1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.10: Explotació 2

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs:** 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Explotació vulnerabilitat ElasticSearch**](#_rqxd06nwt9aj) **3**

[a. Explica breument en què consisteix aquesta vulnerabilitat.](#_vsuyp9wfzzlv) 3

[b. Explota-la amb Metasploit indicant tots els passos què has seguit, mostrant les captures amb els resultats obtinguts.](#_8fle1m8gpuxz) 3

[c. Des de Meterpreter, mostra quin usuari ets executant —> getuid](#_pv6ripyfu167) 4

[**Exercici 2 – Explotació vulnerabilitat Jenkins**](#_1wh47boek00x) **7**

[a. Busca què és i per a què serveix l’aplicació Jenkins que incorpora la màquina Metasploitable 3](#_q9csqdp3i8bk) 7

[b. Busca informació sobre la vulnerabilitat de Jenkins de la versió instal·lada a Metasploitable 3](#_5j9550zh55kj) 7

[c. Prova d’explotar-la amb l’exploit —> exploits/multi/http/jenkins\_script\_console —> Segurament hauràs de tocar alguns paràmetres més dels habituals](#_8g61fn28cg8p) 8

[d. Des de Meterpreter per a saber quins permisos d’usuari tens, executa —> getuid](#_gam56vc178jg) 12

[**Exercici 3 – Explotació de GlassFish per força bruta**](#_jwtn53fr3p6t) **13**

[a. Busca què és i per a què serveix el servei de GlassFish que incorpora la màquina Metasploitable 3](#_ebummda2kevp) 13

[b. Fes un nmap executant l’script vuln i comprova quina informació extreus del port 4848](#_6khjsahcgxsa) 13

[c. Des del navegador web de Kali Linux, mostra la plana web inicial de GlassFish que pots trobar pel port 4848 de Metasploitable 3](#_onq7ihpfwsbu) 14

[d. Utilitzant Metasploit busca algún auxiliary per a fer un atac de força bruta al servidor GlassFish.](#_cvbqcw1pxvjp) 15

[**Exercici 4 – Explotació vulnerabilitat Slowloris**](#_khx9c49xv55s) **19**

[a. Què és un atac de DoS?](#_j2x3ifygkij0) 19

[b. Busca què és la vulnerabilitat Slowloris](#_wtwhrr629w88) 19

[c. Prova d’explotar-la sabent que és CVE-2007-6750](#_hxwsvgor6z40) 20

# Exercici 1 – Explotació vulnerabilitat ElasticSearch

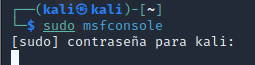
Dins de les vulnerabilitats crítiques que vam trobar a través de Nessus, existia una relacionada amb el programa Elastic Search, una eina per a fer analítica web. Concretament la vulnerabilitat es diu Elasticsearch REST API 1.1.1 (CVE-2014-3120)

### a. Explica breument en què consisteix aquesta vulnerabilitat.

Aquesta vulnerabilitat consisteix en la configuració predeterminada a Elasticsearch abans de la 1.2 permet l'escriptura dinàmica, que permet als atacants remots executar expressions MVEL arbitràries i codi Java mitjançant el paràmetre font de \_search. NOTA: això només infringeix la política de seguretat prevista del venedor si l'usuari no executa Elasticsearch a la seva pròpia màquina virtual independent.

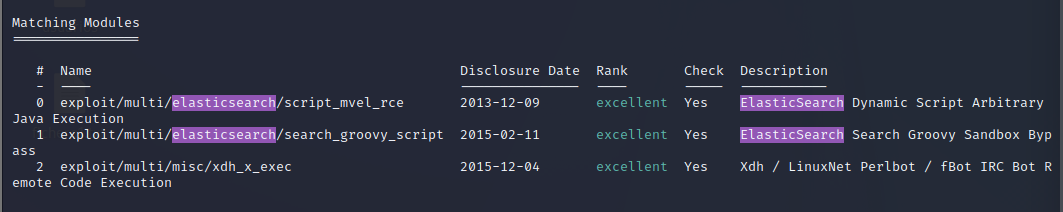
### b. Explota-la amb Metasploit indicant tots els passos què has seguit, mostrant les captures amb els resultats obtinguts.

Primer de tot entrarem a la consola de msf6:

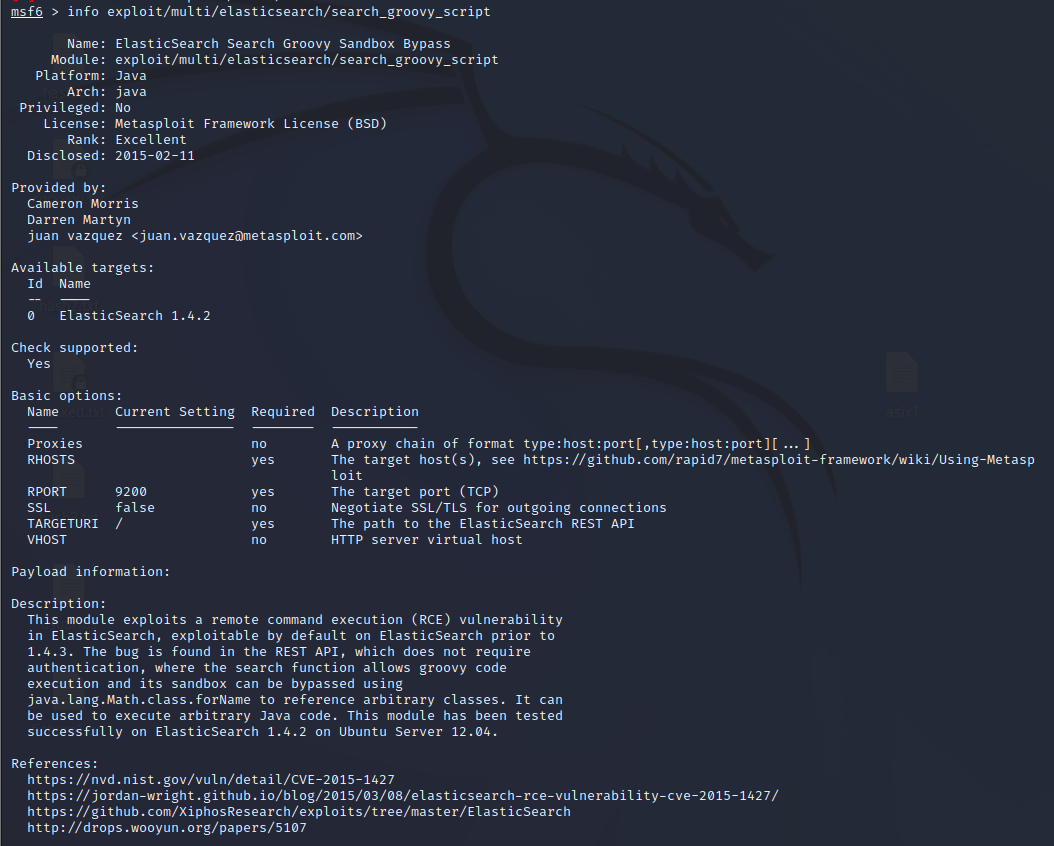


Dins buscarem el exploit amb el nom ElasticSearch



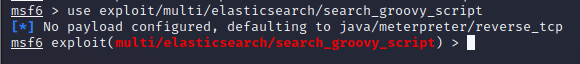


Seguidament, direm a la consola que ens digui informació sobre aquesta vulnerabilitat:

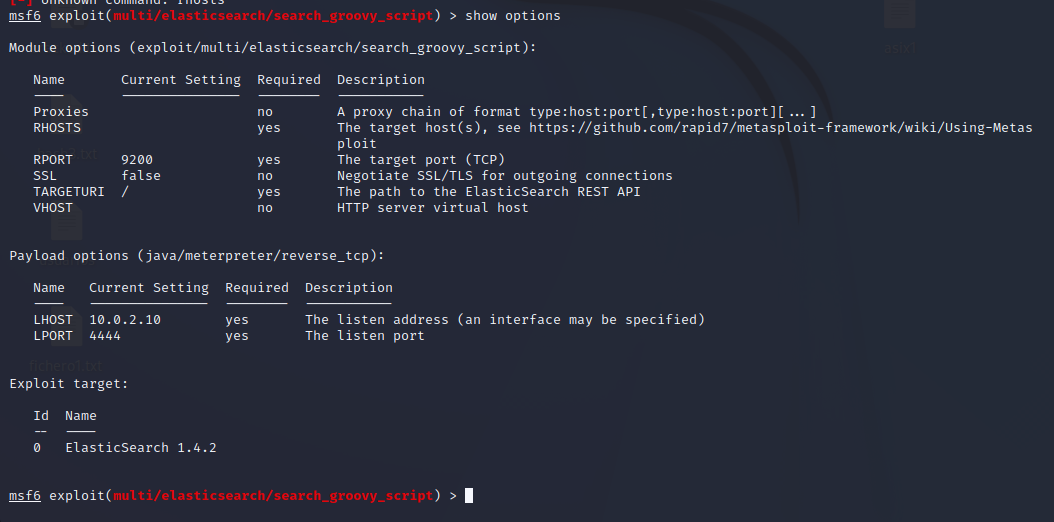


### c. Des de Meterpreter, mostra quin usuari ets executant —> getuid

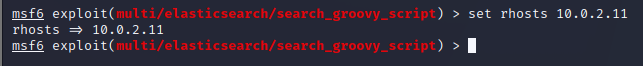
Abans d’entrar a meterpreter, haurem de fer uns passos, primer de tot escollirem utilitzar el exploit:



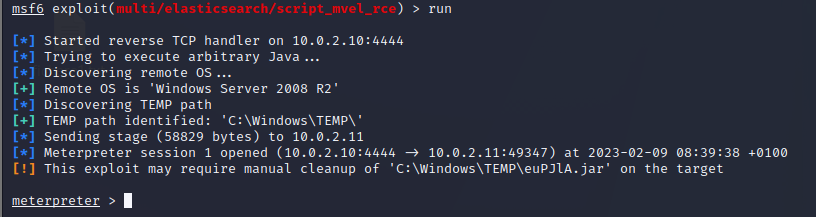
Farem un show options:



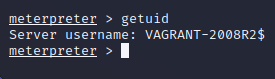
Seguidament, haurem de fer un rhosts amb la maquina victima:



Ara executarem un run (he hagut de canviar el exploit per el 0 ja que no deixava entrar amb el run a l’altre):



Ara ja podrem fer el getuid dins del meterpreter:

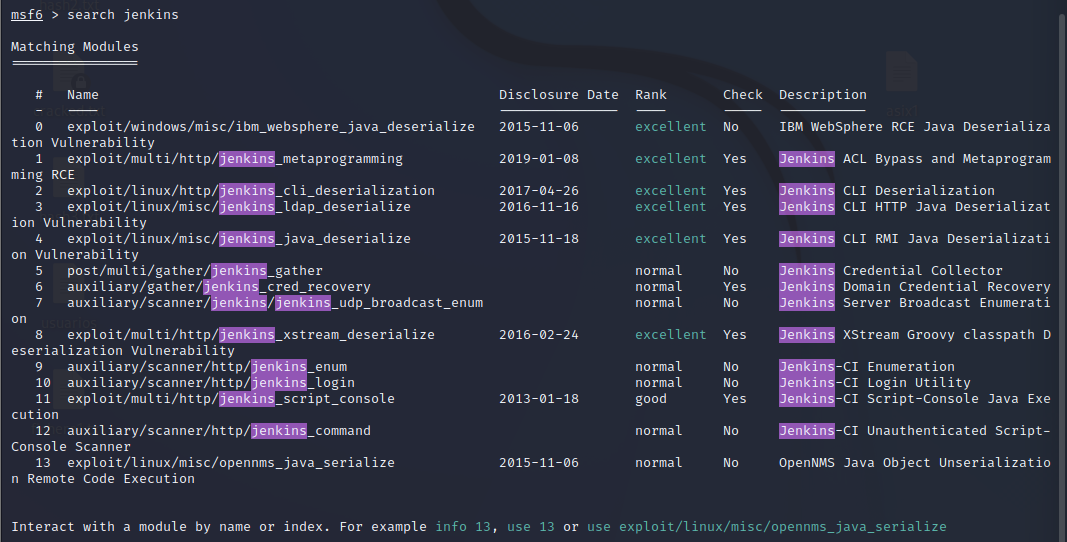


# Exercici 2 – Explotació vulnerabilitat Jenkins

### a. Busca què és i per a què serveix l’aplicació Jenkins que incorpora la màquina Metasploitable 3

Què és Jenkins?

Jenkins és un servidor de codi obert per a la integració contínua. És una eina que s'utilitza per compilar i provar projectes de programari de forma contínua, cosa que facilita als desenvolupadors integrar canvis en un projecte i lliurar noves versions als usuaris. Escrit a Java, és multiplataforma i accessible mitjançant interfície web. És el programari més utilitzat actualment per a aquest propòsit.

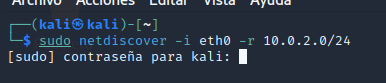


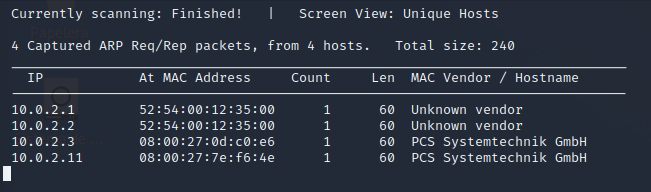
### b. Busca informació sobre la vulnerabilitat de Jenkins de la versió instal·lada a Metasploitable 3

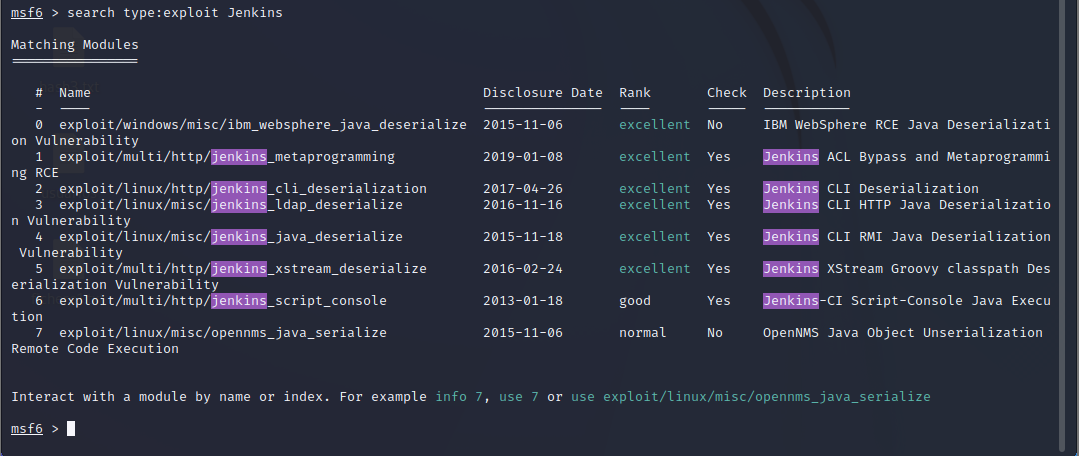
En primer lloc, val la pena esmentar que Jenkins no només té una vulnerabilitat..

