

Description automatically generated

1. Ahora, procederemos a mostrar las opciones y parámetros necesarios para atacar la máquina. Para nuestro caso, solo necesitamos solamente llenar el parámetro RHOSTS con la ip de nuestra victima (192.168.21.10), opcionalmente podemos dejar el parámetro de VERBOSE como true para ver más información del ataque

A screenshot of a computer screen

Description automatically generated

1. Una vez con los parámetros llenos, ejecutamos exploit para atacar.

A screenshot of a computer program

Description automatically generated

1. Podemos ejecutar una lista de cosas muy interesantes con meterpreter, algunas cosas pueden ser como ejecutar programas dentro el directorio que estamos (al conectarnos como administrador, entraremos al directorio de System32 por default), listar webcams o dispositivos de audio con webcam\_list, screenshare, etc. Ahora nos interesa interactuar con el interprete de consola de DOS que viene integrado con Windows, por lo que ejecutaremos el comando ‘execute -f cmd.exe -i -H’, siendo el parámetro -f para poder ejecutar directamente el programa que queremos usar, el parámetro -i para poder interactuar con ese programa, y el parámetro -H para que el programa se ejecute de manera silenciosa, ya que de no ser así, el sistema operativo lanzara un aviso de que cierto programa desea dar un mensaje, cosa que si el usuario hace click en esa ventana, le mostrara el mensaje con los programas que nosotros hemos abierto. Como por ejemplo:



A computer screen with a blue background

Description automatically generated

A screenshot of a computer

Description automatically generated

En caso de que ejecutemos el comando de manera correcta, solamente debería pasar lo siguiente:

A screenshot of a computer

Description automatically generated

En este caso, una vez ejecutamos la cmd, podemos verificar que estamos conectados como administradores gracias a los comandos de whoami y además podemos listar la lista de todos los usuarios que hay registrados en esta maquina haciendo uso del comando de net user. Con esto podemos concluir que la maquina ha sido vulnerada.

## Punto 3

1. Para este ataque, no usaremos metasploit-framework, solamente usaremos nuestro navegador de preferencia, y la máquina de metasploitable2.

A screenshot of a computer

Description automatically generated

1. Necesitaremos conectarnos desde el navegador a nuestra máquina de metasploitable (antes debemos fijarnos que estemos que ambas maquinas estén en la misma red nat), la ip que tiene asignada nuestra maquina víctima es 192.168.21.4

A screenshot of a computer

Description automatically generated

1. Usaremos el servidor o servicio de DVWA para ejecutar nuestra inyección sql, antes nos logueamos con las credenciales de admin y password

A screenshot of a computer

Description automatically generated

1. Cambiamos el nivel de seguridad de la pagina en general a low

A screenshot of a computer

Description automatically generated

1. Nos conectaremos mediante ssh a la maquina victima para intentar hacer un poco de ingeniería inversa con las tablas haciendo uso de mysql

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Descubrimos que la inyección la podemos hacer desde la bbdd dvwa, desde la tabla de usuarios.

1. Ahora procederemos a construir nuestra inyección. A screenshot of a computer

   Description automatically generated

Haciendo uso de la sentencia 1’ OR 1=1 UNION SELECT, COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME=’USERS’ # Podemos darnos cuenta de que la tabla tiene 6 columnas, las cuales son las de user\_id, first\_name, last\_name, user, password, y avatar. Estas columnas son las ultimas que retorna el resultado de la inyección (las que tiene de first name : 1)

1. Finalizando, construiremos la inyección para poder retornar todos los datos de los usuarios

A screenshot of a computer

Description automatically generated

Estamos obteniendo los datos del user\_id, avatar, first\_name\_last\_name, user, y password. El uso de valores ASCII hexadecimales es para darle formateo al texto, debido a las restricciones con el uso de las comillas. Cada vez que imprime ‘0x0020,0x007c,0x007c,0x0020’ lo interpretara como ‘ || ’, de esta forma, la información se vera mas agradable a la vista.

Query: %’ and 1=1 union select null, concat(user\_id, 0x0020,0x007c,0x007c,0x0020,avatar, 0x0020,0x007c,0x007c,0x0020,first\_name, 0x0020,0x007c,0x007c,0x0020,last\_name, 0x0020,0x007c,0x007c,0x0020,user, 0x0020,0x007c,0x007c,0x0020,password) from users #’