

Máquina Build (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 04 octubre



Comenzamos con averiguar la dirección IP de la Máquina Víctima, para ello primeramente utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

```
$ netdiscover -i eth1 -r 10.0.2.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:ae:b4:76	1	60	PCS Systemtechnik GmbH
10.0.2.19	08:00:27:76:b2:53	2	120	PCS Systemtechnik GmbH

- Kali (Máquina Atacante): 10.0.2.4
- Máquina Víctima: 10.0.2.19

Comprobamos si tenemos conexión con la Máquina Víctima, para ello ejecutamos el siguiente comando:

```
$ ping -c 1 10.0.2.19
```

```
PING 10.0.2.19 (10.0.2.19) 56(84) bytes of data:
64 bytes from 10.0.2.19: icmp_seq=1 ttl=128 time=1.25 ms

— 10.0.2.19 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.252/1.252/1.252/0.000 ms
```

Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Windows**.

A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

\$ nmap -Pn 10.0.2.19 -sVC

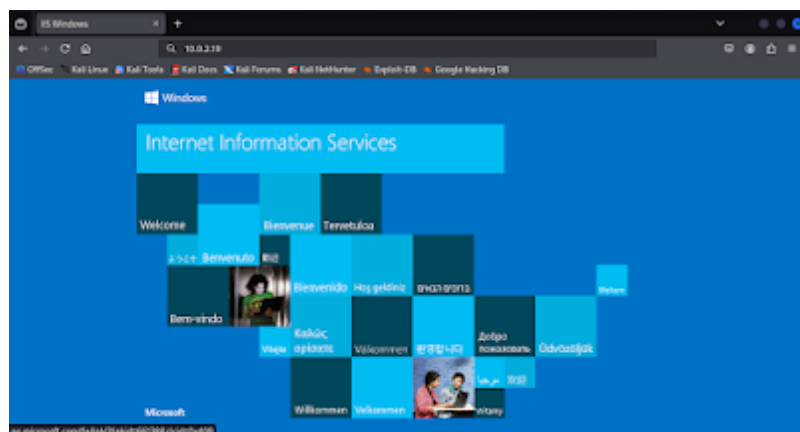
```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-21 15:59 CEST
Nmap scan report for 10.0.2.19
Host is up (0.0000s latency).
Not shown: 995 closed tcp ports (reset)
Host: 10.0.2.19
80/tcp open http Microsoft IIS httpd 30.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
8080/tcp open http Jetty 12.0.39
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-server-header: Jetty/12.0.39
MAC Address: 08:00:27:76:B2:53 (PCS Systemtechnik/Oracle VM VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ hostinfo: NetBIOS name: BUIDL, NetBIOS user: unknown, NetBIOS MAC: 08:00:27:76:B2:53 (PCS Systemtechnik/Oracle VM VirtualBox virtual NIC)
