INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

PENETRATION TESTING AND CYBER OPERATIONS LABORATORY								
VI Semester: CSE(CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCC10	**CORE**	1	0	2	2	30	70	100
Contact Classes: 12	**Tutorial Classes: Nil**	**Practical Classes: 33**				**Total Classes: 45**		
Prerequisite: Network security								

I. COURSE OVERVIEW:

The purpose of this course is to provide a clear understanding of assessing an application or infrastructure for vulnerabilities in an attempt to exploit those vulnerabilities, and circumvent or defeat security features of system components through rigorous manual testing.

II. COURSES OBJECTIVES:

The students will try to learn

I. The tools that can be used to perform information gathering.
II. The Various attacks in various domains of cyberspace.
III. How vulnerability assessment can be carried out by means of automatic tools or manual investigation.
IV. The vulnerabilities associated with various network applications and database system.

III. COURSE OUTCOMES:

At the end of the course students should be able to:

CO 1 **Make use of** Google and Whois tools to gather information about the target specification.

CO 2 **Apply** appropriate tools to encrypt and decrypt passwords in network.

CO 3 **Make Use of** Nessus tool to identify vulnerabilities and monitor the networking mechanism.

CO 4 **Compare** different OSINT tools to detailed network information of the target.

CO 5 **Make use of** Virus Total tool to scan the network and detect malware on the network.

CO 6 **Apply** Ettercap tool to scan the network and performing an ARP poisoning attack.

IV. COURSE CONTENT:

EXERCISES FOR PENETRATION TESTING AND CYBER OPERATIONS LABORATORY

Note: Students are encouraged to bring their own laptops for laboratory practice sessions.

1. Getting Started with Understanding of scanning and reconnaissance process.

Introduction:

A penetration test, colloquially known as a pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system. Penetration tests usually simulate a variety of attacks that could threaten a business. They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system.

Softwares used:

Osint Tools
Vulnerability Tools
Attack detection Tools
Encryption Tools

1.1 Scanning any of the target with domain name

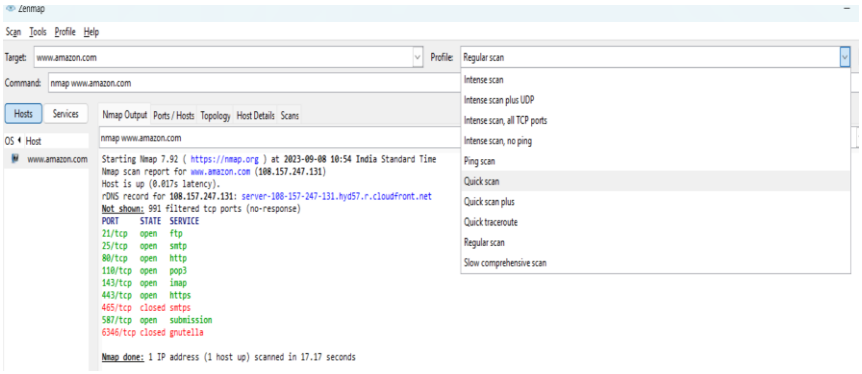
To Perform Scanning of the target we need to understand all scanning types as shown in below

There are different types of scans available

Syntax: Nmap domain name

Example: nmap www.amazon.com

Type of scan: Regular



Try

Students can use different types of scans to perform on the target.

Hint

Select type of scan from Nmap tool on target.

1.2 Scanning any of the target with IP Address

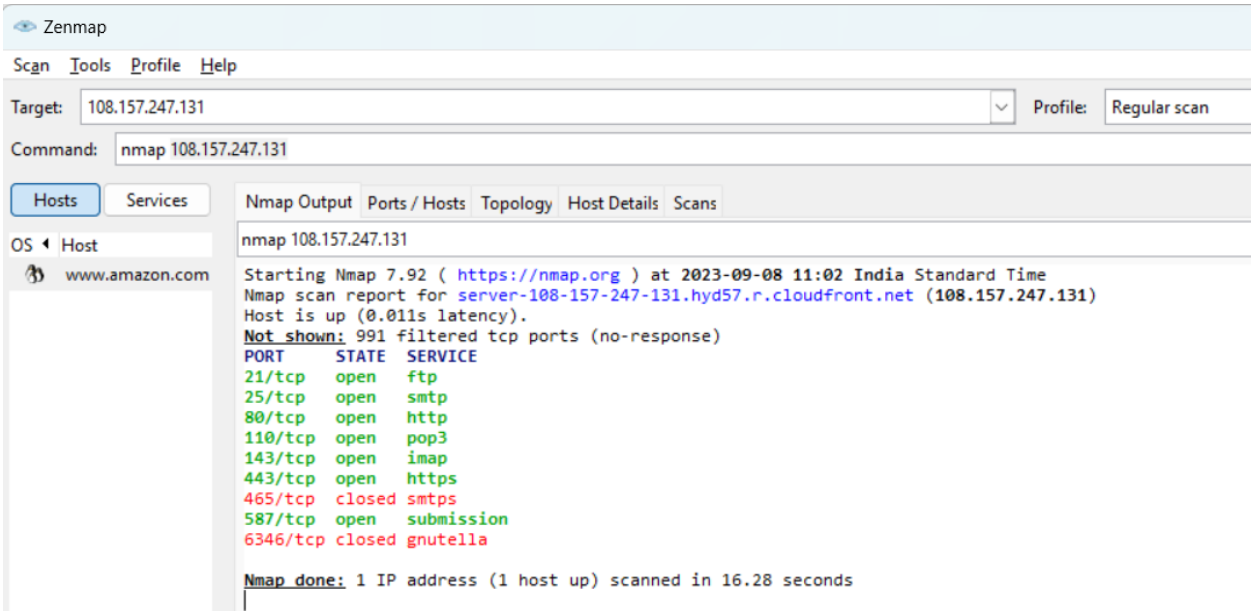
Perform Scanning of the target we need to understand all scanning types as shown in below
There are different types of scans available

Syntax: Nmap IP Address

Example: nmap 108.157.247.131

Type of scan: Regular

Output:



Try

Students should perform scanning of the target with variety of scan types as shown in above.

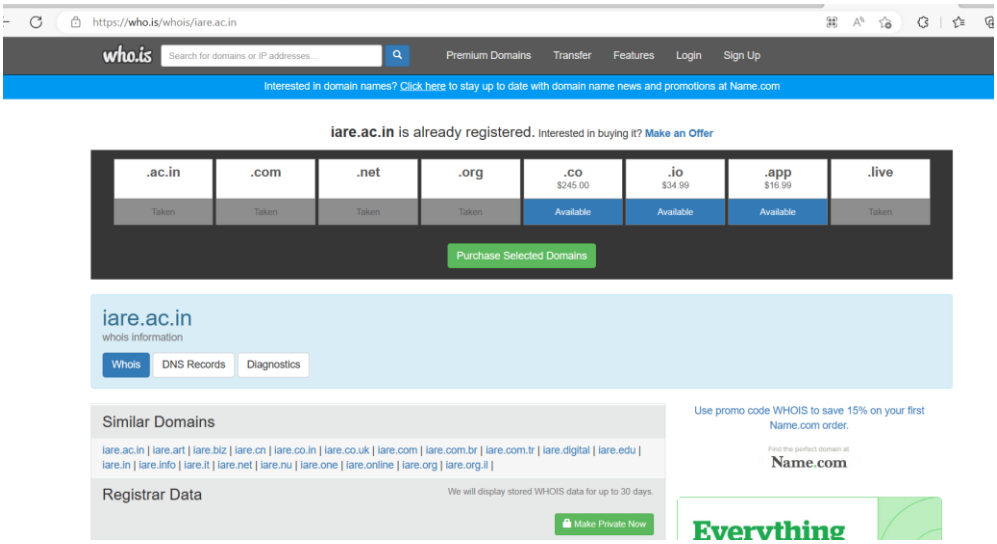
Hint:

Select the type of scan from dropdown window appeared on screen

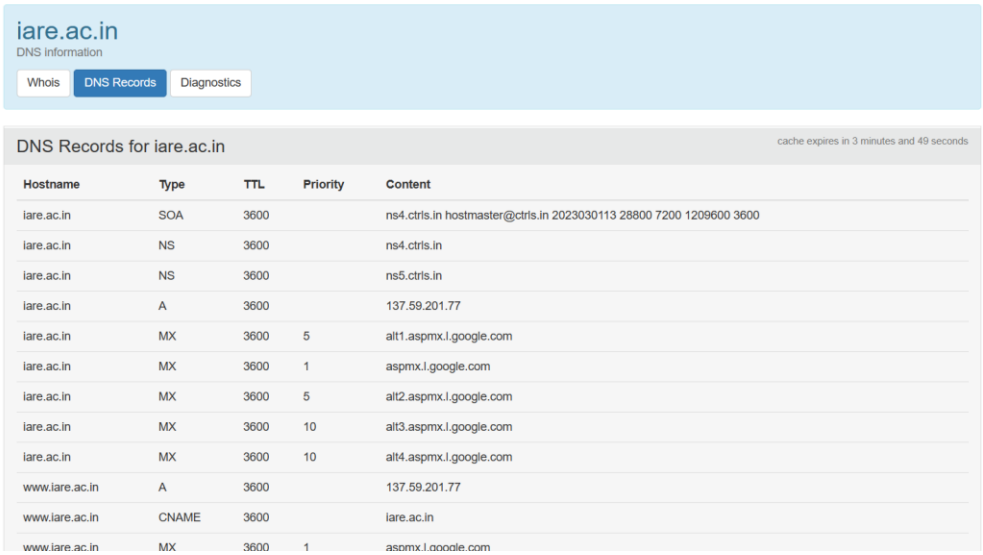
2. Use Google and Whois for Reconnaissance to gather information about target.

Open-Source Intelligence (OSINT) is the collection, analysis, and dissemination of information that is publicly available and legally accessible. Right now, OSINT is used by a organizations, including governments, businesses, and non-governmental organizations.

Step1: open Google
Step2: Type Whois on google
WHOIS Search, Domain Name, Website, and IP Tools - Who.is

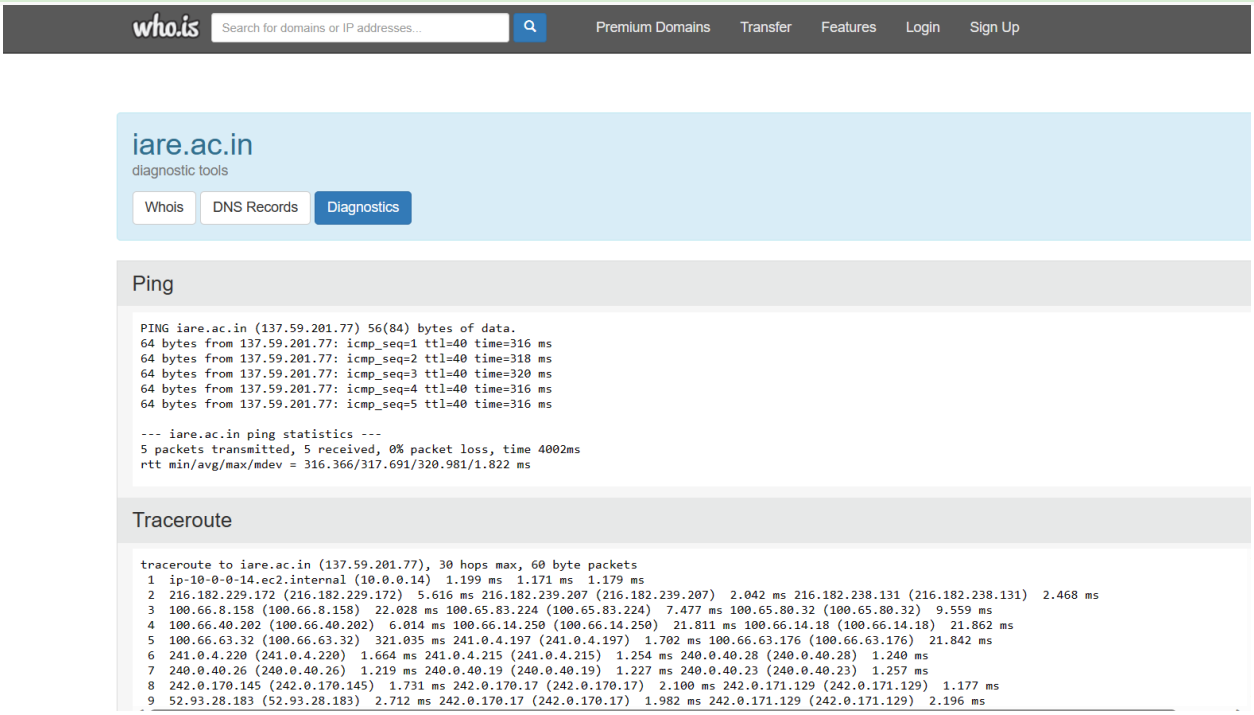


Step3: check DNS Records



Hostname	Type	TTL	Priority	Content
iare.ac.in	SOA	3600		ns4.ctrls.in hostmaster@ctrls.in 2023030113 28800 7200 1209600 3600
iare.ac.in	NS	3600		ns4.ctrls.in
iare.ac.in	NS	3600		ns5.ctrls.in
iare.ac.in	A	3600		137.59.201.77
iare.ac.in	MX	3600	5	alt1.aspmx.l.google.com
iare.ac.in	MX	3600	1	aspmx.l.google.com
iare.ac.in	MX	3600	5	alt2.aspmx.l.google.com
iare.ac.in	MX	3600	10	alt3.aspmx.l.google.com
iare.ac.in	MX	3600	10	alt4.aspmx.l.google.com
www.iare.ac.in	A	3600		137.59.201.77
www.iare.ac.in	CNAME	3600		iare.ac.in
www.iare.ac.in	MX	3600	1	aspmx.l.google.com

Step 4: check all diagnostics



Try:

Use other OSINT tools to gather information to find information of target network.

Hint:

Use Google Dorks, Babel X as a OSINT tools

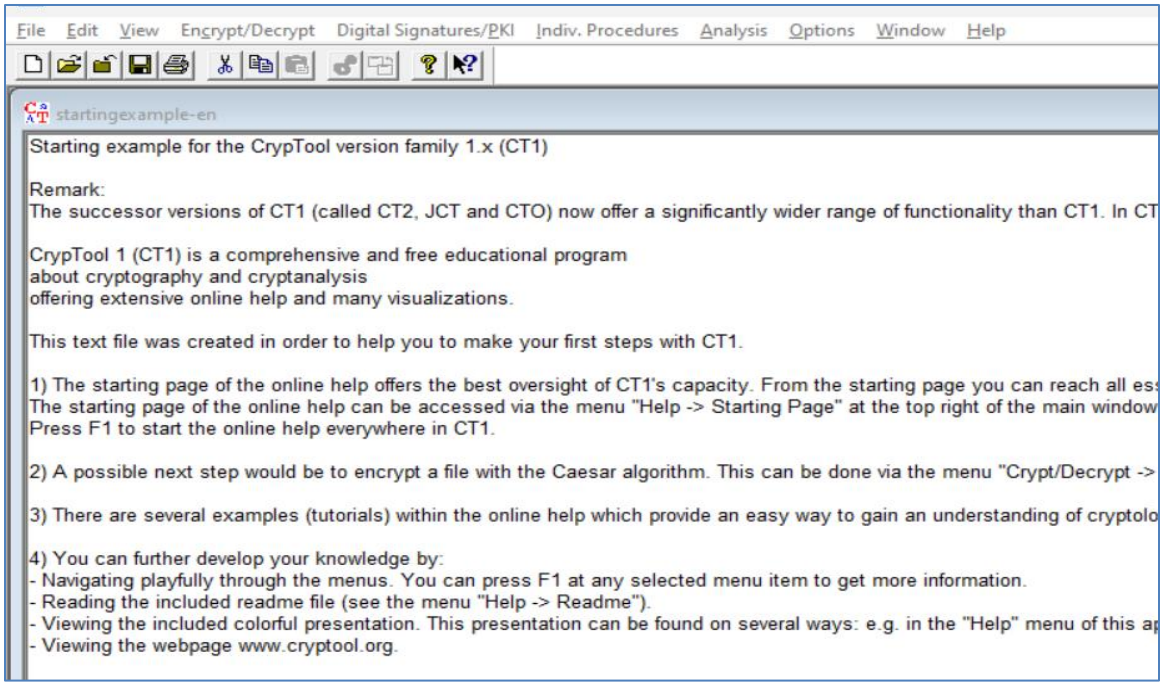
3. Make use of Crypt tool for Encryption and decryption procedure

