Práctica 2

Tests de intrusión y explotación de vulnerabilidades: uso básico de Mestasploit

Jacobo Martínez Gómez

19/20

## Resumen general: escenario, herramientas usadas y objetivos

### Escenario

La practica busca hacer una aproximación a la explotación de vulnerabilidades en los sistemas informáticos, usando la herramienta metasploit.

### Herramientas usadas

Para la realización de esta practica se van a usar las diferentes herramientas:

* NMAP y NESSUS para la obtención de información
* METASPLOIT para la detección y explotación de vulnerabilidades.

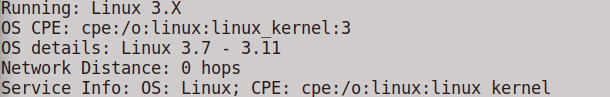
### Objetivos

* Identificar los servicios activos en una red y localizar las posibles vulnerabilidades de ellos.
* Atacar las vulnerabilidades encontradas y conseguir comprometer la seguridad del sistema.

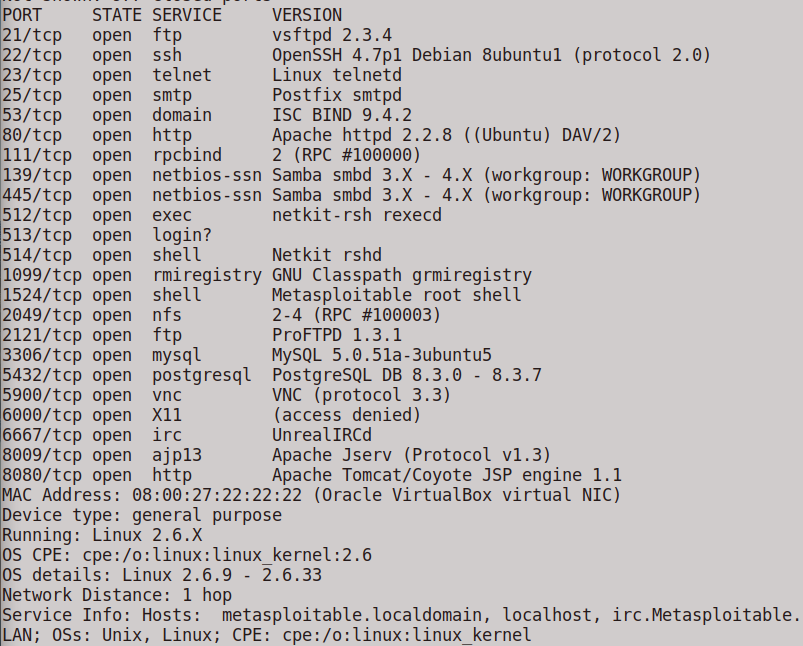
## Equipos y servicios identificados

Maquina atacante (198.51.100.111):



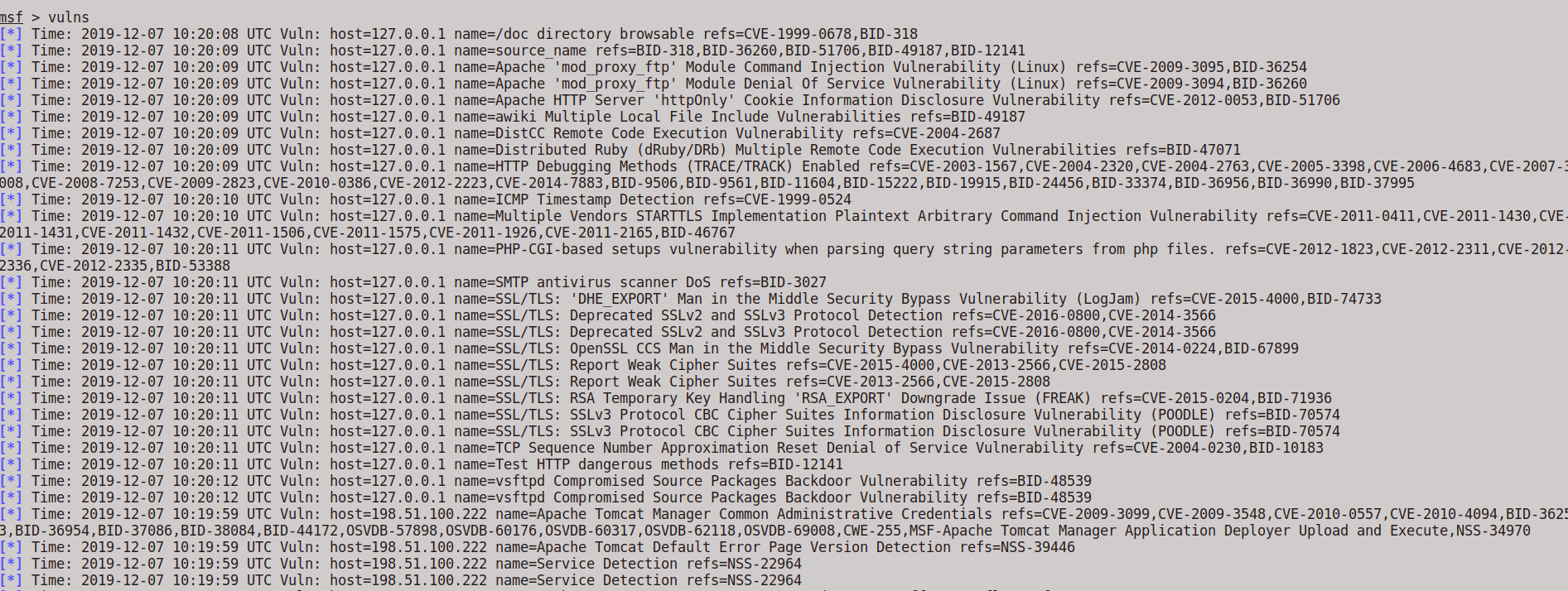


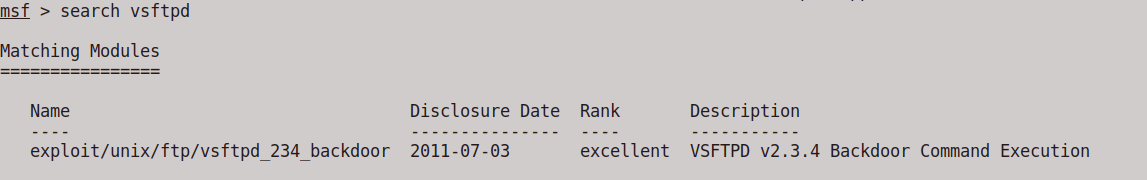
Maquina metasploitable2 (198.51.100.222):

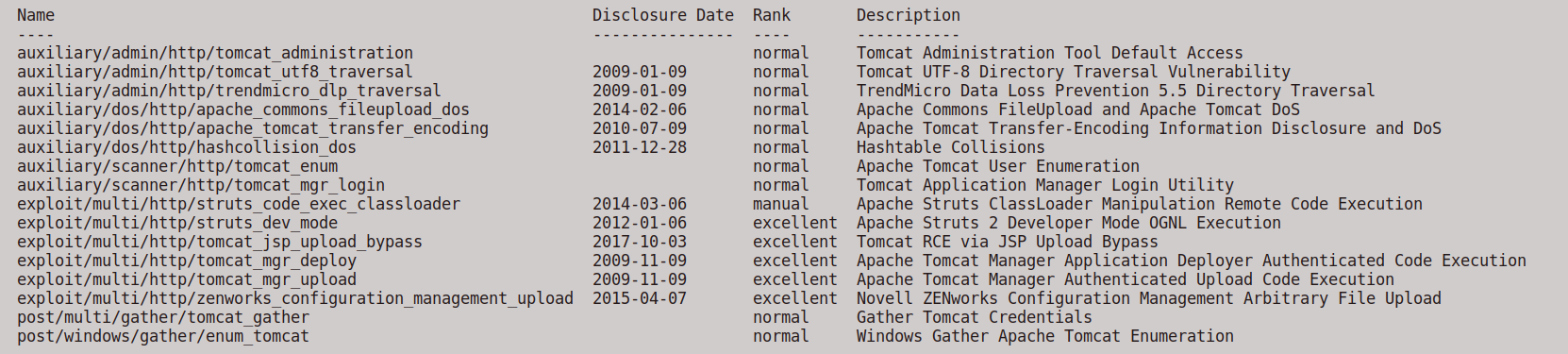


## Vulnerabilidades detectadas y posibilidades de explotación

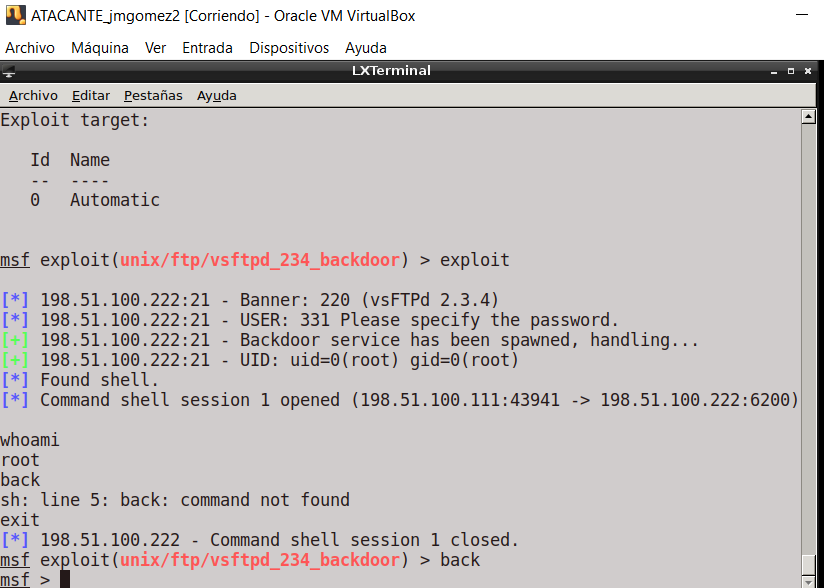
### Resumen/listado general





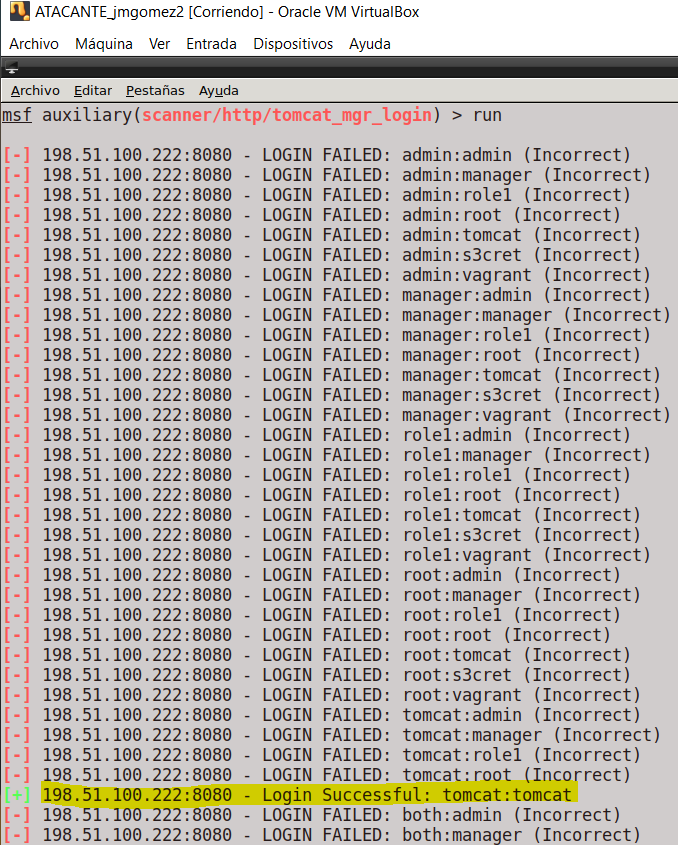


### Informe de explotación



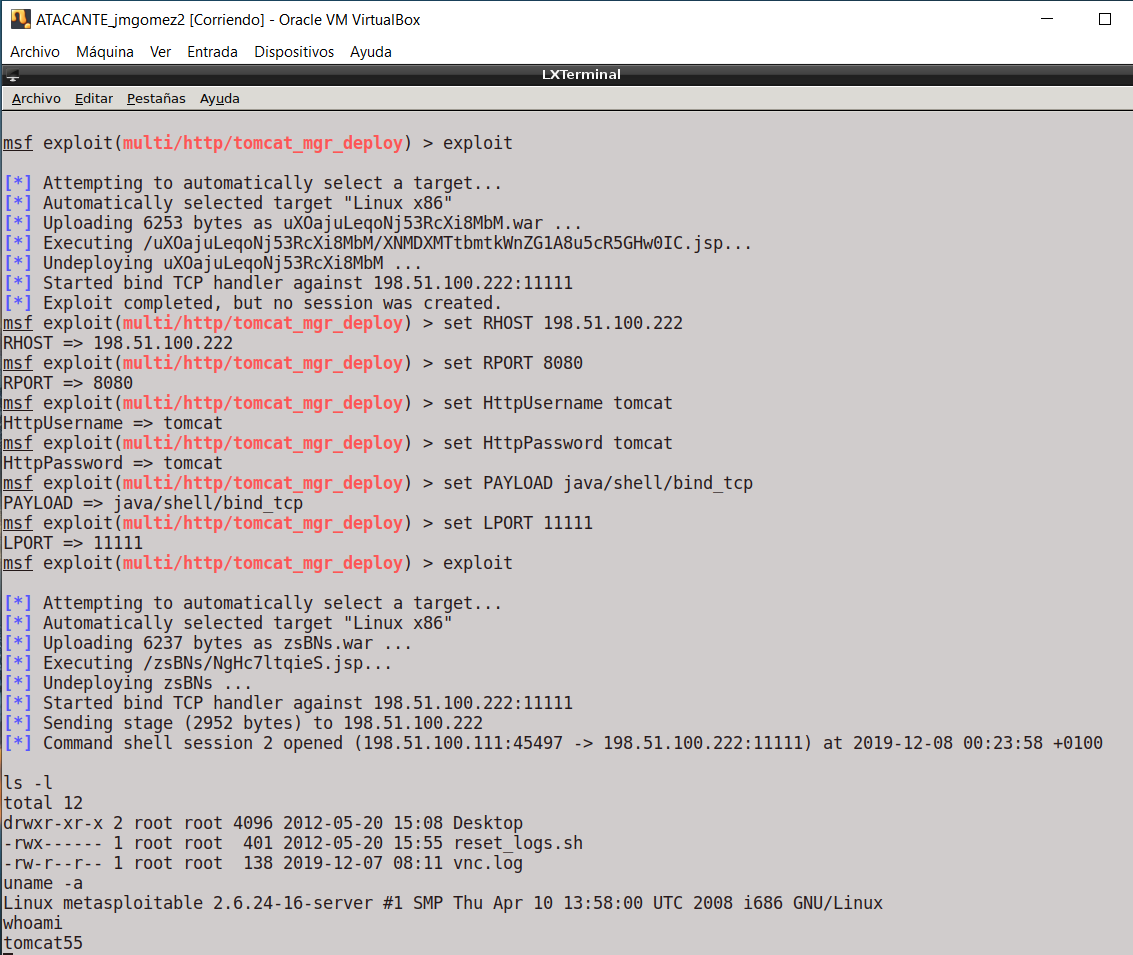
Tras lanzar el exploit vsftpd\_234\_backdoor comprobamos que obtenemos una conexión shell a la maquina metasploitable. Probamos a lanzar algunos comandos para ver que realmente estamos en esa máquina.

Primero vamos a usar el expoit tomcat\_mgr\_login, para obtener un usuario y contraseña validos

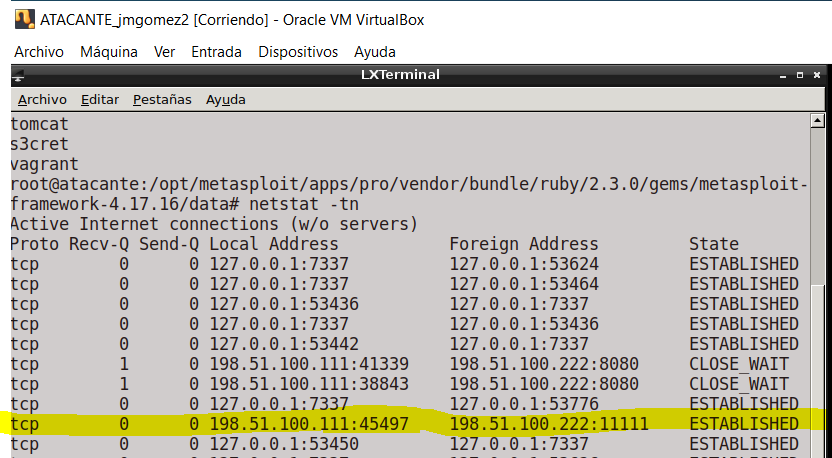


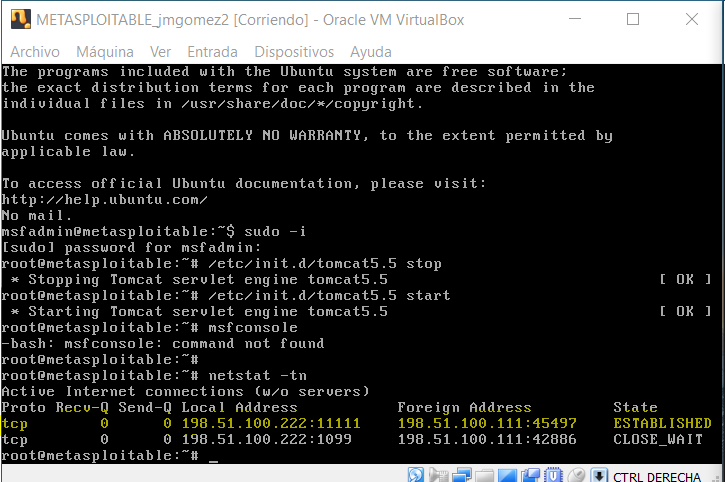
Una vez obtener el par usuario y contraseña valido podemos pasar a usar el exploit: tomcat\_mgr\_deploi para obtener un enlace via Shell a la maquina auditada.´

Para obtener la Shell se usa el payload java/Shell/bind\_tcp que abre un puerto de escucha en la maquina auditada donde estableceremos la conexión LPORT:11111

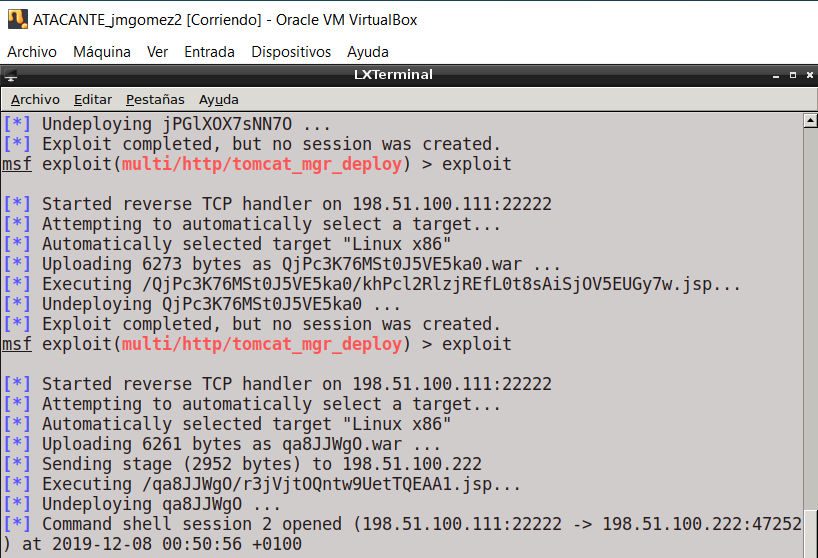


Comprobamos que la conexión esta establecida:

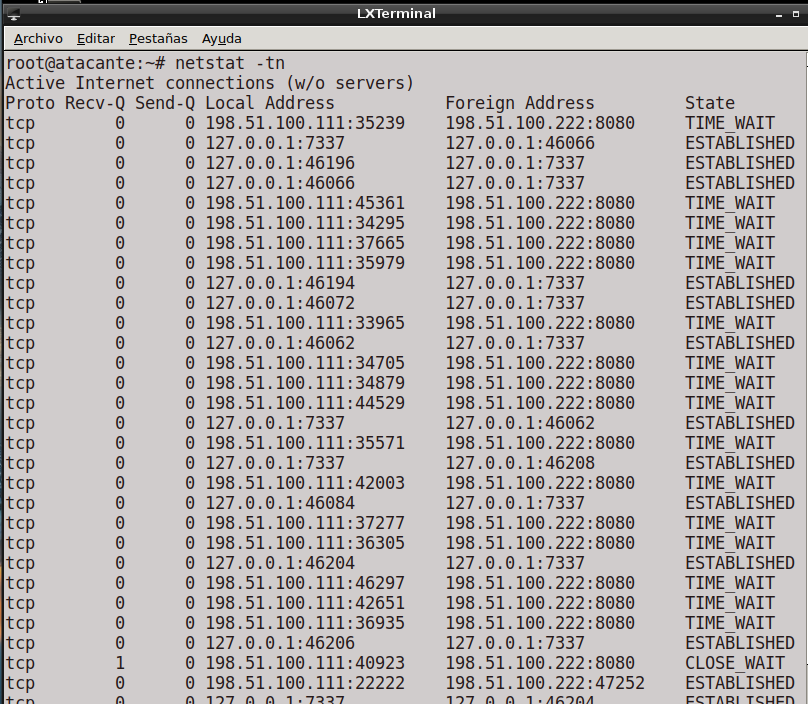


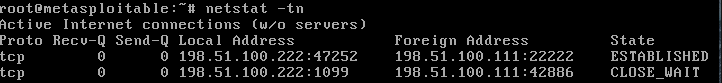


Ahora pasamos a usar el PAYLOAD java/shell/reverse\_tcp para que sea la maquina auditada la que se conecte en un puerto de nuestra maquina.



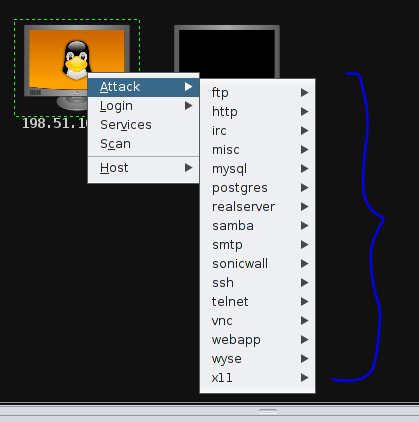
Comprobamos que está establecida la conexión en ambas maquinas:



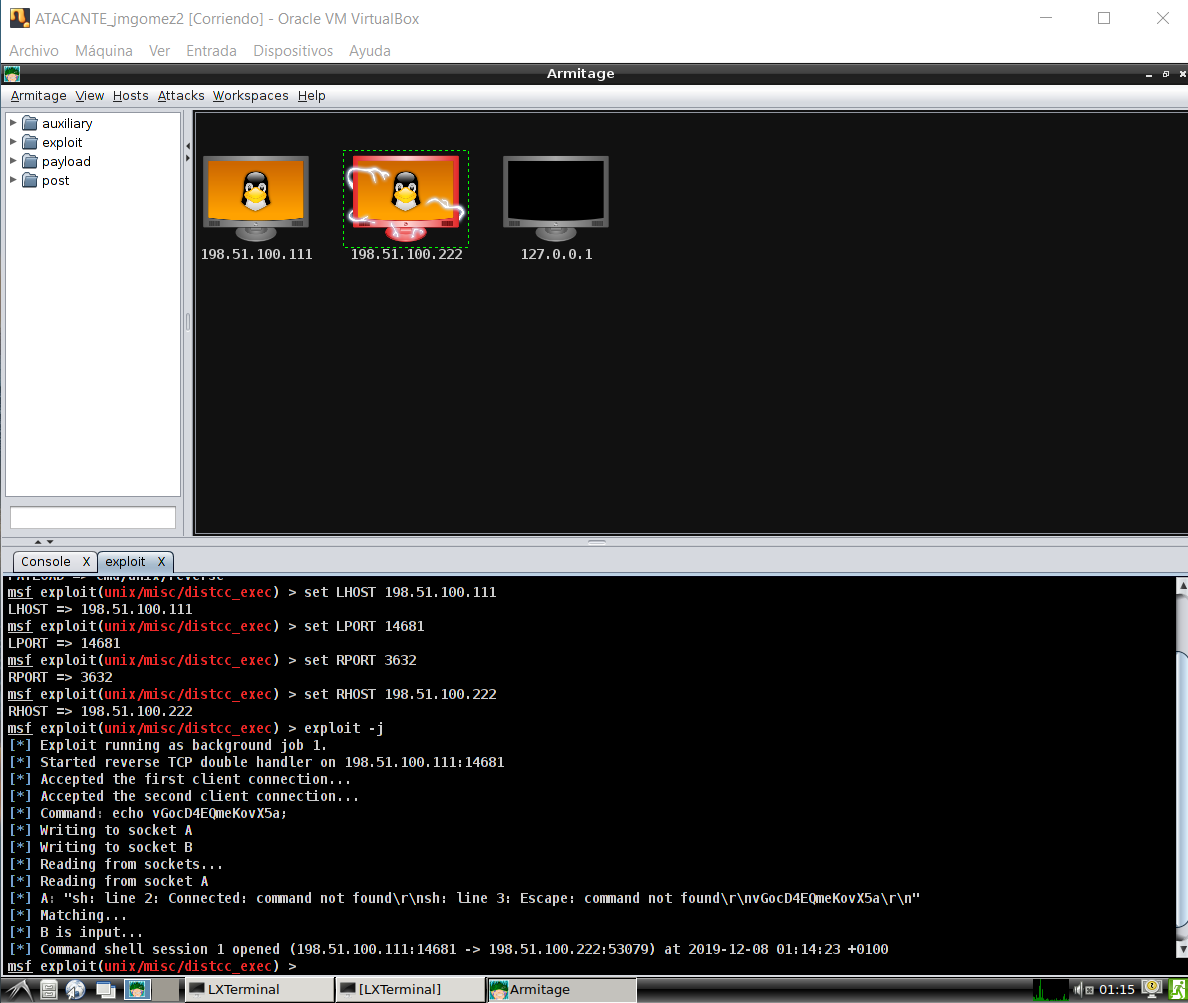


## Armitage: uso interfaz gráfica

Vincular posibles ataques a un host víctima en el menú Attack/Find Attacks. Esto rellena el menú del host auditado:

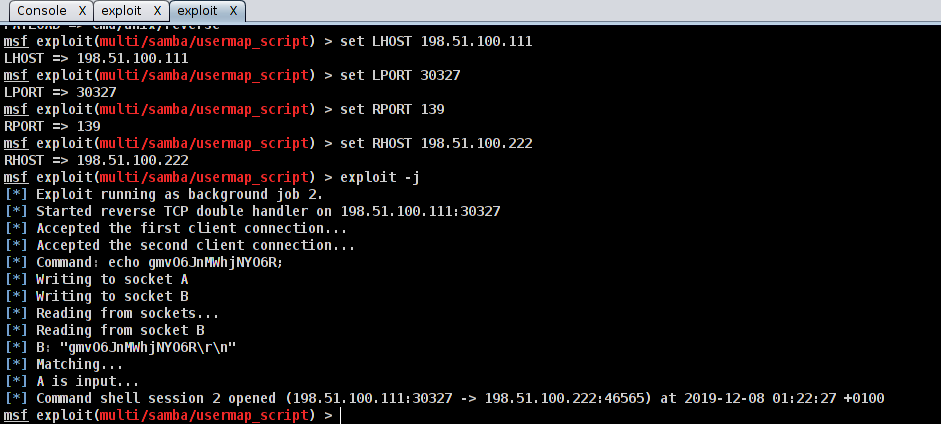


#### Explotar el servicio distcc (compilación distribuida).

Lanzamos el exploit ‘exploit/unix/misc/distcc\_exec’ lo que nos proporciona una Shell para acceder al host. Sabemos que se realiza correctamente el exploit cuando cambia el icono del host al que se lo hacemos. 

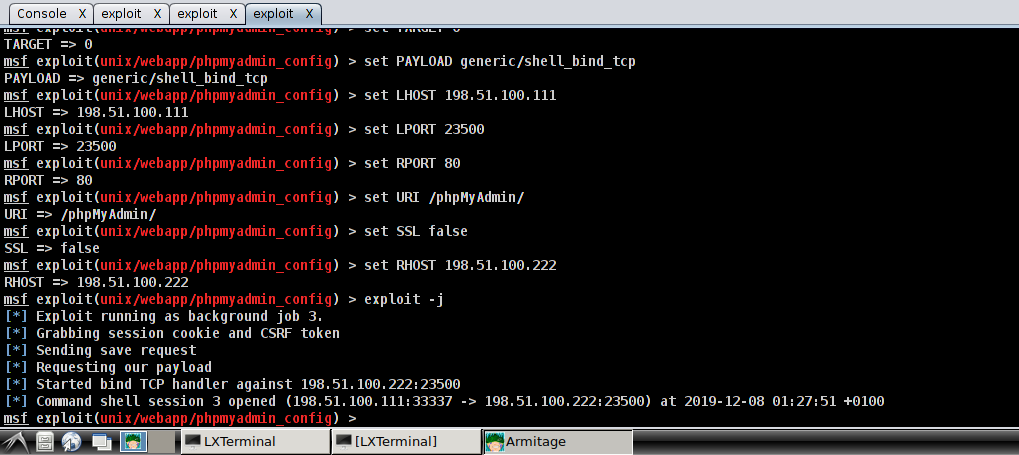
#### Explotar el servicio SMB (samba)

Lanzando el exploit ‘exploit/multi/samba/usermap\_script’ nos proporciona una Shell para acceder al host auditado.

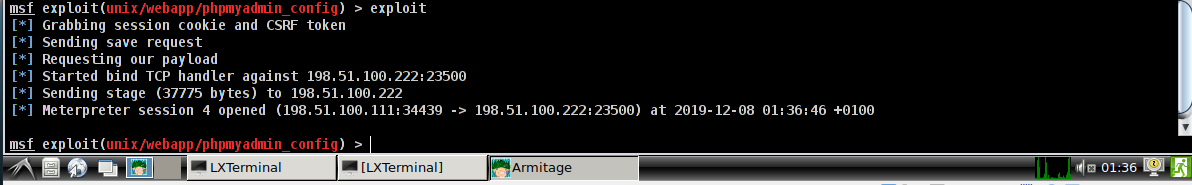


#### Explotar una versión vulnerable de phpMyAdmin y uso de Meterpreter

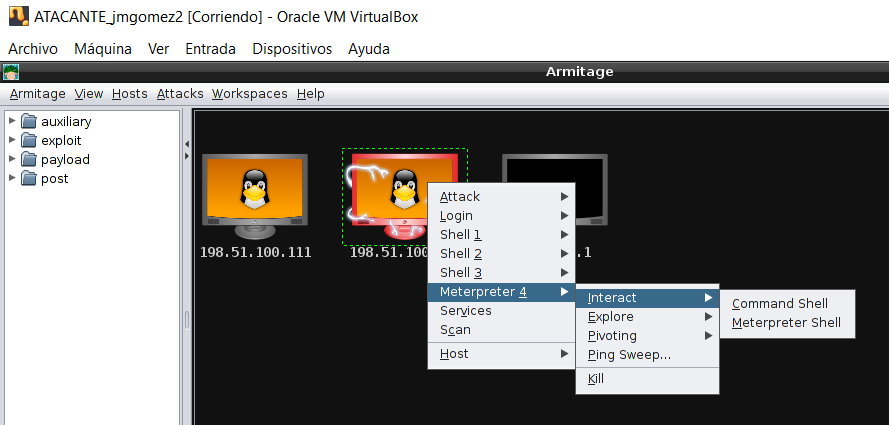
Lanzamos el exploit ‘exploit/unix/webapp/phpmyadmin\_config’ que nos proporcionara una Shell para acceder al host auditado.



Para usar meterpreter cambiamos el payload del exploit anterior a ‘php/meterpreter/bind\_tcp’ a continuación ejecutamos el exploit manualmente.

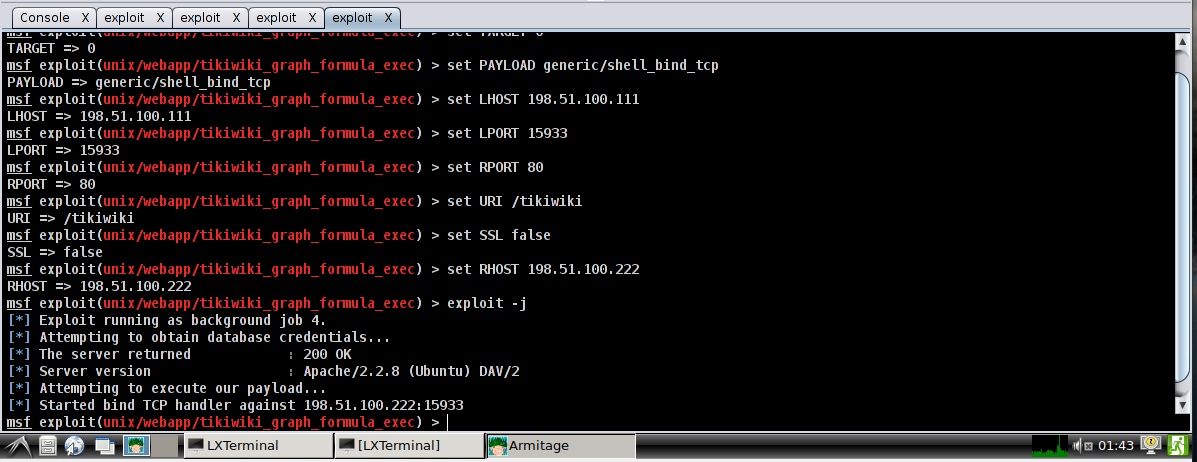


Con esto obtenemos un nuevo menú con mas opciones:



#### Explotar la aplicación web TikiWiki

Lanzamos el exploit ‘exploit/unix/webapp/tikiwiki\_graph\_formula\_exec’



## Propuesta de contramedidas y correcciones en dos escenarios

### Escenario 1: es posible la actualización/reemplazo de los equipos/servicios vulnerables.

Siempre que se puedan actualizar o reemplazar los servicios afectados es lo primero que tenemos que hacer. Después de actualizar el servicio deberíamos hacer una nueva auditoría para comprobar que la nueva versión funciona correctamente y no tiene vulnerabilidades. Además, deberíamos mantener un programa de auditorías programadas periódicamente dado que se pueden encontrar nuevas vulnerabilidades en cualquier momento.

Un servicio que no sea confiable, del que no podemos asegurar que no es vulnerable no debe estar activado en nuestro sistema, dado que esto implicaría dejar el sistema expuesto. Por lo tanto, deberíamos eliminarlo y buscar otra alternativa segura.

### Escenario 2: no es posible la actualización/reemplazo de los equipos/servicios vulnerables

Si no se actualizar o reemplazar un servicio que compromete la integridad de nuestro sistema deberíamos buscar otras alternativas para evitar la intrusión.

Deberíamos controlar de una manera mas efectiva quien se conecta al sistema. Se podría incorporar filtrado de MAC para controlar los equipos, autentificación por certificados para controlar a los usuarios, tunneling para hacer comunicaciones seguras y por último firewalls para separar las zonas mas sensibles de las menos. Con un sistema de firewalls en los que se restringe el trafico que no sea imprescindible, las vulnerabilidades pierden importancia dado que el atacante no puede explotarlas al no poder acceder a la maquina.