|  |  |
| --- | --- |
| Practical Manual | Sep 2, 2025 |

**Practical Manual – Cyber Security & Networking Commands**



|  |  |
| --- | --- |
| information | |
| **Name** | Barad Vishal |
| **Roll Number** | C05 |
| **Subject** | Ethical Hacking |
| **Faculty Name** | Prof. Khushali Vala |

Executive Summary

**The manual covers 14 practicals, beginning with basic command-line operations and progressively advancing toward real-world security analysis tools. Each practical includes aim, theory, commands with examples, execution steps, and output verification. The structured approach enables learners to not only understand the syntax of commands but also apply them in network troubleshooting, vulnerability assessment, and ethical hacking scenarios.**

Highlights

Key Highlights of the Manual:

* **Practical 1 – 2: Basic system and networking commands in Windows CMD and Kali Linux.**
* **Practical 3 – 5: Google Dorking and OSINT framework for passive information gathering.**
* **Practical 6 – 8: Active information gathering using Nslookup, Nmap, TCPdump, and Malware Analysis.**
* **Practical 9 – 12: Phishing simulations and exploitation tools (Zphisher, Camphish, Mitaka).**
* **Practical 13 – 14: Web server vulnerability scanning using Nikto and additional security testing tools.**

Subject Name: Ethical Hacking                                                                                       Subject Code: 150123705



**Integrated Master of Computer Applications**

**7th Semester**

Subject Name: Ethical Hacking

Subject Code: 150123705

Submitted To: Prof. Khushali Vala

Submitted By: Barad Vishal MahipatSinh(22003501210005)

Subject Name: Ethical Hacking                                                                                        Subject Code: 150123705

**CERTIFICATE**

*This is to certify that Mr .****Vishalsinh Mahipalsinh Barad*** *with enrollment number* ***22003501210005*** *Semester 7th has successfully completed his/her laboratory experiments in the* ***Ethical Hacking******(150123705)*** *from the department of* ***IMCA*** *during the academic year* ***2025 – 2027.***

*Date of Submission : 06-09-2025*

Staff in charge: Prof. Khushali Vala

Table of Contents

Subject Name: Ethical Hacking Subject Code: 150123705

Here’s a **professional Table of Contents (ToC)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Practical Title** | **Page No.** | **Sing** |
| **1** | **Perform basic commands in Windows Command Prompt (CMD)** | **9** |  |
| **2** | **Perform basic Linux commands** | **24** |  |
| **3** | **Perform Google Dorking for advanced web search** | **36** |  |
| **4** | **Gather information of a Domain using OSINT (Passive Information Gathering)** | **49** |  |
| **5** | **Gather information of an IP & Username using OSINT** | **53** |  |
| **6** | **Perform Active Information Gathering (Nslookup, Host, Nmap, TCPdump)** | **57** |  |
| **7** | **Gather & Analyze Email Information using OSINT** | **62** |  |
| **8** | **Perform Malware Analysis using OSINT** | **64** |  |
| **9** | **Create & Test a Simulated Phishing Email using Zphisher** | **66** |  |
| **10** | **Use Mitaka tool for Link, Email ID & Information Analysis** | **69** |  |
| **11** | **Create a Worm in C language to demonstrate self-replication** | **72** |  |
| **12** | **Use CamPhish tool to exploit a mobile device** | **75** |  |
| **13** | **Demonstrate Dictionary Attack using John the Ripper in Kali Linux** | **77** |  |
| **14** | **Perform Web Server Vulnerability Scan using Nikto** | **79** |  |
| **15** | **Utilize functionalities of Symmetric Key Cryptography Algorithms using Cryptii** | **83** |  |
| **16** | **Utilize functionalities of Asymmetric Key Cryptography Algorithms using AnyCrypt** | **86** |  |

Practical – 1

**Windows Command Prompt – Basic Commands**

Aim :- To perform basic commands in the Windows Command Prompt (CMD).

**Theory**

The Windows Command Prompt (CMD) is a command-line interpreter that allows users to interact with the operating system using text-based commands. It is widely used for system administration, file management, and network troubleshooting.

|  |  |  |
| --- | --- | --- |
| **Command** | **Description** | **Example** |
| systeminfo | Displays detailed system configuration. | systeminfo |
| ping | Tests network connectivity with a target host. | ping google.com |
| dir | Lists files and directories in the current directory. | dir C:\Users |
| cd | Changes the current working directory. | cd Documents |
| copy | Copies files from one location to another. | copy file1.txt D:\ |
| mkdir | Creates a new directory. | mkdir Project |
| move | Moves files from one location to another. | move file.txt D:\ |
| echo | Displays a message. | echo Hello World |
| find | Searches for a text string in a file. | find "test" file.txt |
| tasklist | Displays a list of currently running processes. | tasklist |
| taskkill | Terminates tasks by image name or PID. | taskkill /IM notepad.exe |
| ipconfig | Displays IP address, subnet mask, and gateway. | ipconfig /all |
| help | Displays available commands or help for a command. | help ping |
| shutdown | Shuts down or restarts the computer. | shutdown /r /t 0 |

**Command 1: Systeminfo**

**Detail:** Displays detailed system configuration.

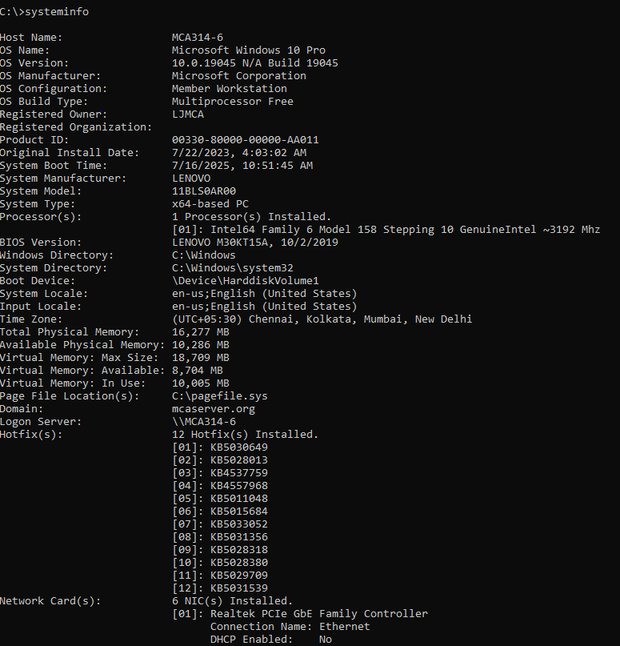
**Procedure**:

1. Open Command Prompt (Win + R → cmd → Enter).
2. Type the command:



3.Press **Enter**.

**Screenshot**:



**Output:**   
 Displays OS details, system manufacturer, system model, BIOS version, network configuration, etc.

**Command 2 : Ping (Packet Internet Groper)**

**Detail:** Sends packets to test network connectivity.

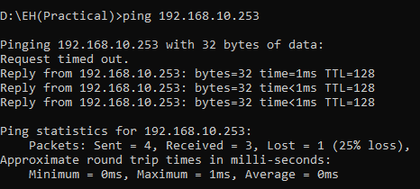
**Procedure**:

1. Open Command Prompt (Win + R → cmd → Enter).
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 Shows reply from the server with time (ms) and TTL, confirming network connectivity.

**Command 3: Dir (Directory)**

**Detail:** Lists files and directories in the current directory.

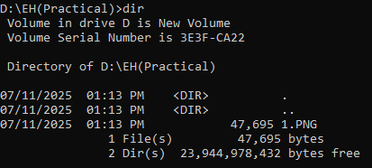
**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 Displays a list of files and subfolders in the current directory.

**Command 4: cd (Change Directory)**

**Detail:** Changes the current working directory.

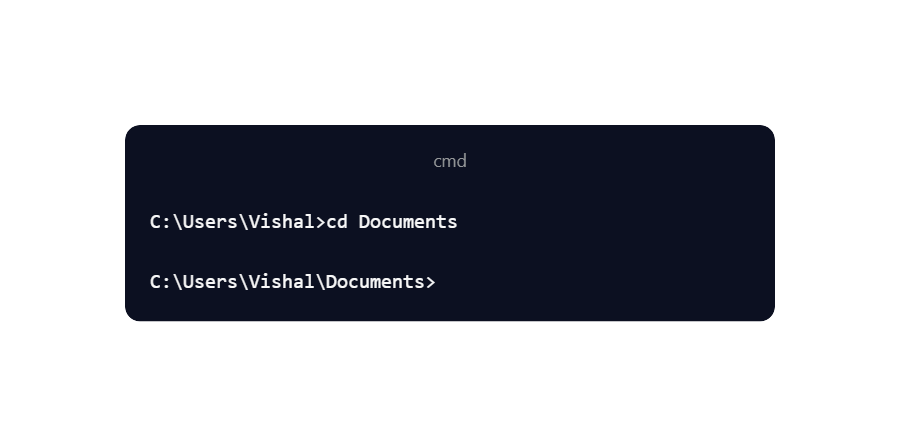
**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**The working directory changes to C:\Users\Vishal\Documents.**

**Command 5: Copy**

**Detail:** Copies files from one location to another.

**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**

543b6b21c150d39301e2455bfee5b3f8.png

**Output:**   
 The file file1.txt is copied successfully to the D:\Backup\ folder.

**Command 6: mkdir (Make Directory)**

**Detail:** Creates a new directory.

**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**  
 A new folder named Project is created in the current directory.

**Command 7: Move**

**Detail:** Moves files from one location to another.

**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**  
 The file file1.txt is moved from its original location to the D:\ directory.

**Command 8: Echo**

**Detail:** Displays a message.

**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 The text Hello, Welcome to CMD is displayed in the command prompt window.

**Command 9: Find**

**Detail:** Searches for a text string in a file.

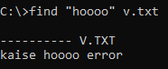
**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 Displays the lines in file1.txt containing the word "keyword".