3.1 Install Crypt tool

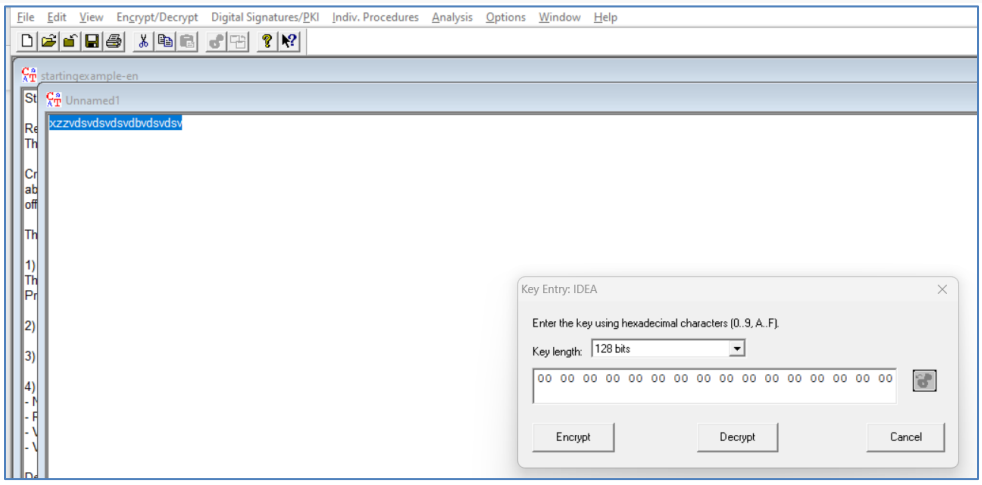
Software Requirements:

- Supported operating systems:
- Windows 10/11/ Linux
- 64-bit OS X/macOS 10.6 or later

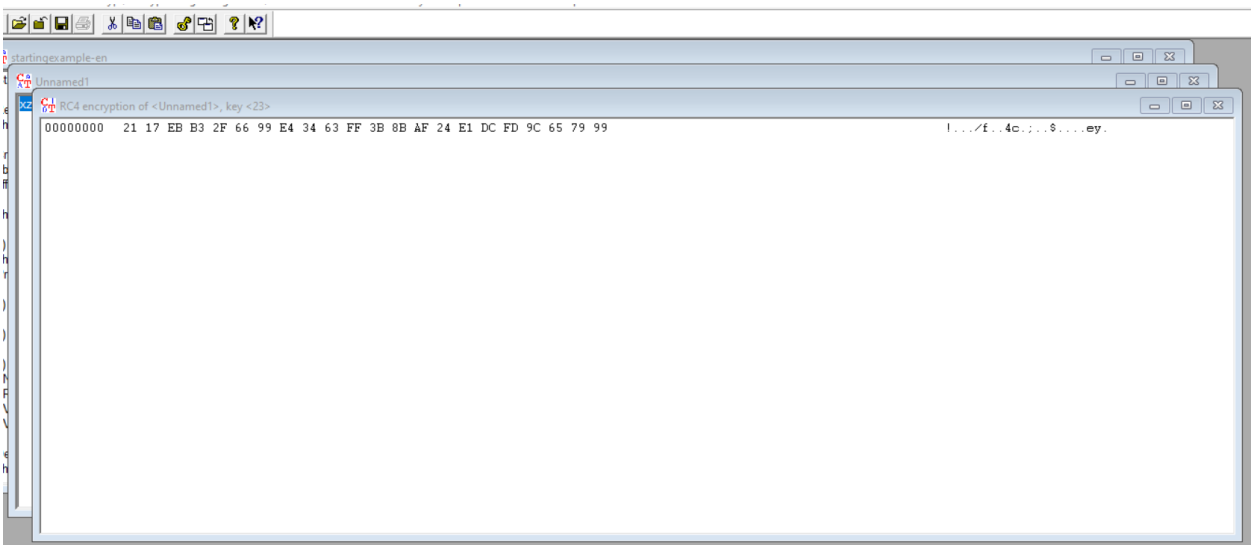
Step1: Download and install crypt tool
Step2: open software



Step3: click on file to new file
Step 4: enter data to encrypt and decrypt file
Step 5: select any of algorithm to encrypt



Step6: based on selection of algorithm enter password
Step 7: again, open file to decrypt



Step8: enter the password to decrypt
Step9: file will be decrypted

Try:
Use different cryptographic algorithms for perform encrypt and decrypt procedure
Hint:
use symmetric modern algorithms like IDEA, RC2, RC4
use symmetric classic algorithms like Caesar, Hill, substitution algoriths

4. Install Password Cracking tool Cain and able to Crack the password

4.1 installing Cain and able Tool

Requirements

The actual version requires the following items:

10Mb Hard-Disk space-

Microsoft Windows 2000/XP/2003/Vista-

Winpcap Packet Driver (v2.3 or above; AirPcap adapter is supported from Winpcap version 4.0).

Setup

Just run the Self-Installing executable package and follow the installation instructions.

The package will copy all the files needed by the program into the installation directory.

Installation Files

Cain's setup program will install and/or replace these files in your system:

- Cain.exe [the main executable program]

- Cain.exe.sig [author's PGP signature of the file Cain.exe]

- CA_UserManual.chm [this file]

- Abel.exe [the executable of the Windows service named Abel]

- Abel.exe.sig [author's PGP signature of the file Abel.exe]

- Abel.dll [a DLL file needed by the program]- Abel.dll.sig [author's PGP signature of the file Abel.dll]

- Uninstal.exe [the uninstallation program]

- Wordlist.txt [a little word list file]

- Install.log [the log file of the installation package, you can check everything modified on your system here]

- Whatsnew.txt [contains differences between versions]

- oui.txt [a list file that contains vendor's information about MAC addresses]

- <Installation Dir>\winrtgen\winrtgen.exe [Winrtgen - a windows utility to generate Rainbow Tables]

- <Installation Dir>\winrtgen\winrtgen.exe.sig [author's PGP signature of the file winrtgen.exe]

- <Installation Dir>\winrtgen\charset.txt [an example file containing charset definitions for winrtgen.exe and Cain's cryptanalysisattacks]

- <Installation Dir>\Driver\WinPcap_4_1_beta5.exe [the original distribution package of the Winpcap drivers] All the above files will be installed in the Installation directory and subdirectories.

Abel Installation

Abel is a Windows NT service composed of two files: "Abel.exe" and "Abel.dll".

These files are copied by the installation packageinto the program's directory but the service is NOT automatically installed on the system.

Abel can be installed locally or remotely (using Cain) and requires Administrator's privileges on the target machine.

LOCAL INSTALLATION:

1) Copy the files Abel.exe and Abel.dll into the %WINNT% directory (E.G.: C:\WINNT or C:\Windows)

2) Launch Abel.exe to install the service (it is not automatically started)

3) Start the service using the Windows Service Manager (services.msc)

REMOTE INSTALLATION:

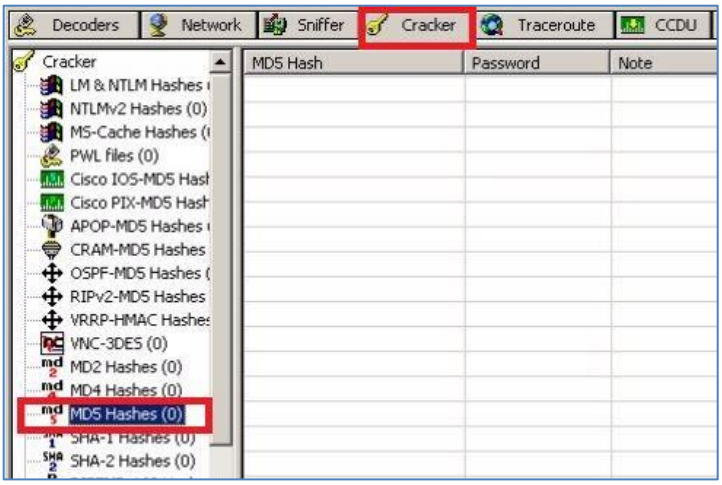
1) Use the "Network TAB" in Cain and choose the target remote computer where you want to install Abel
2) Right click on the computer icon in the left tree and select "Connect As"
3) Provide Administrator's credentials for the remote system
4) Once connected right click on the "Services" icon and select the menu entry "Install Abel"
5) That's it! The two files 'Abel.exe' and 'Abel.dll' will automatically be copied to the remote machine's root directory i.e. C:\winnt,C:\Windows); the service will automatically be installed and started.

4.2 Dictionary attack

Dictionary attack uses a predetermined list of words from a dictionary to generate possible passwords that may match the MD5 encrypted password. This is one of the easiest andquickest way to obtain any given password.

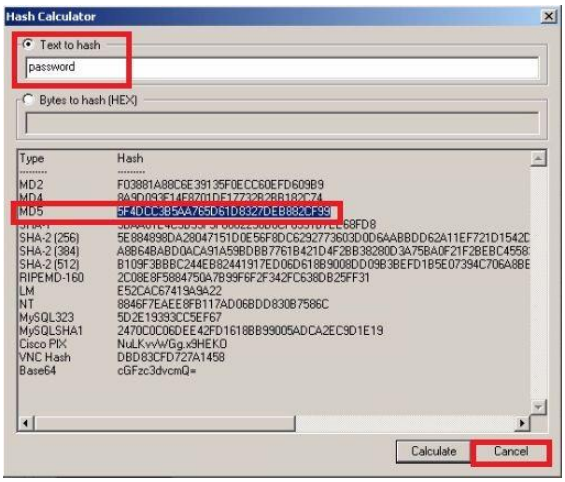
Start Cain & Abel via the Desktop Shortcut 'Cain' or Start menu.
(Start > Programs > Cain > Cain).

Choose 'Yes' to proceed when a 'User Account Control' notification pops up regarding software authorization.
Once on, select the 'Cracker' tab with the key symbol, then click on MD5 Hashes. The result should look like the image below.

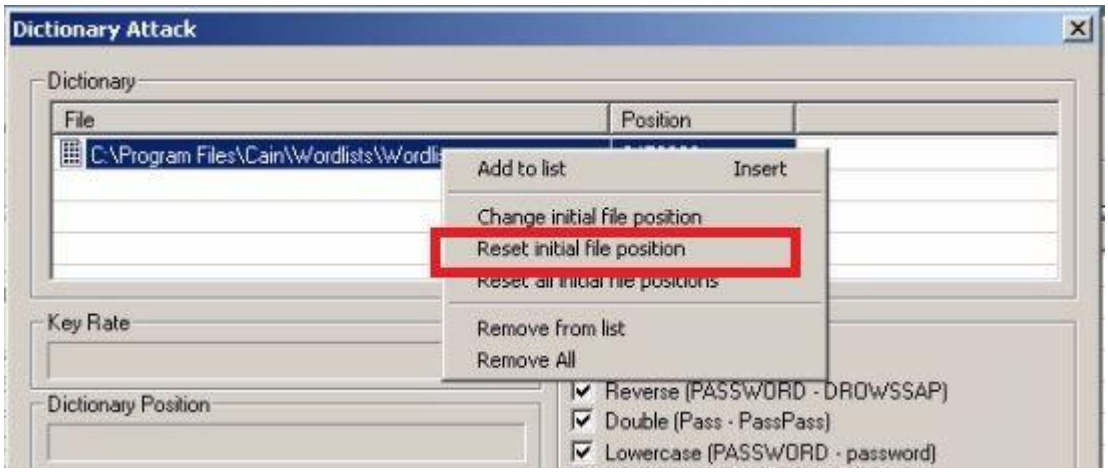


1. As you might have noticed we don't have any passwords to crack, thus for the next few steps we will create our own MD5 encrypted passwords. First, locate the Hash Calculator among a row of icons near the top. Open it.

2. Next, type into **'Text to Hash'** the word **password.** It will generate a list of hashes pertaining to different types of hash algorithms. We will be focusing on **MD5 hash** so copy it. Then exit calculator by clicking **'Cancel'** (Fun Fact: Hashes are case sensitive so any slight changes to the text will change the hashes generated, try changing a letter or two and you will see. This is called the **avalanche effect**.)



3. After you exit, right click and select **'Add to list'**, paste your hash then click **OK**. Your first encrypted password! But don't stop there, add the following MD5 hashes from the words **PaSS**, **13579**, **15473** , **sunshine89**, and **c@t69**.
4. With all the encrypted MD5 passwords on hand, we can finally start! Move your cursor and select all **six passwords**, then right click and press **'Dictionary Attack'**.
5. Once the window opens, go up to the dictionary and select **'Wordlist.txt'**, right click and select **'Reset initial file position'**. You'll know you've resetted when there's nothing under the position column. **Note: Make sure to do this every time you want to restarta dictionary attack!**



9.Click **'start'** and watch the magic happens before your eyes! Once it ends **'exit'**. Your result should be the same as below.

Try:
Apply different cracking methods to crack the passwords.

Hint:
Rain bow tables, Brute force Attacks methods can use for crack passwords.

5. Find the Vulnerabilities of the target using Nmap tool.

We can use and apply variety of commands on Nmap tool to find the vulnerabilities on target network.

Cmd: nmap -sV --script vulners www.bookmyshow.com

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 13:55 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.45.182)
Host is up (0.0016s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.46.182 104.16.47.182 104.16.49.182 104.16.48.182
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp?
25/tcp   open   smtp
| fingerprint-strings:
|   GenericLines:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
80/tcp   open   http     Cloudflare http proxy
|_http-server-header: cloudflare
110/tcp  open   pop3?
143/tcp  open   imap?
443/tcp  open   ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
465/tcp  closed smtps
587/tcp  open   smtp
| fingerprint-strings:
|   GenericLines:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
```

nmap -sV --script vuln `www.bookmyshow.com`

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 14:14 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.46.182)
Host is up (0.0048s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.49.182 104.16.48.182 104.16.45.182 104.16.47.182
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp?
25/tcp   open   smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| fingerprint-strings:
|   GenericLines:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
80/tcp   open   http     Cloudflare http proxy
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-server-header: cloudflare
110/tcp  open   pop3?
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
|_ssl-dh-params: ERROR: Script execution failed (use -d to debug)
|_ssl-heartbleed: ERROR: Script execution failed (use -d to debug)
|_ssl-cert-intaddr: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: ERROR: Script execution failed (use -d to debug)
|_ssl-poodle: ERROR: Script execution failed (use -d to debug)
143/tcp  open   imap?
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
```

5.1 using csrf as NSE script

http-csrf: Cross-Site Request Forgery (CSRF)
vulnerabilities are detected by this script.
nmap -sV --script http-csrf `www.bookmyshow.com`

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 14:23 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.45.182)
Host is up (0.0048s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.46.182 104.16.48.182 104.16.49.182 104.16.47.182
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp?
25/tcp   open   smtp
| fingerprint-strings:
|   GenericLines:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
80/tcp   open   http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-csrf: Couldn't find any CSRF vulnerabilities.
110/tcp  open   pop3?
143/tcp  open   imap?
443/tcp  open   ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-csrf: Couldn't find any CSRF vulnerabilities.
465/tcp  closed smtps
587/tcp  open   smtp
| fingerprint-strings:
```

5.2 using password

Attempts to retrieve /etc/passwd or boot.ini to see if a web server is vulnerable to directory traversal.

nmap -sV --script http-passwd `www.bookmyshow.com`

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-10 14:23 India Standard Time
Nmap scan report for www.bookmyshow.com (104.16.45.182)
Host is up (0.0048s latency).
Other addresses for www.bookmyshow.com (not scanned): 104.16.46.182 104.16.48.182 104.16.49.182 104.16.47.182
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp?
25/tcp   open   smtp
| fingerprint-strings:
|   GenericLines:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
80/tcp   open   http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-csrf: Couldn't find any CSRF vulnerabilities.
110/tcp  open   pop3?
143/tcp  open   imap?
443/tcp  open   ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-csrf: Couldn't find any CSRF vulnerabilities.
465/tcp  closed smtps
587/tcp  open   smtp
| fingerprint-strings:
```

Try:
Use slowloris command to check vulnerabilities on target
Hint:
nmap -sV --script http-slowloris-check www.bookmyshow.com

6. Analyze web application digital history of the target address using Way back Machine tool.

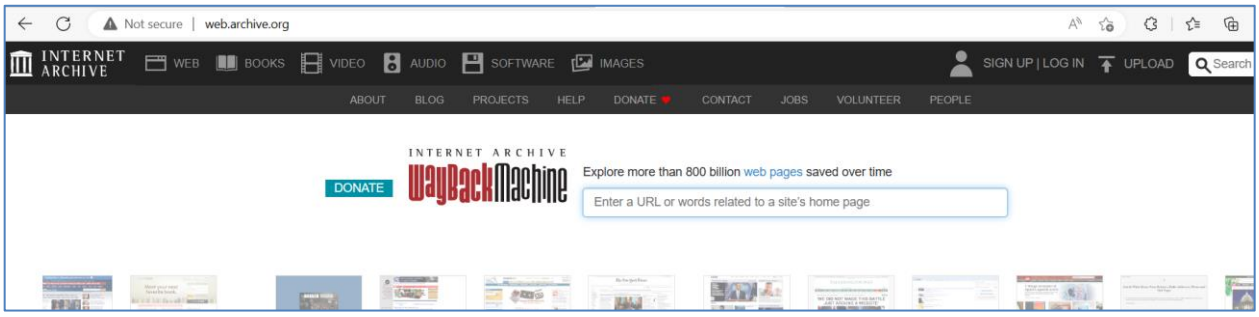
Use Wayback Machine Tool

Way back Machine is an online tool for maintaining of digital library (internet achieve) of web application, captured records of previous data related to different types of web applications.