|_ clock-slow: 859009s
|_ smb2-security-mode:
|_ 3.1.1
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2025-08-21T23:00:00
|_ start-date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
```

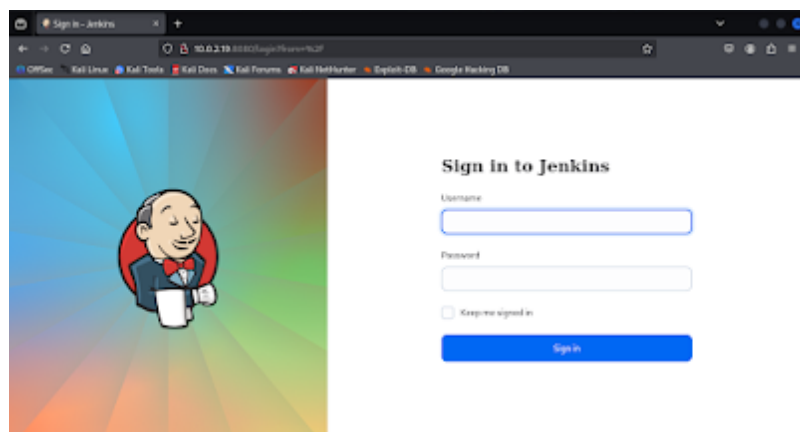
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **80**, **135**, **139**, **445** y **8080**.

Comprobamos que es lo que corre por el puerto 80.



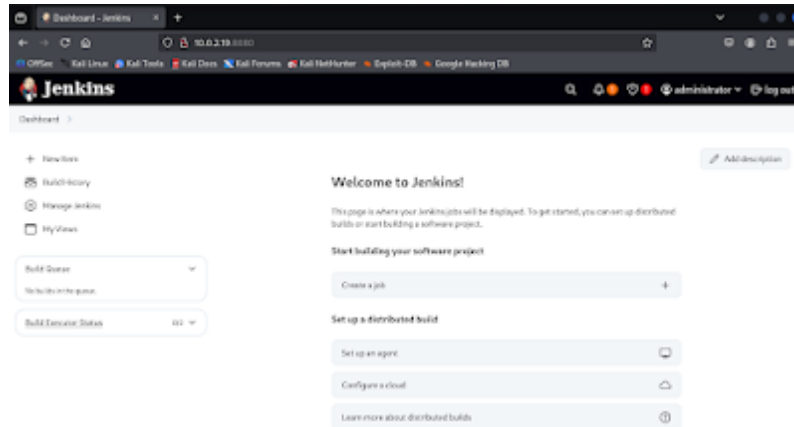
Nos encontramos con la pagina por defecto del servicio **IIS**, si realizamos con la herramienta **gobuster** un fuzzing web, no encontramos nada.

Comprobamos que es lo que corre por el puerto 8080.

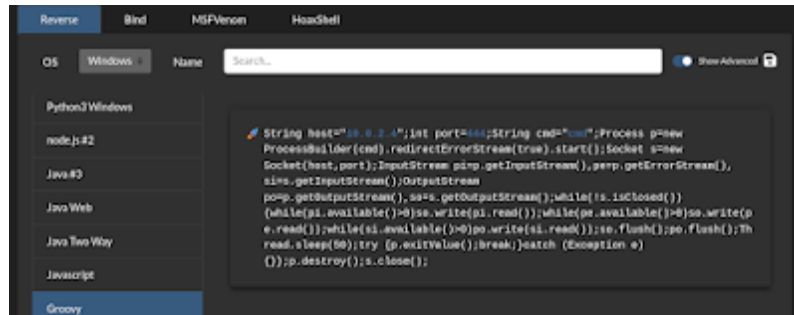


Nos encontramos con un panel de login de un **Jenkins**.

Probamos diferentes contraseñas por defecto, siendo posible acceder con las credenciales **admin:admin**.



Investigando un poco en [hacktricks cloud](#) nos encontramos con que podemos obtener **RCE** ejecutando un *script* en **Groovy**, siendo este más sigiloso que crear un nuevo proyecto, por lo tanto, nos creamos una reverse shell en Groovy.

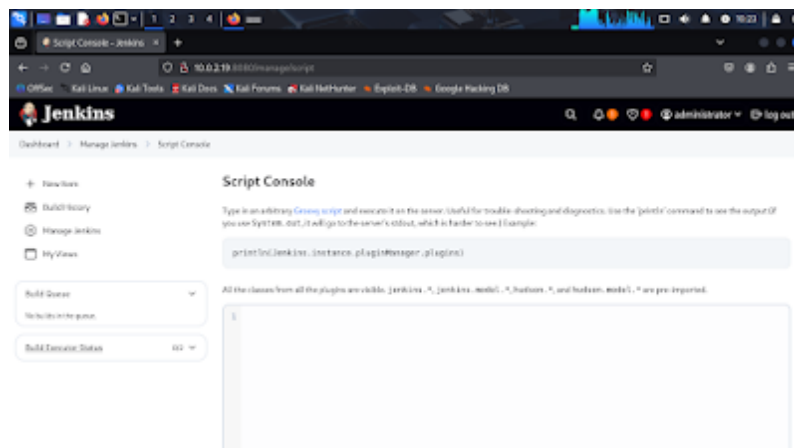


En nuestra Máquina Atacante con la ayuda de la herramienta **netcat (nc)** nos ponemos a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

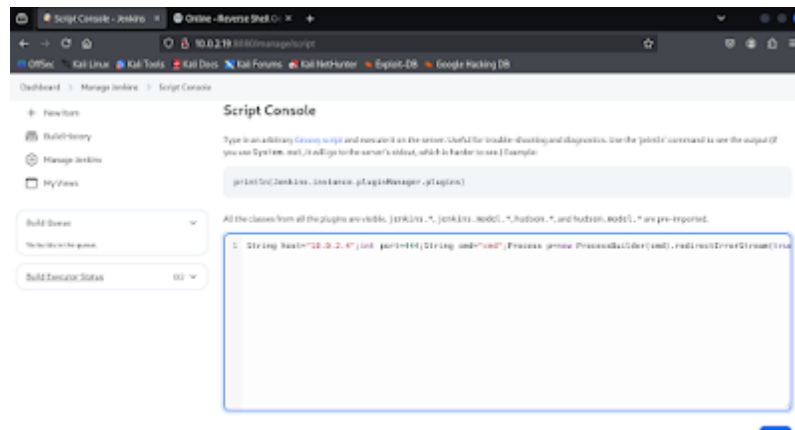
```
$ nc -lvp 444
```

```
listening on [any] 444 ...
```

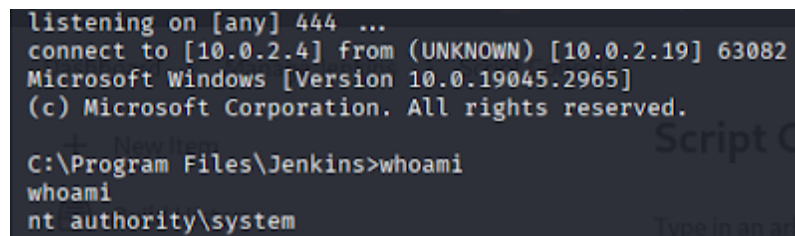
En el Jenkins nos dirigimos a *Manage Jenkins > Script Console*.



Pegamos nuestra reverse shell y pulsamos *Run*.



Y recibimos la conexión como ¡¡¡Administrador!!!.



También pudiendo leer las flags de **user** y **root**.