**Command 10: Tasklist**

**Detail:** Displays a list of currently running processes.

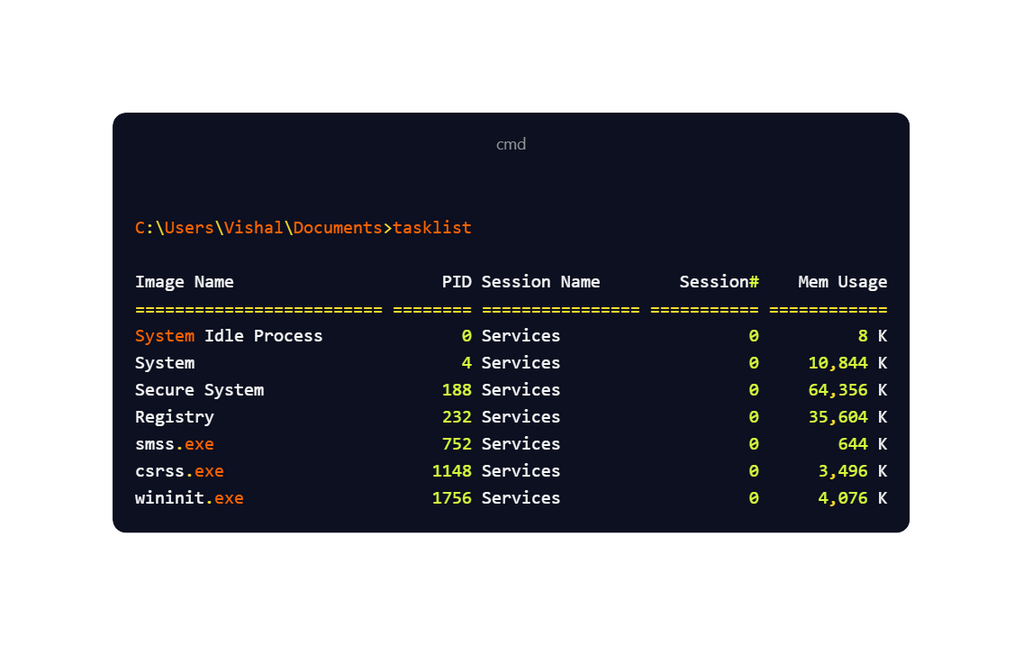
**Procedure:**

1. Open Command Prompt.
2. Type:



1. Press **Enter**.

**Screenshot:**



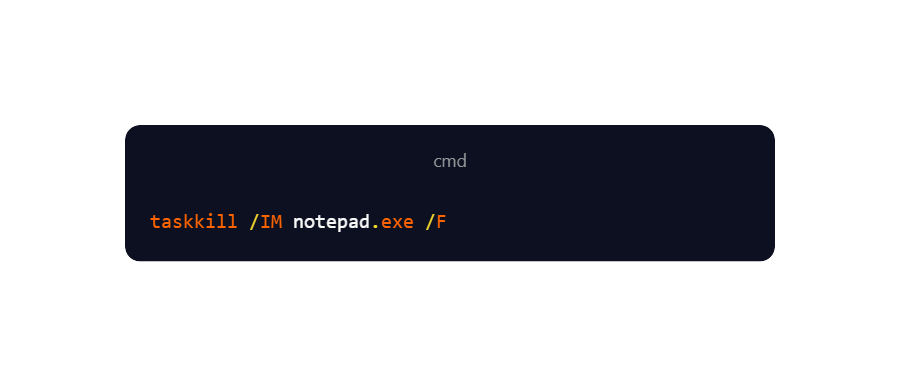
**Output:**  
 Displays all running processes with their PID, memory usage, and status.

**Command 11: Taskkill**

**Detail:** Terminates tasks by image name or process ID (PID).

**Procedure:**

1. Open Command Prompt.
2. To close **Notepad**, type:



1. Press **Enter**.

**Screenshot:**



**Output:**  
 The process notepad.exe is forcefully terminated.

**Command 12: Ipconfig (Internet Protocol Configuration)**

**Detail:** Displays IP address, subnet mask, and gateway.

**Procedure:**

1. Open Command Prompt.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**  
Shows details of the system’s network configuration including IPv4, IPv6, Subnet Mask, and Default Gateway.

**Command 13: Help**

**Detail:** Displays a list of available commands or help for a specific command.

**Procedure:**

1. Open Command Prompt.
2. Type



3.Press **Enter**.

**Screenshot:** 



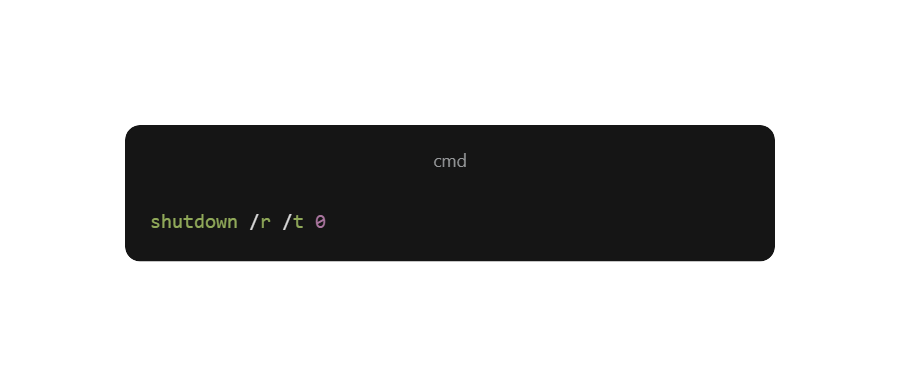
**Output:**   
 Lists all available commands with a short description. When used with a command name (e.g., help dir), it shows detailed usage of that command.

**Command 14: Shutdown**

**Detail:** Shuts down or restarts the computer.

**Procedure:**

1. Open Command Prompt.
2. To restart the computer immediately, type:



Press **Enter**.

**Screenshot:**  


**Output:**   
 The system shuts down or restarts based on the parameters provided.

**Conclusion :** By performing basic commands, we understood how to navigate, manage files, check system details, and perform network operations in Windows, which built a foundation for administrative tasks and troubleshooting.

Practical – 2

**Kali Linux – Basic Commands**

**Aim :**To perform and understand basic Linux commands for file system management and networking in Kali Linux.

**Theory**

Linux (Kali) is a command-line based operating system widely used in cyber security, ethical hacking, and system administration. Learning essential Linux commands is important for navigating directories, managing files, configuring networks, and performing administrative tasks.

**Command 1: ls (List)**

**Detail:** Displays files and folders in the current directory.

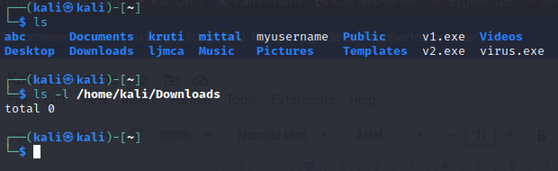
**Procedure:**

1. Open Kali Linux Terminal.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 Shows the list of files and directories in the current working directory.

**Command 2: cd (Change Directory)**

**Detail:** Moves to a different folder in the file system.

**Procedure:**

1. Open Terminal.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 The working directory changes to the Documents folder. 

**Command 3: ifconfig / ip a**

**Detail:** Displays IP address and network settings.   
 👉 If ifconfig doesn’t work, use ip a.

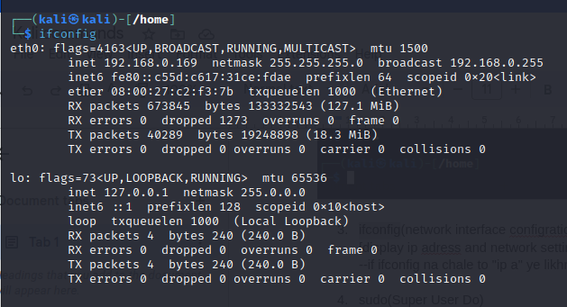
**Procedure:**

1. Open Terminal.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 Displays details of network interfaces including IP, MAC, and broadcast addresses.

**Command 4: sudo (Super User Do)**

**Detail:** Runs commands with administrative (root) privileges.

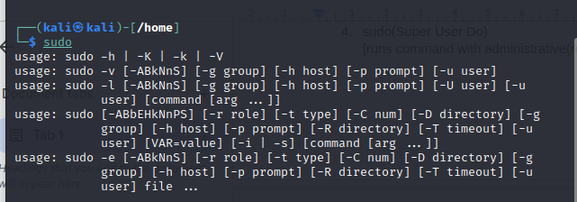
**Procedure:**

1. Open Terminal.
2. Type:



3.Press **Enter**, provide password if asked.

**Screenshot:** 



**Output:**   
 The command runs with root permissions and updates package lists.

**Command 5: mkdir (Make Directory)**

**Detail:** Creates a new folder.

#“mkdir -p path/foldername”

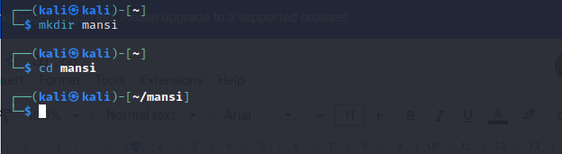
**Procedure:**

1. Open Terminal.
2. Type:



3.Press **Enter**.