Steps for Analyzing:

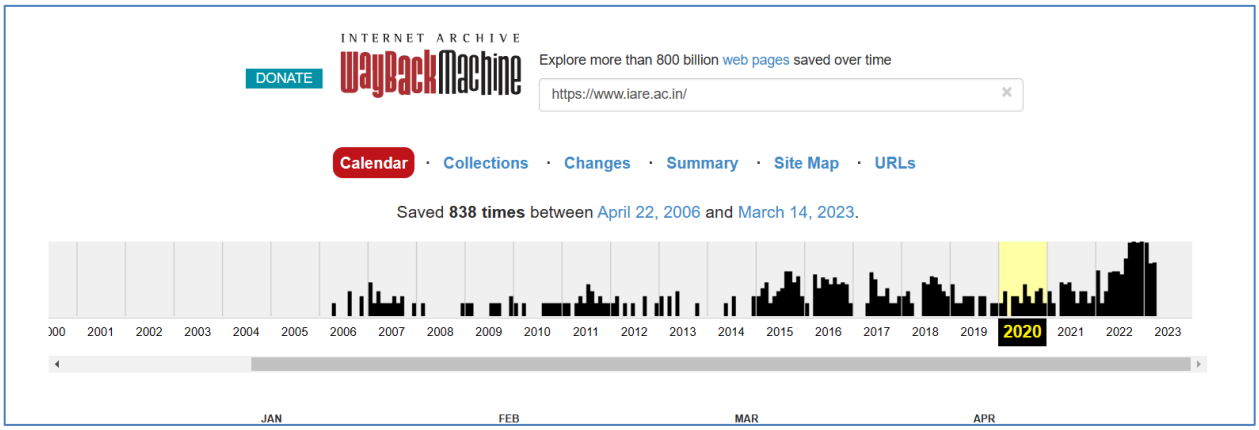
1.Open Way back machine tool in online

2. After opening it on online displays like this,



3.Type URL or target on search box.

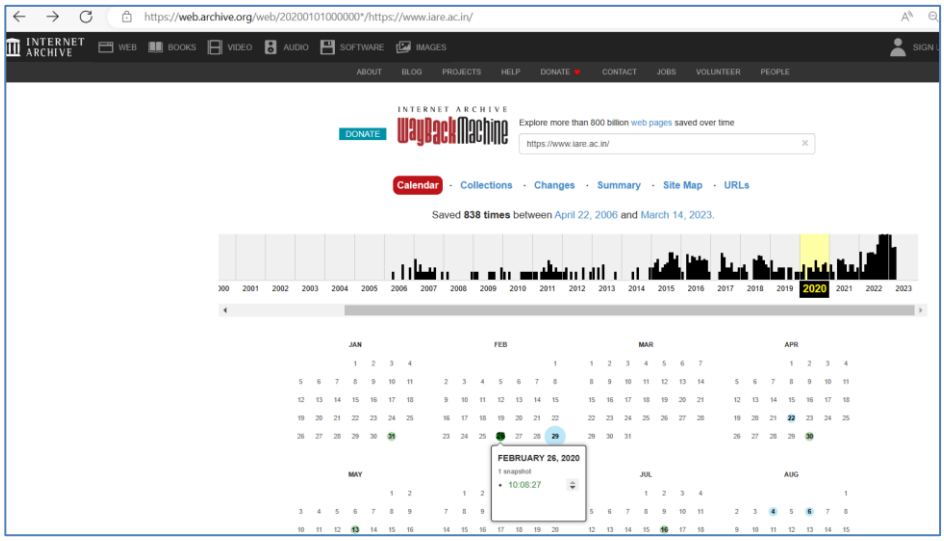
4.the fallowing information will be displayed about target.



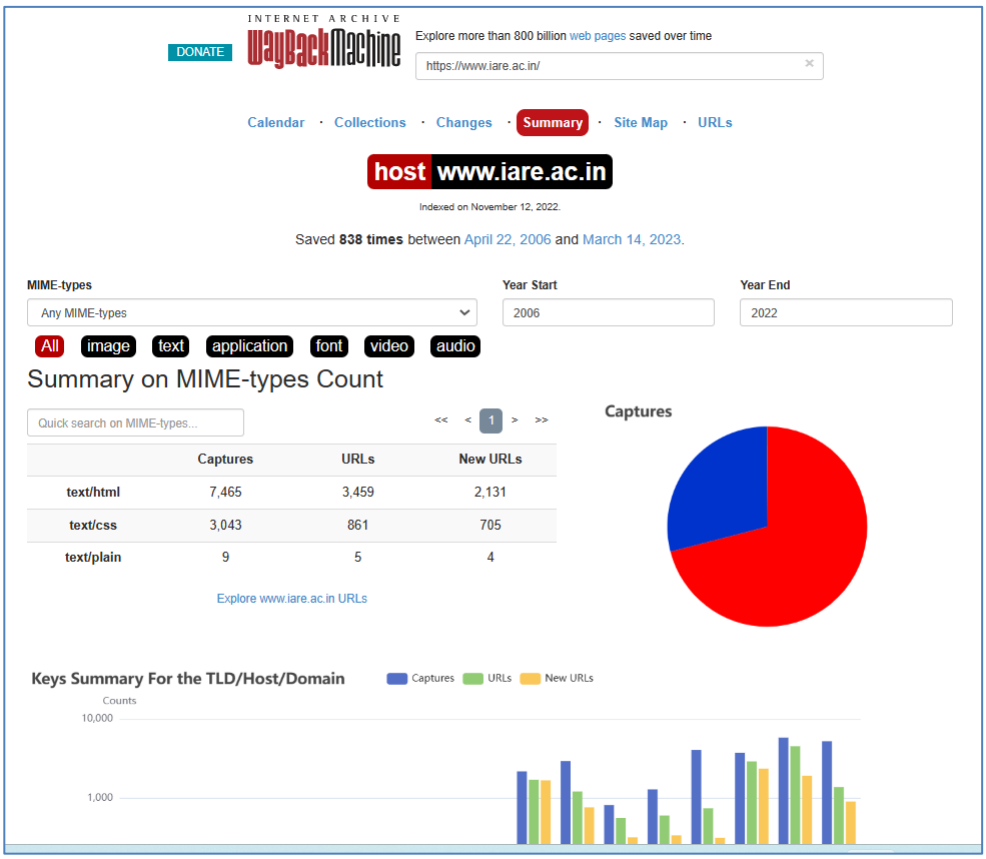
5. See the data in different ways mentioned in the diagram

- Calendar wise
- Collections wise
- Changes wise
- Summery wise
- Site Map wise
- URLs wise
-

Ex: In the calendar wise we can observe each and every captured record on particular day of month Select any of the day and displays what time it has been captured also



6. Click on the type wise as mentioned above to see the information of target Suppose I can click on summary wise I can see the information in fallowing way.



Try:

Find the information of target that updated on URL's wise

Hint:

Use URLs information then click on URLs or Explore target URLs that displays URL's information of target

7. Download and install Nessus tool in windows operating system, to run Vulnerability Scan with Nessus tool

7.1 Download and Install Nessus.

- Download Nessus from the Tenable Downloads site.
- When we download Nessus, ensure the package selected is specific to your operating system and
- processor. There is a single Nessus package per operating system and processor. Nessus Manager, Nessus Professional, and Nessus Expert do not have different packages; your activation code determines which Nessus product is installed.

Start Nessus Installation:
1. Navigate to the folder where you downloaded the Nessus installer.
2. Next, double-click the file name to start the installation process.

Complete the Windows InstallShield Wizard with the fallowing steps

1. First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue.
2. On the **License Agreement** screen, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** option, and then click **Next**.
4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder.
5. On the **Ready to Install the Program** screen, select the **Install** button.

The **Installing Tenable, Inc. Nessus** screen appears and a **Status** indication bar shows the installation progress. The process may take several minutes.
After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser.

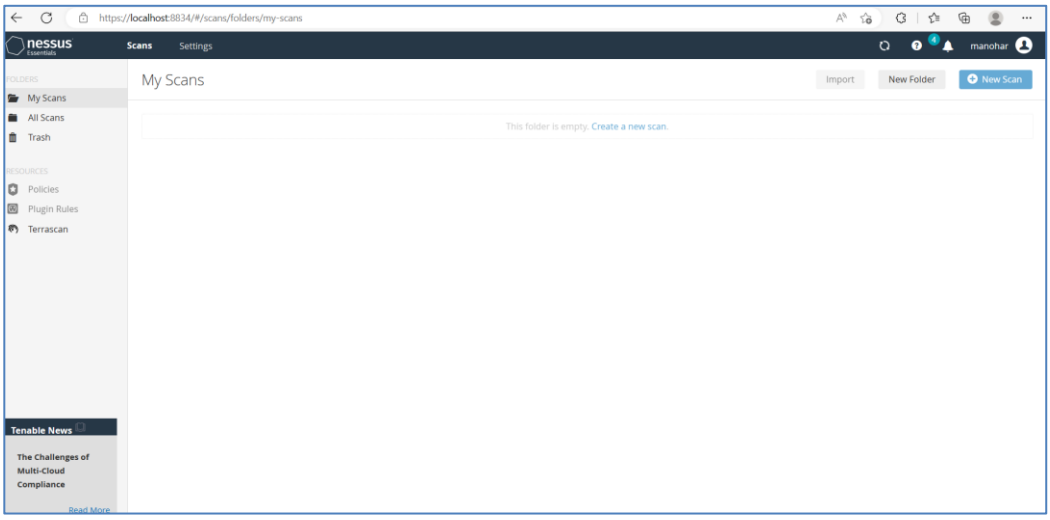
To access a locally installed Nessus instance, go to https://localhost:8834.
Perform the remaining Nessus installation steps (Adding plug-ins) in your web browser.

7.2 Run Your First Vulnerability Scan with Nessus tool.

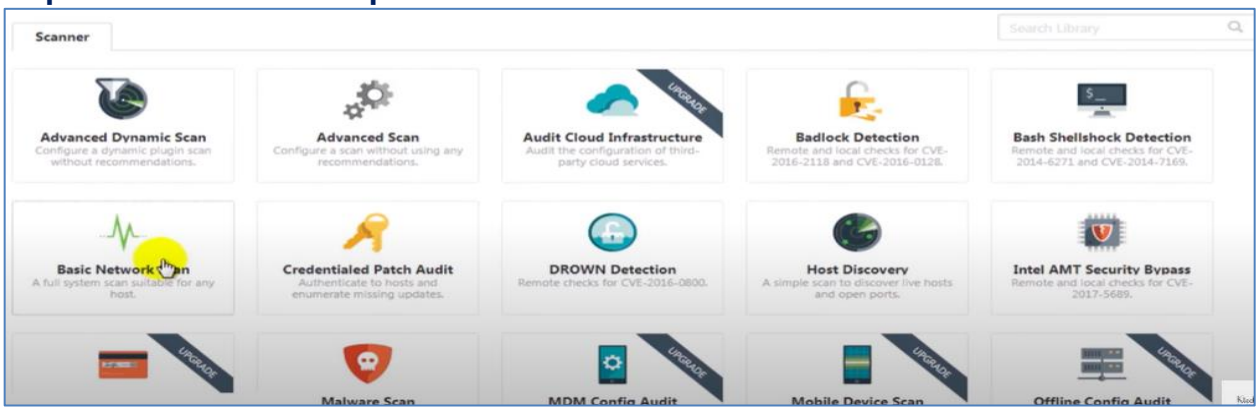
Step 1: Creating a Scan

Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan:

In the top navigation bar, click Scans.
In the upper-right corner of the My Scans page, click the New Scan button.



Step 2: Choose a Scan Template



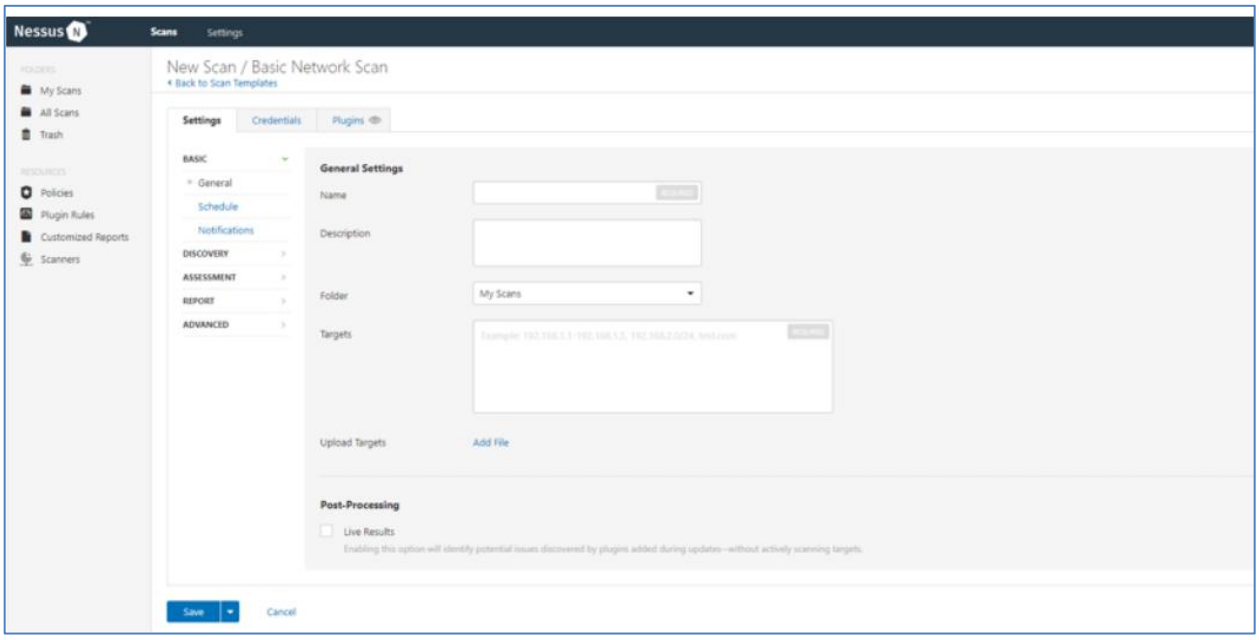
- Next, click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set. For a detailed explanation of all the options available, refer to Scan and Policy Settings in the Nessus User Guide.
- A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see Create a Policy in the Nessus User Guide.
- The Nessus interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of Nessus Professional.
- To see a full list of the types of templates available in Nessus, see Scan and Policy Templates. To quickly get started with Nessus, use the Basic Network Scan template.

Step 3: Configure Scan Settings

Prepare your scan by configuring the settings available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

Follow these steps to run a basic scan:

1. Configure the settings in the Basic Settings section.



The following are Basic settings:

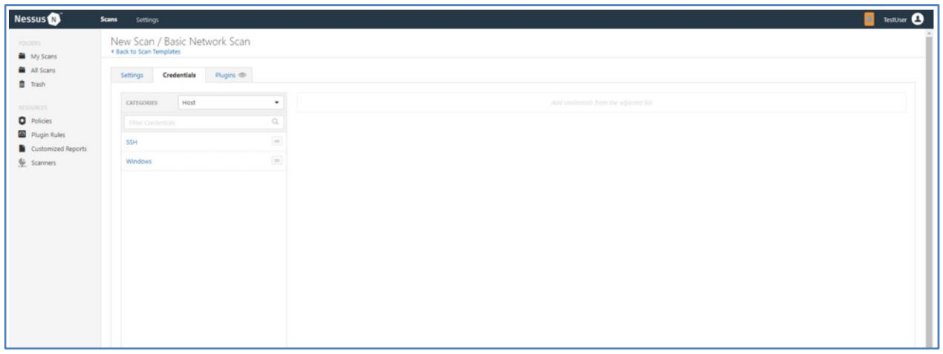
Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the Nessus interface.
Description	(Optional) Specifies a description of the scan or policy.
Folder	Specifies the folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

2. Configure remaining settings

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

3. Configure Credentials

Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.



4. Launch Scan

- After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.
- If you want to launch the scan immediately, click the down button, and then click Launch. Launching the scan will also save it.
- The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

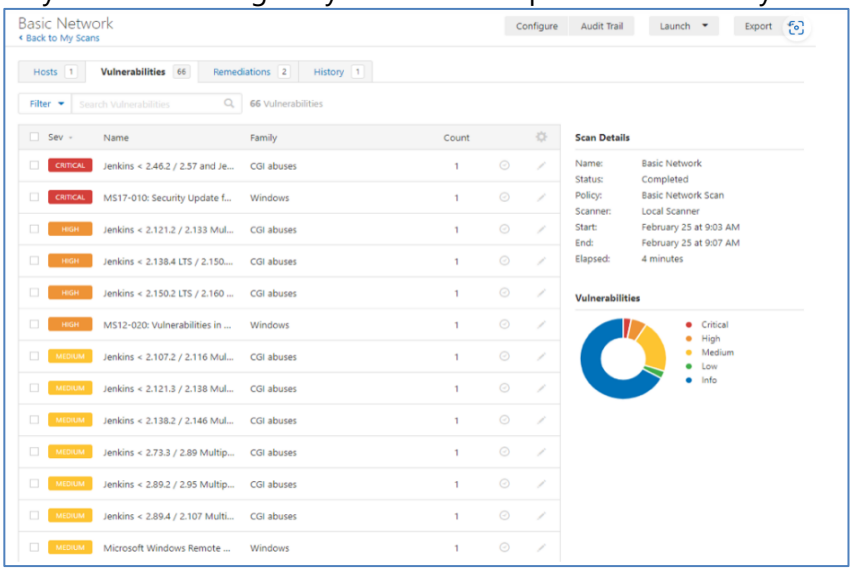
Step 4: Viewing Your Results

Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.

You can view scan results in one of several views:

Page	Description
Hosts	Displays all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity.
Remediations	If the scan's results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.
Notes	Displays additional information about the scan and the scan's results.
History	Displays a list of scans: Start Time, End Time, and the Scan Statuses.

Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

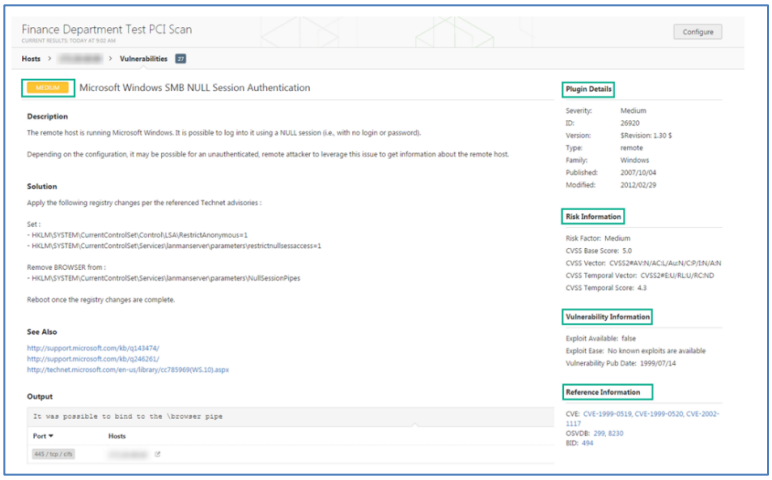


To view vulnerabilities:

In the top navigation bar, click Scans.

- Click the scan for which you want to view results.
- Do one of the following:
- Click a specific host to view vulnerabilities found on that host.
- Click the Vulnerabilities tab to view all vulnerabilities.
- (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.

- Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.



Step 5: Reporting Your Results

Scan results can be exported in several file formats.

To Export a Scan Report:

- Start from a scan's results page
- In the upper-right corner, click Export.
- From the drop-down box, select the format in which you want to export the scan results.
- Click Export to download the report.

Try:

Find Vulnerabilities based on Host discovery content

Hint:

Select the option from menu as "Host discovery content" and choose the target

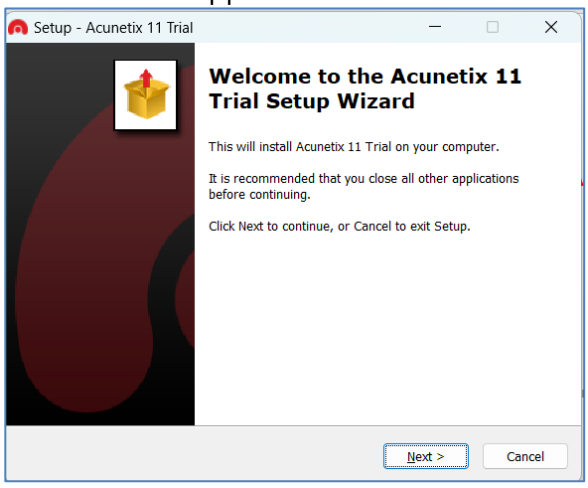
8. Install Acunetix tool to understand and perform scanning for variety of vulnerabilities in web application.

8.1 Install Acunetix tool

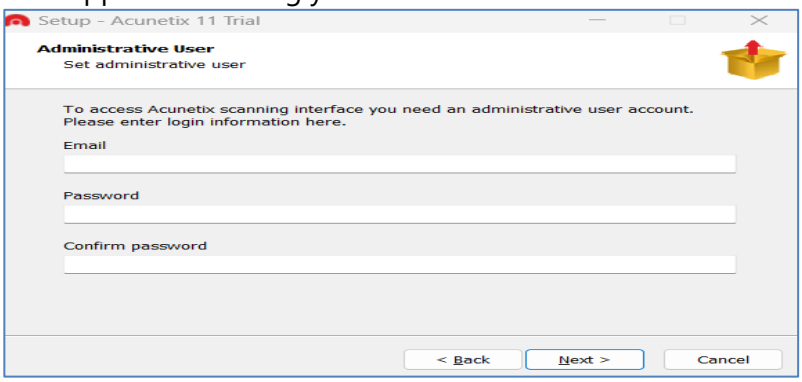
Step1: go to the location to find the official URL of Acunetix tool as mentioned below

Acunetix Web Vulnerability Scanner 11.0 Download (Free trial)... (informer.com)

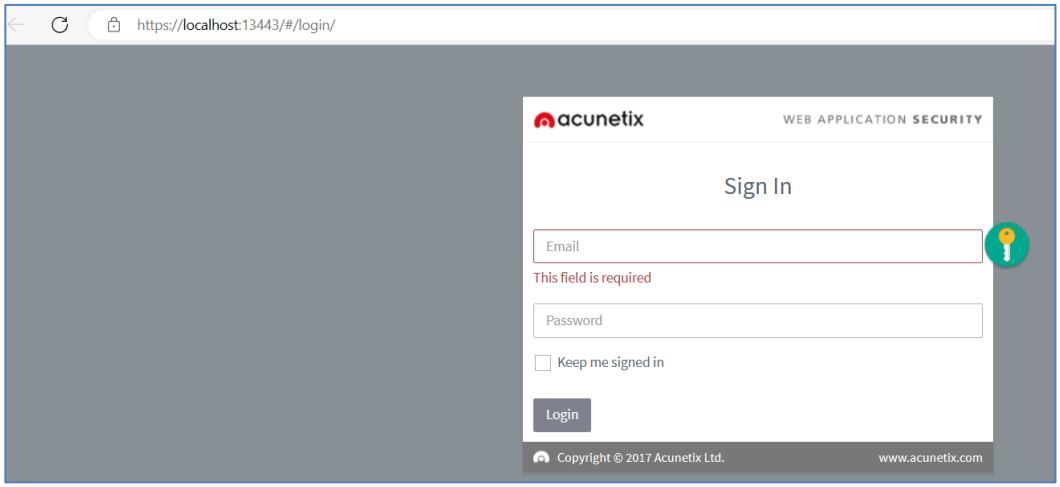
Step2: after downloading it double click on application file.



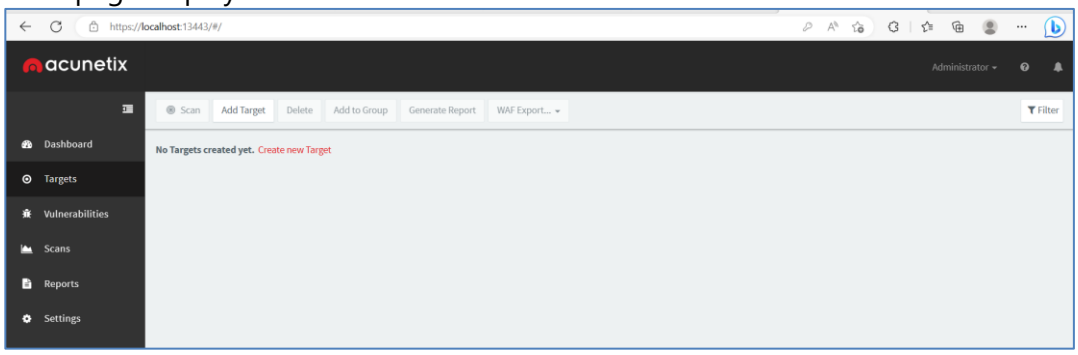
Step3: perform sequence of steps to complete the process of installation.
In the installation process application asking you to set administrative user account mentioned below



Step 4: mention username and password
Step 5: server port default it is taken, else customize if you want
Step 6: complete and finish the process has been completed
Step 7: after completion of installation

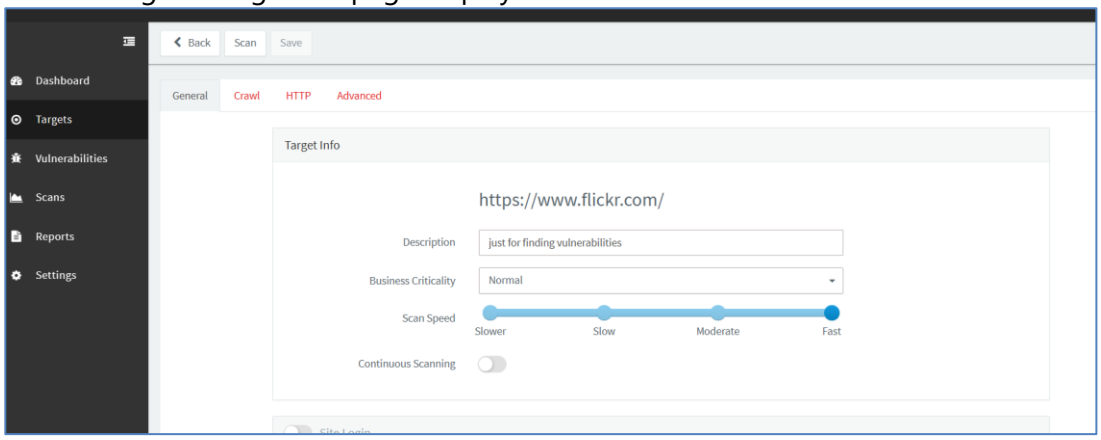


Step 8: enter mail Id and password to log on to the application page
After enter the page displays as fallows

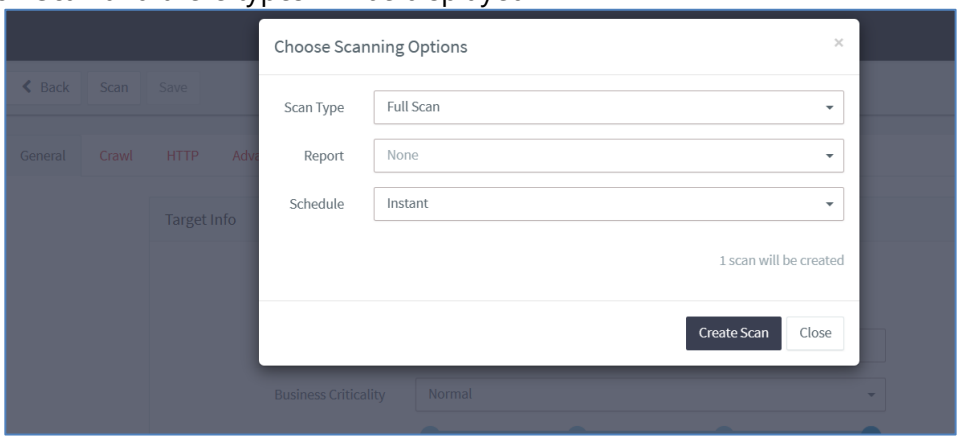


Step 9: check all the options for knowledge of each and every option
Step 10: click on Targets
In targets click on Add target or Create new Target as fallows

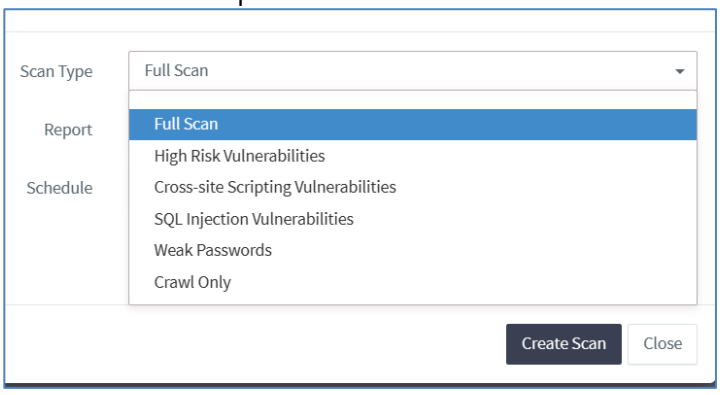
Step 11: after adding the target the page displays like this



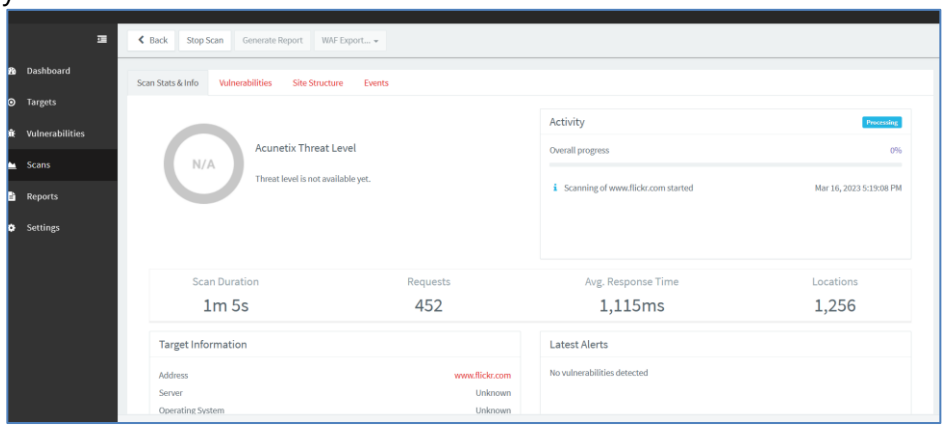
Step 12: click on Scan and there types will be displayed



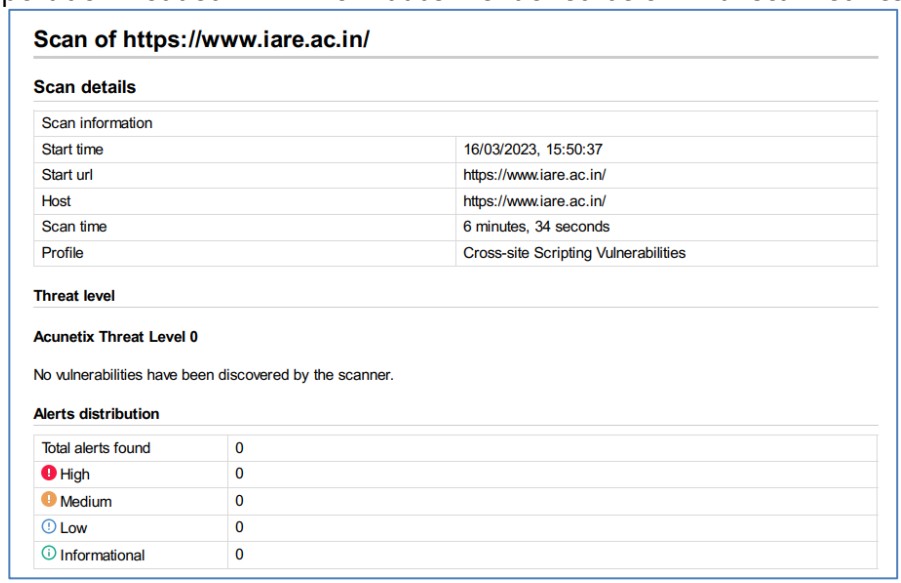
Step 13: choose the type which u want to perform scan as mentioned below



Step 14: after mention the type and schedule scan instant click on create scan. After clicking on that the page displays as fallows



In the above we can see scan start and stop options, vulnerabilities, site structure, events
Step 15: wait till the process of scanning completed
Step 16: after completed generate the report for scanned results.
Step 17: after generated download the report of scanned results.
By default, the report downloaded in PDF format as mentioned below with scanned results



Scan of https://www.iare.ac.in/

Scan details

Scan information	
Start time	16/03/2023, 15:50:37
Start url	https://www.iare.ac.in/
Host	https://www.iare.ac.in/
Scan time	6 minutes, 34 seconds
Profile	Cross-site Scripting Vulnerabilities

Threat level

Acunetix Threat Level 0

No vulnerabilities have been discovered by the scanner.