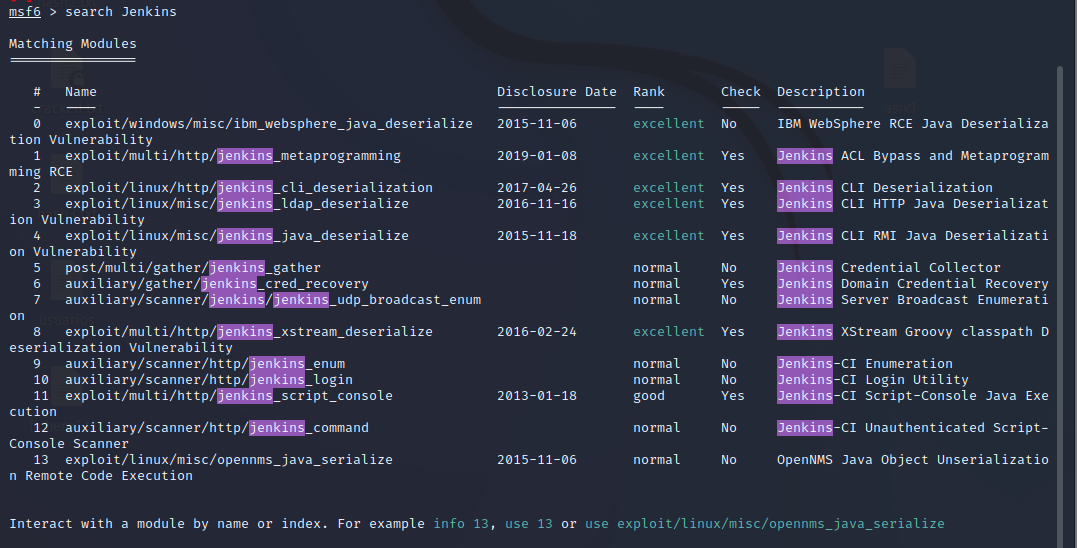
* Execució remota de codi (RCE): permet que un atacant executi codi maliciós a través d'una aplicació per obtenir accés no autoritzat a un sistema.
* Cross-Site Scripting (XSS): permet als atacants injectar codi maliciós (malware) en pàgines web per executar codi arbitrari al navegador d'un usuari.
* Falsificació de sol·licitud entre llocs (CSRF): permet que un atacant faci accions no autoritzades en nom d'un usuari autenticat.

### c. Prova d’explotar-la amb l’exploit —> exploits/multi/http/jenkins\_script\_console —> Segurament hauràs de tocar alguns paràmetres més dels habituals

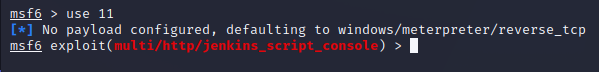




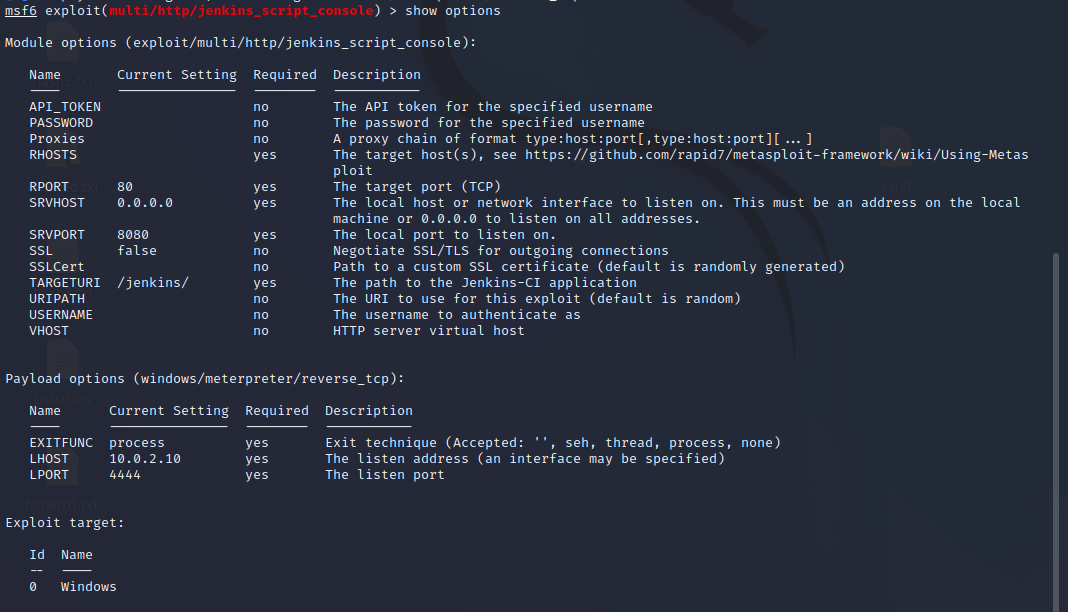




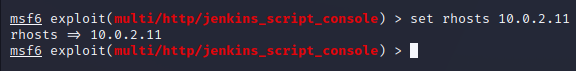
L’exploit demanat es el número 11, per tant:



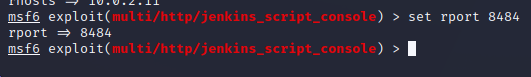
Farem un show options:



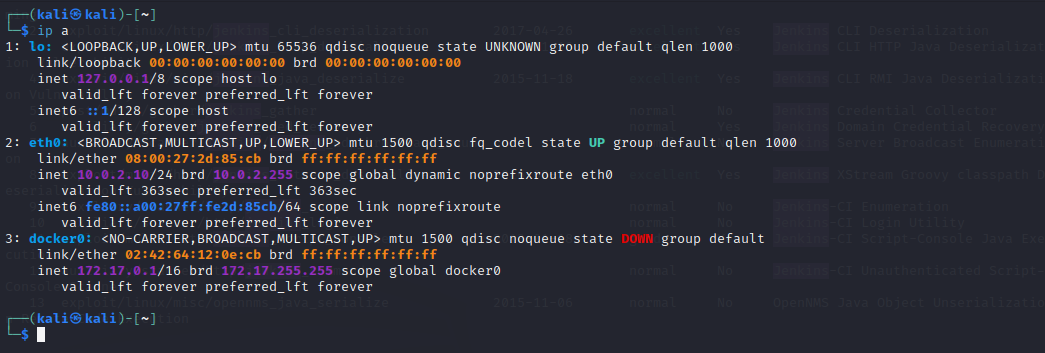
Seguidament, farem un rhosts a la màquina Metasploitable3



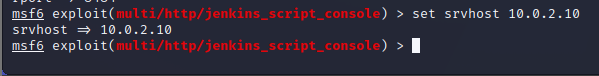
També configurarem el port:



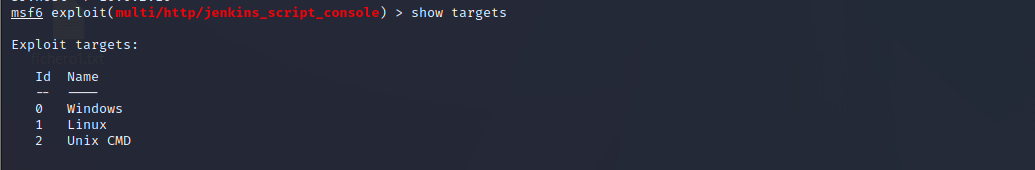
Agafarem la ip del kali:



I configurarem aquesta ip com a màquina que escolta:



Farem un show targets:



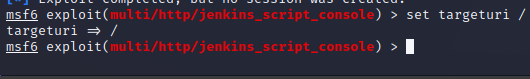
Afegirem el payload a continuació:



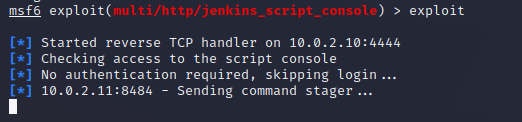
Afegirem també el lhost:

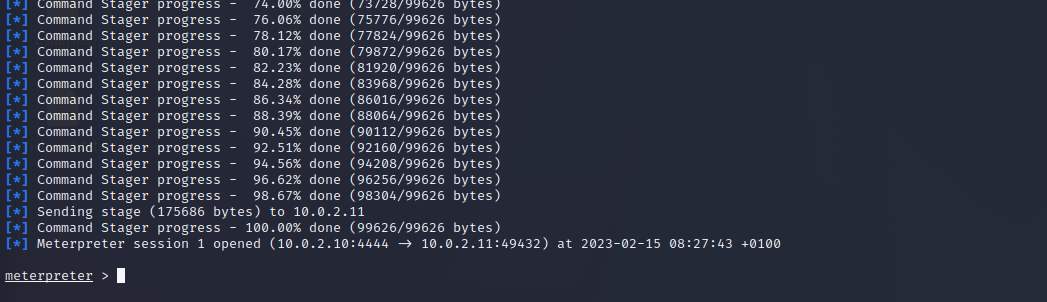


Configurarem el targeturi:

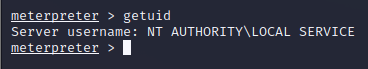


Executarem ara exploit.





### d. Des de Meterpreter per a saber quins permisos d’usuari tens, executa —> getuid

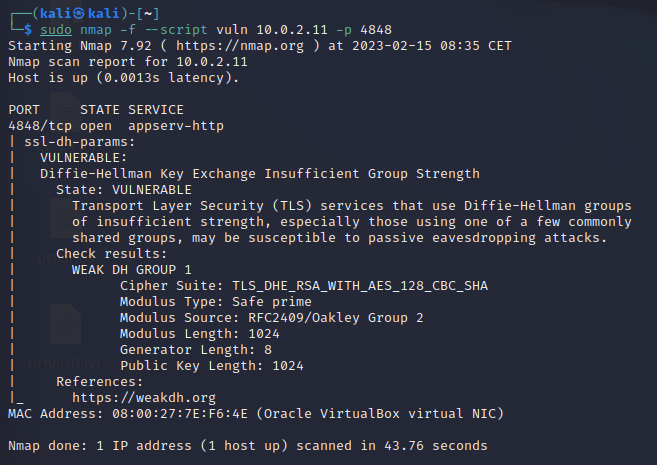


# Exercici 3 – Explotació de GlassFish per força bruta

### a. Busca què és i per a què serveix el servei de GlassFish que incorpora la màquina Metasploitable 3

GlassFish és un servidor d'aplicacions de programari lliure desenvolupat per Sun Microsystems, companyia adquirida per Oracle Corporation, que implementa les tecnologies definides a la plataforma Java EE i permet executar aplicacions que segueixen aquesta especificació. És gratuït, de codi lliure i es distribueix sota un llicenciament dual a través de la llicència CDDL i la GNU GPL. La versió comercial és denominada Oracle GlassFish Enterprise Server (abans Sun GlassFish Enterprise Server).