**Screenshot:**



**Output:**   
 A new folder named Projects is created.

**Command 6: pwd (Print Working Directory)**

**Detail:** Displays the full path of the current directory.

**Procedure:**



**Screenshot:**

41135c7130196c204dd1f1f4fcb2d677.png

**Output:**   
 Shows the absolute path (e.g., `/home/user)

**Command 7: rmdir (Remove Empty Directory)**

**Detail:** Deletes an empty directory.

**Procedure:**



**Screenshot:**



**Output:**   
 Removes the directory OldFolder if it is empty.

**Command 8: rm (Remove File/Directory)**

**Detail:** Deletes files and directories.

**Procedure:**



**Screenshot:**

73550083007cc48ea69ff867efbd4483.png

**Output:**   
 Deletes the specified file or folder.

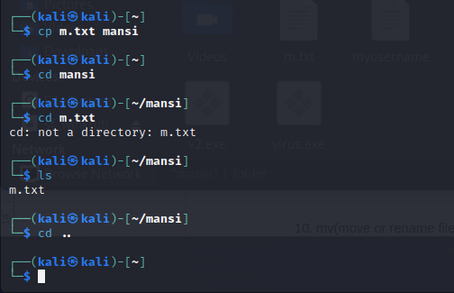
**Command 9: cp (Copy Files and Folders)**

**Detail:** Copies files and directories.

**Procedure:**



**Screenshot:**



**Output:**   
 Copies the file/folder to the target directory.

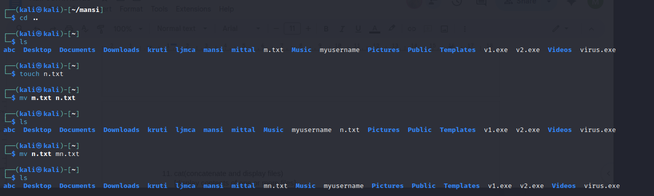
**Command 10: mv (Move / Rename Files)**

**Detail:** Moves or renames files and directories.

**Procedure:**



**Screenshot:**



**Output:**   
 File is either renamed or moved to a new location.

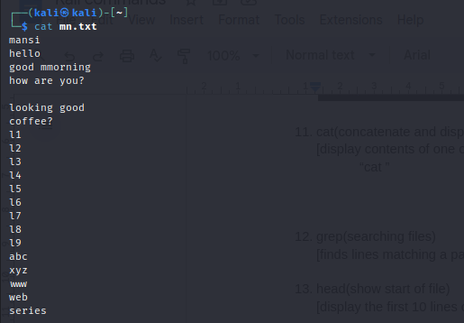
**Command 11: cat (Concatenate and Display)**

**Detail:** Displays contents of one or more files.

**Procedure:**



**Screenshot:**



**Output:**   
 Shows the content of file.txt.

**Command 12: grep (Search Inside Files)**

**Detail:** Finds lines matching a pattern or keyword.

**Procedure:**



**Screenshot:**

428b0540e98ff29b26d22215727e2bb6.png

**Output:**   
 Displays lines containing the word "keyword".

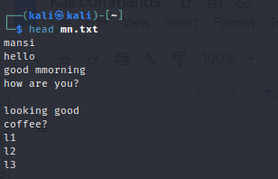
**Command 13: head (Show Start of File)**

**Detail:** Displays the first 10 lines of a file.

**Procedure:**



**Screenshot:**



**Output:**   
 Shows the top 10 lines of file.txt.

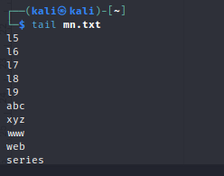
**Command 14: tail (Show End of File)**

**Detail:** Displays the last 10 lines of a file.

**Procedure:**



**Screenshot:**



**Output:**   
 Shows the last 10 lines of file.txt.

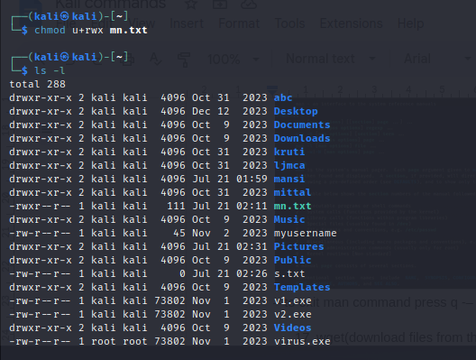
**Command 15: chmod (Change Permissions)**

**Detail:** Modifies read, write, and execute permissions.

**Procedure:**



**Screenshot:**



**Output:**   
 Sets permissions: owner (rwx), group (rx), others (rx).

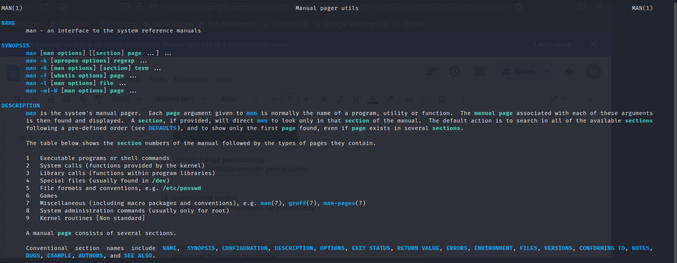
**Command 16: man (Manual Pages)**

**Detail:** Displays documentation/help for commands.

**Procedure:**



**Screenshot:**



**Output:**   
 Shows detailed documentation for the ls command.   
 👉 Press **q** to exit.

**Command 17: wget (Download Files)**

**Detail:** Downloads files from the internet.

**Procedure:**



**Screenshot:**



**Output:**   
 Downloads file.txt to the current directory.

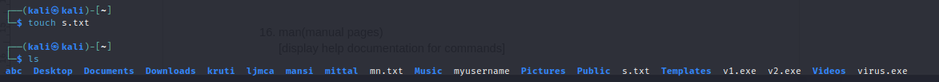
**Command 18: touch (Create Empty File / Update Timestamp)**

**Detail:** Creates a new empty file or updates the last modified time.

**Procedure:**



**Screenshot:**



**Output:**   
 Creates an empty file s.txt

Practical – 3

**Google Dorking – Advanced Web Search**

**Aim:** To perform **Google Dorking** for advanced web searches and information gathering using Google search operators.

**Theory**

Google Dorking is a technique that uses **advanced search operators** to find specific information that is not easily accessible through normal searches. Security researchers and ethical hackers use Google Dorks to identify sensitive information, misconfigured websites, login pages, exposed files, and more.

Google Dorking is powerful for **OSINT (Open-Source Intelligence)** and **ethical hacking** but must only be used for **legal and educational purposes**.

**Commands / Operators Used**

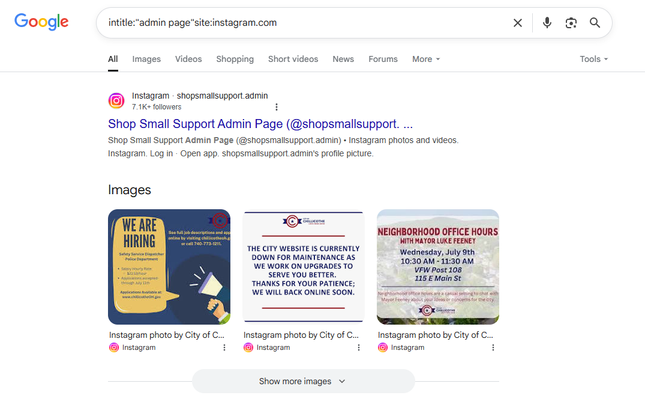
**Command 1: intitle**

**Detail:** Searches for pages that have a specific word in the title.

**Procedure:**

18a299219-6c80-42de-ab5f-8fd776cae7e4.png

**Screenshot:**



**Output:** Google shows results with the phrase *admin page* in the page title, limited to Instagram.

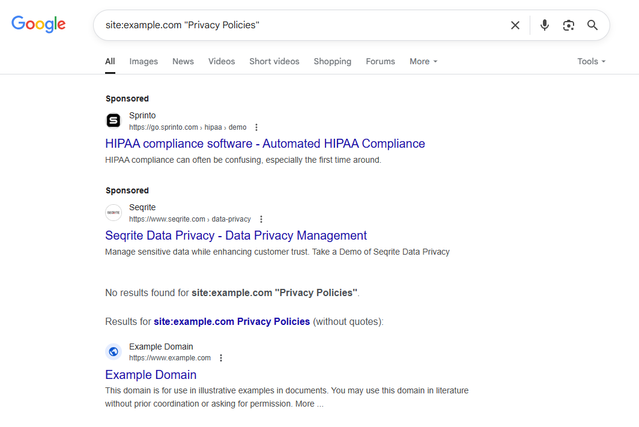
**Command 2: site**

**Detail:** Restricts search results to a specific domain or website.

**Procedure:**

15829e47d-8dd4-40ab-ae20-5aa1be4e6863.png

**Screenshot:**



**Output:**  
 Displays pages related to *Privacy Policy* within the domain *example.com*.

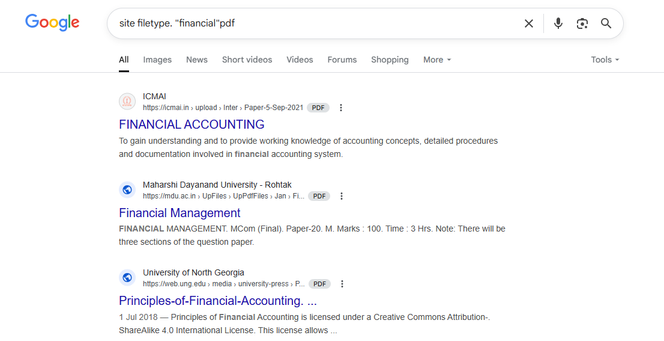
**Command 3: filetype**

**Detail:** Searches for a particular file type mentioned in the query.

**Procedure:**

1a75019dc-a5af-49e2-b160-fde9772ed89a.png

**Screenshot:**



**Output:**   
 Shows PDF files containing the phrase *cyber security notes*.

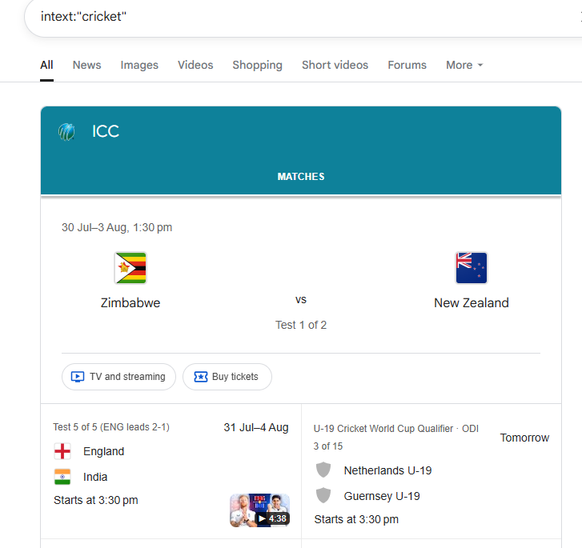
**Command 4: intext**

**Detail:** Searches for a word inside the page content (not just title/URL).

**Procedure:**

1577993fc-f535-4cda-b082-d2df4828561f.png

**Screenshot:**



**Output:**  
 Displays web pages containing the word *confidential* in their text content.

**Command 5: inurl**

**Detail:** Searches for a word inside the URL.

**Procedure:**

18e0ccf82-3ac9-4c02-8319-f459b79d25f5.png

**Screenshot:**



**Output:**   
 Lists URLs containing *login*, often pointing to login pages.

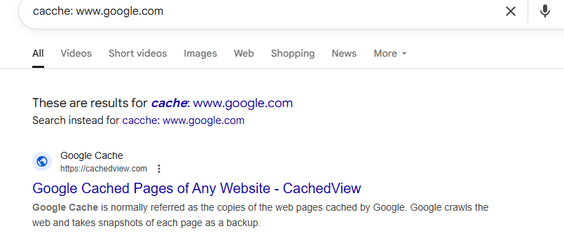
**Command 6: cache**

**Detail:** Displays the cached version of a web page stored by Google.

**Procedure:**

15d6479aa-86ed-43ed-9cda-6e455abfe698.png

**Screenshot:**



**Output:**   
 Shows Google’s cached copy of the website.

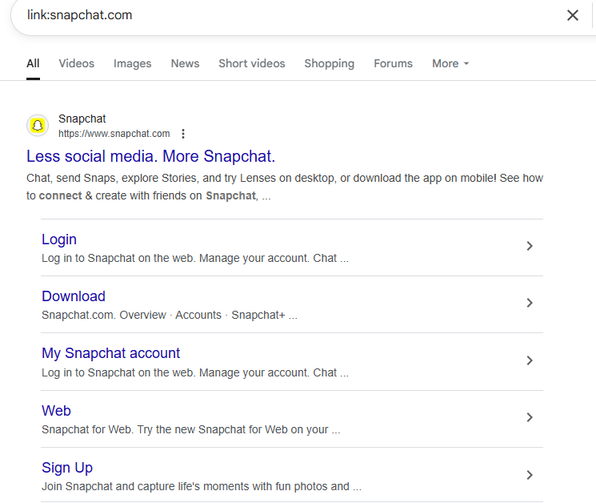
**Command 7: link**

**Detail:** Finds web pages that link to a specific site.

**Procedure:**

12d93e4b0-e626-437a-a4da-b579ef78cc09.png

**screenshot :**



**Output:**  
 Displays sites that have backlinks to *example.com*.

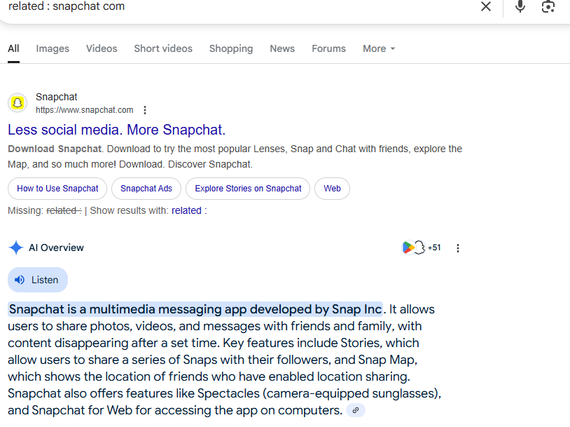
**Command 8: related**

**Detail:** Finds websites related to a given domain.

**Procedure:**

1717221a0-8e46-42f2-a14c-e472c14b9781.png

**screenshot :**



**Output:**   
 Shows websites related to YouTube (e.g., Vimeo, Dailymotion).

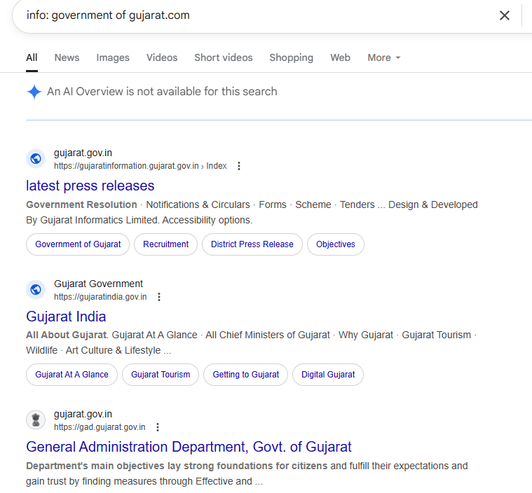
**Command 9: info**

**Detail:** Provides information about a site.

**Procedure:**

168c31f5a-443f-4fe4-b7d5-675b81bda84b.png

**screenshot :**



**Output:**   
 Shows Google’s summary info about *gujrat.com*.

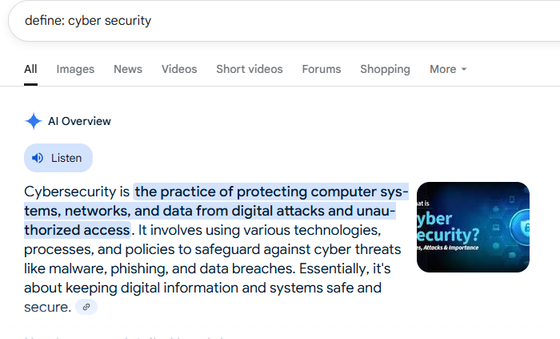
**Command 10: define**

**Detail:** Provides dictionary definitions of a term.

**Procedure:**

1a9a3682d-7774-4ec3-bb60-b5135098434d.png

**screenshot :**



**Output:**   
 Displays the definition of *cybersecurity*.

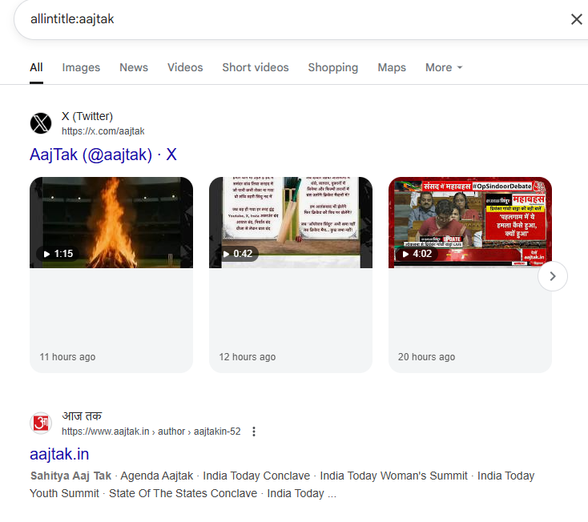
**Command 11: allintitle**

**Detail:** Searches for pages that have all specified words in the title.

**Procedure:**

17263ce9b-82b1-4b06-b10d-d44ea5cc0304.png

**screenshot :**



**Output:**   
 Displays results with both words (aajtak) in the page title.

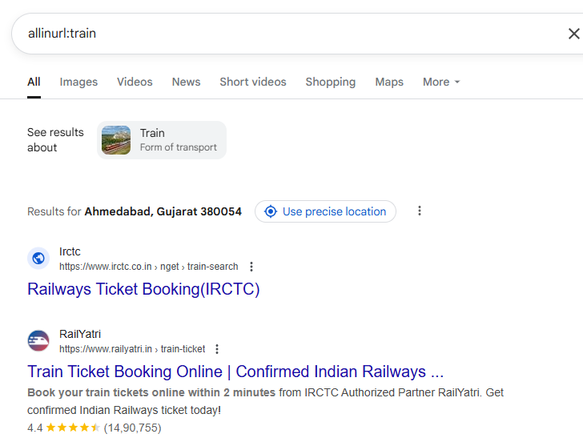
**Command 12: allinurl**

**Detail:** Searches for pages with all specified words in the URL.

**Procedure:**

13371a117-9a0b-409a-ae8e-159ad113c65b.png

**screenshot :**



**Output:**   
 Displays results with Trin in the URL.

**Conclusion**

We successfully used **Google Dorking operators** like *intitle, site, filetype, intext, inurl, cache, link, related, info, define, allintitle, allinurl*. These operators improve search efficiency, help discover hidden information,

Practical – 4

**OSINT Framework – Domain Information Gathering**

**Aim:** To gather information about an IP address and Username in order to understand **passive information gathering** using OSINT tools.

**Theory**

OSINT (Open-Source Intelligence) refers to the collection and analysis of information from publicly available sources. Using OSINT, cybersecurity professionals and ethical hackers can gather valuable insights about domains, websites, IPs, and organizations without directly interacting with the target (passive reconnaissance).

For domain analysis, tools such as **WHOIS lookup, PassiveDNS, and Wayback Machine** are commonly used. These tools provide details like **domain owner, registration date, DNS records, email IDs, phone numbers, and website archives**.

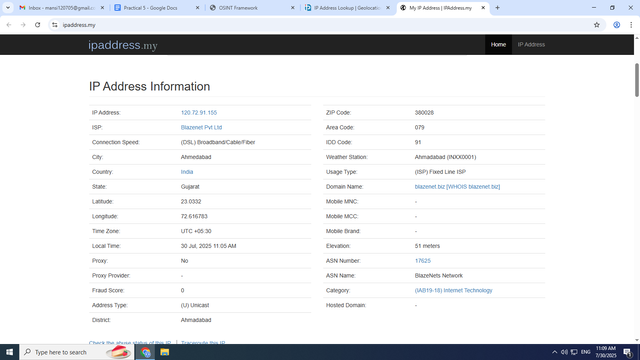
**Steps / Procedure**

**Part A – IP Information Analysis**

**1. Geolocation – My IP Address**

* Go to 👉 https://whatismyipaddress.com
* Enter target IP or view your own.

**Screenshot to Insert:** *(Result showing IP location on map)*

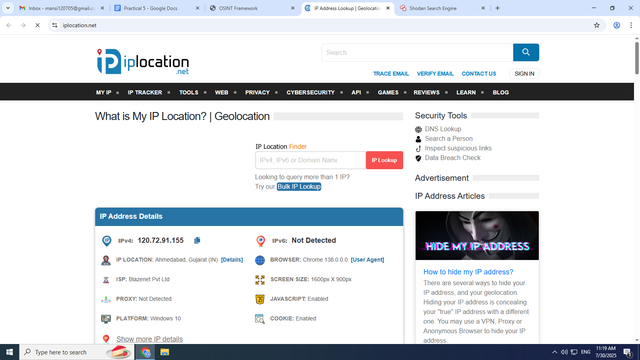


**Output:** Shows approximate geolocation (city, country, ISP).

**2. Geolocation – IP Location Finder**

* Visit 👉 https://iplocation.net
* Enter target IP.

**Screenshot to Insert:** *(Result page with location details)*

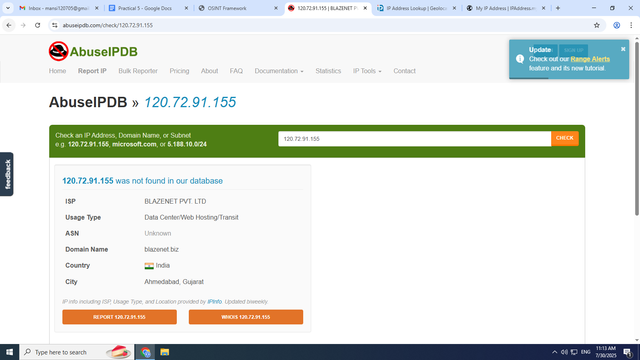


**Output:** Displays IP details with multiple geolocation database checks.

**3. Blacklists – AbuseIPDB**

* Visit 👉 https://www.abuseipdb.com
* Enter target IP.

**Screenshot to Insert:** *(Abuse report history of IP)*

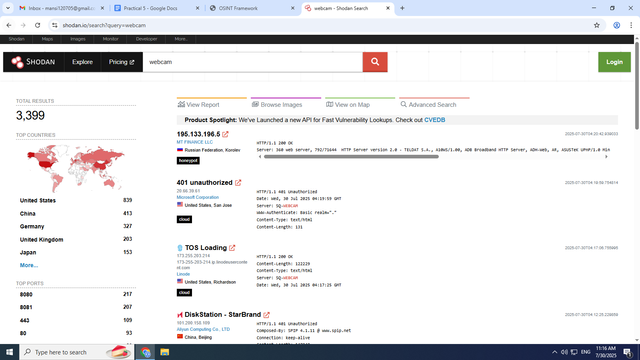


**Output:** Shows if IP is blacklisted or reported for abuse.

**4. Host / Port Discovery – Shodan**

* Visit 👉 https://www.shodan.io
* Search target IP.

**Screenshot to Insert:** *(Shodan search results with open ports/services)*

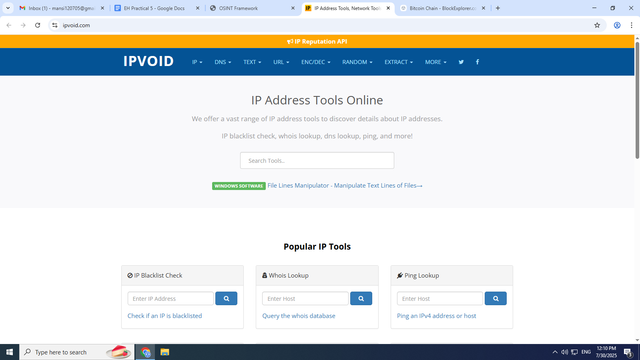


**Output:** Displays open ports, running services, and vulnerabilities of the IP.

**5. Reputation – IP Void**

* Visit 👉 https://www.ipvoid.com
* Enter target IP.

**Screenshot to Insert:** *(Reputation check result)*



**Output:** Shows security reputation of IP across various blacklists.

Practical – 5

**OSINT framework(IP & Username) [practical-5]**

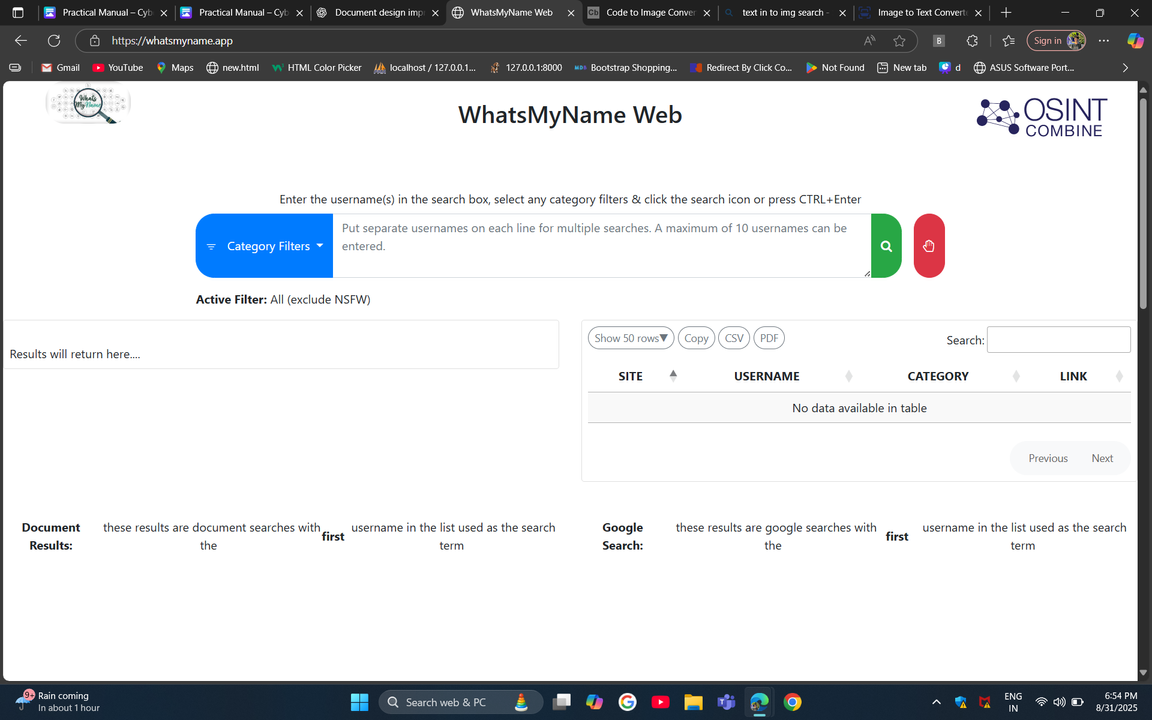
**AIM** :- Gather information of any IP & UserName in order to understand passive information gathering using OSINT

**Part B – Social Media Profiling (Username Analysis)**

**1. WhatsMyName Tool**

* Go to 👉 https://whatsmyname.app
* Enter username.

**Screenshot to Insert:** *(Result page showing platforms with matching username)*

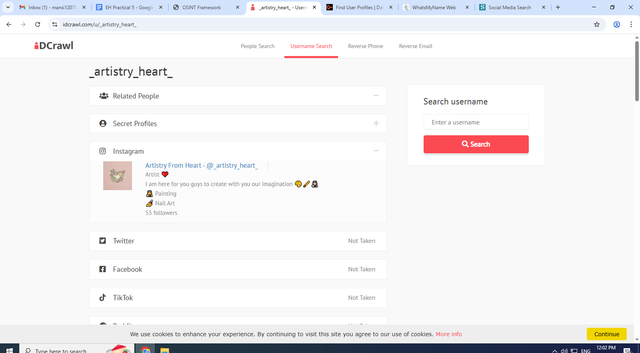


**Output:** Finds accounts associated with the username across multiple sites.

**2. IDCrawl Username Search**

* Visit 👉 https://idcrawl.com
* Enter username.

**Screenshot to Insert:** *(List of user profiles found)*



**Output:** Collects publicly available profiles, social links, and mentions.

**3. Social-Searcher**

* Go to 👉 [https://www.social-searcher.com](https://www.social-searcher.com/?utm_source=chatgpt.com)
* Enter username.

**Screenshot to Insert:** *(Dashboard showing mentions on social media)*



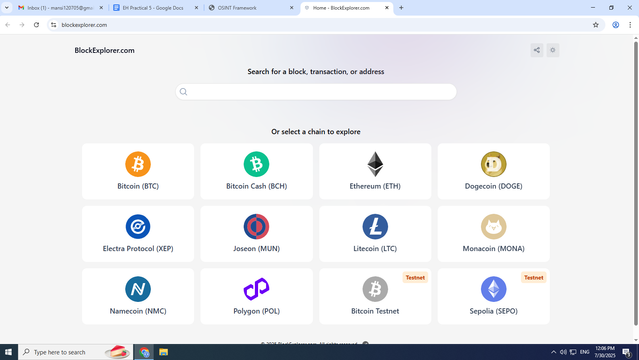
**Output:** Displays real-time mentions of username across social platforms.

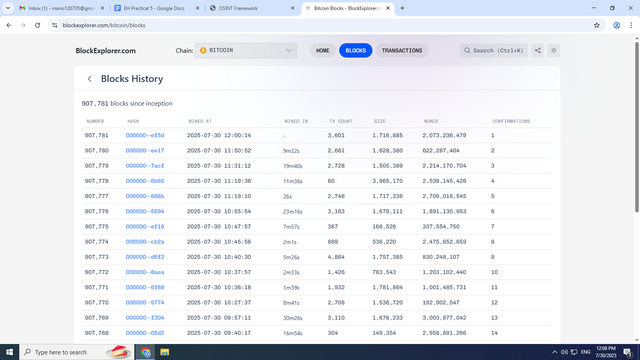
**Part C – Digital Currency Analysis**

**Bitcoin Block Explorer**

* Visit 👉 https://www.blockchain.com/explorer
* Enter Bitcoin wallet address.

**Screenshot to Insert:** *(Transaction history of the wallet)*





**Output:** Displays balance, transactions, and wallet history for given Bitcoin address.

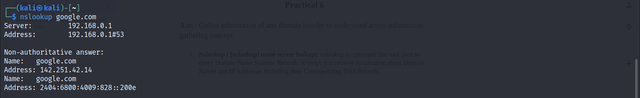
**Conclusion**

We successfully performed **IP and Username OSINT analysis** using tools like **MyIP, IP Location Finder, AbuseIPDB, Shodan, and IPVoid** for IPs, and **WhatsMyName, IDCrawl, Social-Searcher** for usernames. Additionally, we used a **Bitcoin Block Explorer** to analyze digital currency transactions. These OSINT tools are useful for cybersecurity investigations, threat intelligence, and social media profiling.

Practical – 6

**AIM**: Gather information of any domain in order to understand the active information gathering concept.

**1.Nslookup ( [nslookup] name server lookup)**: nslookup is a command line tool used to query Domain Name Systems Records. It Helps you retrieve information about Domain Names and IP Addresses Including their Corresponding DNS Records



**2 .Host (written as host)** : The **host** command is a DNS lookup utility used to query domain name information like IP addresses and DNS records from the command line.

f158110cfc9caeb2119992af4ecffd25.png

**3. Nmap (written in cmd as nmap)**: Nmap is a powerful open-source tool used for network discovery and security auditing by scanning hosts and services on a computer network.

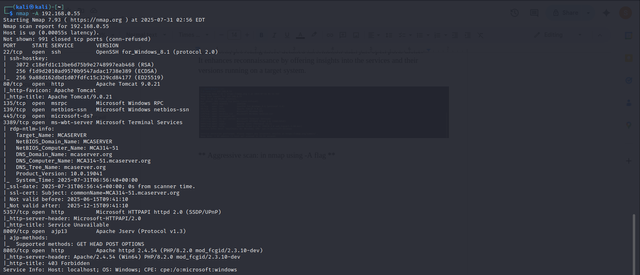


* Using -sV(Service Version) Flag

The **nmap -sV** flag enables version detection in Nmap. This means that Nmap will attempt to identify the specific software and versions running on open ports, providing more detailed information than just open ports alone. It enhances reconnaissance by offering insights into the services and their versions running on a target system.



* Aggressive scan: in nmapusing -A flag



* Scan Multiple Hosts

* **TCP :** This performs a **default TCP scan** on the target IP.It scans the most common 1000 TCP ports to check which are open.

nmap <target\_ip>

* **Syn scan :** Sends SYN packets to ports but doesn’t complete the TCP handshake.Faster and less likely to be logged by the target system’s firewall.Useful for stealthy scanning.

nmap -sS <target\_ip>

* **Tcp connect scan :** This performs a full TCP handshake (connect system call).Slower and noisier compared to SYN scan.Used when you don’t have raw packet privileges.

nmap -sT <target\_ip> # -smeans scan and **T** means which service we need

* **Specific port**

nmap -p 80,443,25 <target\_ip> #http,https,smtp

* **All port**

nmap -p -<target\_ip>

* **Service version**

nmap -sV <target\_ip>

* **Aggressive Scan**

nmap -A <target\_ip>

* **Range**

nmap -p 10-100 <target\_ip>

* **UDP**

nmap -pU 80 <target\_ip>

**TCP DUMP**

**Meaning :** TCP is a powerful command line tool for capturing and analyzing network traffic. It allows you to see the buckets travelling over your network interface in real time,which can be incredibly useful for network troubleshooting , performance monitoring and security analysis.

**Commands :**

* **TCP port specific**

tcpdump port 22,23

tcpdump smtp,ftp,icmp,http

* **Host and Hosting check**

tcpdump host <target\_ip>

* **Checking the source file where travel**

tcpdump src <target\_ip> # source

tcpdump dst <target\_ip> #destination

* **Ethernet specific port**

tcpdump -i eth0 port 80

**Conclusion :** This experiment demonstrated active reconnaissance techniques such as port scanning, DNS queries, and packet capturing, which provided practical exposure to real-world penetration testing methodologies.

Practical – 7

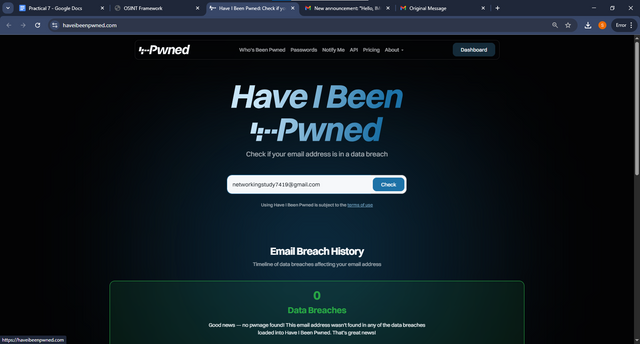
**AIM :** Gather and Analyze Email Information Using OSINT in Order to understand the E-mail Architecture and Working.

**SPF(Sender Policy Framework)**

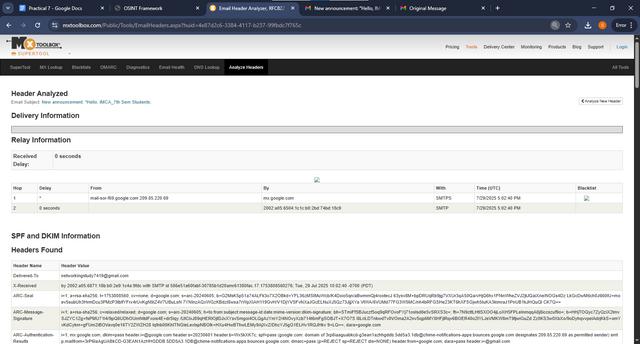
**DKIM (Domain keys identify Mail)**

**DMARC (Domain-based Message Authentication, Reporting, and Conformance)**

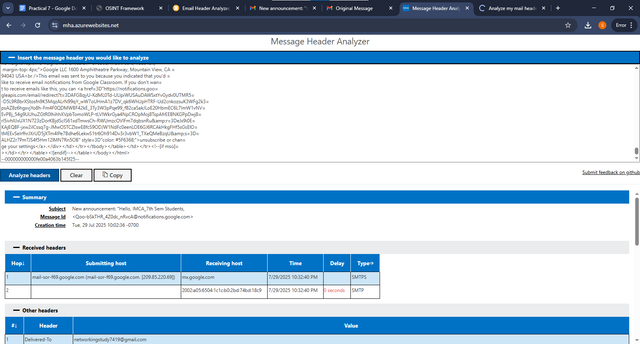
* [haveibeenpwned.com](http://haveibeenpwned.com) **:** A website that lets users check if their email or personal data has been compromised in known data breaches.



* **MXToolbox:** An online toolset for diagnosing and troubleshooting email servers, DNS records, and blacklist status.



* **Microsoft Header Analyzer:** A tool that helps analyze email headers to detect spoofing, phishing, and other email security issues.

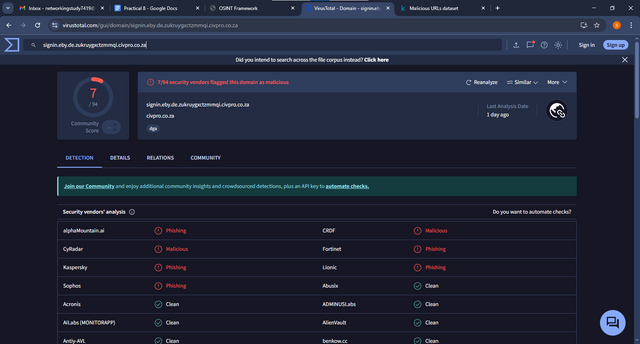


**Conclusion :** Gathering and analyzing email headers allowed us to trace email origins, detect spoofing, and understand how email architecture works, which is crucial for email security.

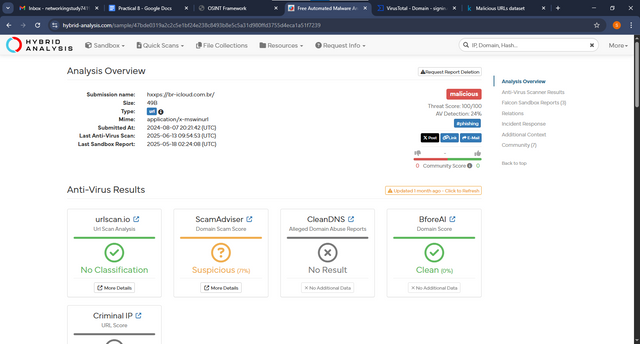
Practical – 8

**Aim :** Do malware analysis using OSINT to understand the concept of file and URL.

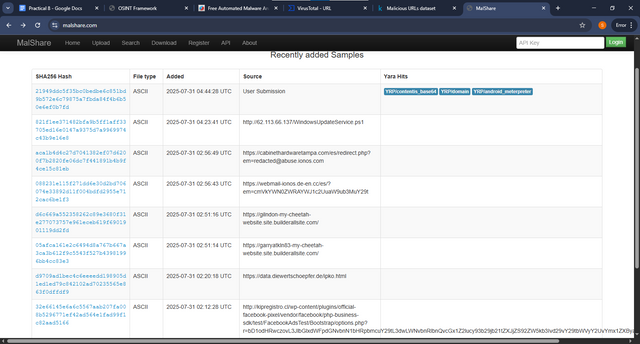
1. Malicious File analysis > Hosted automated analysis :
   1. **Virustotal :** VirusTotal.com is a free online service that scans files and URLs using multiple antivirus engines to detect malware and threats.



* 1. **HybridAnalysis:** A malware analysis service that provides detailed reports on files and URLs to detect and understand potential threats.



**MalShare:** A free malware repository offering a large collection of samples for researchers and analysts to study and examine threats.



**Conclusion :** Analyzing suspicious files and URLs with OSINT tools taught us how to detect malicious patterns, strengthening awareness of malware threats and safe analysis methods.

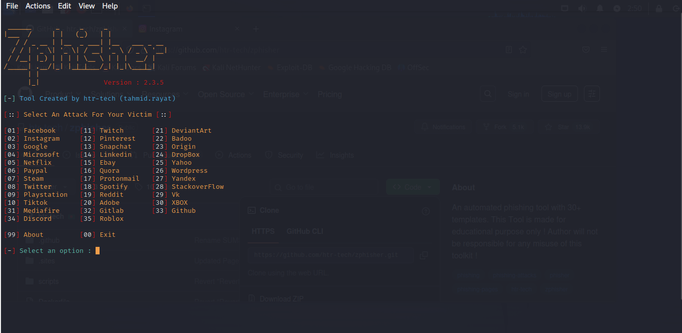
Practical – 9

**AIM :** Create a Simulate Phishing Email and Test it on Classmate with Permission to understand how to Identify Phishing Attempt and Discuss Red Flag best practices for avoiding them using Zphisher Tool.

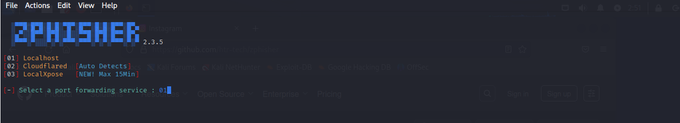
**Initial Setup**: Download/Clone Zphisher from GitHub repo and run [zphisher.sh](http://zphisher.sh) file

* **cd <zphisher directory>**

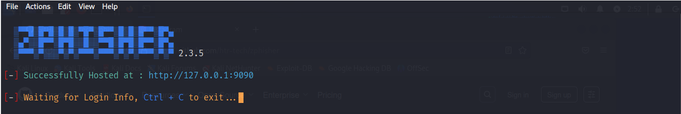
* **bash zphisher.sh**



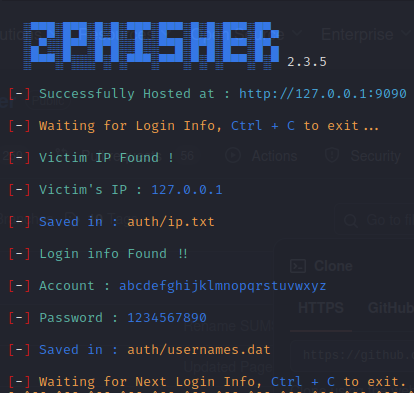
* Select any Page you want to clone



* Localhost and run in custom host : 9090



* Click the link to open the Phishing page and enter credentials



* The Credentials Will be shown in zphisher console and saved in usernames.dat file

* You can customise the link to make it look like legit and gather credentials

**Conclusion** **:** By creating and analyzing phishing emails using Zphisher, we understood social engineering tactics, red flags of phishing attempts, and best practices for avoiding such attacks.

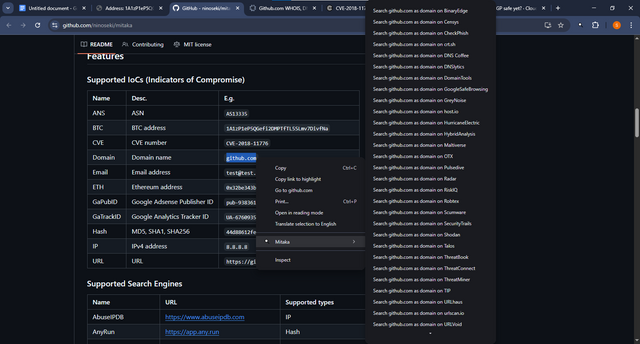
Practical – 10

**AIM :** Use Mitaka Tool in order to understand link, EmailID and Information Gathering and analysis.

Mitaka is a Browser Extension for Chrome and Firefox that Helps in Searching, Co-relating and Analysing Indicators of Compromise

* **Tools:**

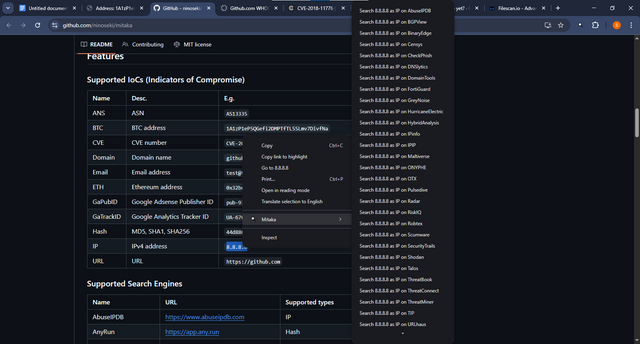
1. **Domain Analysis Tools:** Select any URL and Right Click, You will see mitaka Option click it and You will see all the OSINT tools available on Domain Analysis.



**Output :**

* Right-click on a domain/URL → Mitaka shows OSINT tools.
* Lets you check WHOIS, DNS records, blacklist status, subdomains.

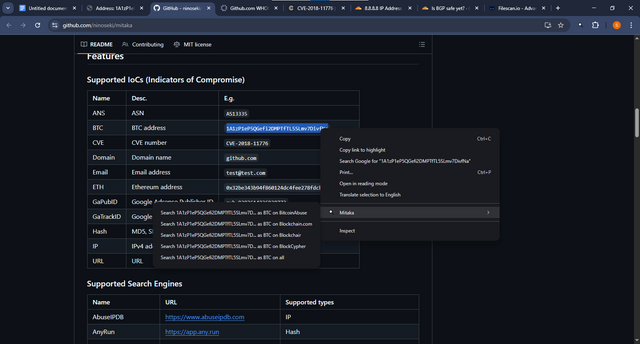
1. **IP analysis:** Similar to Domain You Just select an IP Address and Right Click to see all the available OSINT Options.



**Output :**

* Right-click on an IP → Mitaka gives lookup options.
* Shows geolocation, ISP/ASN, blacklist check, reverse DNS.

1. **Bitcoin Address Analysis:** Similarly Just Select Right Click and see Available OSINT Options.



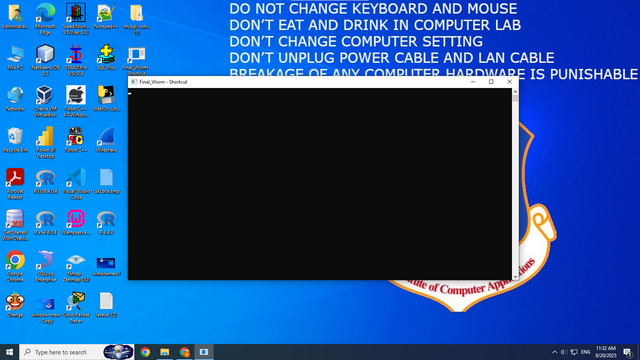
**Output :**

* Right-click on a Bitcoin wallet → Mitaka tools appear.
* Lets you view transactions, balance, blockchain history, scam reports.

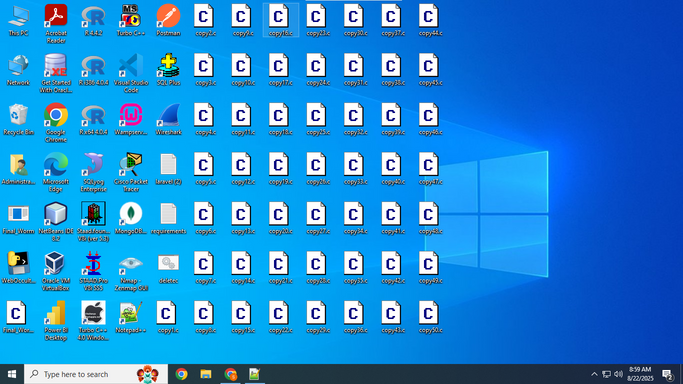
**Conclusion :** Using the Mitaka tool, we learned how to extract information about domains, IPs, email IDs, and links, which enhanced our ability to perform OSINT-based investigations effectively.

Practical – 11

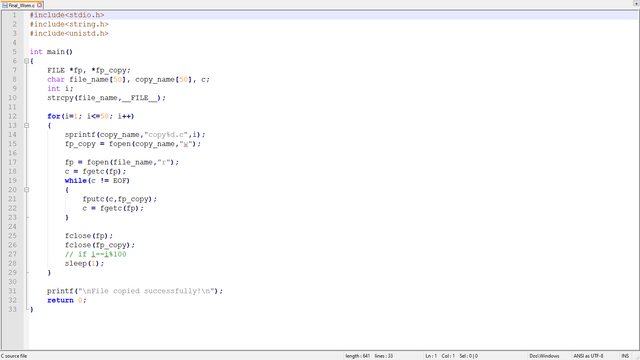
**AIM** : Create Worm in C language in order to understand how Worm works and Replicates itself without any Human Interference.



**Explanation :** Shows **Final\_Worm.exe** executing from the command line, indicating the replication process running to completion.



**Explanation :** Displays the newly created files on the desktop (**e.g.,** **copy1.c … copy50.c**), confirming self-replication.



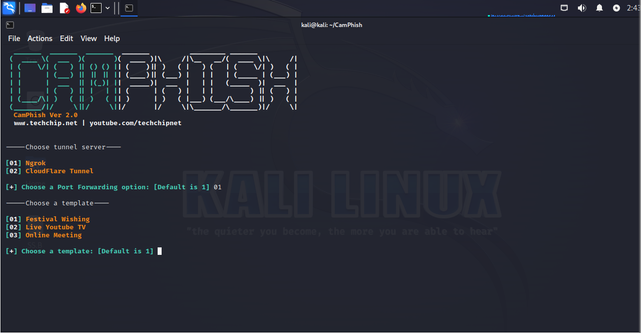
**Explanation :** This C program is a simple **worm demonstration** that shows how a file can replicate itself. Using the **\_\_FILE\_\_** macro, it reads its own source code and, in a loop, creates 50 copies named **copy1.c** to **copy50.c**. Each copy is made by reading the original file character by character and writing it into a new file, with a 1-second delay between copies. In the end, it prints *“File copied successfully!”*. This explains the basic working of a worm that can **self-replicate without user help**.

**Conclusion** **:** Developing a simple worm program in C gave us insights into how self-replicating malware works and spreads, emphasizing the importance of secure coding and malware defenses.

Practical – 12

**AIM :** Use Camphish tool to exploit mobile device inorder to understand phishing scan.









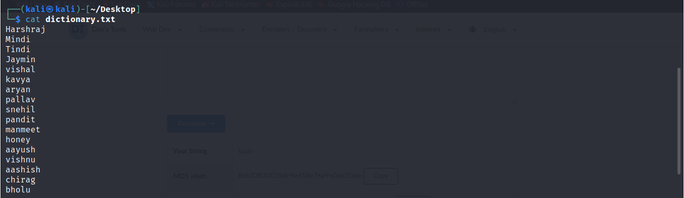
**Conclusion :** We demonstrated phishing on mobile devices using CamPhish, which highlighted how attackers exploit human behavior and the importance of mobile security awareness.

Practical – 13

**AIM :** Demonstrate dictionary attack by implementing password hash cracking using John The Ripper tool in kali linux.

* A dictionary attack is when an attacker or security attacker tries to crack the password hashes by comparing them with a predefined list of possible password called a dictionary or word list.

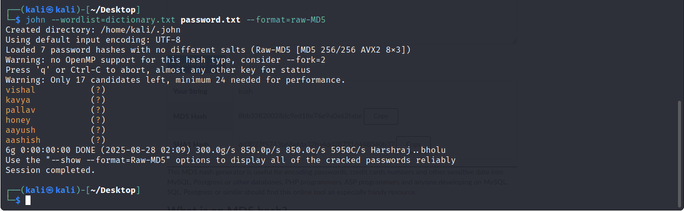
* First we search on google **MD5 Hash Generator** then click the first link and open it.





* **MD5 Hash Generator :**

* + john --wordlist=dictionary.txt password.txt --format=raw-MD5



**Conclusion :** Password hash cracking showed us how weak passwords can be easily broken, reinforcing the importance of using strong, complex passwords and implementing password security policies.

Practical – 14

**AIM :** Perform web server vulnerability scan with various options of nikto tool.

**Use :** Active Scanning

Nikto is an Open Source Web Server Scanner that checks for :

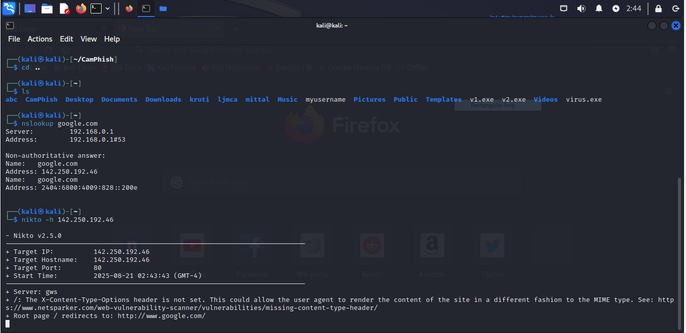
1. Insecure files / Script
2. Outdated Server Versions
3. Configuration Issue
4. Default credentials

* **Basic Scan :**

First we need a domain ip so we can find this with the help of nslookup command :

nslookup [google.com](http://google.com) (http)

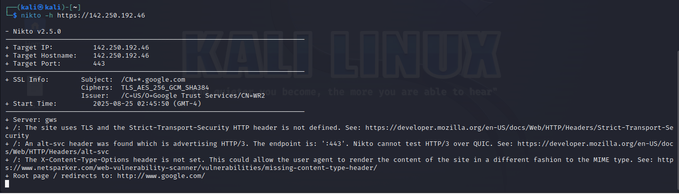
**CMD :** nikto -h 142.250.192.46(http)Where -h is host



* **SSL Scan :**

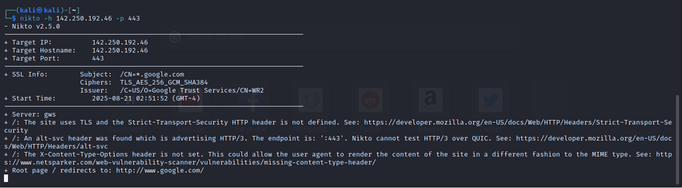
Nikto -h domain ip (https)

**CMD :** nikto -h <https://142.250.192.46>



* **Specific Port :**

**CMD :** nikto -h 142.250.192.46 -p 443



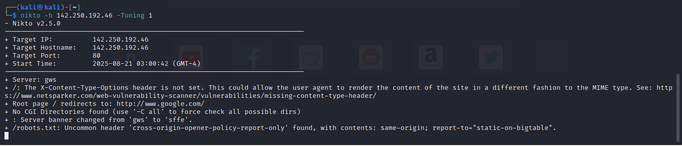
**Tuning Scan :**

**For Sinlge :** nikto -h Domain\_IP -Tuning 2

**For Multiple :** nikto -h Domain\_IP -Tuning 234

Where **X** is ,

1. File Upload
2. Misconfiguration
3. Information disclosure
4. Injection ( Cross-site,SQL)
5. Remote File Retrieval
6. Denial Of Service (DOS)
7. Remote Vulnerabilities
8. Command Execution
9. SQL Injection



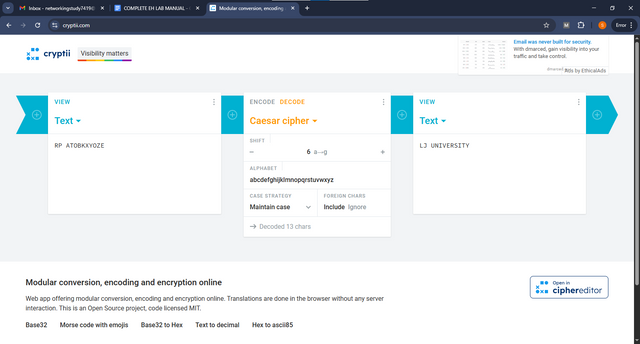
**Conclusion :** By scanning web servers with Nikto, we identified potential vulnerabilities, which is a fundamental step in web application security testing.

Practical – 15

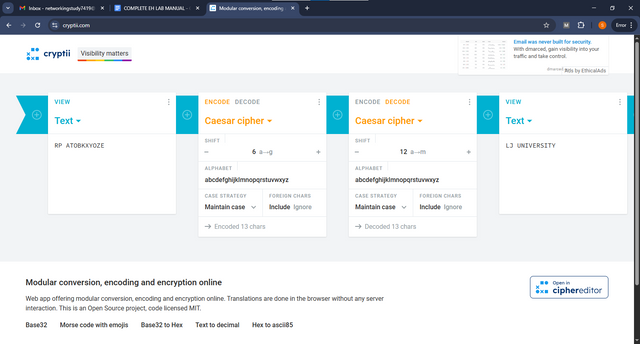
**AIM :** Utilising the functionalities of various Symmetric Key Cryptography Algorithms using cryptii.



* **Encoding:** We encoded “LJ UNIVERSITY” using the Caesar cipher with a shift of 6, and the output is “RP ATOBKXYOZE”.



* **Decoding:** We decoded “RP ATOBKXYOZE” using the Caesar cipher with a shift of 6, and the output is “LJ UNIVERSITY”.



* In the first step, we use a shift of 6, and in the second step, we use a shift of 12 to get the correct output.
* We are using two methods to encode and decode the message 'RP ATOBKXYOZE', and the final output is 'LJ UNIVERSITY'.

**Conclusion :** Exploring symmetric encryption algorithms helped us understand fast, secure data encryption methods used in real-world applications like file encryption and secure communication.

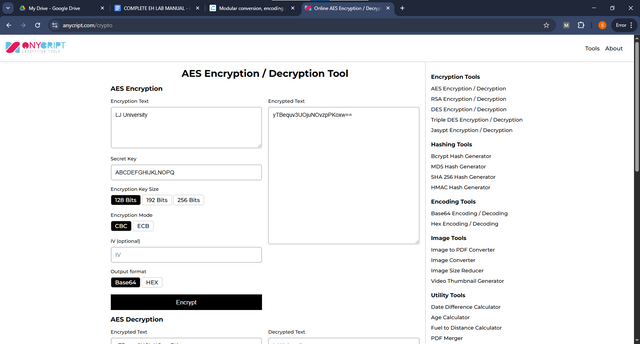
Practical – 16

**AIM:** Utilising the functionalities of various Asymmetric Key Cryptography Algorithms using anycript.

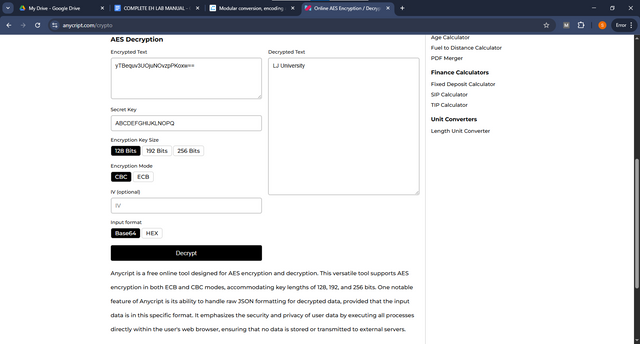
[anycript.com](http://anycript.com)

1. **AES Encryption and Decryption(Advanced Encryption Standard):**

1. Encryption

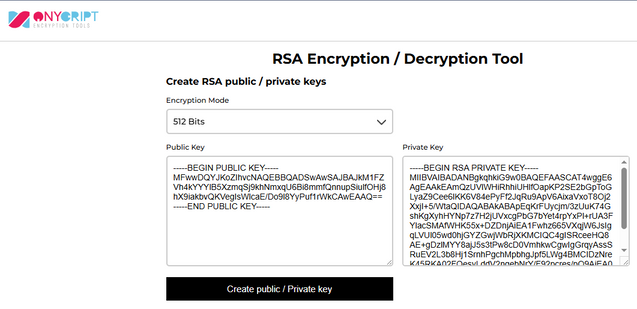


1. Decryption



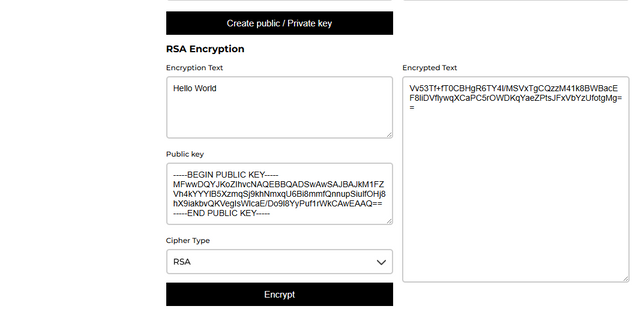
1. **RSA (Rivest–Shamir–Adleman) :**

1. Create a Public and Private Key

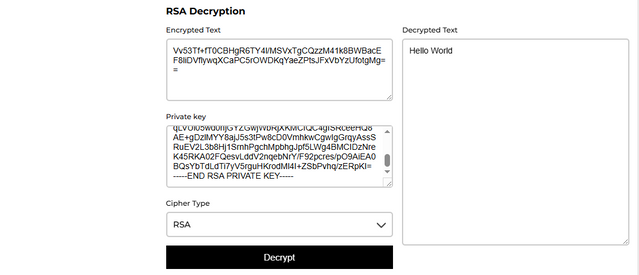


2

1. Encrypt Message Using The **“ Public Key ”** We Just Created Above



1. Decrypt Message Using The **“ Private Key ”** We Just Created Above to Get Our Message Back!



**Conclusion :** Implementation of asymmetric encryption enhanced our knowledge of public-private key concepts, digital signatures, and secure key exchange mechanisms, widely used in SSL, authentication, and secure communication.