Alerts distribution

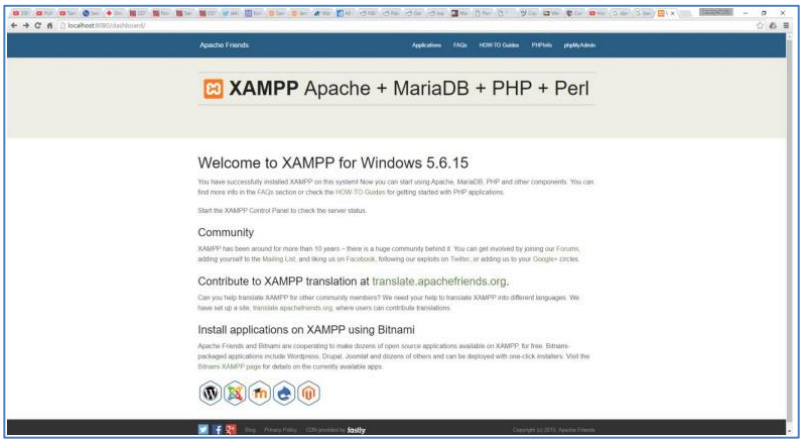
Total alerts found	0
High	0
Medium	0
Low	0
Informational	0

Try:
Use type of scan High Risk Vulnerabilities to find the target vulnerabilities

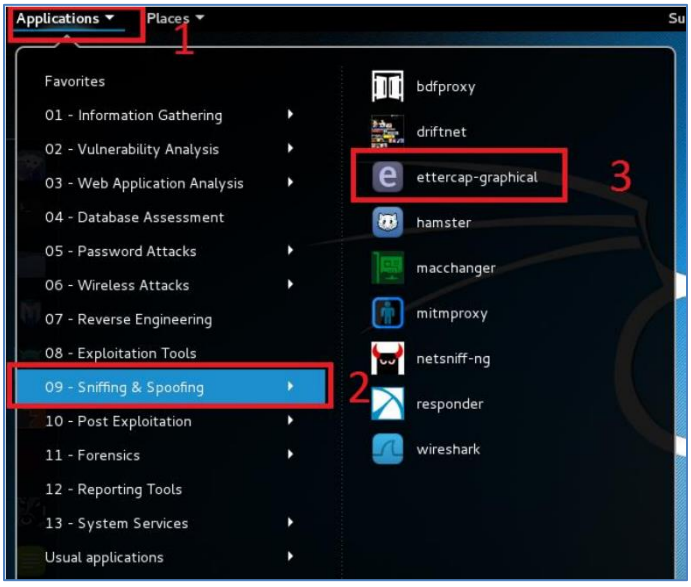
Hint:
Select the scan type from scans as Highrisk vulnerability category

9. Perform ARP Poisoning on target network.

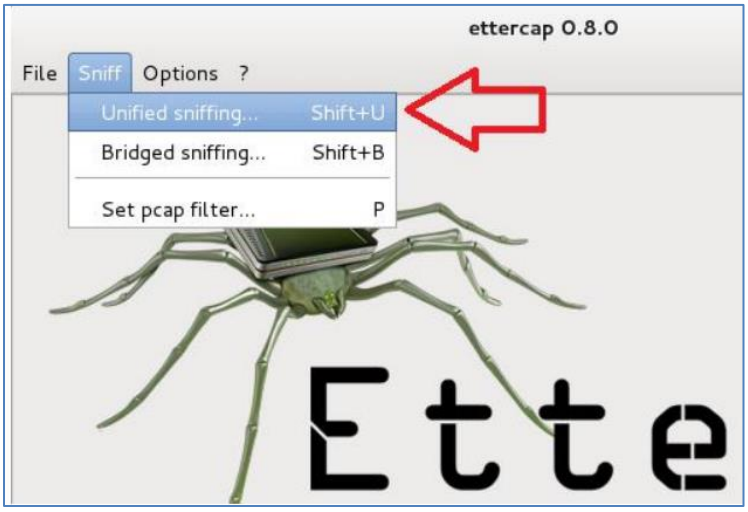
1. **Open three virtual machines :** In this you shall require a Kali 2.0 VM (we'll call this VM1), and two more VM's running operating systems Windows 7/8/8.1/10 (VM2 and VM3)
2. On all 3 virtual machines, go to settings and make sure that the network adapter is set to NAT. This is important, you cannot set it to bridge or host only, it must be NAT. This is for all 3 machines.
3. On VM1, open terminal and run "ifconfig". On VM2 and VM3, open up cmd and run "ipconfig". Take note of your IP address and MAC address on each of the respective machines. 4. On VM3, go on the Internet and download a windows application XAMP. Download version "7.0.4 / PHP 7.0.4" under XAMPP for Windows on this page: https://www.apachefriends.org/download.html
4. Install XAMP using the downloaded installer file. Don not change any settings or check/uncheck any boxes. Just keep pressing "next" until you finish.
5. Once done installation, run XAMPP Control Panel on VM3. Once the main window pops up, start the Apache server by pressing he Start button on the Apache module row.
6. To test the server, go on the internet on VM2 and type in http://. It should display a generic welcome page that looks like the following:



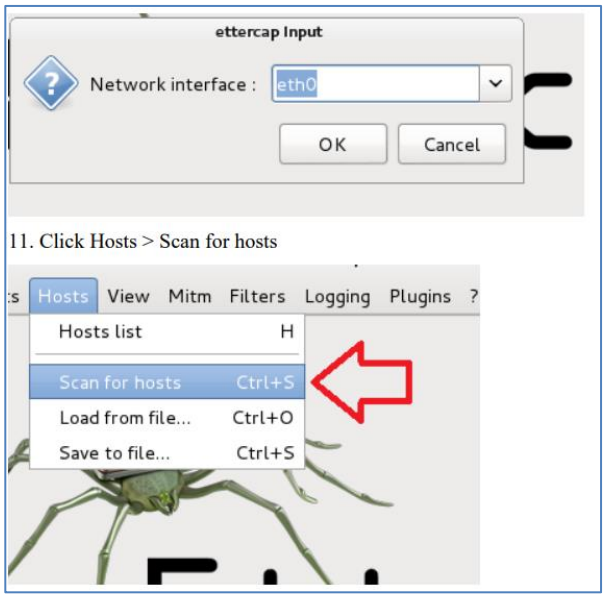
7. If successful, now go to VM1 (reminder – the one running Kali Linux 2.0. Arnold's should have the credentials root/toor). Go to applications and select "Applications > 09 – Sniffing & Spoofing > ettercap-graphical".



6. Go to Sniff > Unified Sniffing OR Pres Shift+U

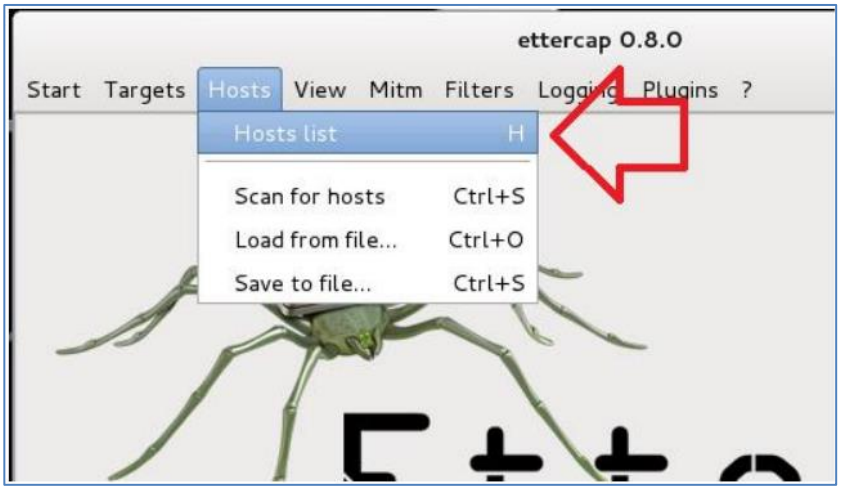


7. Select interface eth0

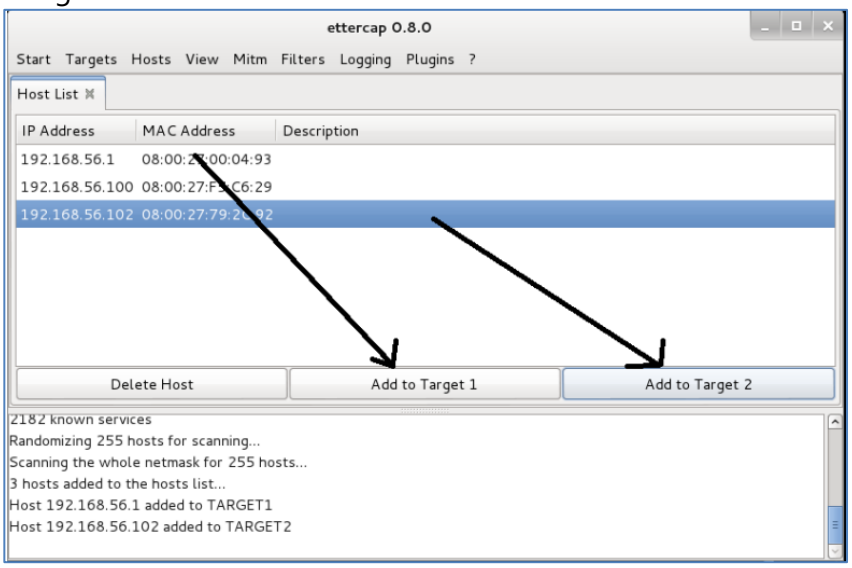


11. Click Hosts > Scan for hosts

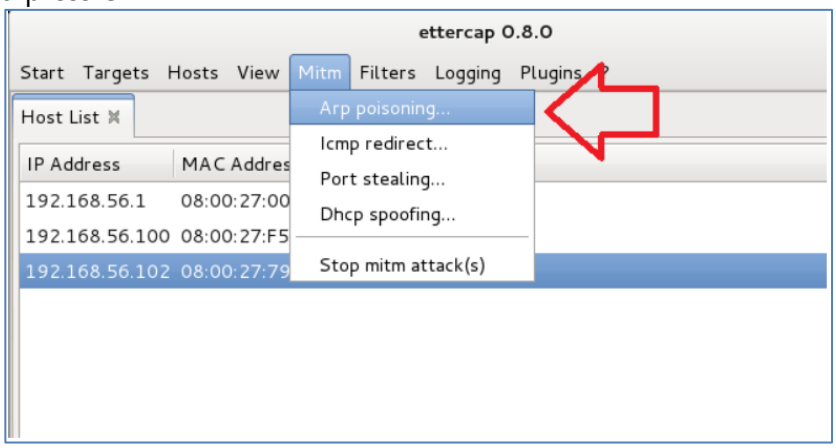
12.Click Hosts > Hosts List



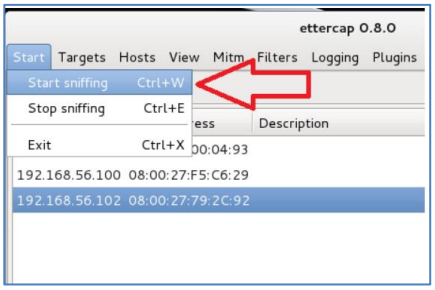
13. From the new tab that appeared, you will see a list of IP's. Add the IP of VM3 to target #1 and add the IP of VM2 to target #2.



14. Go to Mitm > Arp Poisoning. In the pop up window that appears, only check "sniff remote connections" and press OK



15. Click on Start > Start Sniffing



16. Now go to "Applications > 09 – Sniffing & Spoofing > wireshark"
17. Select eth0 and start scan
18. Now type in "arp" in the filters to only retrieve arp messages. Take note of the MAC addresses compared to the IP's. Also take note of the frequency of said messages
19. Now go to VM2 and repeat Step 7
20. Go back to VM1 and now type in a filter "ip.src==&&http" to get all http requests to server. You should notice there being 2 HTTP requests sent from VM2 to VM3. However, take note of the MAC addresses. One of the requests should go from VM2 to VM1 and the next should go to from VM1 to VM3. If this is the case, you know we see a successful ARP poisoning.
21. Repeat step 20, just flip make VM3 the source IP and analyze all HTTP responses outgoing from the server. Similar idea, there should be two – one going from VM3 to VM1 and another going from

VM1 to VM2, but both in the name of VM3 to VM2 in the sniffed packets frame.

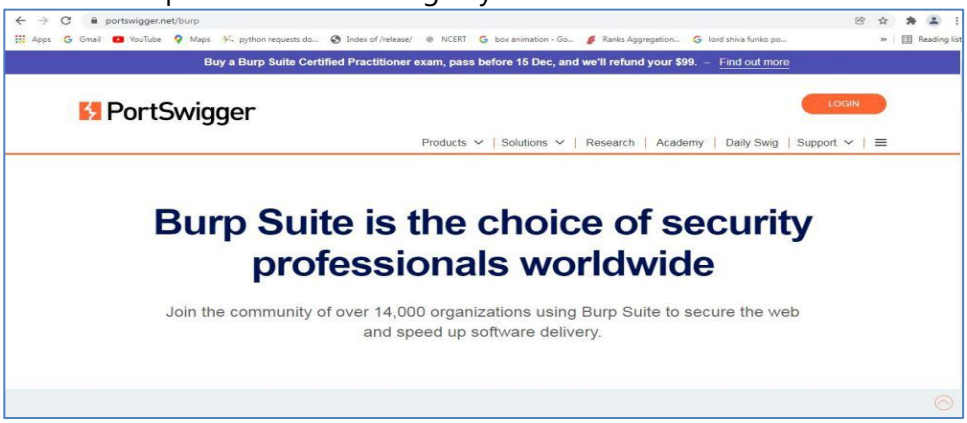
22. Congrats, you now know how to successfully ARP poison

10. Performing security testing of web applications using Burp Suite toolkit.

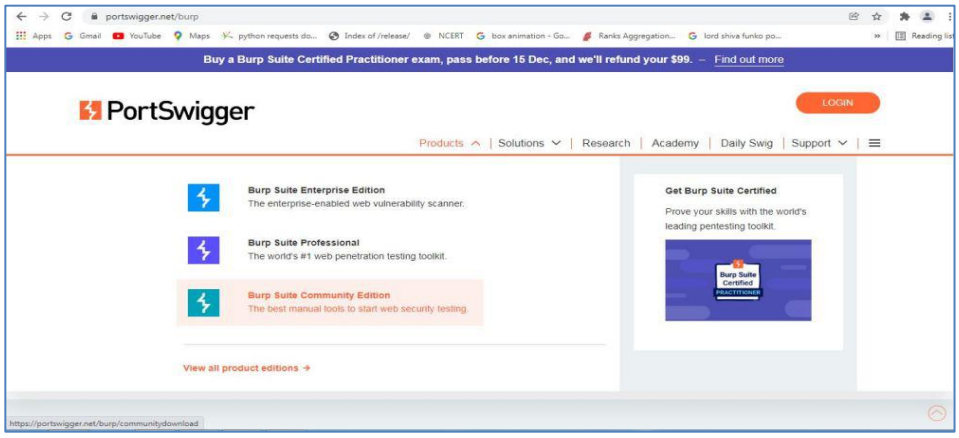
10.1 Installing Burp Suite on Windows:

Follow the below steps to install Burp Suite on Windows:

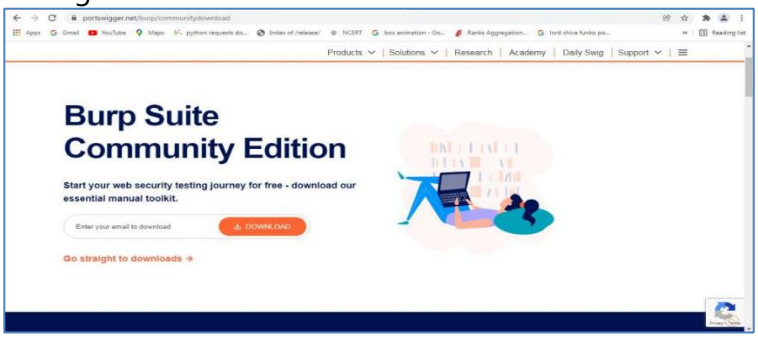
Step 1: Visit the official Burp Suite website using any web browser.



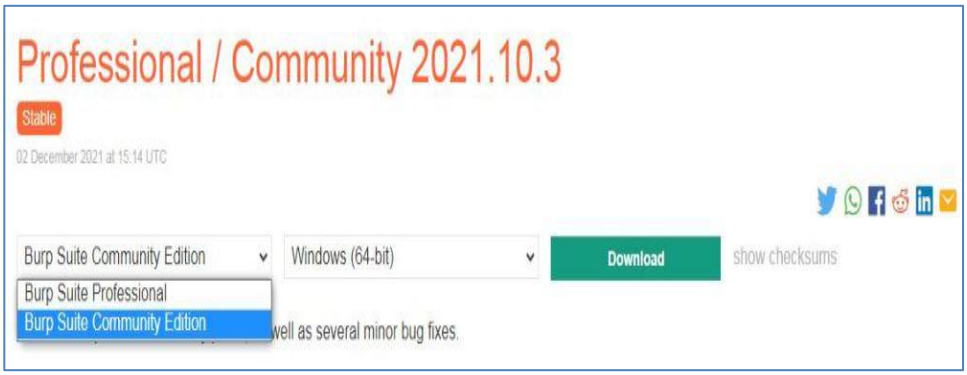
Step 2: Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.

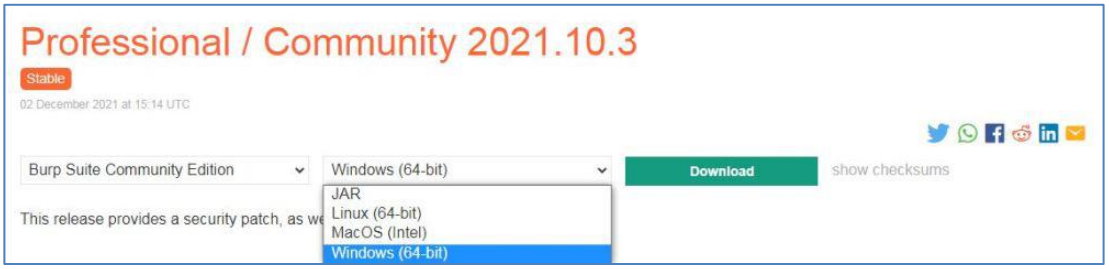


Step 3: New webpage will open, which will ask for email id, and other option is Go Straight to downloads. Click on Go straight to downloads.