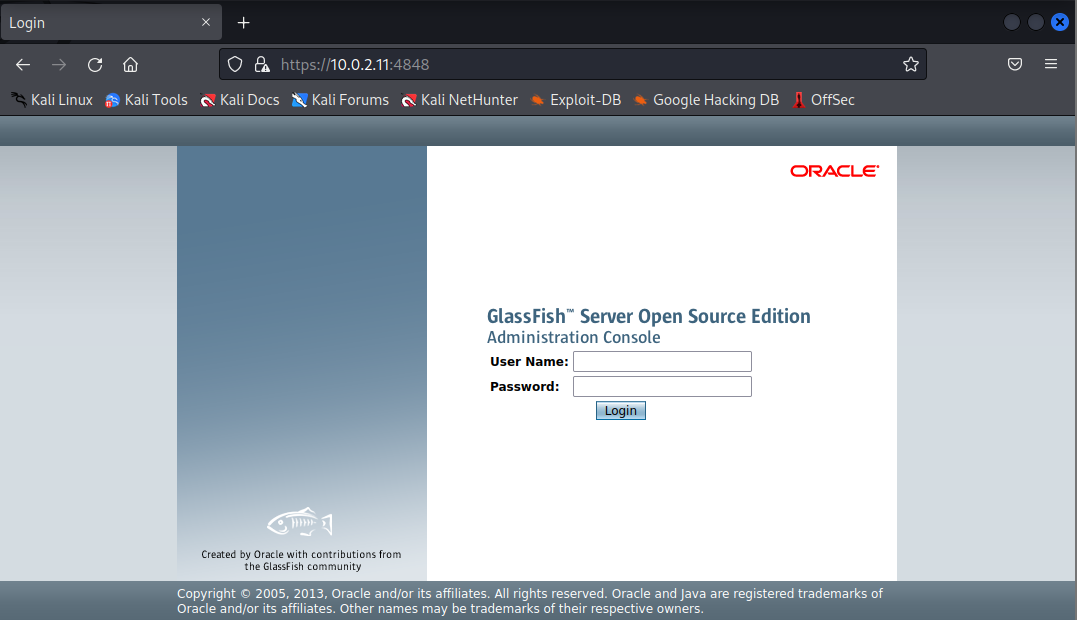
### b. Fes un nmap executant l’script vuln i comprova quina informació extreus del port 4848



Observem que el port 4848 esta obert.

### c. Des del navegador web de Kali Linux, mostra la plana web inicial de GlassFish que pots trobar pel port 4848 de Metasploitable 3

Posarem la ip i el port al navegador:



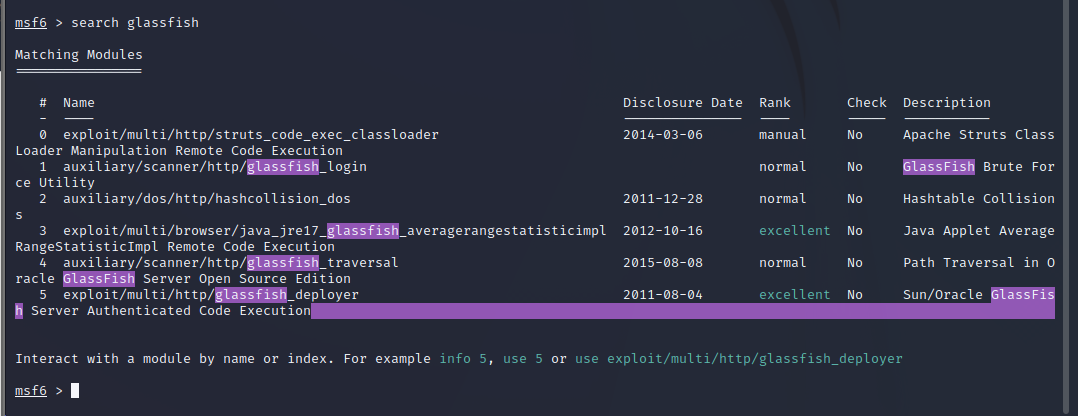
### 

### d. Utilitzant Metasploit busca algún auxiliary per a fer un atac de força bruta al servidor GlassFish.

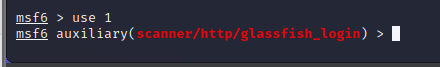
Seguidament obrirem la consola:



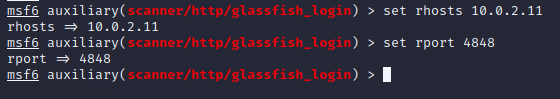
Buscarem el GlassFish:



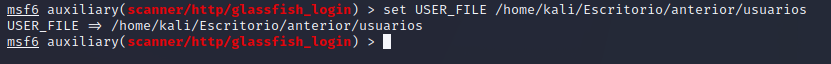
Farem servir la opció 1:



Ficarem el port i el host:

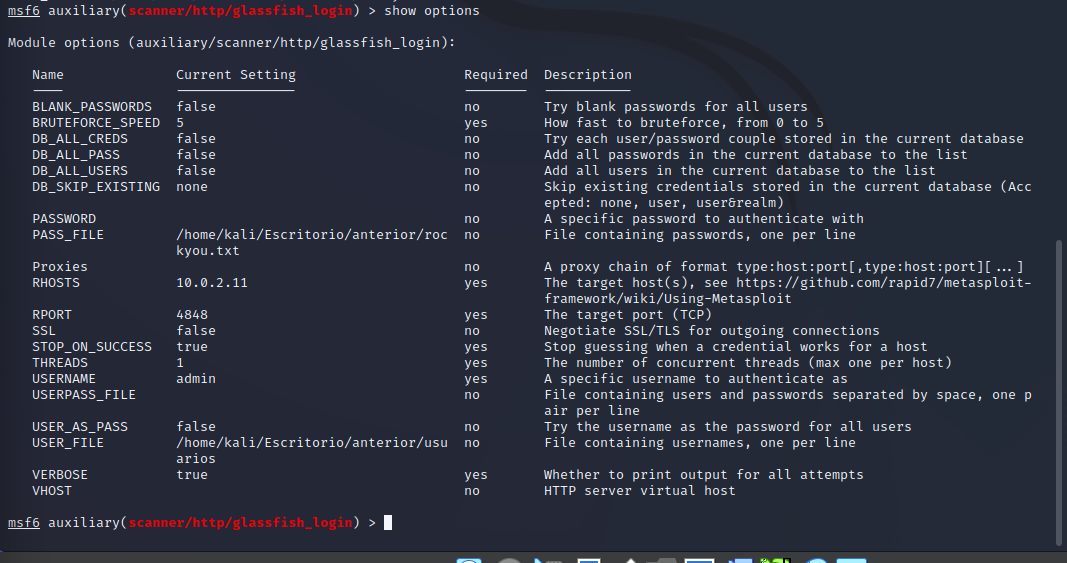


Posarem el document de usuaris i el del diccionari:

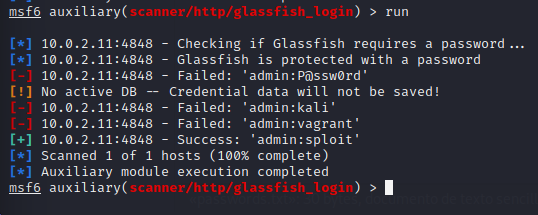




Farem un show options:

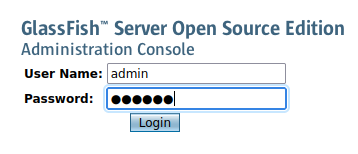


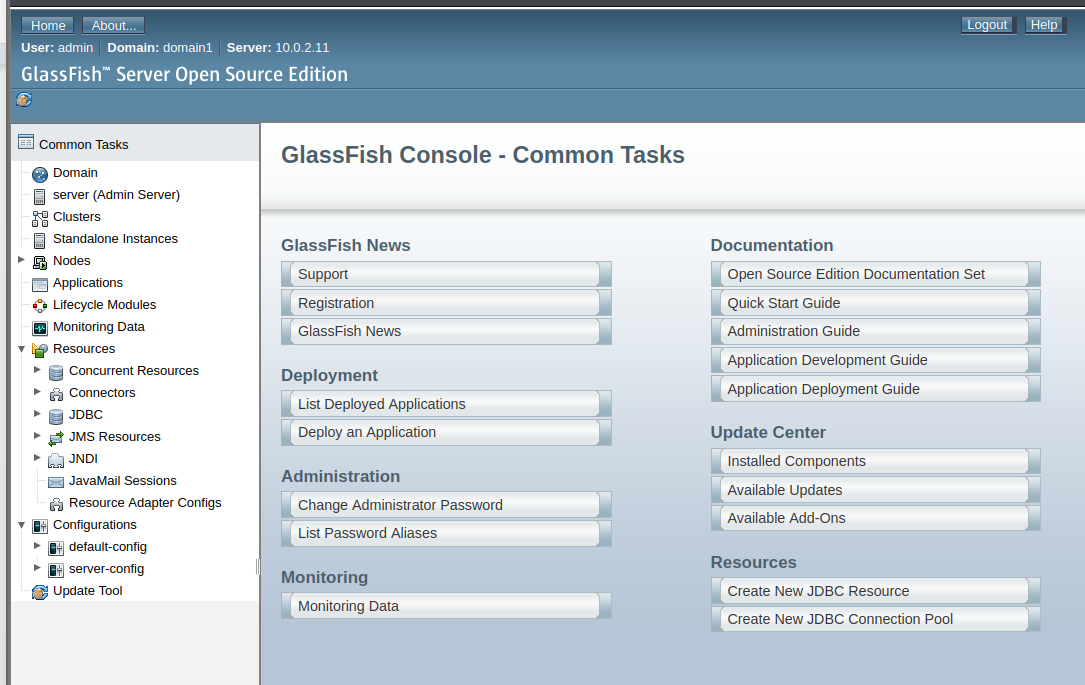
Farem un run:



Podem veure que ens ha trobat la password del admin que es sploit.

Per acabar de comprovar, tornarem a la plana web de GlassFish i posarem de user name admin i de password sploit





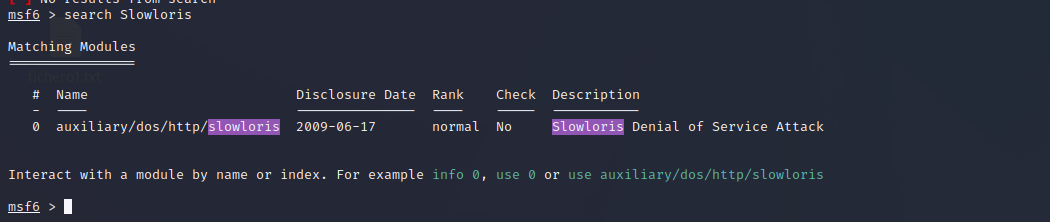
La password es correcte.