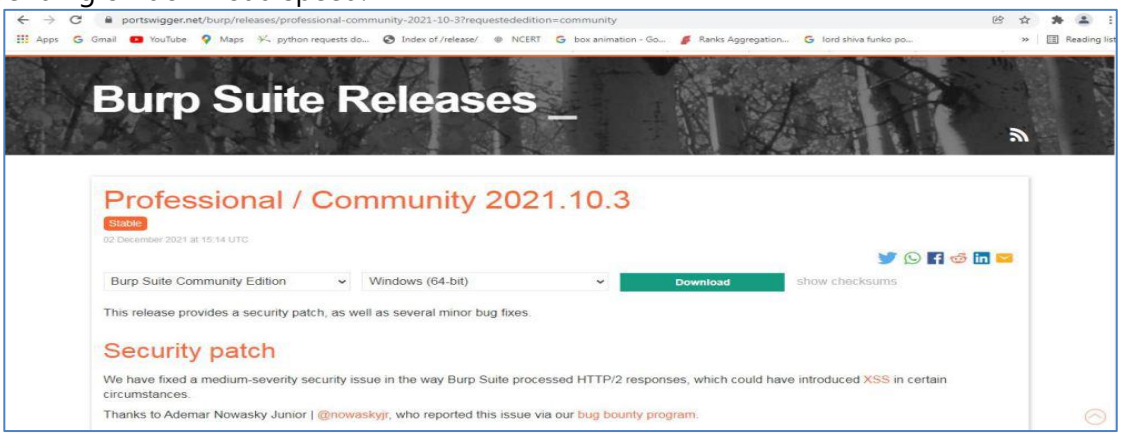


Step 4: After clicking on Go straight to downloads new webpage will open which will contain two versions of burp suite one is Burp suite community edition and the other is burp suite professional along with compatibility for different operating systems.

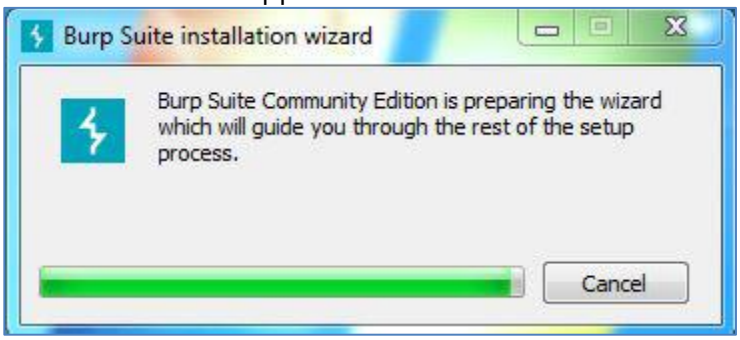




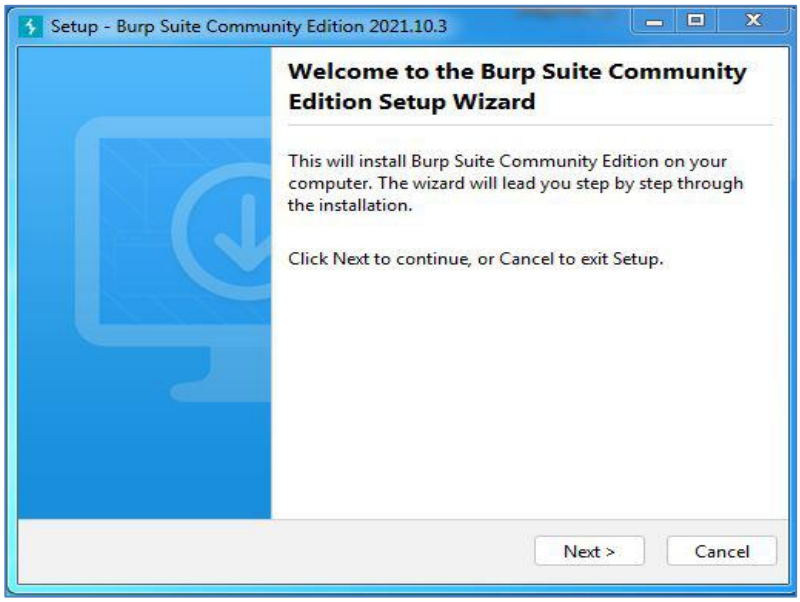
Step 5: Choose Burp suite Community Edition along with Windows (64-bit). Click on the download button, downloading of the executable file will start shortly. It is a big 210 MB file that will take some time depending on download speed.



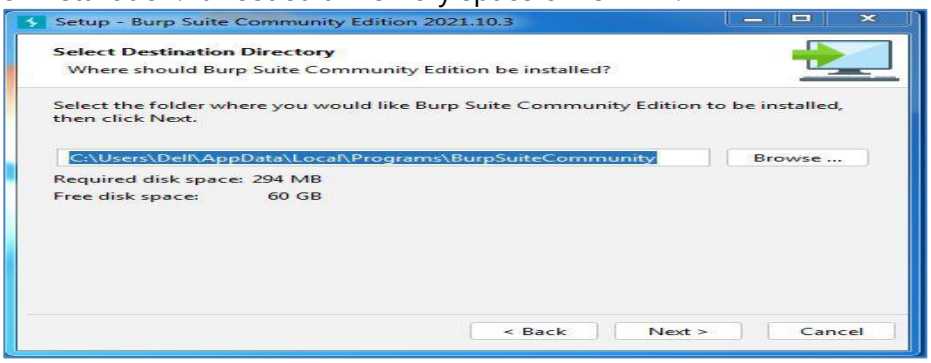
Step 6: Now check for the executable file in downloads in your system and run it.
Step 7: Loading of Installation Wizard will appear which will take a few seconds



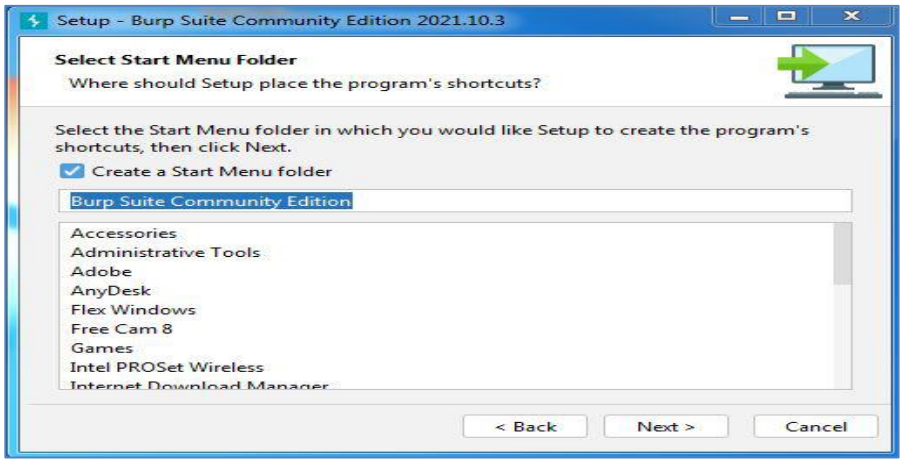
Step 8: After this Setup screen will appear, click on Next.



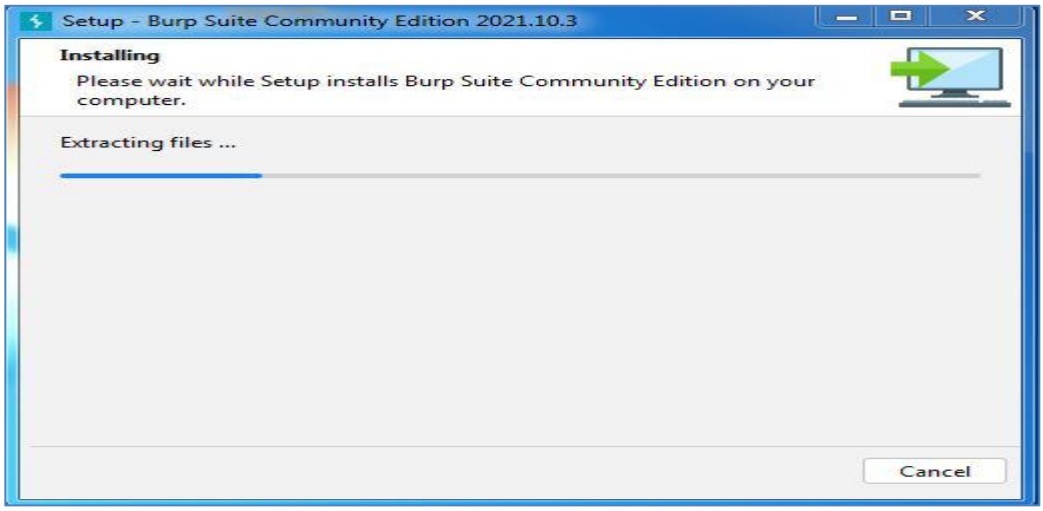
Step 9: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.



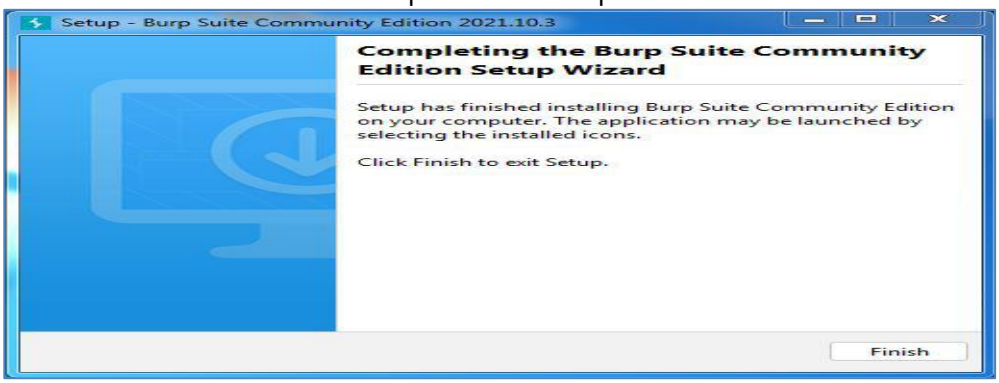
Step 10: Next screen will be of choosing Start menu folder so don't do anything just click on Next Button.



Step 11: After this installation process will start and will hardly take a minute to complete the installation.

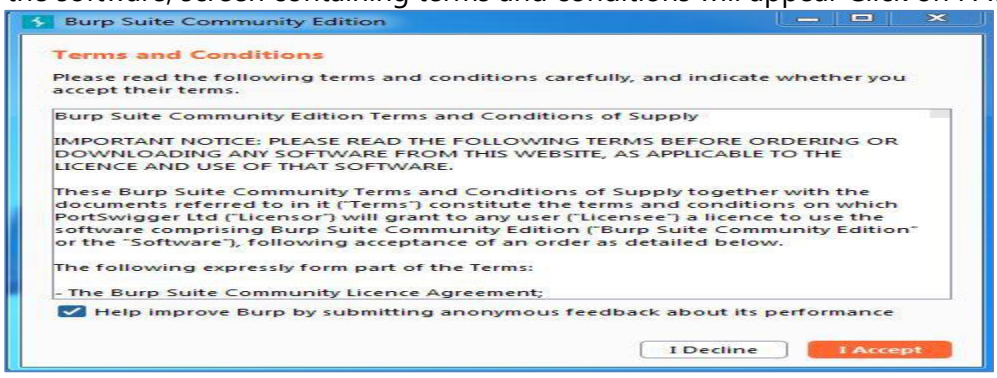


Step 12: Click on Finish after the installation process is complete.

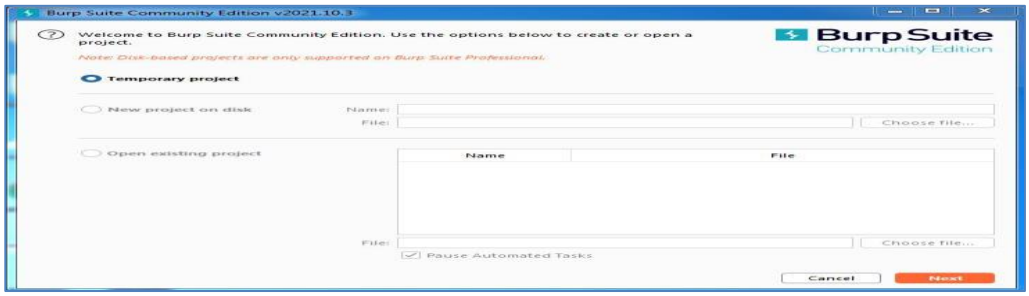


Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop.

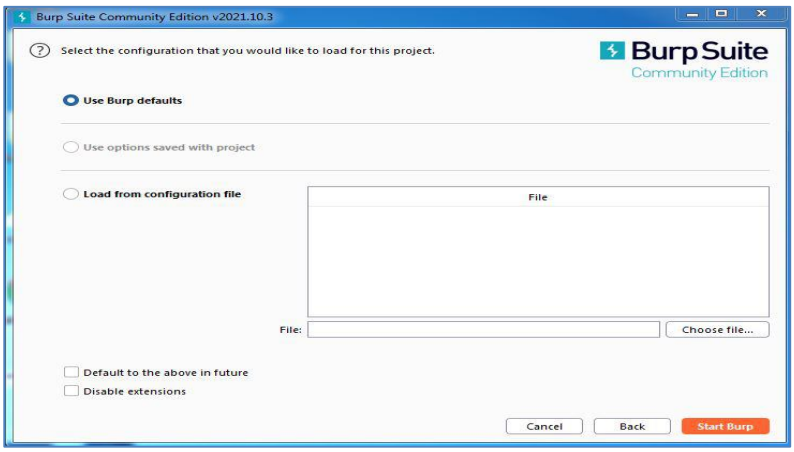
Step 14: Run the software, screen containing terms and conditions will appear Click on I Accept.



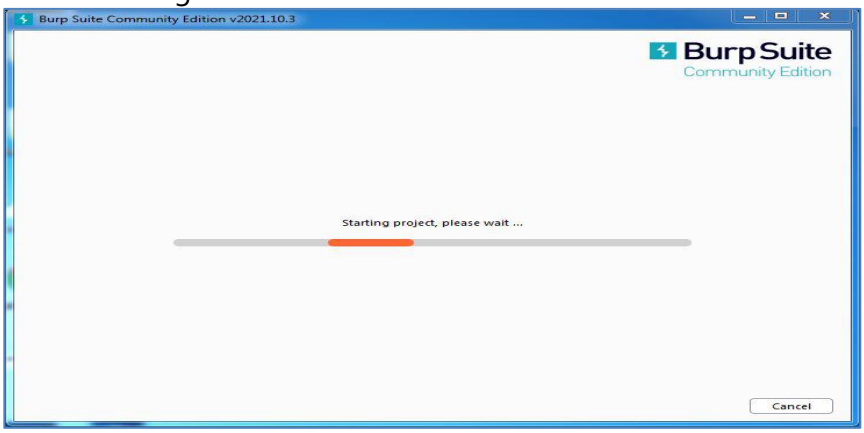
Step 15: New screen containing information regarding the project will appear, choose temporary project and click Next.



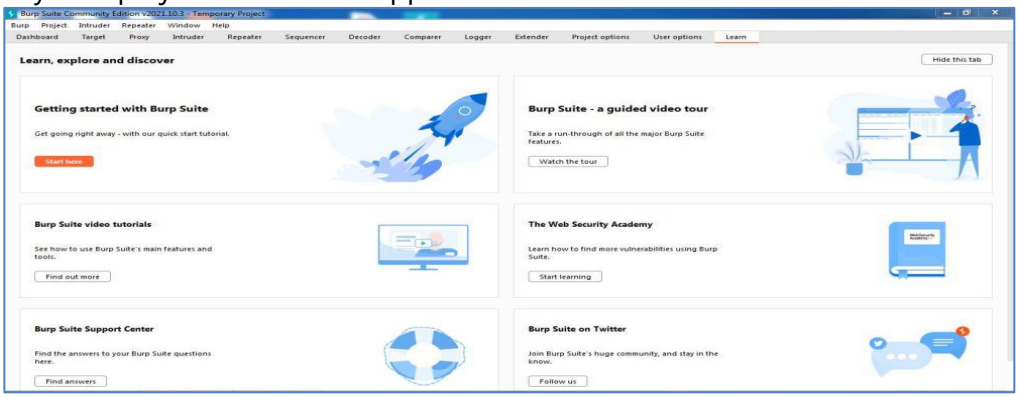
Step 16: Next screen is about using default settings or loading from configuration file, click on Use Burp Defaults.



Step 17: Project will start loading.

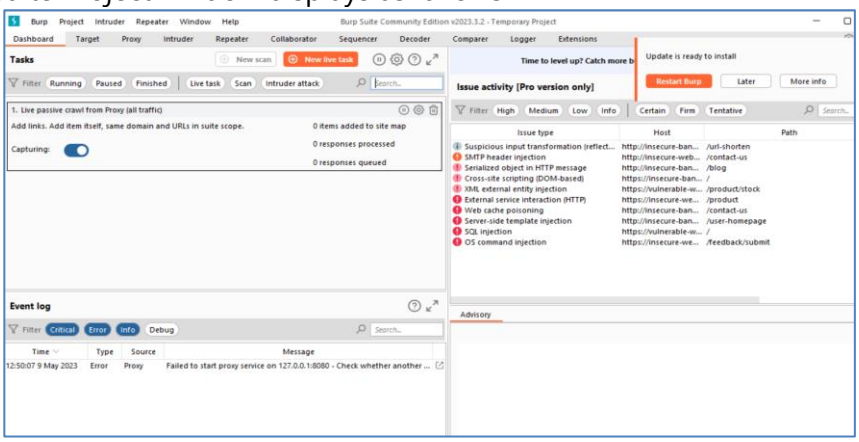


Step 18: Finally new project window will appear.

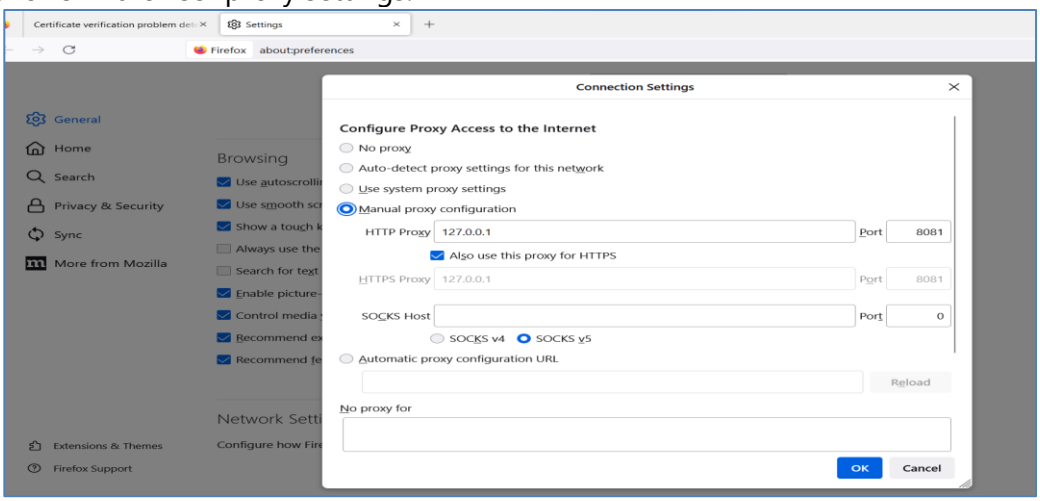


Process for performing security testing:

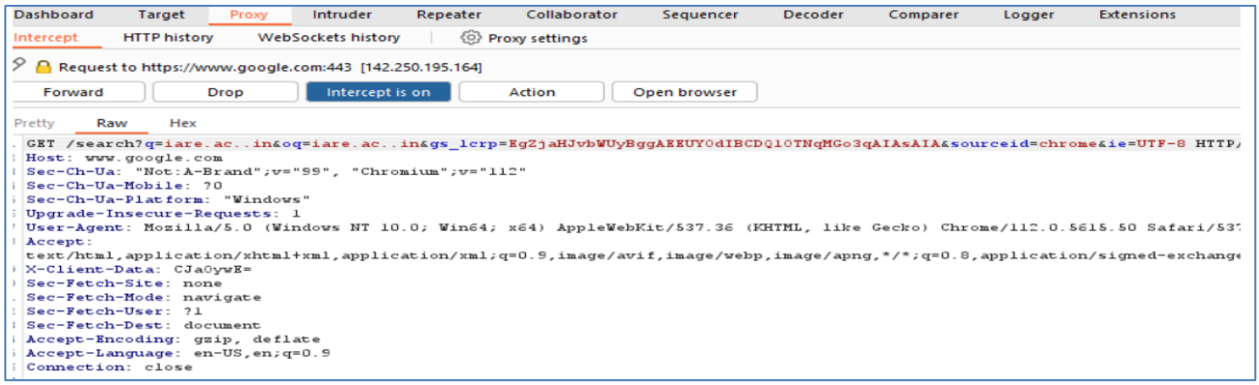
- Open Burp suite application on your desktop / Laptop
- By default, selected as “Temporary project” for project selection
- Click on next
- Use by default “burp defaults”
- Click on start burp
- Now burp suite Project window displays as fallows



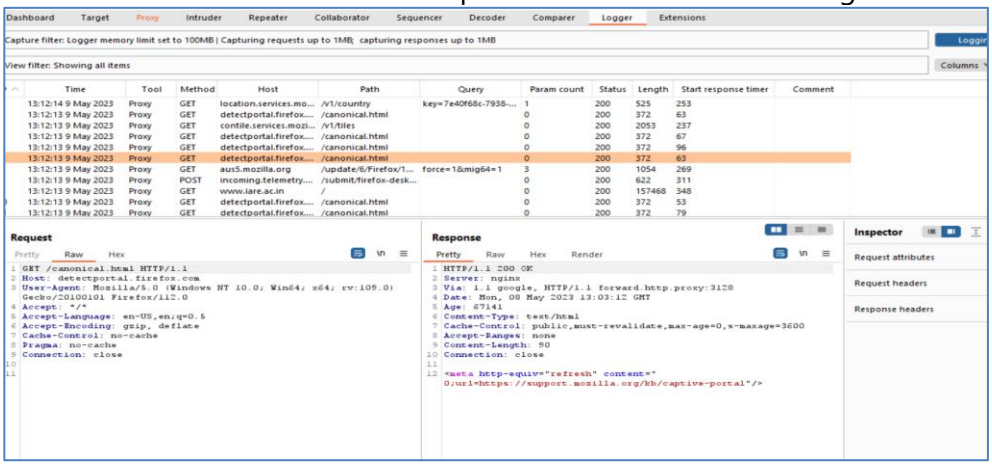
- Open “proxy” tab on menu
- Check “intercept” is on / off
- If intercept is “off” make it as “on”
- Check proxy with proxy address
- As fallows in browser proxy settings.



- Once intercept is “on”
- Go to the target menu
- Open any browser
- After open browser event log will be recorded.
- Give any target
- Record the response as shown in below



Check and observe all the menus for different responses based on different targets



Try:
Use Collaborator, Sequencer to find the issues on activity of target

Hint:
Click on the menu's called Collaborator and Sequencer, perform scans the issues for report.

11. Install and Perform Web Applications Testing On Attacks Using Owasp Zap Tool

11.1 Owasp Zap Installation process

Step1: go to the official site of OWASP ZAP and visit downloads on site as shown in below

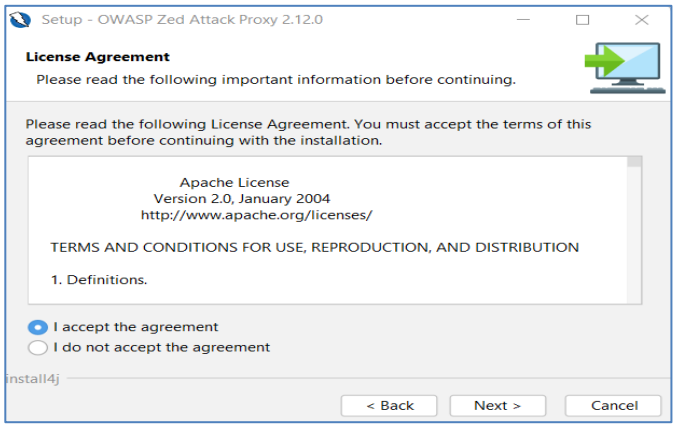
OWASP ZAP – Download (zaproxy.org)

Step2: click on download by choosing the operating system

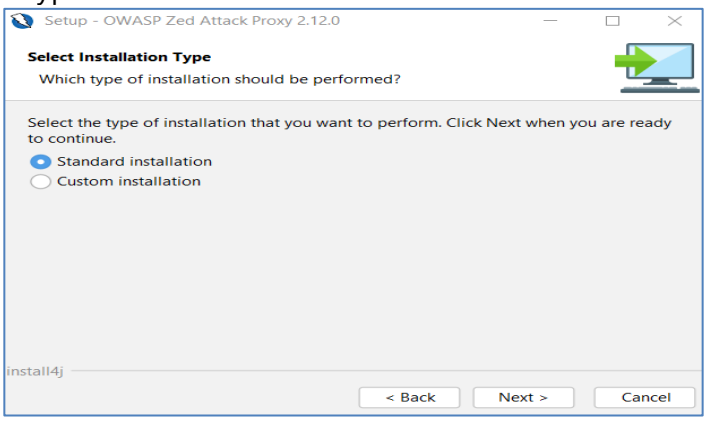
Step3: after downloaded tool in your system double click on that setup file

Step4: click on next

Step5: accept the terms and conditions and click on next



Step6: choose installation type “standard” and click on “next”



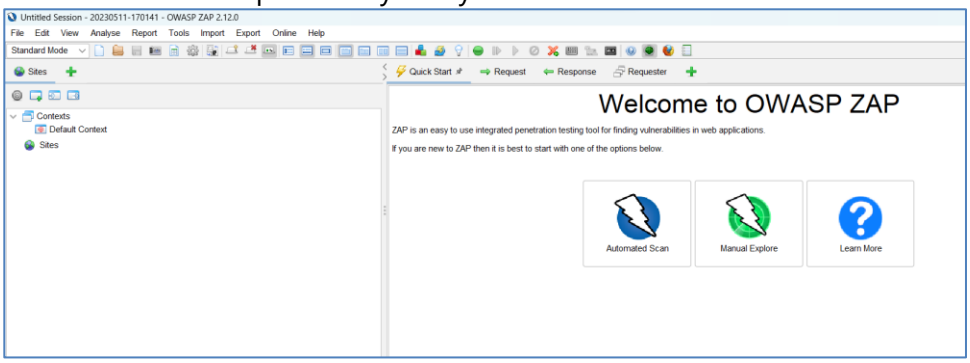
Step7: installation process being started and displays finish window once it is completed

Step 8: click on finish to complete installation.

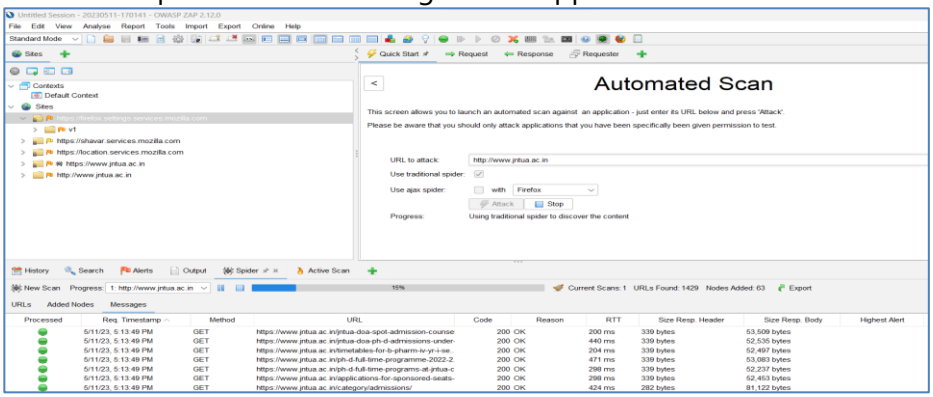
11.2 Perform Web application testing

Automated

After installation of OWASP ZED open it on your system as shown in below

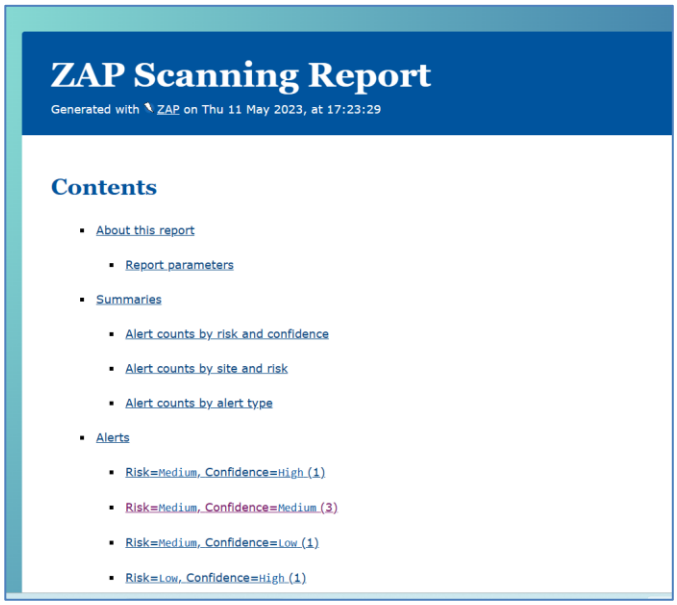


Click on automated scan to perform the scanning of web application



During scanning of the process just pause the scan process and right click on any url to see content
To see content rightclick on URL and select “open URL in browser” as shown in below

After completing scanning, it shows the history of scanned results
Generate the reports as shown in below



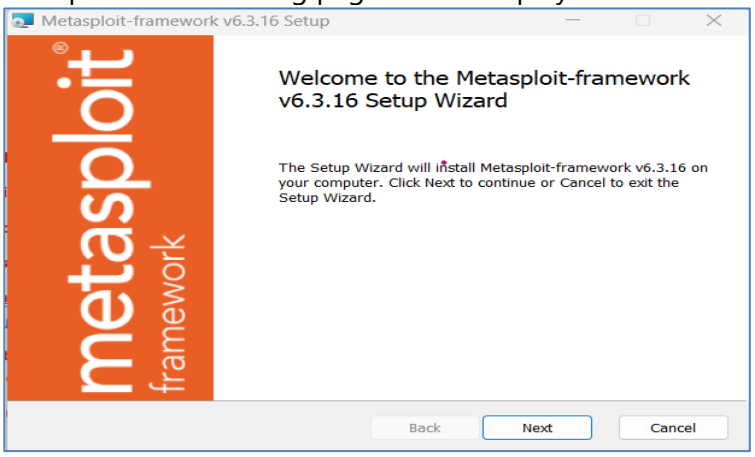
Try:
Perform web application testing In manual mode using Owasp Zap

Hint:
Select the option in manual for any target and perform web application testing.

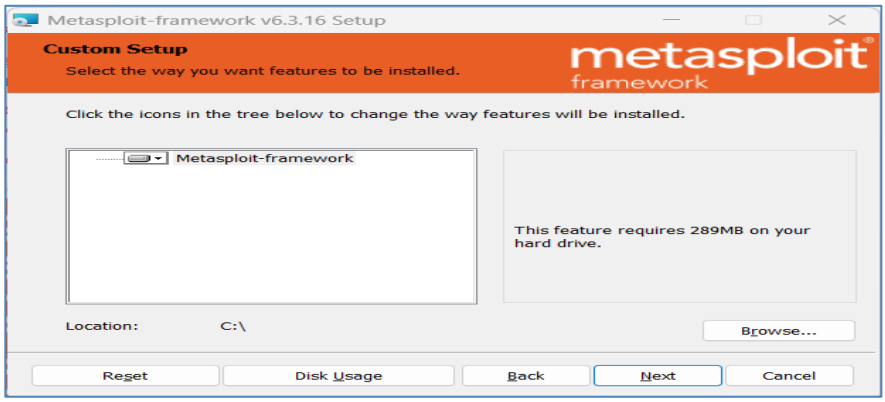
12. Install meta sploit framework tool to perform various exploitation tasks about the security vulnerabilities of a target machine

12.1 Installation of Metasploit framework

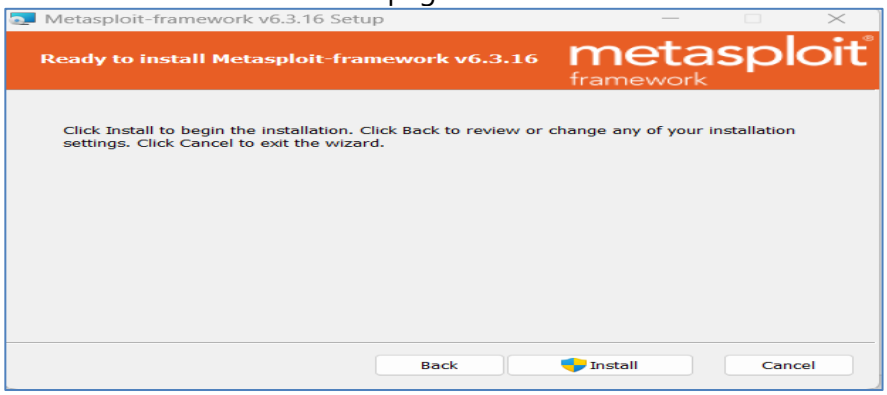
Step1: To install Metasploit framework tool go to official site https://www.metasploit.com/ and Click on download
Step2: it is redirected to github page and click on nightly installer.html file
Step3: again it is redirected to https://docs.metasploit.com/docs/using-metasploit/getting-started/nightly-installers.html this link
step 4: in the above link select "latest windows installer" on that page now the setup file will be downloaded**.**
Step 5: double click on setup file the fallowing page will be displays



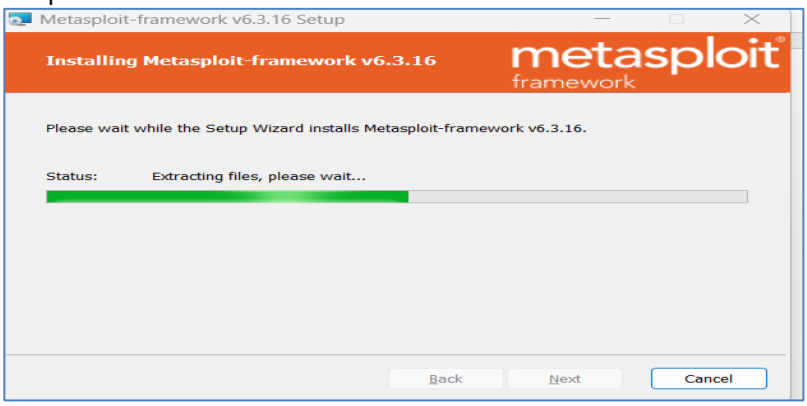
Step 6: click on "next" and accept terms and conditions on that page, click on next
Step 7: choose the location to store the installation as shown in below



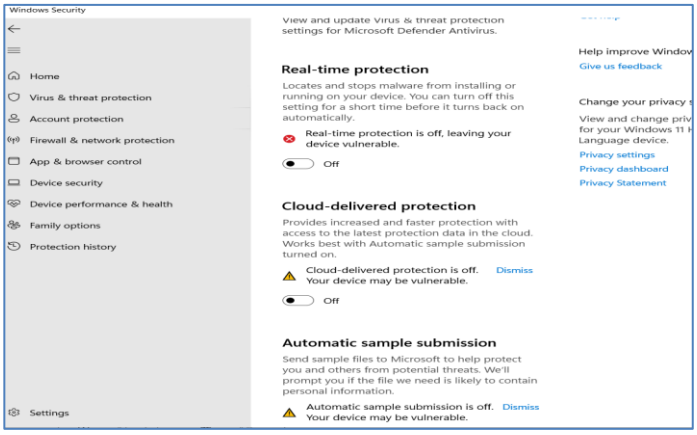
Step 8: click on next and click on install on this page



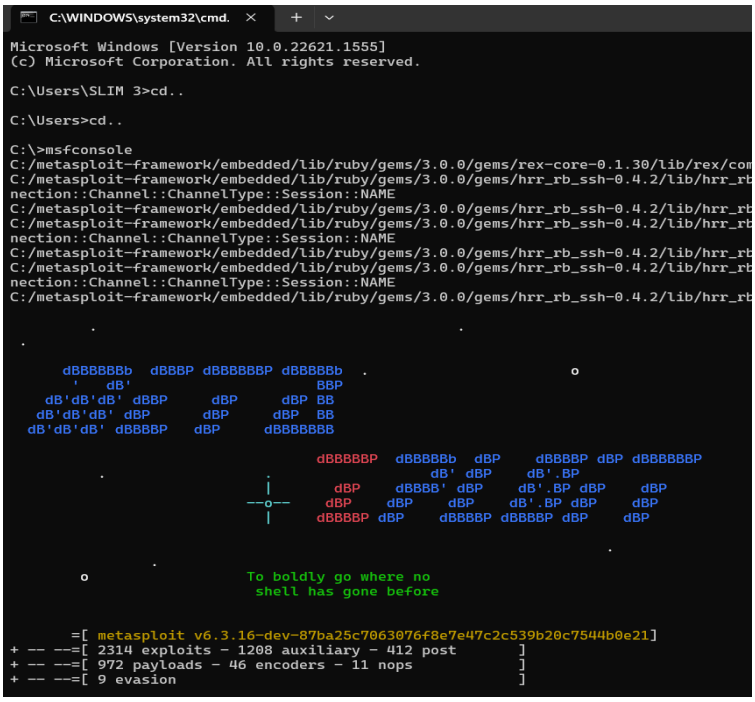
Step 9: now installation process is started as shown in below



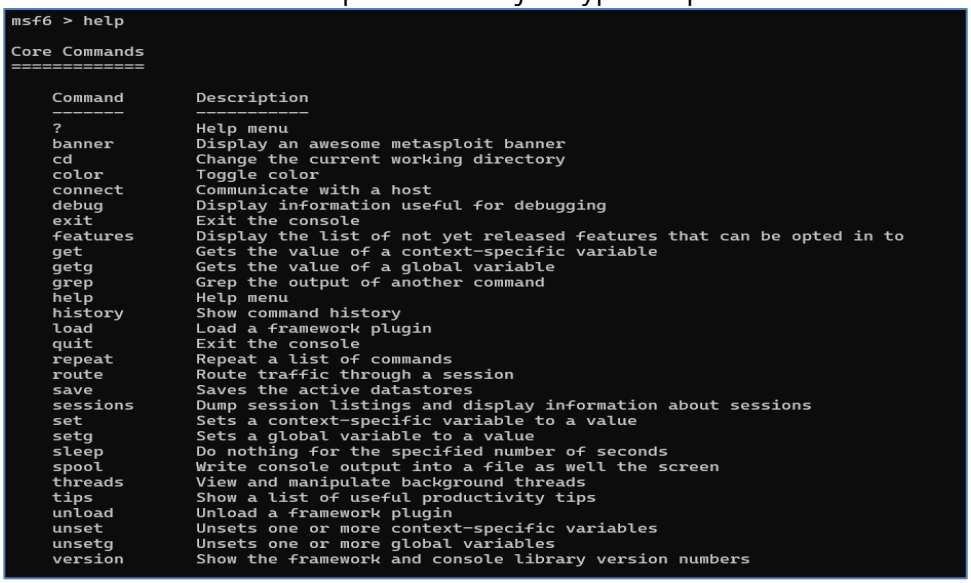
Step 10: after install click on finish to setup has been complete.
(Note: during the installation if any messages u got, we have to do " off" all virus and threat protections on your system)



Now Metasploit framework has been installed on your system.
After installation
Go to the Metasploit frame work folder that installed on your system
Step 11: copy the path upto bin folder as like “C:\metasploit-framework\bin”
Step 12: set path for installed framework
Step 13: To set the path Edit system environment variables on your PC by right clicking on it.
Step 14: Give system variables as “Path” and the value of Path” C:\metasploit-framework\bin”
That we copied from installed location
Step 15: Click on Ok to complete the path setup
Step 16: now open the command prompt to launch frame work
Type “msfconsole” on command window as shown in below



Step 17: to see the commands on Metasploit window just type “help” on window



Step 18: type any of the command that you want to see information about that all.
Step 19: to exit from frame work just type “exit” on screen”.

Try:

Find threads and sessions of the target that using on the same machine.

Hint:

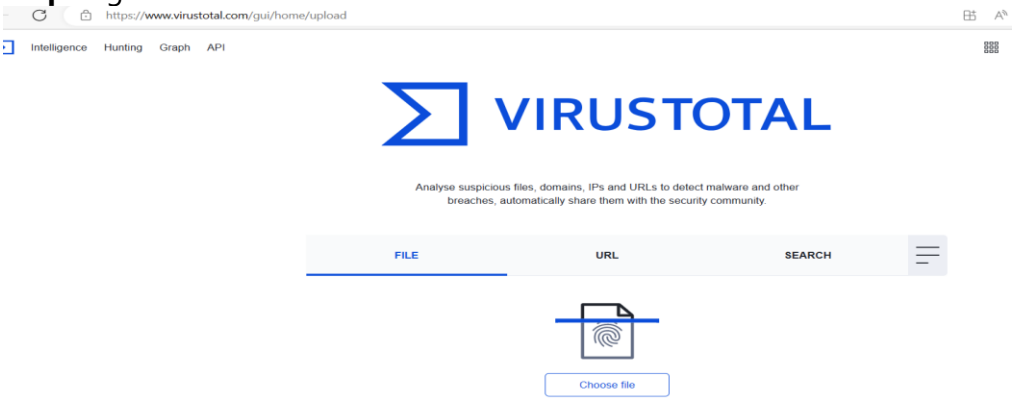
Use Metasploit tool options to find both on target machine.

.

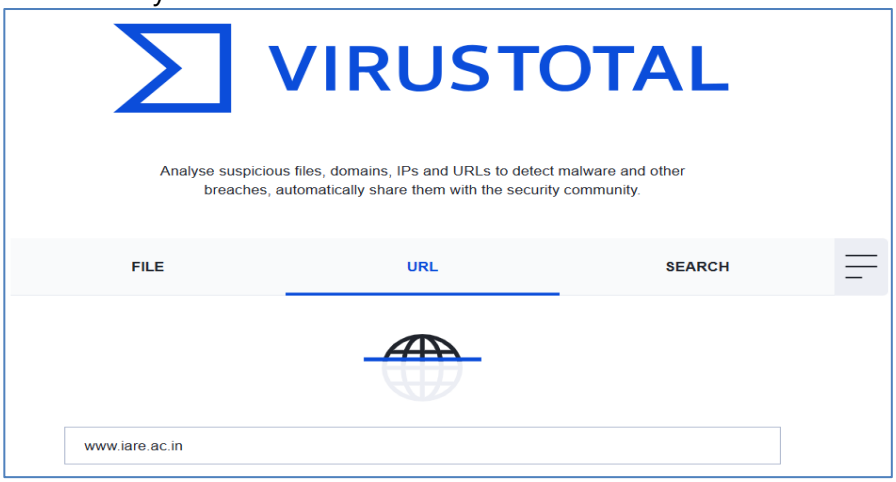
13. Use virus total tool to analyzes files and urls for viruses on target.

13.1 How to use Virus total tool

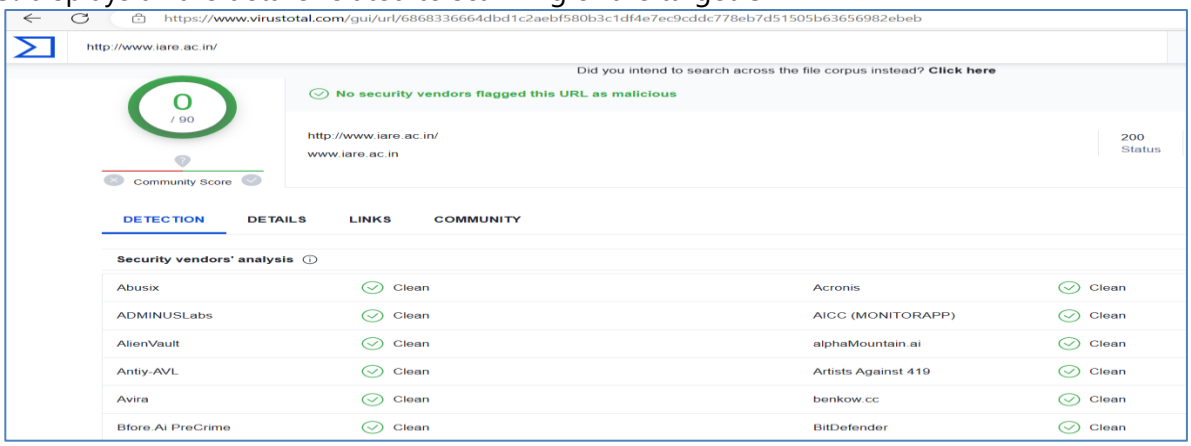
Step 1: go to virus total official site on online



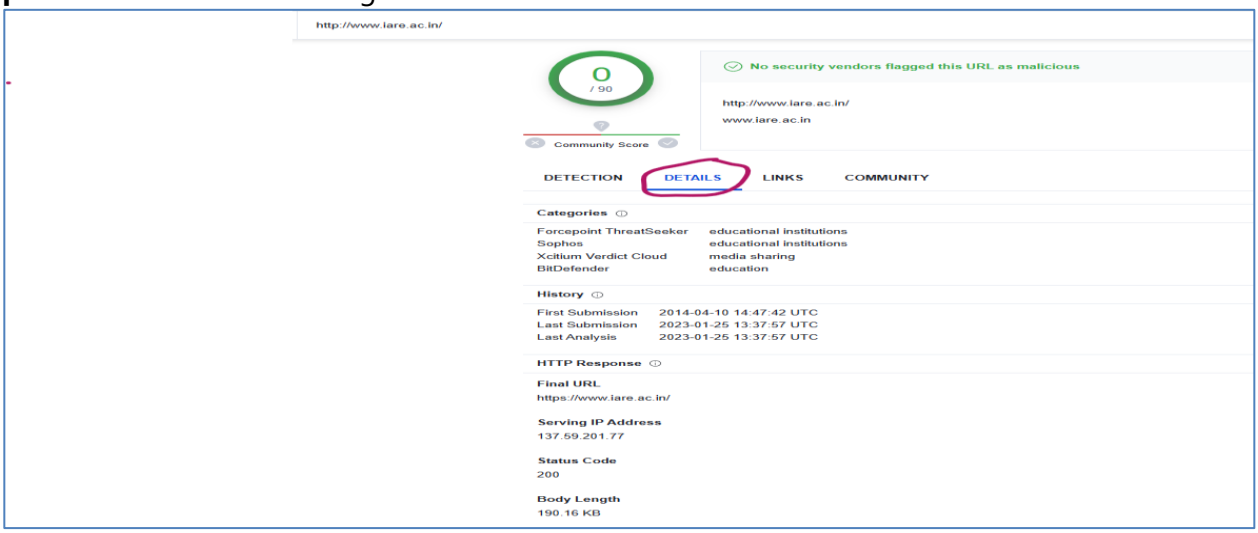
Step 2: upload any files that you downloaded from internet to find viruses and analysis on it
Step 3: select URL to give target to find viruses or not
Step 4: enter the URL to analyze viruses on files and urls



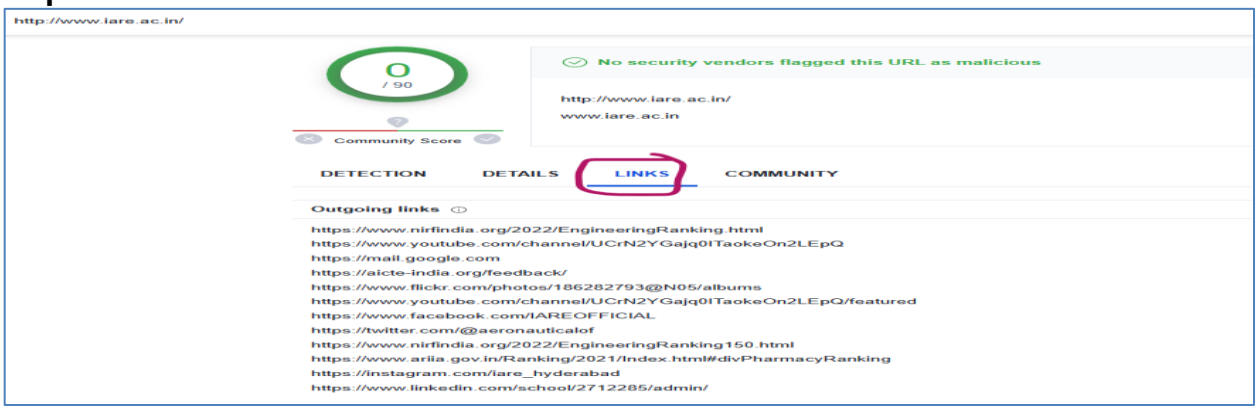
Step 5: displays all the details related to scanning of the target URL



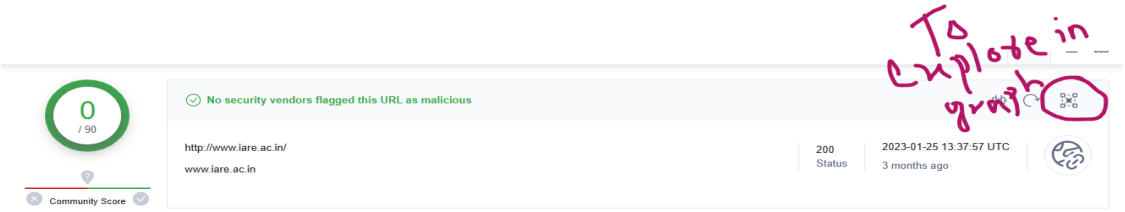
Step 6: if any virus detection, then it displays as a count .so from above figure no detection found.
Step 7: to see details of the target click on details as shown in below



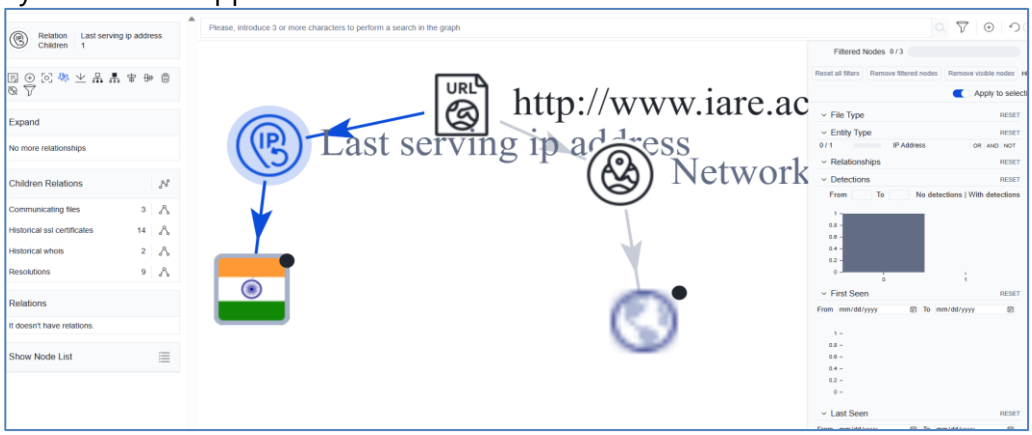
Step 8: to see links that tool have scanned click on "links" as shown in below



Step 9: To explore in graph click on "explore" which appears on right corner of window as shown in below



Step 10: analyze all details appear on window.



Try:

Use different target network to analyze suspicious files on target

Hint:

Give different targets address or IP addresses.

V. REFERENCES:

1. RafayBaloch, “Ethical Hacking and Penetration Testing Guide”, CRC Press, 2015.
2. Dr.Patrick Engebretson, “The Basics of Hacking and Penetration Testing”, Syngress Publications Elseveir, 2013.
3. Prakhar Prasad, “Mastering Modern Web Penetration Testing”, Packt Publishing, 2016.
4. Gilberto Najera Gutierrez, “Kali LinuxWeb Penetration Testing”, Cookbook, 2016.
5. Robert Svensson, “From Hacking to Report Writing: An Introduction to Security and Penetration Testing”, 2016.

VI. MATERIALS ONLINE:

1. Course Content
2. Lab Manual