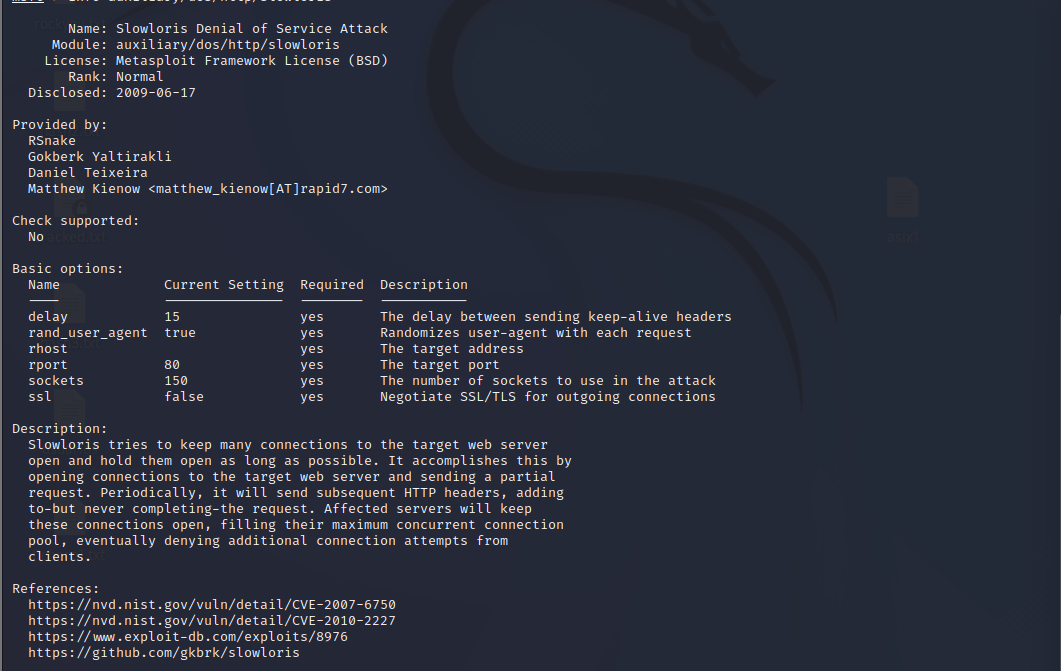
# Exercici 4 – Explotació vulnerabilitat Slowloris

### a. Què és un atac de DoS?

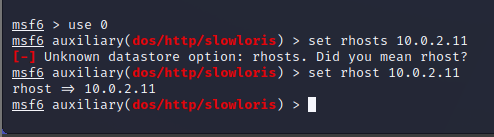
Un atac de Dos és un tipus de ciberatac que intenta fer que un lloc web o recurs de xarxa no estigui disponible col·lapsant-lo amb trànsit malintencionat perquè no pugui funcionar correctament.

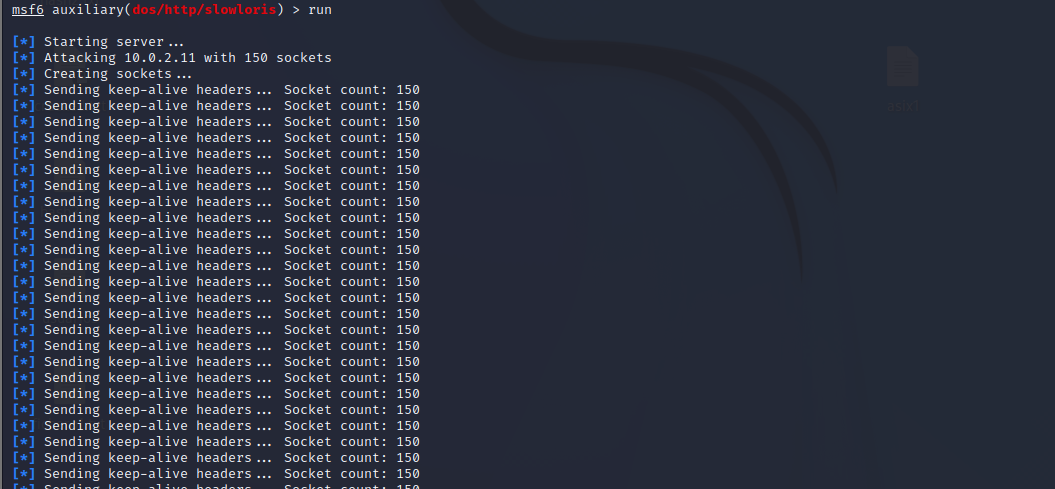
### b. Busca què és la vulnerabilitat Slowloris



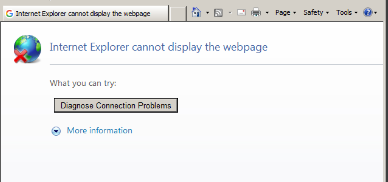


### c. Prova d’explotar-la sabent que és CVE-2007-6750





Ara si mirem la màquina metasploitable i posem internet, veurem que no tenim accés:



Per tornar a tenir internet farem control + c:

