

A large, semi-transparent watermark with the letters 'HIT' is visible across the center of the page.

# **REPORT OF VULNERABILITY ANALYSIS**

**MODULE - 5**

Aniket Sunil Pagare

---

## **Table of Contents: Vulnerability Analysis**

---

### **1. Vulnerability Analysis**

- 1.1 Definition
  - 1.2 Severity Levels of Vulnerabilities
- 

### **2. Vulnerability Analysis Using Acunetix**

- 2.1 Definition
  - 2.2 Perform Activity Using Acunetix
- 

### **3. Vulnerability Analysis Using Nikto**

- 3.1 Definition
  - 3.2 Perform Activity Using Nikto
- 

### **4. Vulnerability Analysis Using MBSA (Microsoft Baseline Security Analyzer)**

- 4.1 Definition
  - 4.2 How to Download MBSA
  - 4.3 Perform Activity Using MBSA
- 

### **5. Vulnerability Analysis Using Nessus**

- 5.1 Definition
  - 5.2 How to Download Nessus
  - 5.3 Perform Activity Using Nessus
-

## **6. Vulnerability Analysis Using Checkmarx ZAP**

- 6.1 Definition
  - 6.2 Perform Activity Using Checkmarx ZAP
- 

## **7. Vulnerability Analysis Using Global Network Inventory**

- 7.1 Definition
  - 7.2 Perform Activity Using Global Network Inventory
- 

### **Extra Activity**

## **8. Vulnerability Analysis Using Smart Scanner**

- 8.1 Definition
  - 8.2 How to Download Smart Scanner
  - 8.3 Perform Activity Using Smart Scanner
- 

## **9. Vulnerability Analysis Using Qualys SSL Labs**

- 9.1 Definition
  - 9.2 Purpose of SSL Lab Scanning
  - 9.3 Key Features
  - 9.4 Perform Activity Using Qualys SSL Labs
-

# VULNERABILITY ANALYSIS

Vulnerability analysis is the process of identifying and assessing security weaknesses in networks, systems, and applications to mitigate potential threats before attackers can exploit them.

Objectives:-

- ❖ Network vulnerabilities.
- ❖ Identify security weaknesses.
- ❖ errors/vulnerabilities.
- ❖ The OS version running on computers or devices.
- ❖ Accounts with weak passwords.
- ❖ Application and services configuration .

## Types of Vulnerabilities:

Category	Examples
Software	SQL injection, buffer overflow
Network	Open ports, weak firewall rules
Configuration	Default credentials, outdated services
Web	XSS, CSRF, insecure cookies
OS-related	Unpatched OS, kernel issues

## Vulnerability Severity Levels (CVSS):

Severity	CVSS Score Range	Meaning
Low	0.1 – 3.9	Minor risk, low impact
Medium	4.0 – 6.9	Moderate risk
High	7.0 – 8.9	Serious risk
Critical	9.0 – 10.0	Immediate risk, easily exploitable

## Vulnerability Analysis Process

### 1. Asset Discovery

→ Identify systems, apps, networks to be scanned.

### 2. Vulnerability Scanning

→ Use automated tools (e.g., Nessus, Nikto, Acunetix).

### 3. Result Analysis

→ Review detected vulnerabilities and remove false positives.

### 4. Prioritization

→ Rank based on CVSS, exploitability, and business impact.

### 5. Remediation

→ Patch vulnerabilities or apply security controls.

### 6. Reporting & Monitoring

→ Document findings and continuously monitor systems.

## Popular Tools for Vulnerability Analysis

Tool	Use Case
Nessus	Deep system and network scanning
Nikto	Web server vulnerability scanner
Acunetix	Web app security testing

Tool	Use Case
<b>MBSA</b>	Windows-specific vulnerability scanning
<b>ZAP (OWASP)</b>	Manual + automated web testing
<b>Trivy</b>	Container and cloud scan tool
<b>Qualys SSL Labs</b>	SSL/TLS misconfiguration tester

HANDBOOK

# Vulnerability Analysis Using Acunetix

Acunetix is a web vulnerability scanner designed to identify and help fix security issues in websites, web applications, and APIs. It automates the process of checking for vulnerabilities

**Download link - :** <https://github.com/securi3ytalent/acunetix-13-kali-linux>

**How to use it - :**

- Step 1 -: Open kali linux / parrot OS
- Step 2 -: type git clone and paste git link
- Step 3 -: copy and paste command one by one

The screenshot shows a terminal window with a dark background. The title bar says "GitHub - securi3ytalent/acunetix-13-kali-linux". The terminal content is as follows:

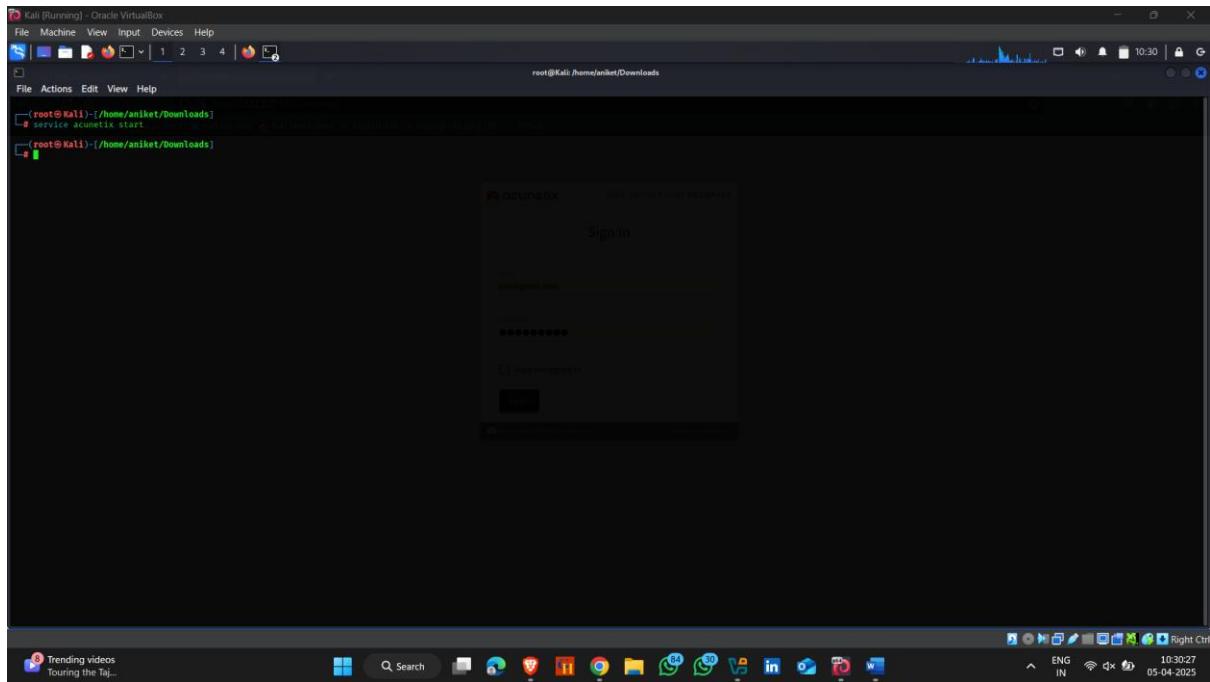
```
acunetix-13 Downloads Now:  
https://drive.google.com/drive/folders/11dmQR4xk0cgvXcTOThK0qPCLwsIdOtIm?usp=sharing  
1. open the downloads directory  
cd Downloads  
2. open the Acunetix_13 directory then  
cd Acunetix_13  
3. Need to file permutation  
chmod +x *  
4. Run command in terminal  
sudo bash ./acunetix_13.0.200217097_x64_.sh  
5. Run command in terminal  
sudo cp wvsc /home/acunetix/.acunetix/v_200217097/scanner/  
6. Run command in terminal
```

On the right side of the terminal window, there is a sidebar with repository information:

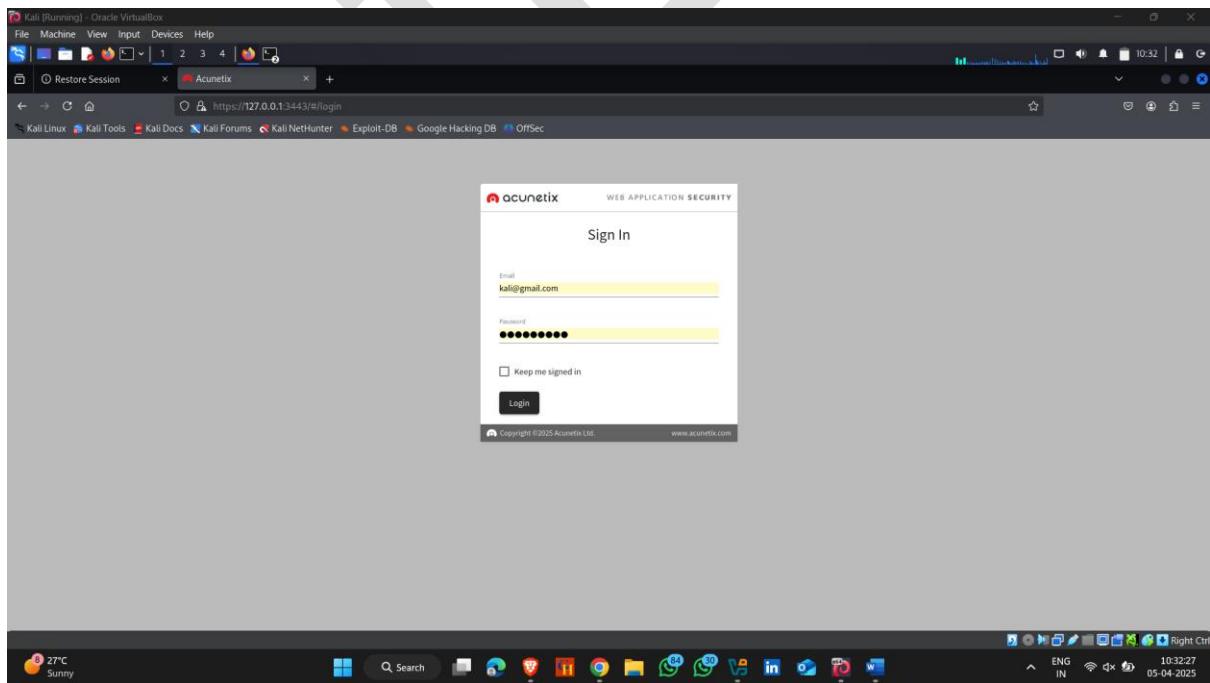
- Readme
- Activity
- 67 stars
- 2 watching
- 30 forks
- Report repository

Below that is a "Releases" section which says "No releases published". At the bottom, there is a "Packages" section which also says "No packages published".

- Start Acunetix using **service acunetix start**



- Now open a firefox and type in url section  
[\*\*https://127.0.0.1:3443\*\*](https://127.0.0.1:3443)
- Enter email and password that you enter on installation process



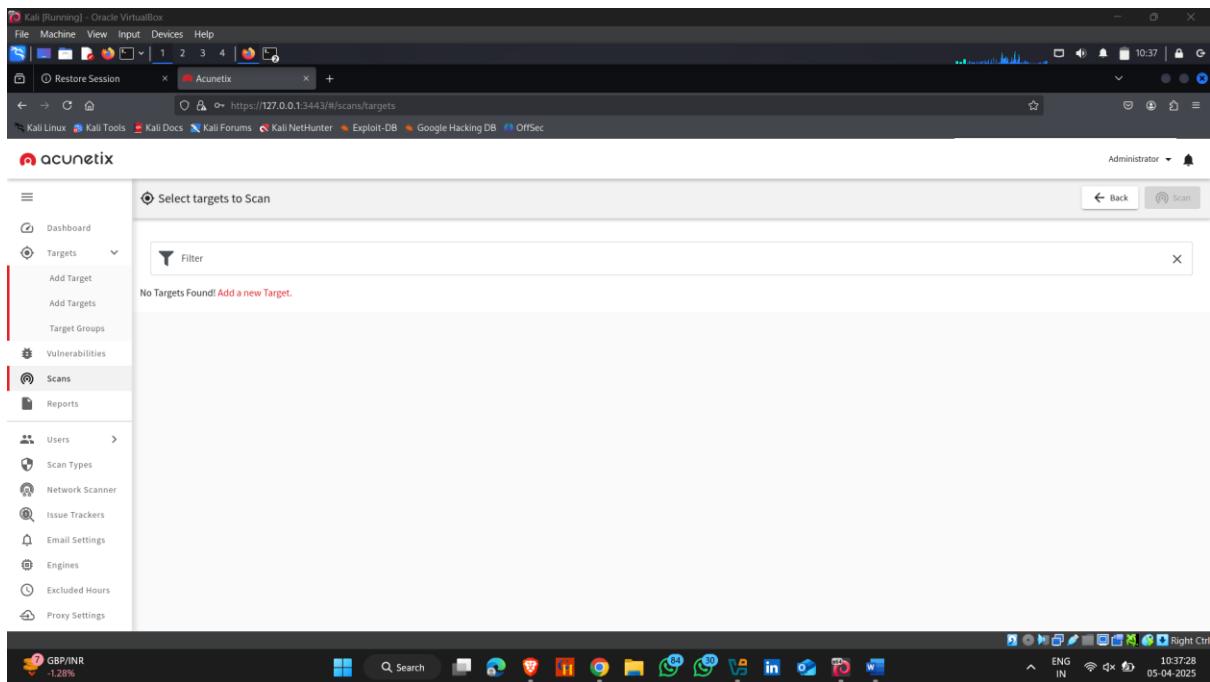
- Successfully login in acunetix

The screenshot shows the Acunetix dashboard. On the left is a sidebar with navigation links like Dashboard, Targets, Vulnerabilities, Scans, Reports, Users, Scan Types, Network Scanner, Issue Trackers, Email Settings, Engines, Excluded Hours, and Proxy Settings. The main area has three large circular summary metrics: one red circle with '1' labeled 'High Severity Vulnerabilities', one orange circle with '4' labeled 'Medium Severity Vulnerabilities', and one blue circle with '1' labeled 'Low Severity Vulnerabilities'. Below these are smaller statistics: 'Scans Running: 0', 'Scans Waiting: 0', 'Total Scans Conducted: 1', 'Open Vulnerabilities: 6', and 'Total Targets: 1'. There are also sections for 'Most Vulnerable Targets' (listing https://certifiedhacker.com/) and 'Top Vulnerabilities' (listing 'HTML form without CSRF protection', 'Directory listing', and 'Possible database backup'). The bottom of the screen shows a Windows taskbar with various icons and system status.

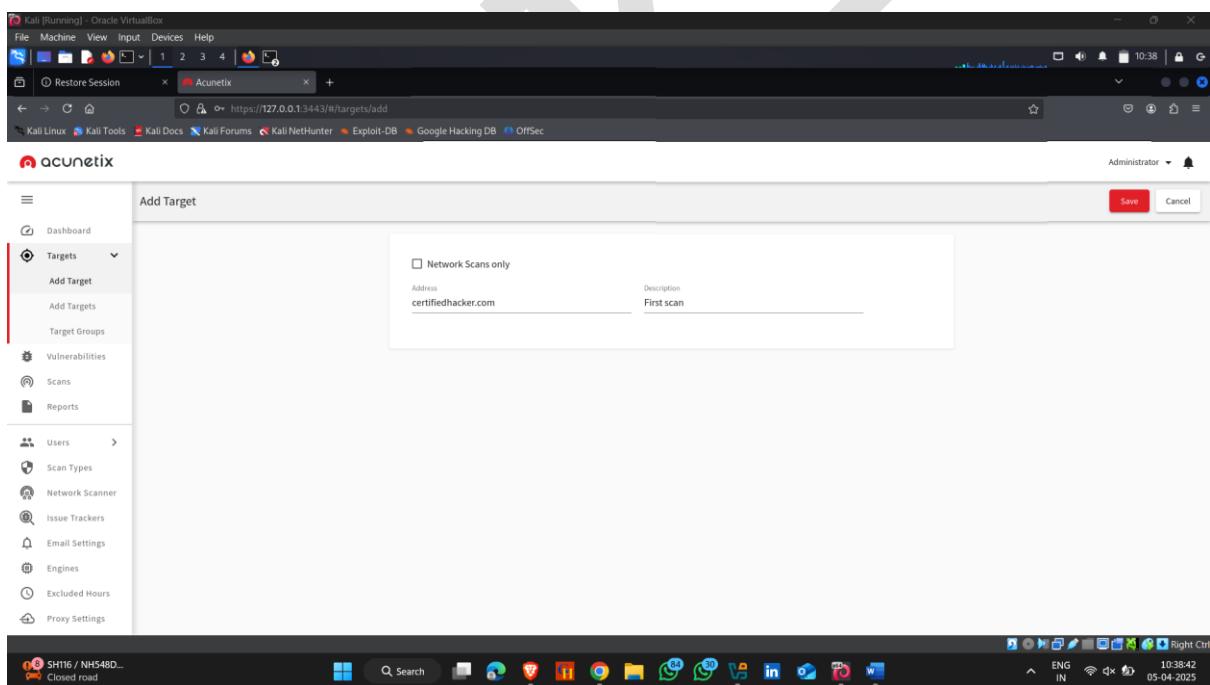
- Then click on scan and then click on new scan

The screenshot shows the 'Scans' page in Acunetix. The sidebar is identical to the dashboard. The main area is titled 'Scans' and includes a 'New Scan' button. Below it is a table with columns for Target, Scan Type, Schedule, Vulnerabilities, and Status. A 'Filter' search bar is at the top of the table. The bottom of the screen shows a Windows taskbar with various icons and system status.

- And then click on add new target



- Enter domain name or website name and click on save



- Click on scan

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Restore Session Acunetix

<https://127.0.0.1:3443/#/targets/113fb686-3741-4627-83c0-366d862b4a88>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Administrator

acunetix

Dashboard Targets Add Target Add Targets Target Groups Vulnerabilities Scans Reports Users Scan Types Network Scanner Issue Trackers Email Settings Engines Excluded Hours Proxy Settings Watchlist Ideas

certifiedhacker.com

Administrator

Scan Save

Target Information

Description: First scan

Business Criticality: Normal

Scan Speed: 10 Concurrent Requests, 0ms Request Delay

Slower Slow Moderate Fast

Continuous Scanning:

Site Login:

AcuSensor:

Crawling

ENG IN 10:40:09 05-04-2025

- Here , scanning start

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Restore Session Acunetix

<https://127.0.0.1:3443/#/scans/73168b40-ed3e-4650-b3bc-d173e6085f93/info>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Administrator

acunetix

Dashboard Targets Vulnerabilities Scan Reports Users Scan Types Network Scanner Issue Trackers Email Settings Engines Excluded Hours Proxy Settings About Help Watchlist Ideas

Scan

Scan Information Vulnerabilities Site Structure Events

Stop Scan Pause Scan Generate Report WAF Export

Acunetix Threat Level 2

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.

MEDIUM

Scan Duration: 0m 15s Requests: 5 Average Response Time: 2,723ms Locations: 2

Overall Progress: In Progress 0%

Start URL changed (initial request to http://certifiedhacker.com/ was redirected to https://certifiedhacker.com/)

Scanning of certifiedhacker.com started

Antivirus not found

Target Information: Address: certifiedhacker.com, Server: nginx/1.25.5, Operating System: Unknown, Identified Technologies: Unknown, Responsive: Yes

Latest Alerts: Slow HTTP Denial of Service Attack (Apr 5, 2025, 10:40:46 AM)

No Hosts Discovered

ENG IN 10:40:55 05-04-2025

- You can also check which vulnerability are till find , just click on **vulnerability option**

The screenshot shows the Acunetix web application scanner interface. The main window displays a table of vulnerabilities found during a scan of the website <https://certifiedhacker.com/>. The table includes columns for Severity, Vulnerability, URL, Parameter, Status, and Confidence %. There are nine entries listed, ranging from possible database backups to Clickjacking issues.

Severity	Vulnerability	URL	Parameter	Status	Confidence %
!	Possible database backup	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>		Open	95
!	Directory listing	<a href="https://certifiedhacker.com/ja/">https://certifiedhacker.com/ja/</a>		Open	100
!	Directory listing	<a href="https://certifiedhacker.com/ja/source/">https://certifiedhacker.com/ja/source/</a>		Open	100
!	HTML form without CSRF protection	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>	<empty>	Open	80
!	HTML form without CSRF protection	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>	<empty>	Open	80
!	Slow HTTP Denial of Service Attack	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>		Open	95
!	Clickjacking: X-Frame-Options header missing	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>		Open	95
!	Content Security Policy (CSP) not implemented	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>		Open	95
!	Password type input with auto-complete enabled	<a href="https://certifiedhacker.com/">https://certifiedhacker.com/</a>	<empty>	Open	95

- Scan completed

The screenshot shows the Acunetix web application scanner interface after the scan has completed. The main window displays the following sections:

- Acunetix Threat Level 3**: A large red circle with the word "HIGH" indicating a high severity threat level. Below it, a message states: "One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website."
- Activity**: A timeline of events with their status (Completed). It includes:
  - Overall Progress: 100% completed
  - Start URL changed (initial request to <http://certifiedhacker.com/> was redirected to <https://certifiedhacker.com/>)
  - Scanning of certifiedhacker.com started
  - Antivirus not found
  - Scanning of certifiedhacker.com completed
  - Login forms were detected but LSR or Autologin are not being used
- Scan Duration**: 40m 9s
- Requests**: 5,887
- Average Response Time**: 876ms
- Locations**: 56
- Target Information**: Details about the target address (certifiedhacker.com), operating system (nginx/1.25.5 Unknown), and technologies (Yes).
- Latest Alerts**: A list of recent findings:
  - Vulnerable Javascript library
  - Login page password-guessing attack
  - Directory listing
  - Directory listing
  - Possible database backup

# Vulnerability Analysis Using Nikto

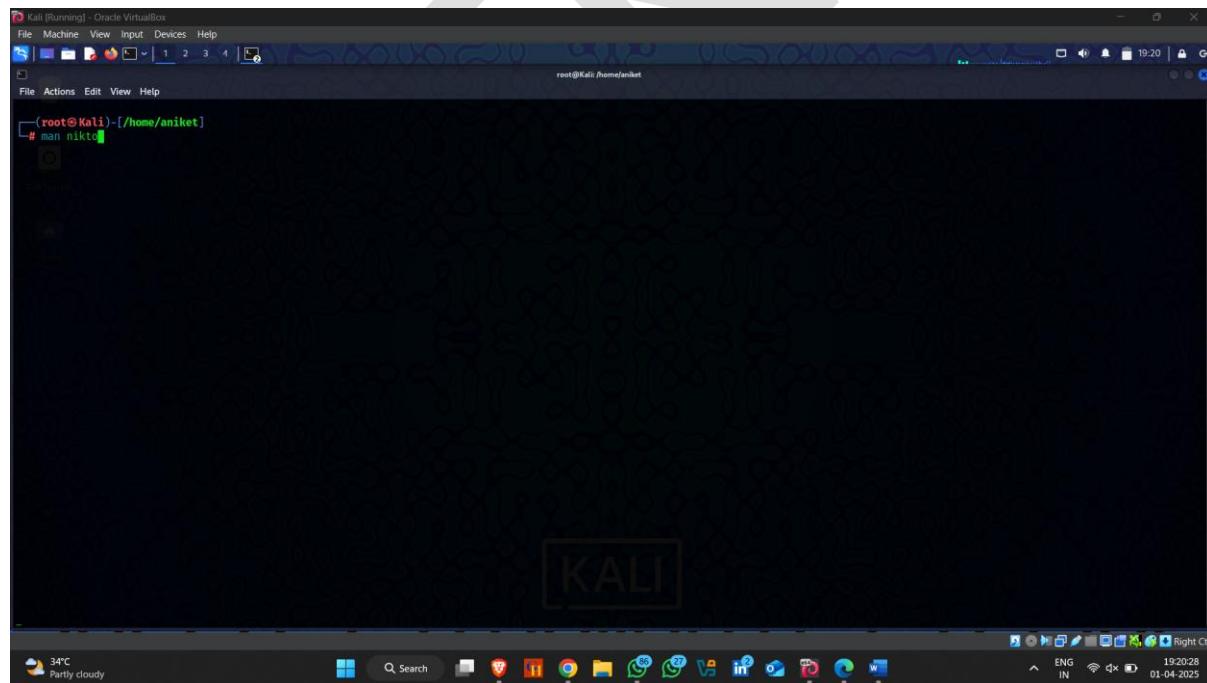
Nikto is an open-source web server scanner used to identify vulnerabilities, misconfigurations, and security issues in web applications.

**Cheat Sheet link for Nikto :**

<https://cdn.comparitech.com/wp-content/uploads/2019/07/Nikto-Cheat-Sheet.pdf>

**Common Commands :-**

- ❖ Man nikto – Details about nikto tool.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'Kali [Running] - Oracle VM VirtualBox'. The command '# man nikto' is entered at the root prompt. The desktop background features a dark theme with a large 'KALI' logo. The taskbar at the bottom displays various application icons, and the system tray shows weather information ('34°C Partly cloudy') and system status.

## ❖ nikto -h – help

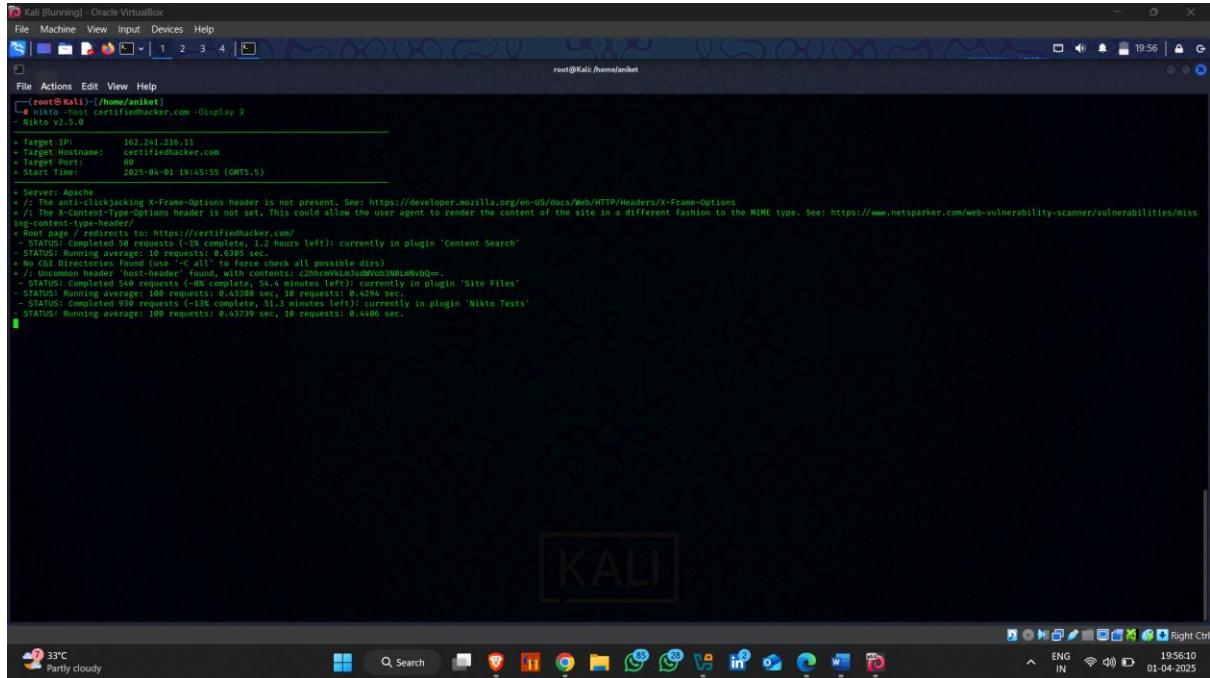
```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions View Help
root@Kali:/home/aniket#
[root@Kali ~]# nikto -h
Option host requires an argument
Options:
  -ask+      Whether to ask about submitting updates
            yes  Ask about each (default)
            no   Don't ask, don't send
            auto Don't ask, just send
  -check6    Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgidirs+  Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+   Use this config file
  -Display+  Turn on/off display outputs:
            1   Show redirects
            2   Show cookies received
            3   Show all 200/OK responses
            4   Show URLs which require authentication
            D   Debug output
            E   Display all HTTP errors
            P   Print progress to STDOUT
            S   Scrub output of IPs and hostnames
            V   Verbose output
  -dbcheck   Check database and other key files for syntax errors
  -evasion+  Encoding technique:
            1   Random URI encoding (non-UTF8)
            2   Directory self-reference (../)
            3   Premature URL ending
            4   Prepend long random string
            5   Fake parameter
            6   TAB as request spacer
            7   Change the case of the URL
            8   Use Windows directory separator (\)
            A   Use a carriage return (0xd) as a request spacer
            B   Use binary value 0x0b as a request spacer
  -followredirs Follow 3xx redirects to new location
  -Format+   Save file (-o) format:
[root@Kali ~]#
```

## ❖ -host – specify a host name or domain name

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions View Help
root@Kali:/home/aniket#
[root@Kali ~]# nikto -host certifiedhacker.com
- Nikto v2.5.0

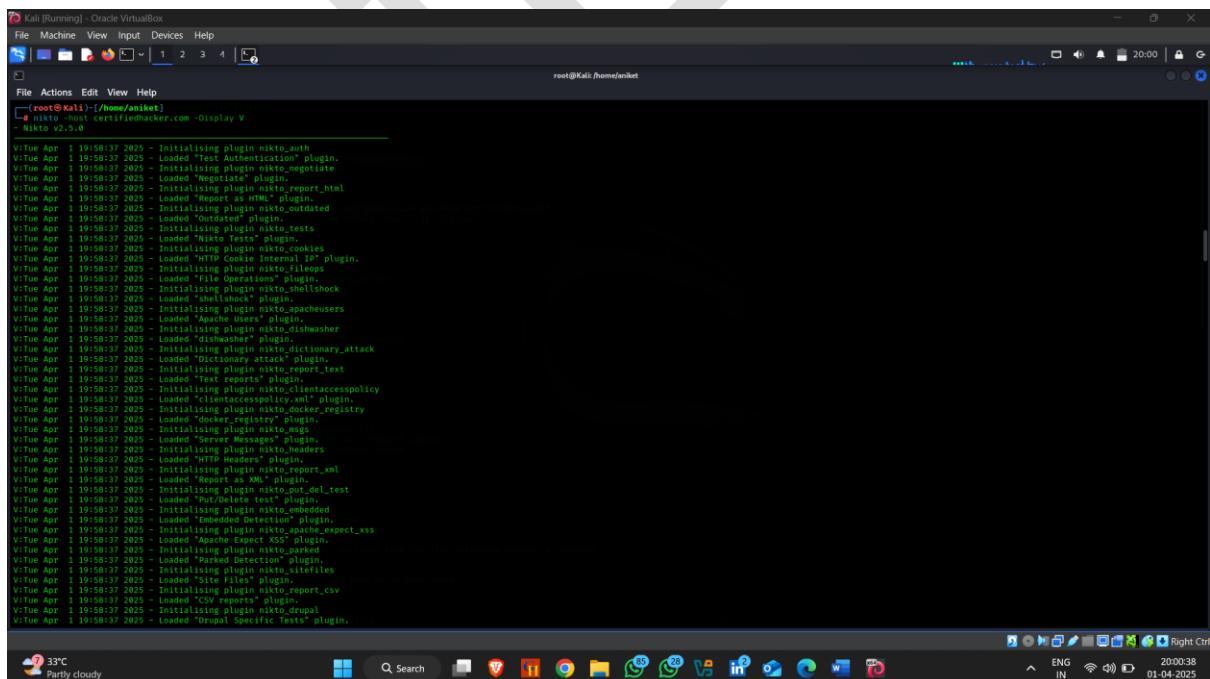
+ 0 host(s) tested
[root@Kali ~]#
```

- ❖ -Display -- the **-Display** option is used to control what information is shown in the scan output.
- ❖ -Display 3 – show all 200/ok response



Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@Kali:~/home/niket|  
niktostart certifiedmacker.com -Display 3  
Nikto v2.5.0  
Target IP: 102.261.216.13  
Target Hostname: certifiedmacker.com  
Target Port: 80  
Start Time: 2025-04-01 19:45:59 (GMT+5)  
Server: Apache  
/: The anti-clickjacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>  
- STATUS: Completed 50 requests (-1% complete, 1.2 hours left) currently in plugin 'Content Search'  
- STATUS: Running average: 100 requests: 0.83/sec.  
- No GET Directories found, will always force check all possible dirs  
/: Uncommon header 'host-header' found, with contents: c2hncWVzL3JsdWVobNOLmV0D=.  
- STATUS: Completed 549 requests (-8% complete, 54.4 minutes left) currently in plugin 'Site Files'  
- STATUS: Completed 938 requests (-13% complete, 51.3 minutes left) currently in plugin 'Nikto Tests'  
- STATUS: Completed 938 requests (-13% complete, 51.3 minutes left) currently in plugin 'Nikto Tests'  
- STATUS: Running average: 100 requests: 0.4739 sec, 10 requests: 0.4486 sec.

- ❖ -Display V – Verbose mode



Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@Kali:~/home/niket|  
niktostart certifiedmacker.com -Display V  
Nikto v2.5.0  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.auth  
V[Tue Apr 1 19:58:37 2025] - Loaded "Test Authentication" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.negotiate  
V[Tue Apr 1 19:58:37 2025] - Loaded "Negotiate" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.report\_html  
V[Tue Apr 1 19:58:37 2025] - Loaded "Report as HTML" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.outdated  
V[Tue Apr 1 19:58:37 2025] - Loaded "Outdated" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.tests  
V[Tue Apr 1 19:58:37 2025] - Loaded "Nikto Tests" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.cookies  
V[Tue Apr 1 19:58:37 2025] - Loaded "HTTP Cookie Internal IP" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.files  
V[Tue Apr 1 19:58:37 2025] - Loaded "File Operations" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto.shellshock  
V[Tue Apr 1 19:58:37 2025] - Loaded "shellshock" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_apacheusers  
V[Tue Apr 1 19:58:37 2025] - Loaded "Apache Users" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_dishwasher  
V[Tue Apr 1 19:58:37 2025] - Loaded "dishwasher" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_dictionary\_attack  
V[Tue Apr 1 19:58:37 2025] - Loaded "Dictionary Attack" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_report\_text  
V[Tue Apr 1 19:58:37 2025] - Loaded "Text Reports" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_clamavpolicy  
V[Tue Apr 1 19:58:37 2025] - Loaded "ClamAV Policy" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_docker\_registry  
V[Tue Apr 1 19:58:37 2025] - Loaded "docker\_registry" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_expect\_xss  
V[Tue Apr 1 19:58:37 2025] - Loaded "Expect XSS" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_parked  
V[Tue Apr 1 19:58:37 2025] - Loaded "Parse Detection" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_headers  
V[Tue Apr 1 19:58:37 2025] - Loaded "HTTP Headers" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_report\_xml  
V[Tue Apr 1 19:58:37 2025] - Loaded "Report as XML" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_del\_test  
V[Tue Apr 1 19:58:37 2025] - Loaded "Delete Test" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_embedded  
V[Tue Apr 1 19:58:37 2025] - Loaded "Embedded Detection" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_expect\_xss  
V[Tue Apr 1 19:58:37 2025] - Loaded "Expect XSS" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_parked  
V[Tue Apr 1 19:58:37 2025] - Loaded "Parse Detection" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_headers  
V[Tue Apr 1 19:58:37 2025] - Loaded "HTTP Headers" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_report\_csv  
V[Tue Apr 1 19:58:37 2025] - Loaded "Report CSV" plugin.  
V[Tue Apr 1 19:58:37 2025] - Initialising plugin nikto\_report\_html  
V[Tue Apr 1 19:58:37 2025] - Loaded "Drupal Specific Tests" plugin.

- ❖ Tuning -- the **-Tuning** option allows you to control the types of tests performed during a scan. but using tuning options helps focus the scan on specific vulnerabilities or types of checks.
- ❖ -Tuning x -- “x specify all tuning test “

**Note :- As You can see our target is vulnerable with different fields .**

```
(root@Kali:[/home/aniket]
# nikto -host 192.168.114.182 -Tuning x
- Nikto v2.5.0

+ Target IP:      192.168.114.182
+ Target Hostname: 192.168.114.182
+ Target Port:    80
+ Start Time:    2025-04-03 18:08:56 (GMT5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wise.it/sectori.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (Current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 684 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:    2025-04-03 18:09:00 (GMT5.5) (4 seconds)

+ 1 host(s) tested

[root@Kali:[/home/aniket]
#
```

- ❖ You can also generate report using nikto

**Command – nikto -host <target ip / domain name > -Tuning x**

**-o filename.txt**

- ❖ -o -- for output /format
- ❖ X – for all tuning command

```

root@Kali:[/]# nikto -host 192.168.114.182 -Tuning x -o nikto.txt
- Nikto v2.5.0

+ Target IP:      192.168.114.182
+ Target Hostname: 192.168.114.182
+ Target Port:    80
+ Start Time:    2025-04-03 19:31:09 (GMT5.5)

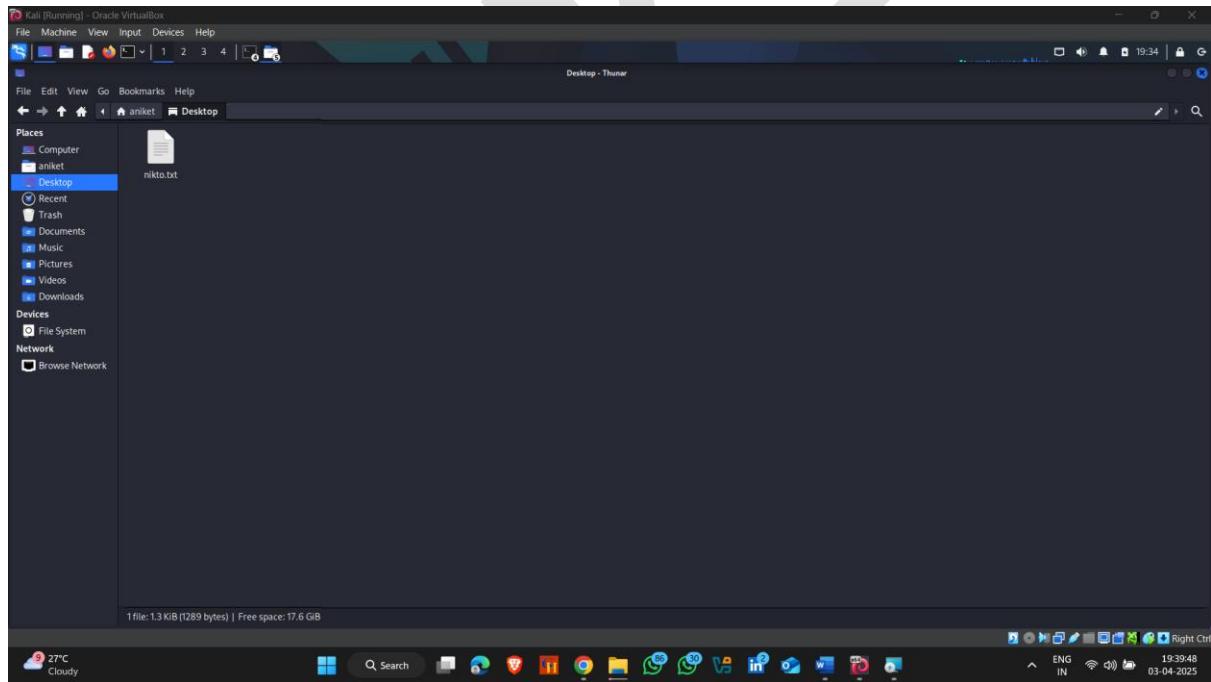
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /index: Uncommon header 'icn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebcd59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XSS. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 684 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:    2025-04-03 19:31:14 (GMT5.5) (5 seconds)

+ 1 host(s) tested

(root@Kali:[/]# )

```

❖ Report generate successfully now open it





Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

File Edit Search View Document Help

1 - Nikto v2.5.0/

2 + Target Host: certifedhacker.com

3 + HEAD /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

4 + GET /: The anti-clickjacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

5 + GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

6 + GET /: Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWob3N0LmVbQ==.

7 + HEAD /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

8 + Target Host: 192.168.114.182

9 + Target Port: 80

10 + GET /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.

11 + GET /: The anti-clickjacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

12 + HEAD /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

13 + GET /index: Uncommon header 'tcn' found, with contents: list.

14 + GET /index: Apache mod\_negotiation is enabled with Multiviews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: <http://www.wisec.it/sectou.php?id=4098ebcd59015>, <https://exchange.xforce.ibmcloud.com/vulnerabilities/8275>

15 + HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

16 + X42PCMBY /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

17 + TRACE /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: [https://owasp.org/www-community/attacks/Cross\\_Site\\_Tracing](https://owasp.org/www-community/attacks/Cross_Site_Tracing)

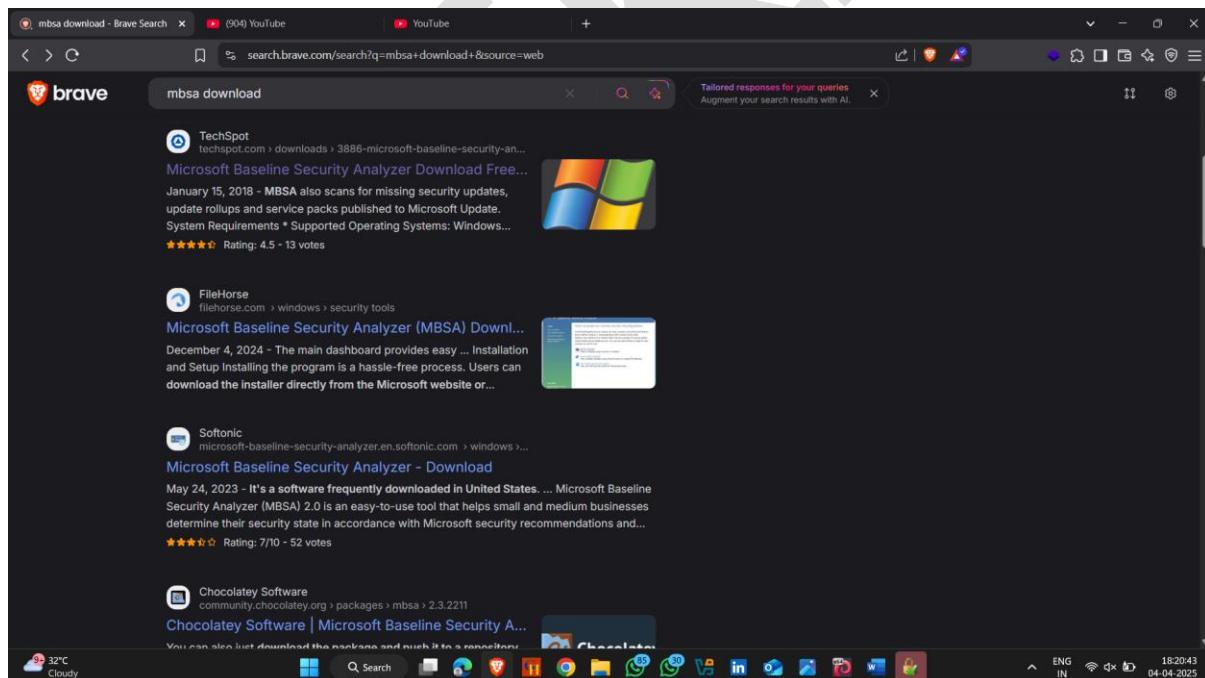
18

# Vulnerability Analysis Using MBSA (Microsoft Baseline Security Analyzer)

The Microsoft Baseline Security Analyzer (MBSA) was a free tool developed by Microsoft to help users scan their Windows systems for common security misconfigurations and missing security updates.

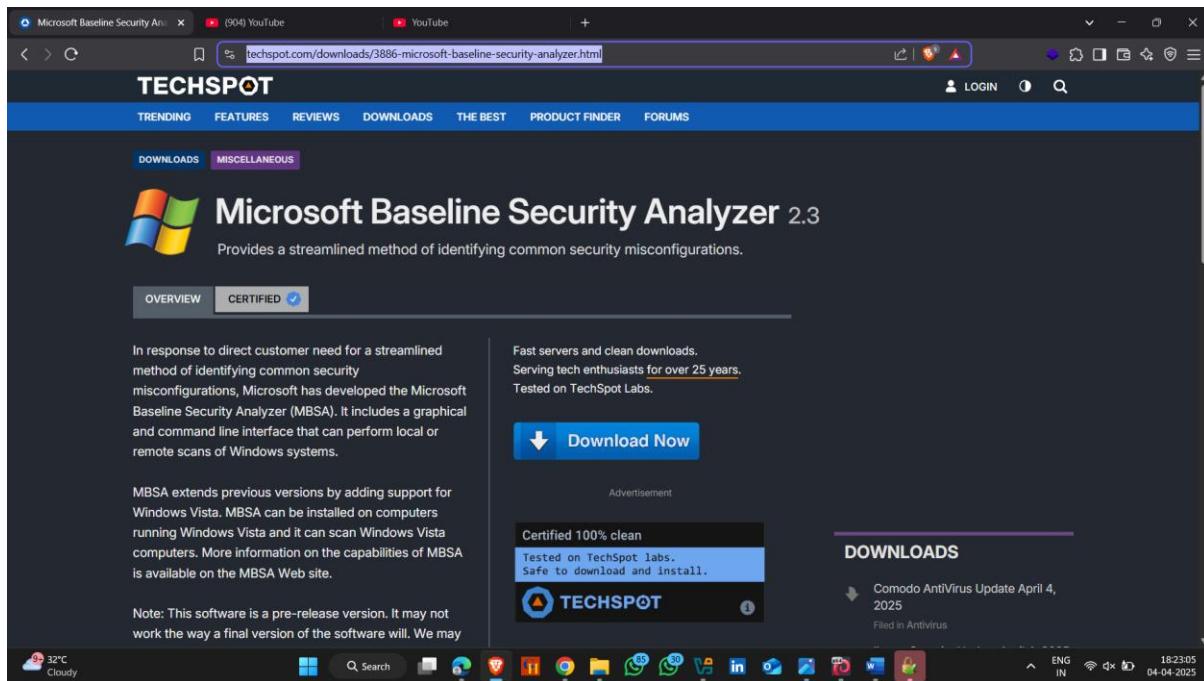
## How To Download MBSA

- ❖ Open Browser
- ❖ Search MBSA Download and click on **Techspot** website
- ❖ Link - : <https://www.techspot.com/downloads/3886-microsoft-baseline-security-analyzer.html>

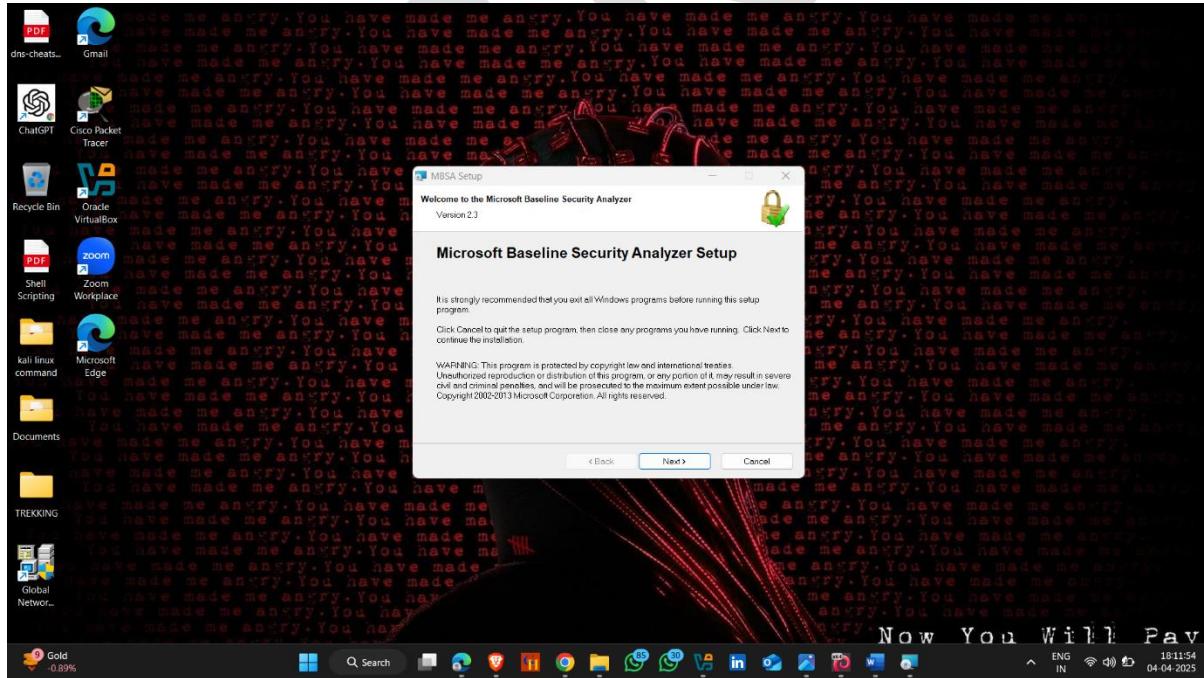


- ❖ Click on

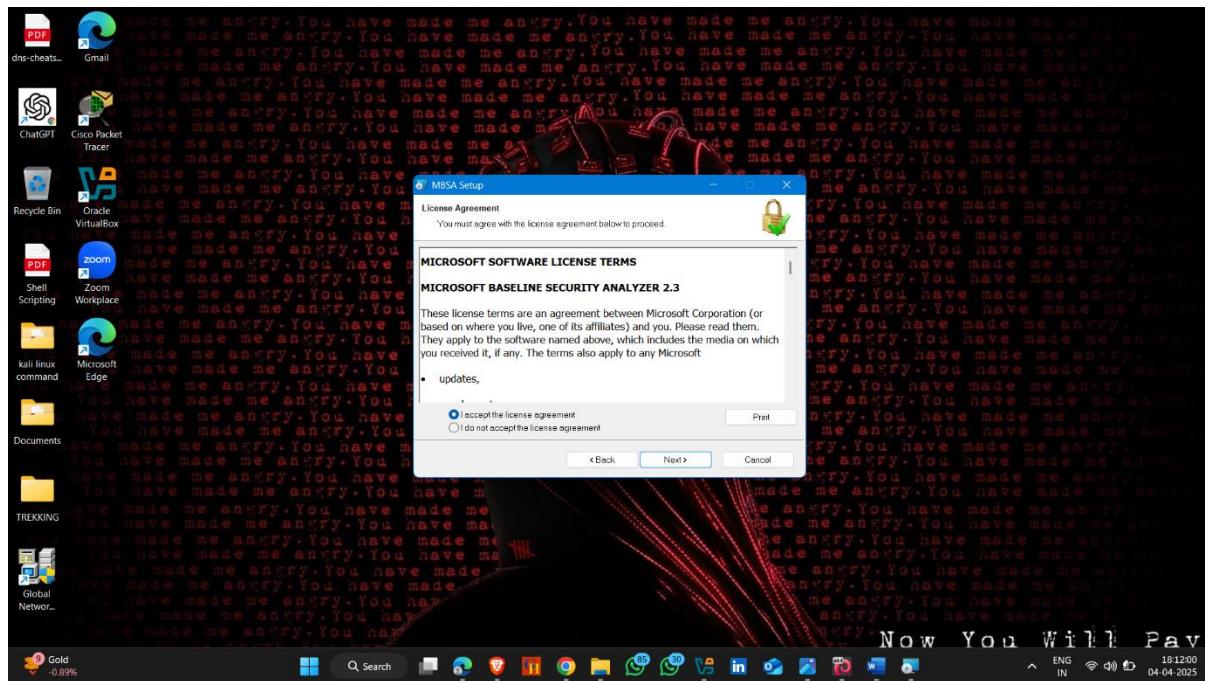
## ❖ Download Now



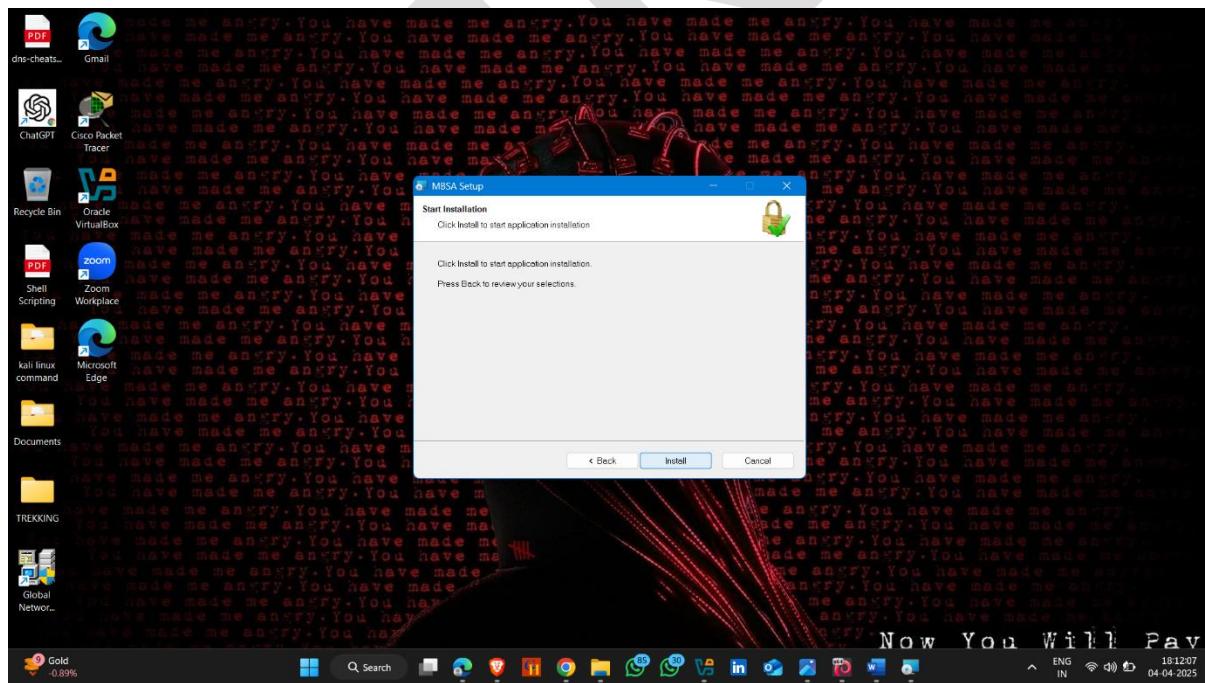
## ❖ After Downloading , open the application and click on next



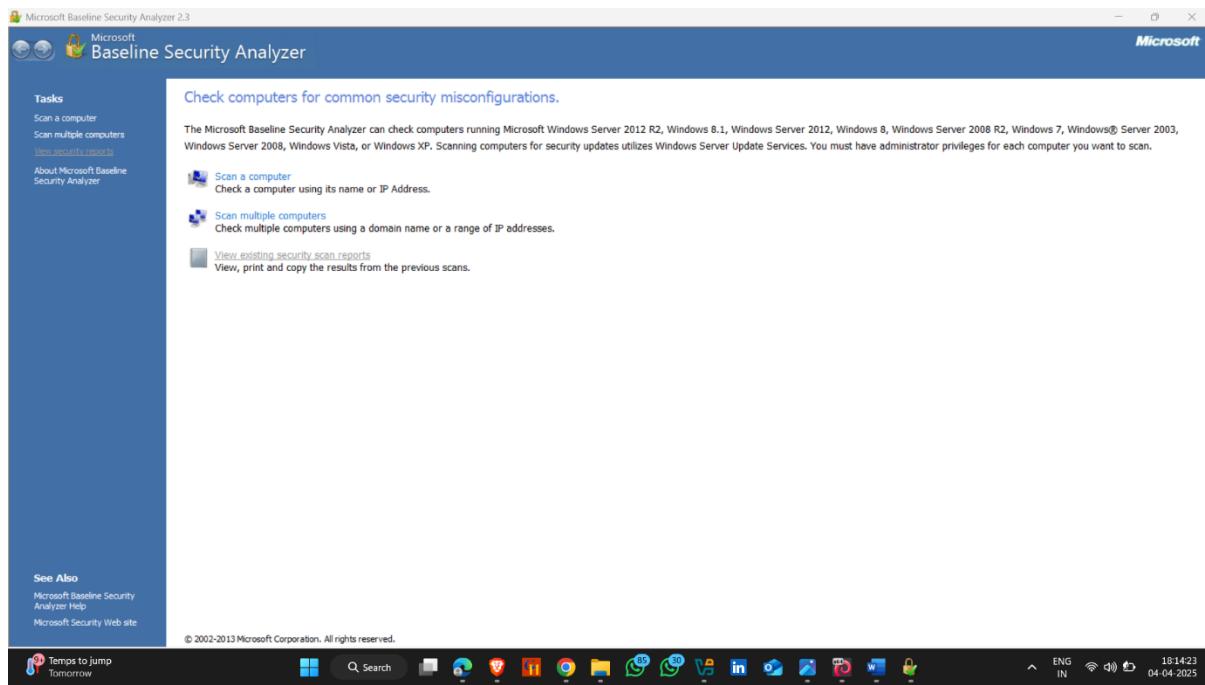
## ❖ Accept the license and click next



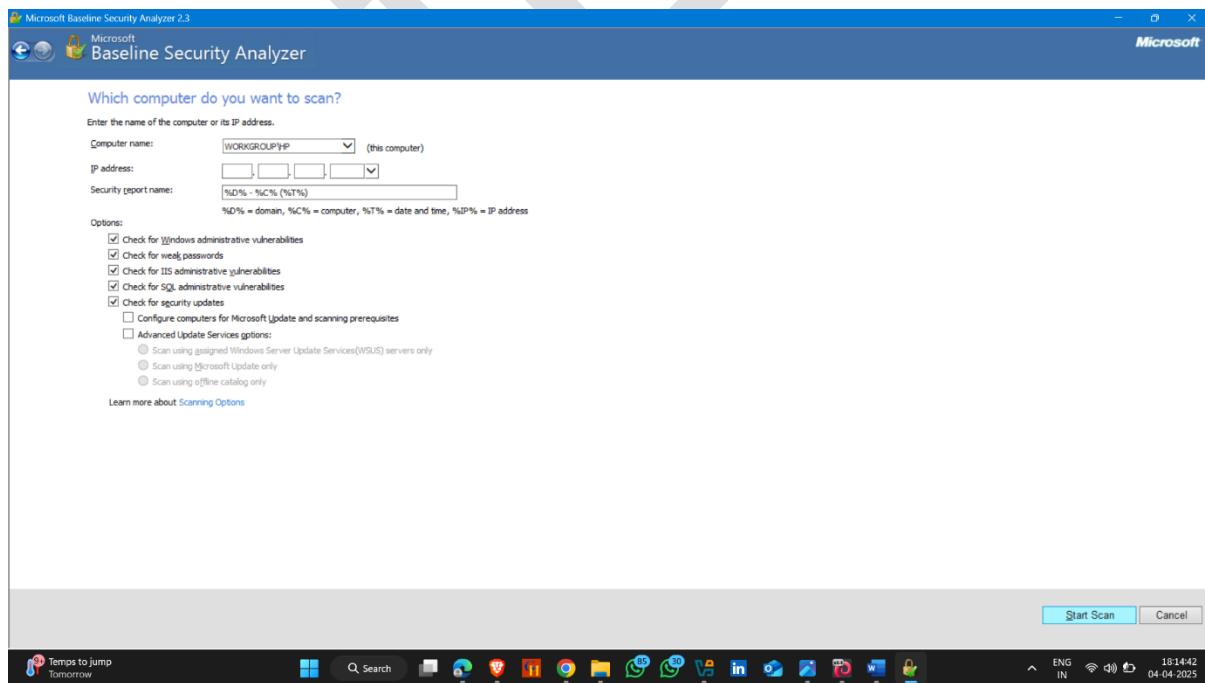
## ❖ Click on install



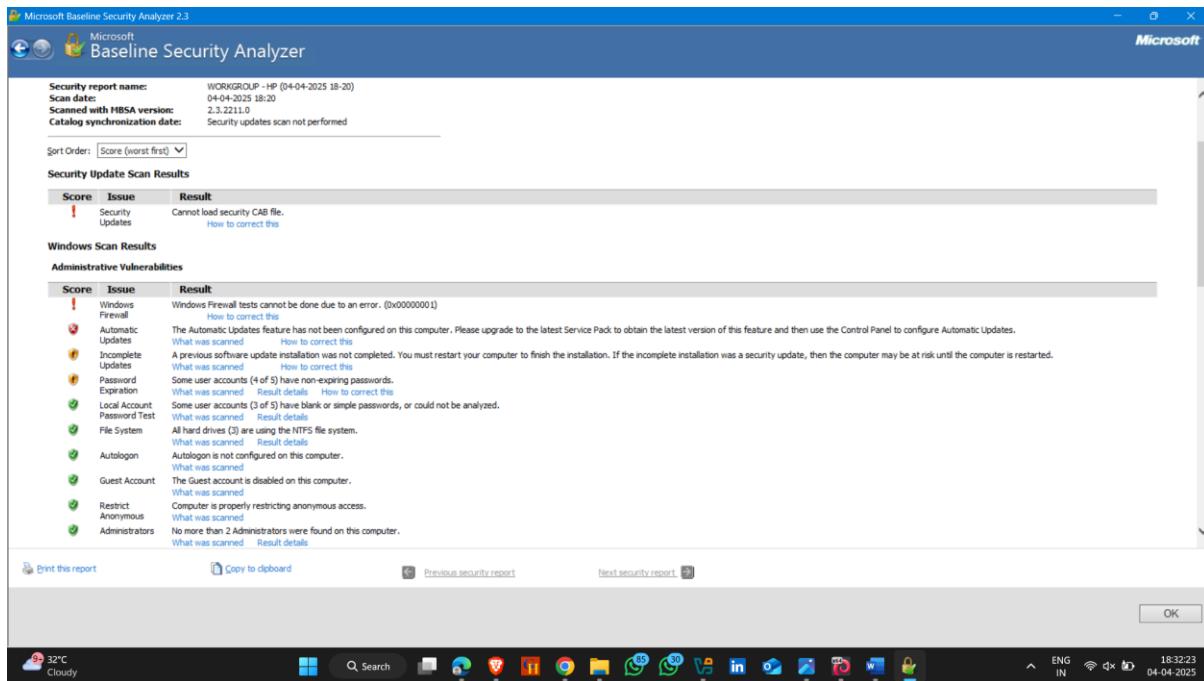
- ❖ After successfully install and setup mbsa , open it and **click on scan computer**



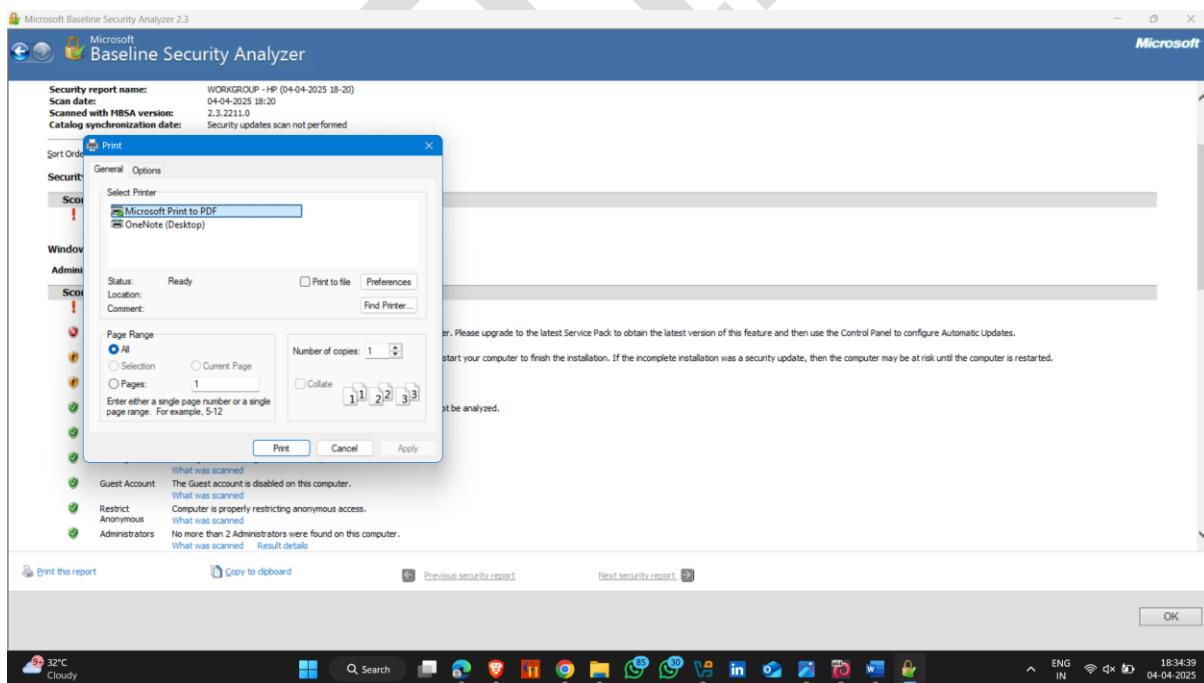
- ❖ As you can see MBSA automatically get your system name
- ❖ Click on start scan



❖ Here , MBSA scan the device



❖ You can also save or print this report , just click on print this report



❖ Click on print (save as a pdf)

# Vulnerability Analysis Using Nessus.

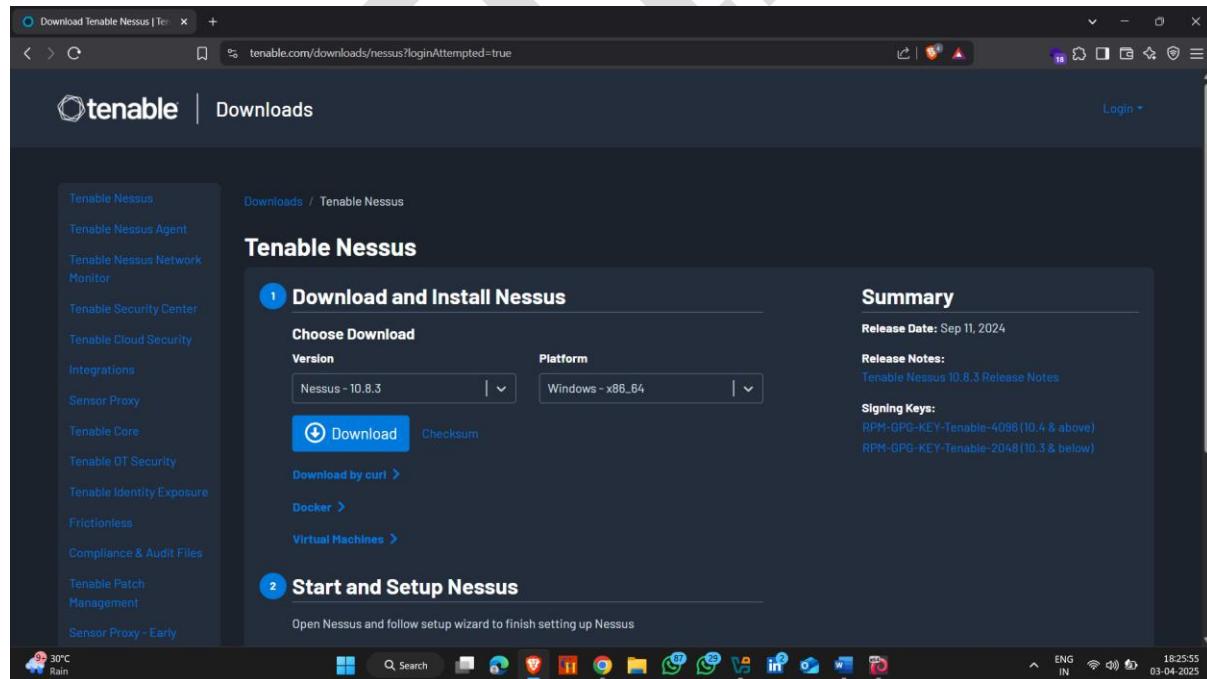
Nessus is a popular vulnerability assessment tool used to scan networks, systems, and applications for security weaknesses. It is developed by Tenable, Inc. and is widely used for penetration testing, compliance auditing, and risk assessment.

**Nessus Download Link –**

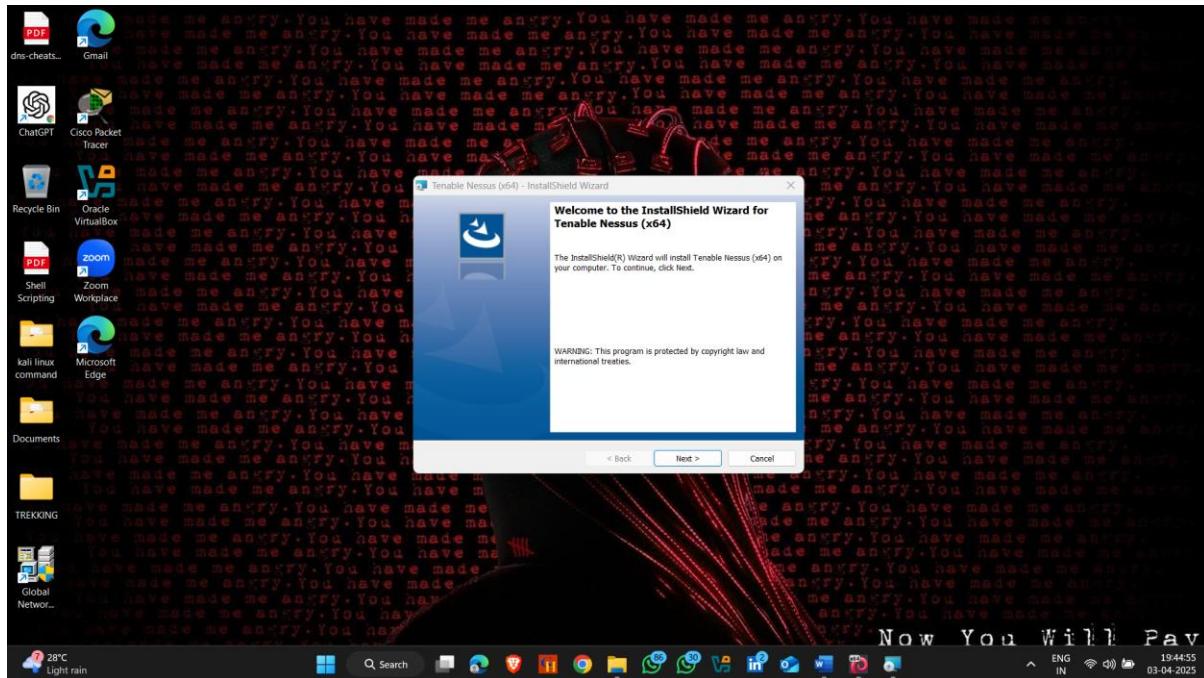
<https://www.tenable.com/downloads/nessus?loginAttempted=true>

**How To Download Nessus –**

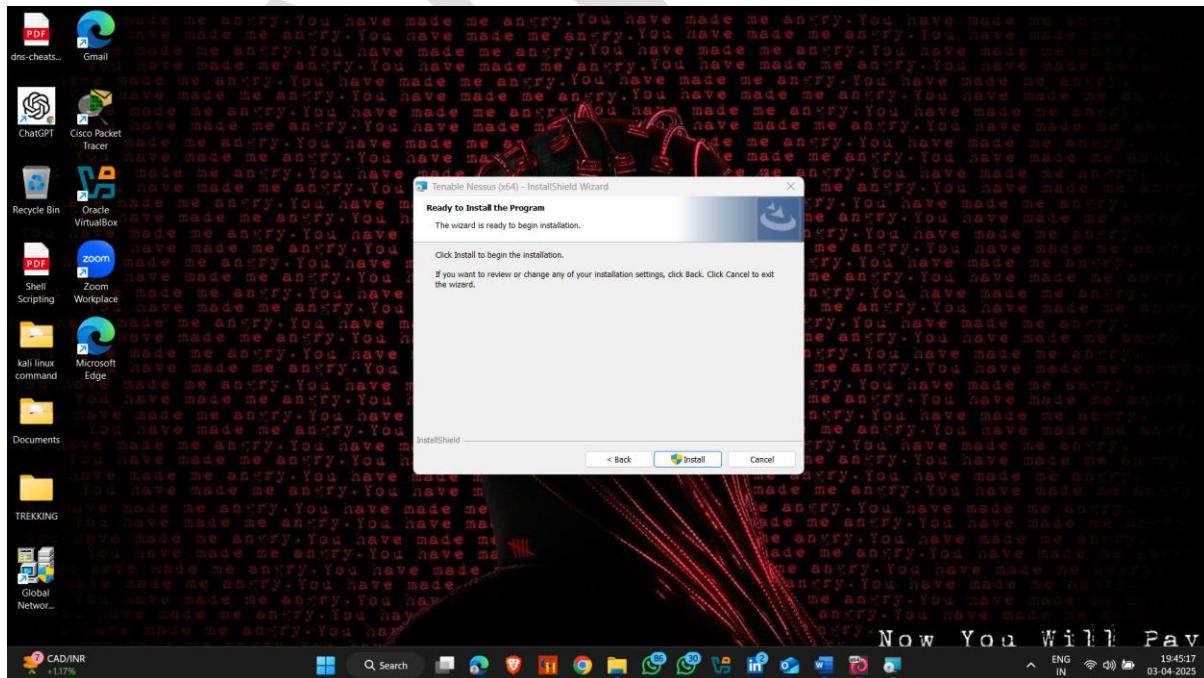
- ❖ Open Browser
- ❖ Search Nessus Download
- ❖ Click first website for official Tenable website and you can redirected to download page



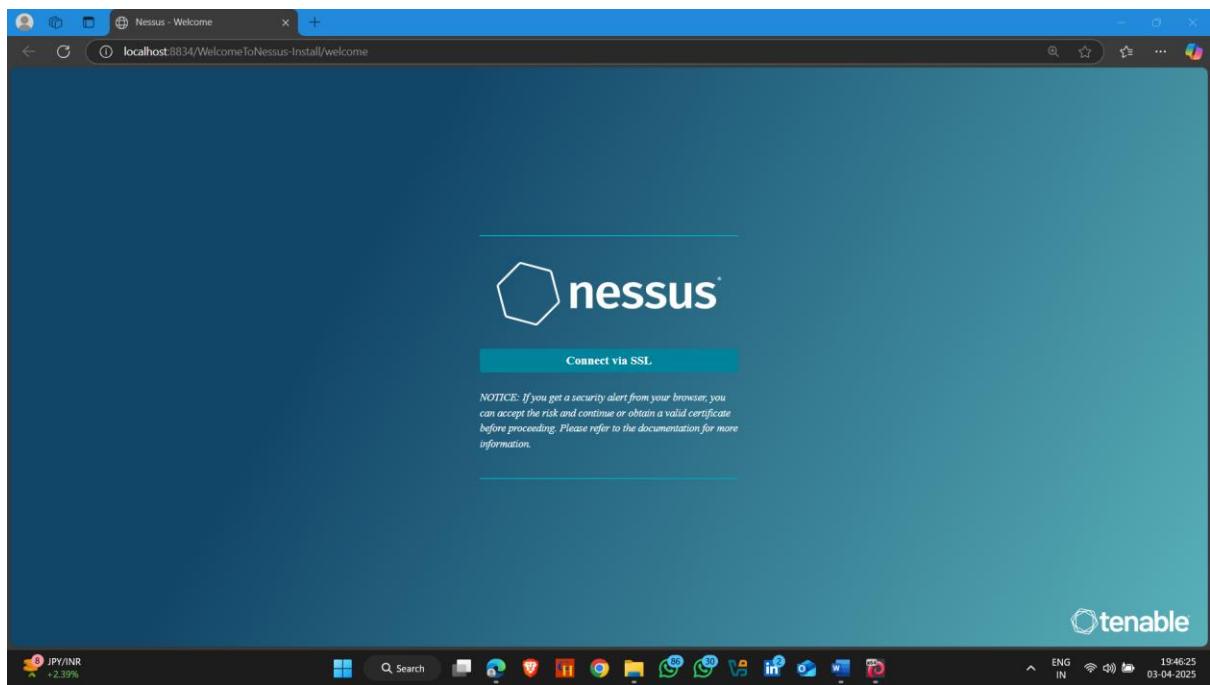
- ❖ Click on Download Button and Download Nessus
- ❖ Open Nessus file /Double click
- ❖ Click on next



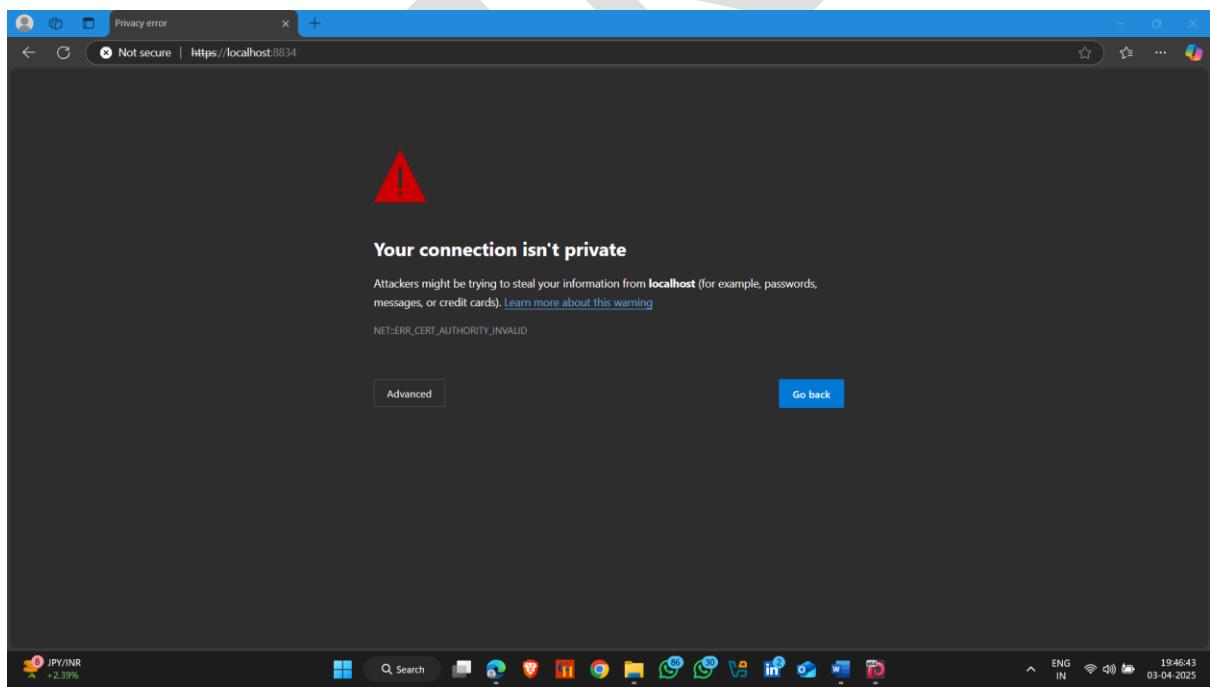
- ❖ Click install



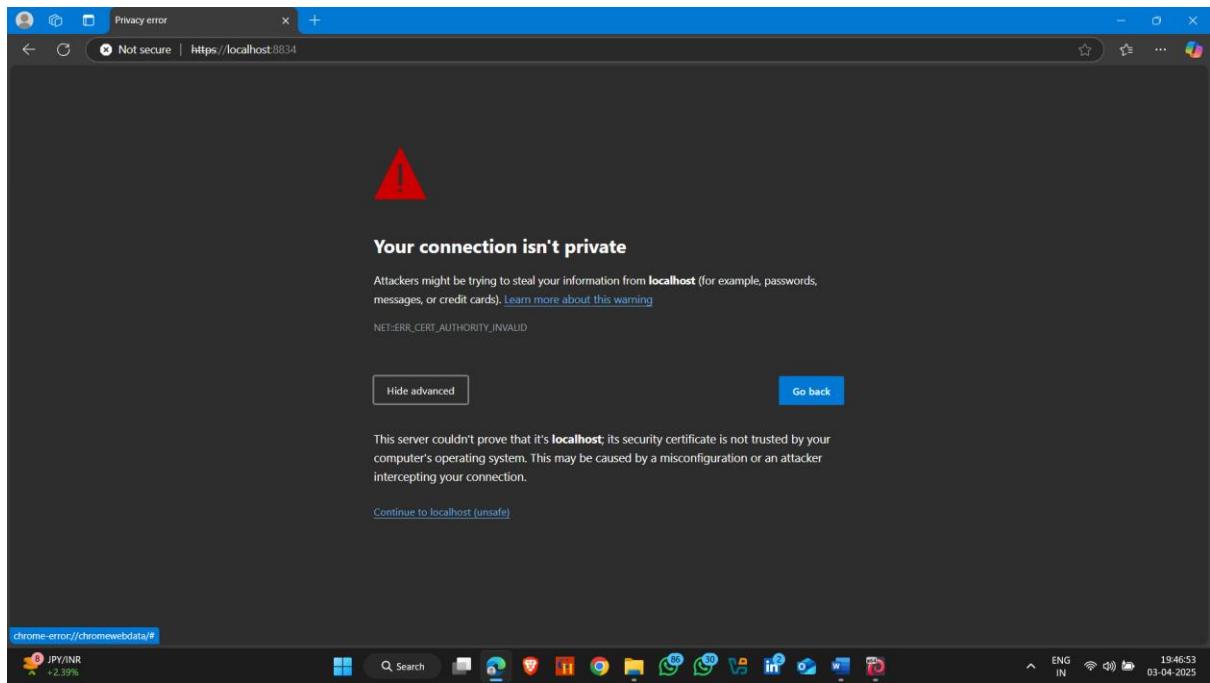
❖ Click on connect via SSL



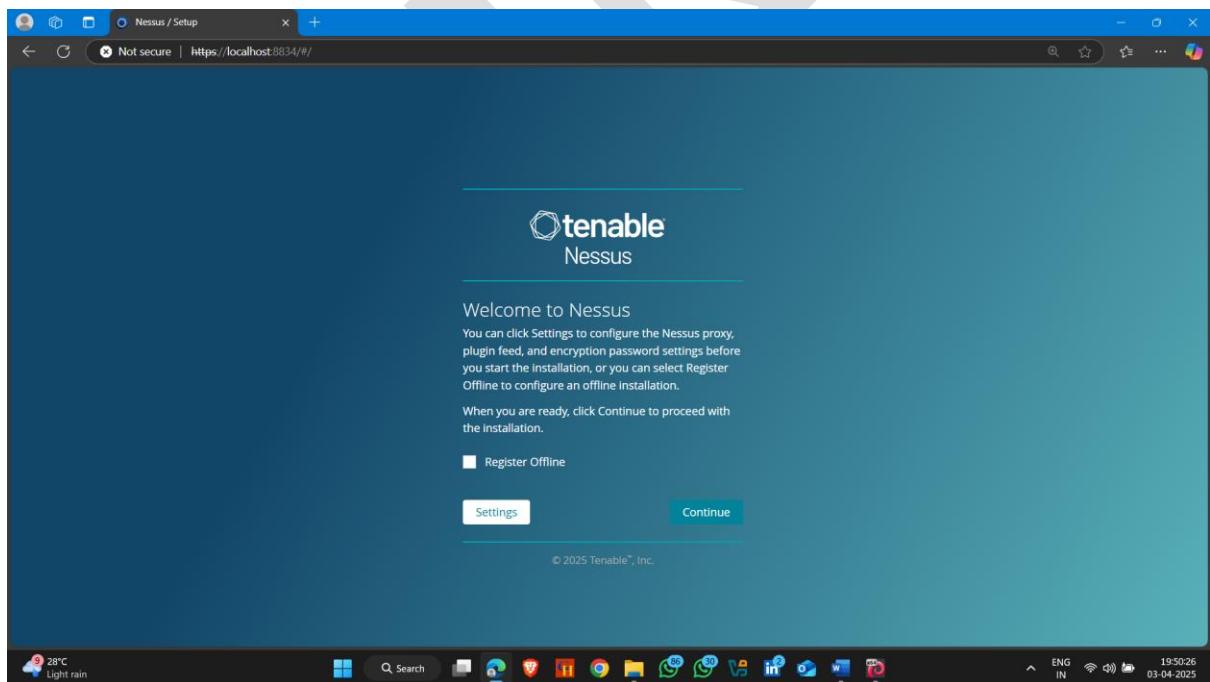
❖ Click on Advance



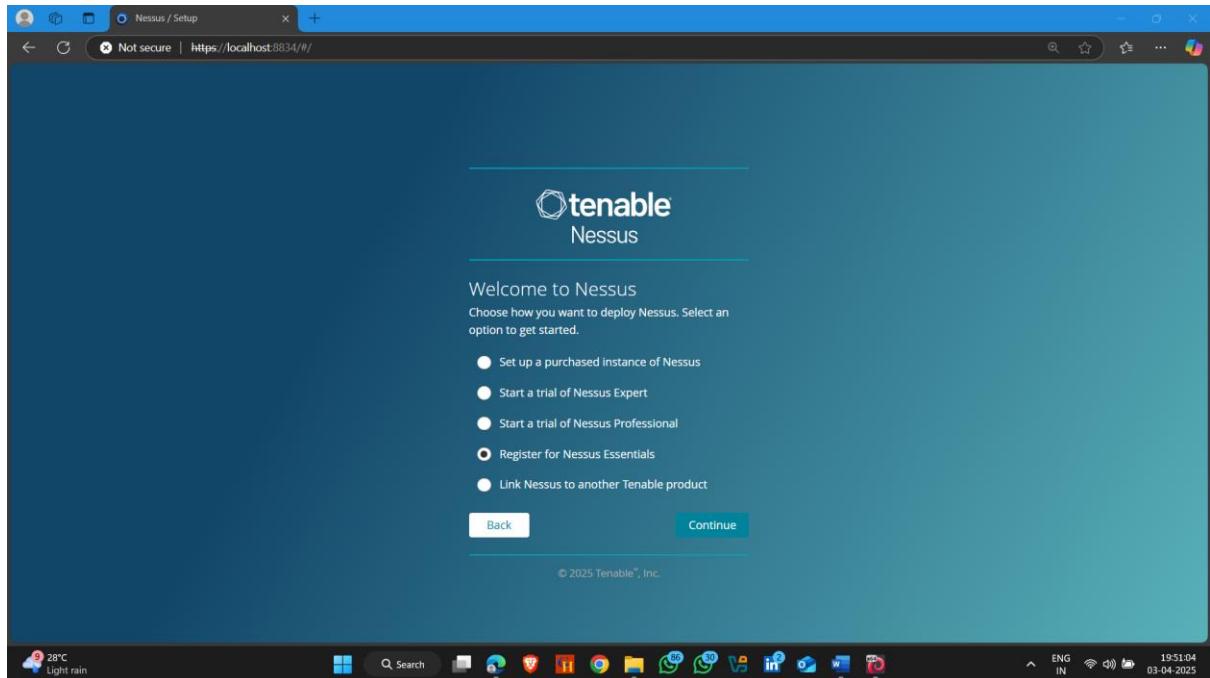
❖ Click continue to localhost(unsafe ! )



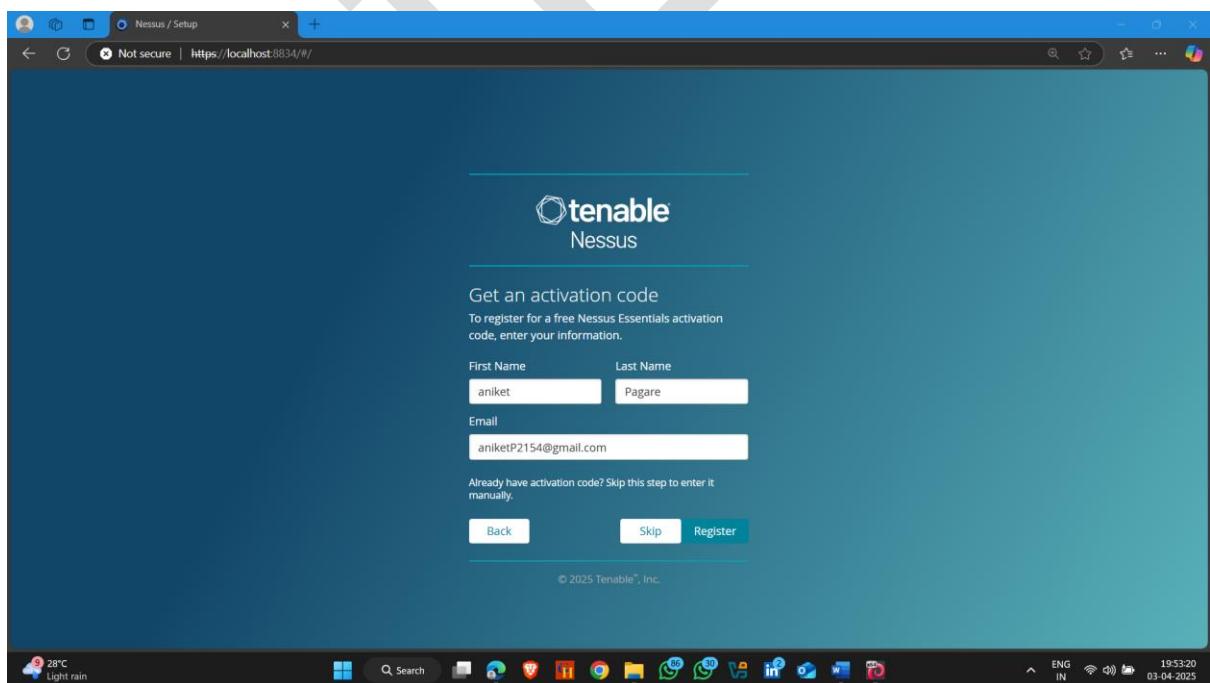
❖ Click on continue



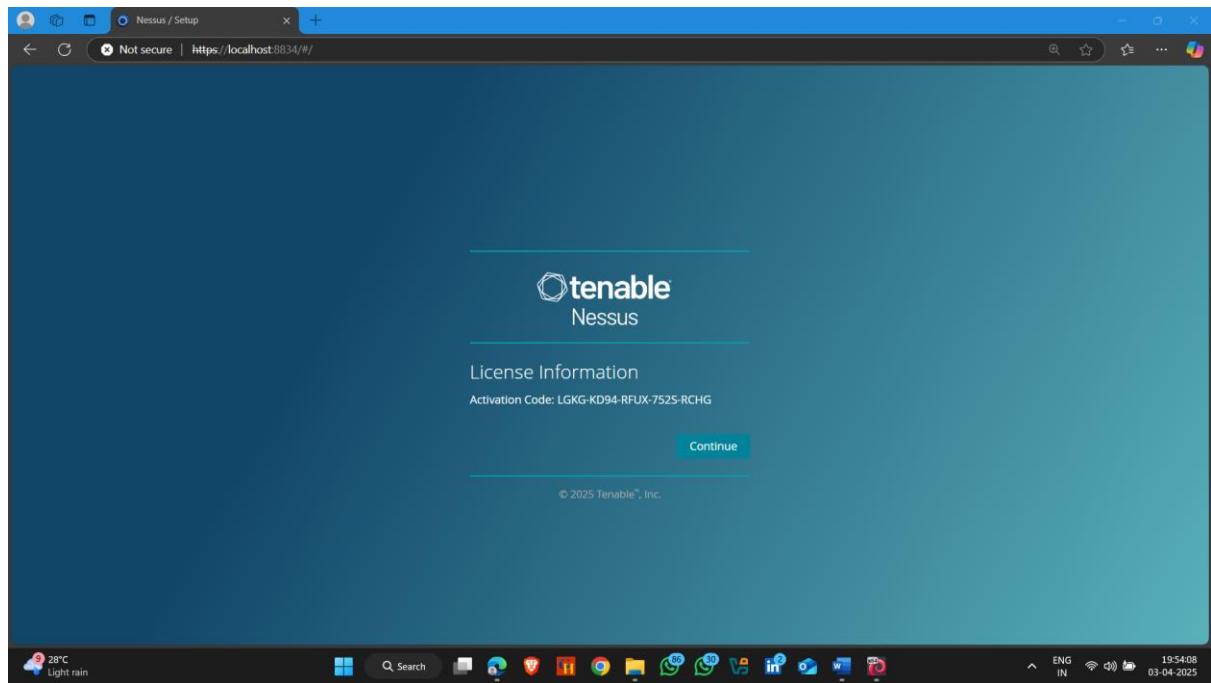
- ❖ Click on second last option **Register for Nessus Essential** And click Continue



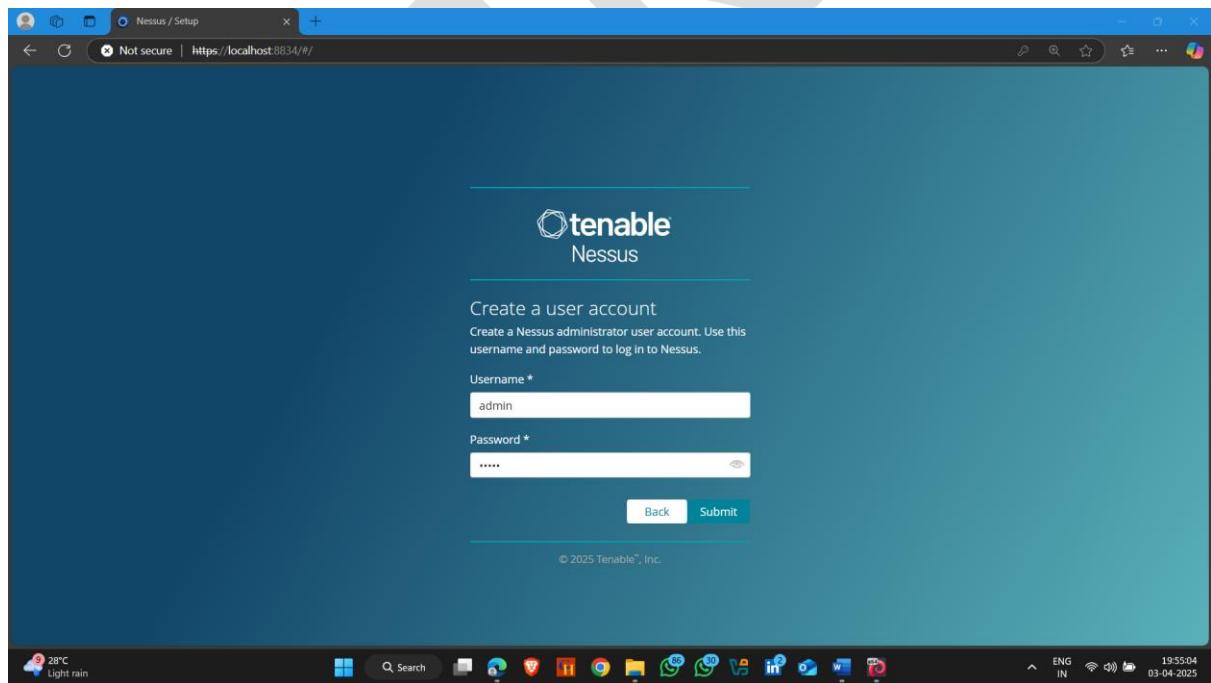
- ❖ Provide name and other things and click register



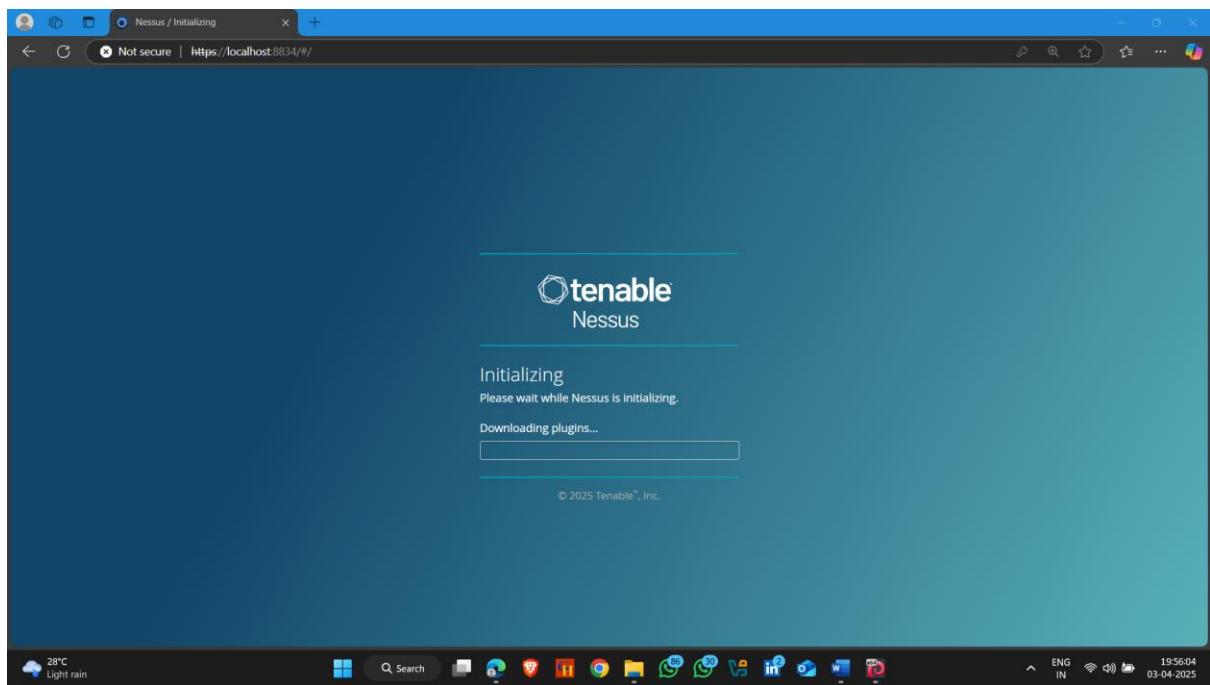
❖ Click on continue



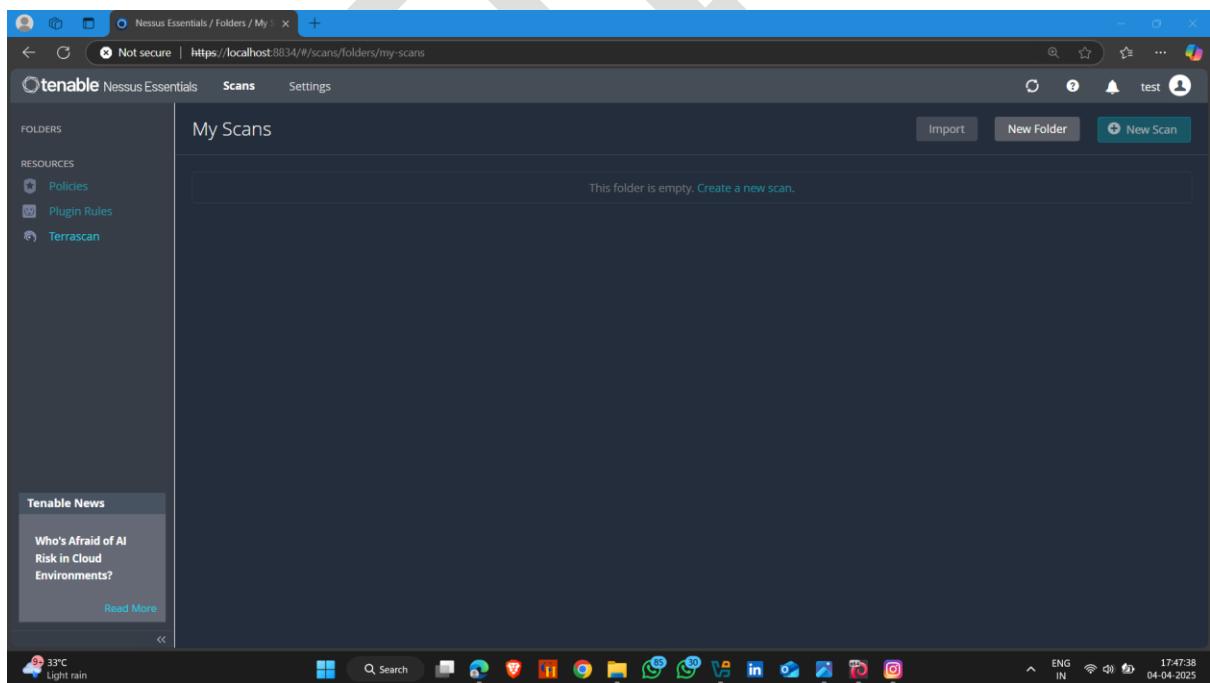
❖ Provide username and password and submit



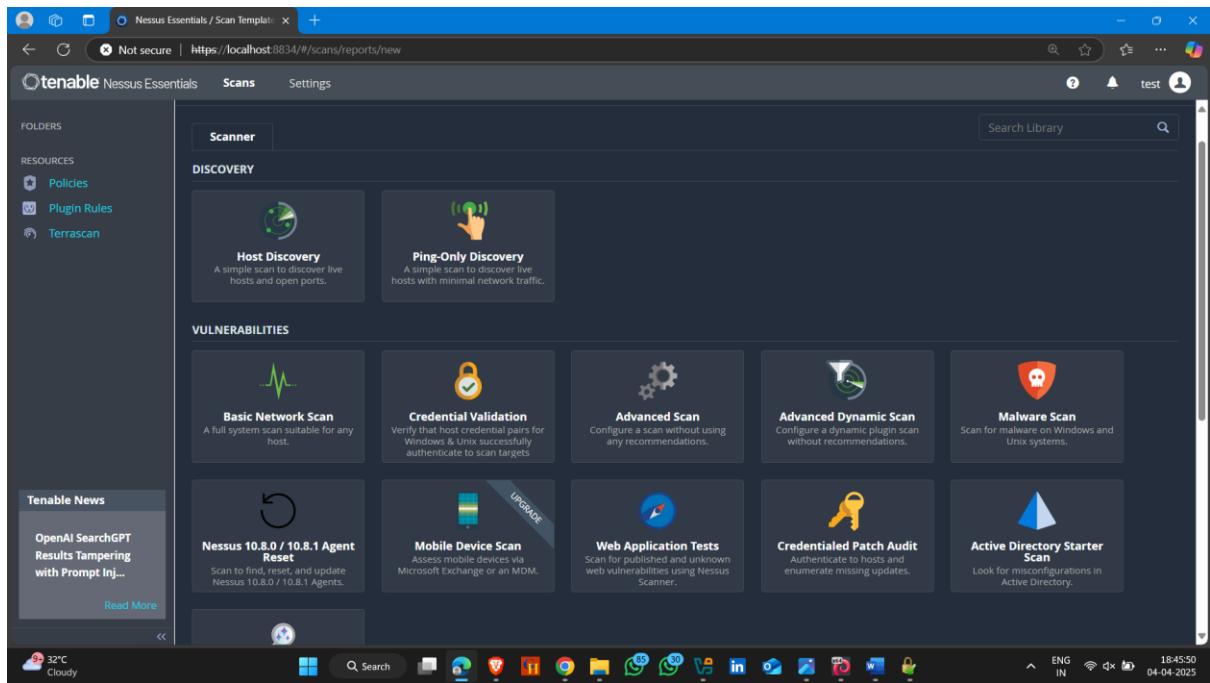
❖ Wait !



- ❖ After Downloading , you see Nessus interface  , TO start a vulnerability scanning click on new scan option

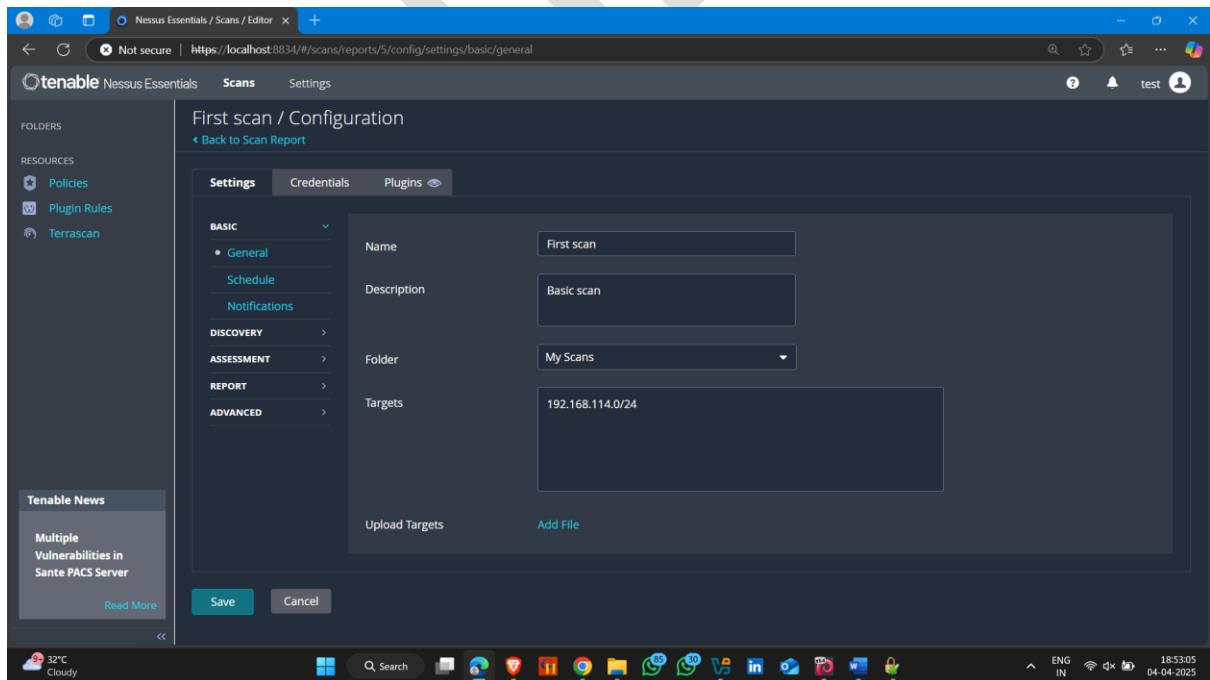


❖ Click on Basic network scan



❖ Provide target

**Note – In my case , I'm scan Entire network , you can also scan a entire network as well as single ip address its all depend on you**



❖ Click on save and then click on launch

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'Folders', 'Resources' (including 'Policies', 'Plugin Rules', and 'Terrascan'), and 'Tenable News' (about OpenAI SearchGPT). The main area is titled 'My Scans' and shows one scan named 'First scan'. The 'Scan Type' is 'Vulnerability' and the 'Schedule' is 'On Demand'. The 'Last Scanned' field shows 'N/A'. There are 'Import', 'New Folder', and 'New Scan' buttons at the top right, and a 'Launch' button next to the scan entry.

❖ Here , scanning start

This screenshot shows the results of the 'First scan'. The left sidebar remains the same. The main area is titled 'First scan' and includes a 'Back to My Scans' link. It displays three hosts: 192.168.114.254, 192.168.114.215, and 192.168.114.236. Each host has a bar chart showing the percentage of vulnerabilities found. To the right, there's a 'Scan Details' section with information like Policy: Basic Network Scan, Status: Running, Severity Base: CVSS v3.0, Scanner: Local Scanner, and Start: Today at 6:52 PM. Below that is a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

- ❖ You can also check vulnerabilities , just click on vulnerabilities section

**Scan Details**

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:52 PM

**Vulnerabilities**

Severity	Count
Critical	1
High	4
Medium	1
Low	2
Info	35

- ❖ Now generate a report using Nessus
- ❖ Click on report (top right side )

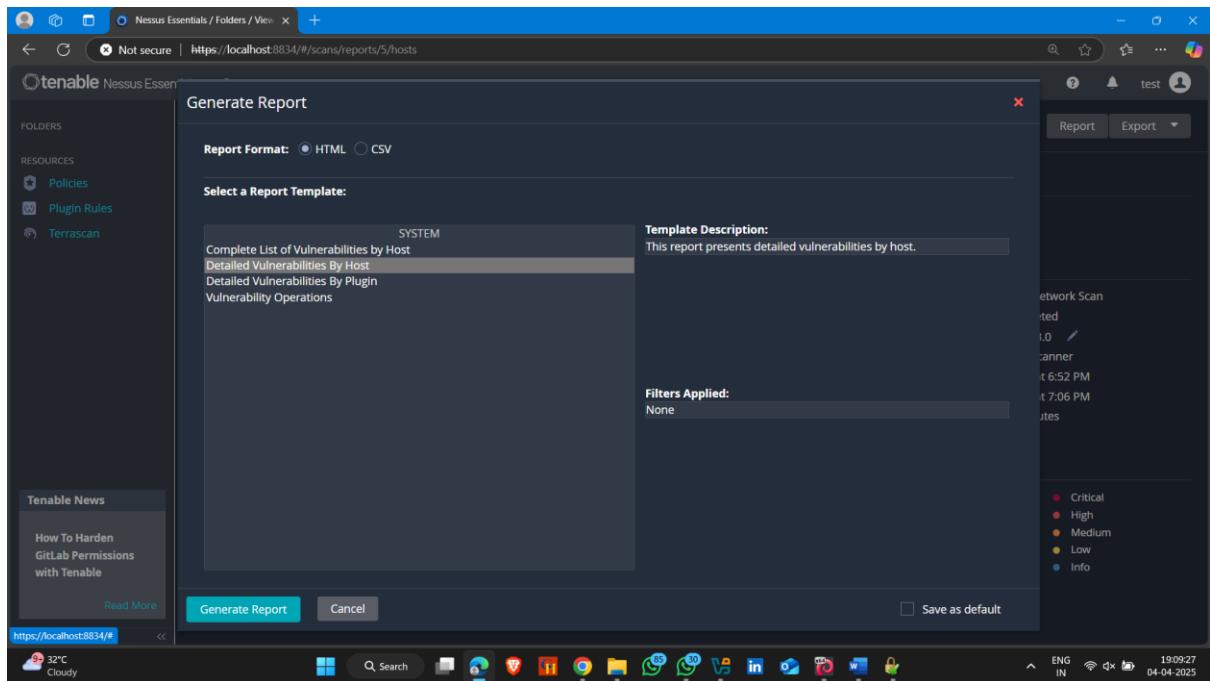
**Scan Details**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:52 PM
- End: Today at 7:06 PM
- Elapsed: 14 minutes

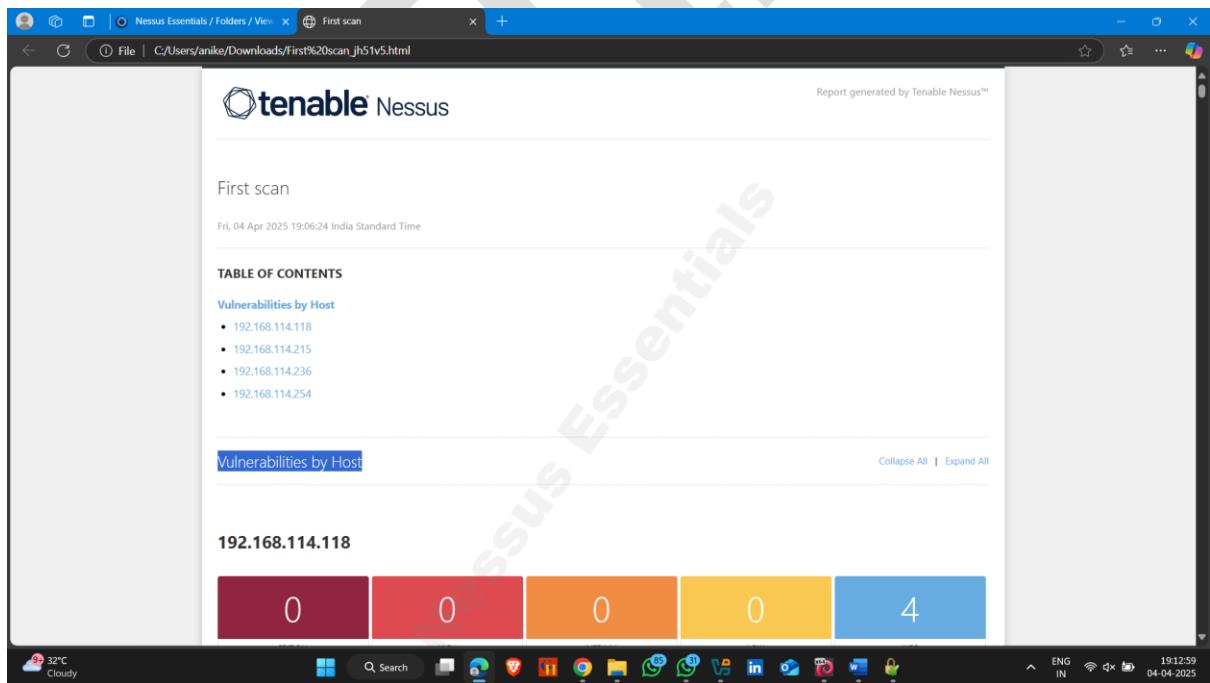
**Vulnerabilities**

Host	Vulnerabilities
192.168.114.254	75
192.168.114.215	4
192.168.114.236	3
192.168.114.118	4

- ❖ Here , you see different report option



- ❖ Click on generate report and see the result , nessus generate in details vulnerability reports

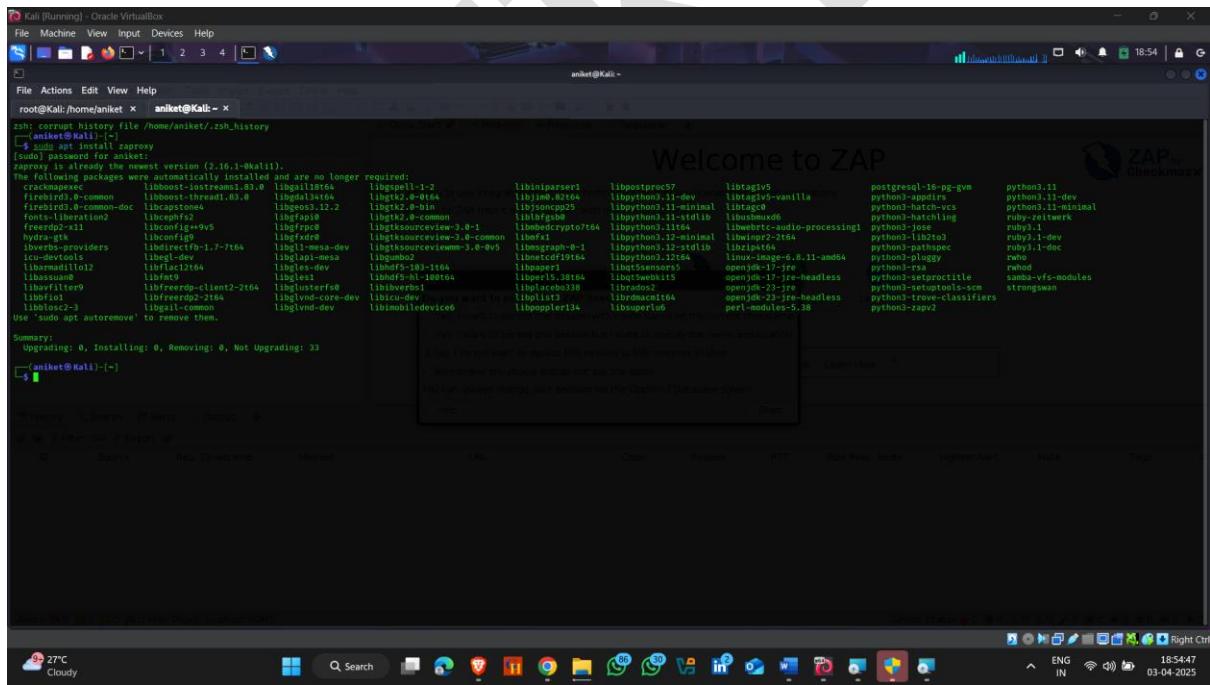


# Vulnerability Analysis Using Checkmarx ZAP

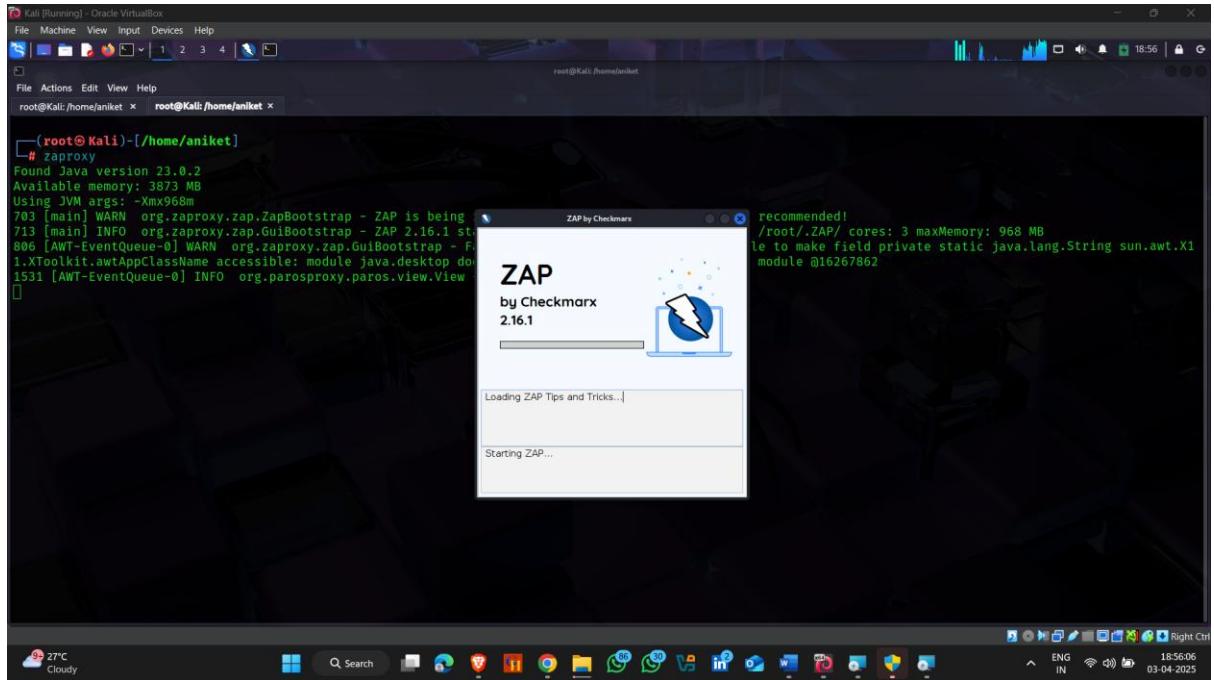
ZAP (Zed Attack Proxy) is a dynamic application security testing tool published under the Apache License. It allows users to manipulate all of the traffic that passes through it, including HTTPS encrypted traffic, when used as a proxy server.

## How to use it –

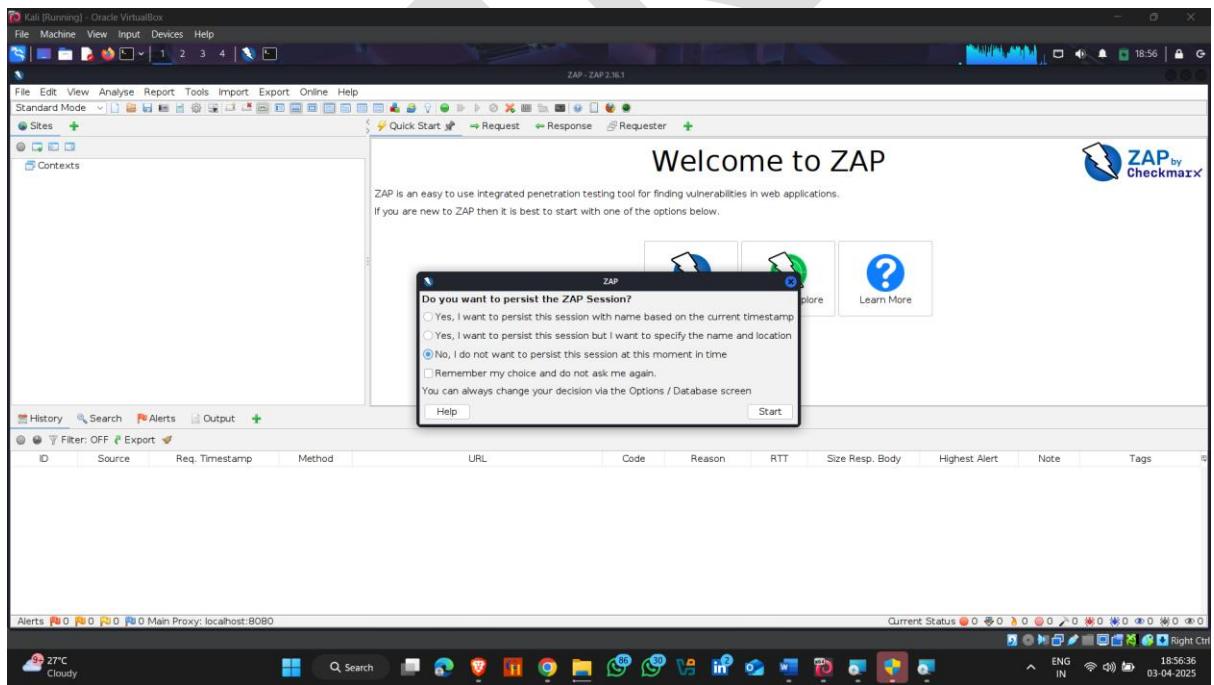
- ❖ Open kali Linux / Parrot OS
  - ❖ Open Terminal And type `sudo apt install zaproxy`



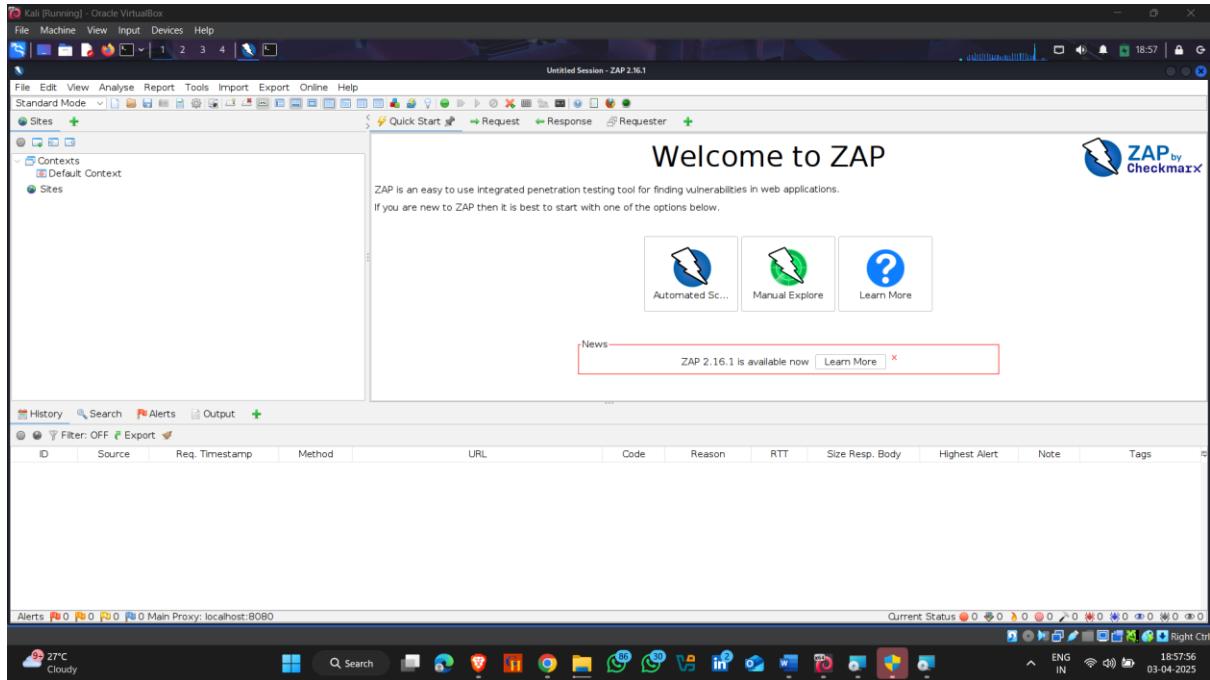
## ❖ Then type zaproxy



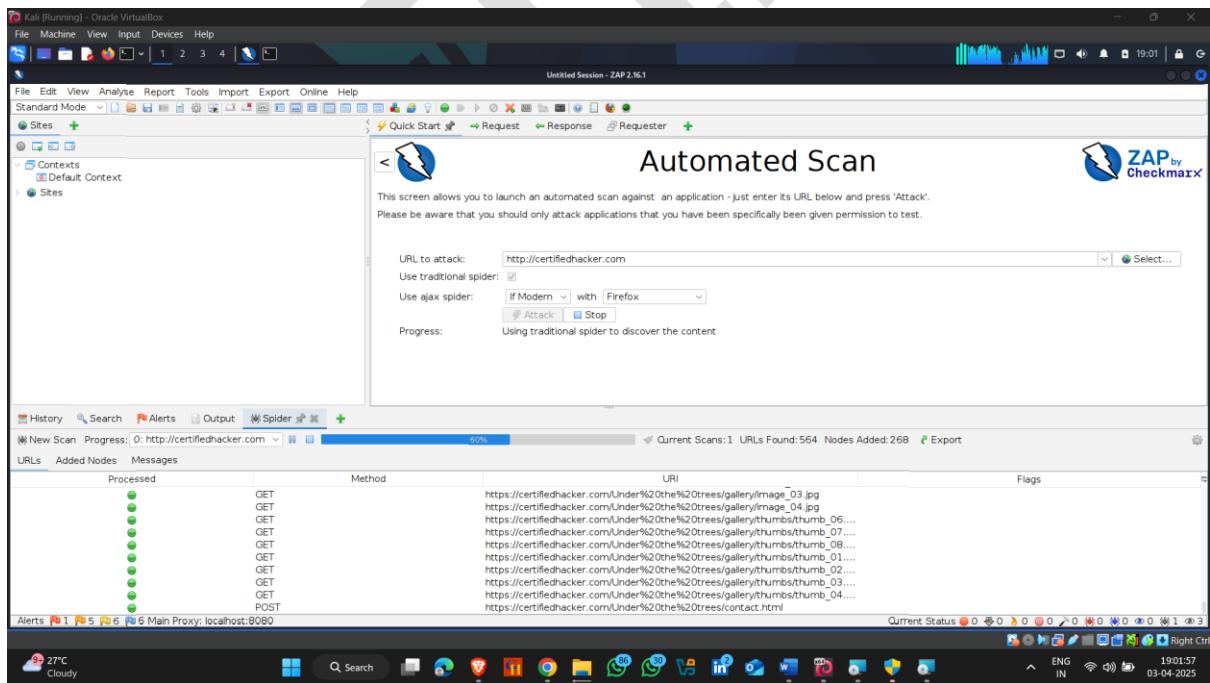
## ❖ Select third option and click on start



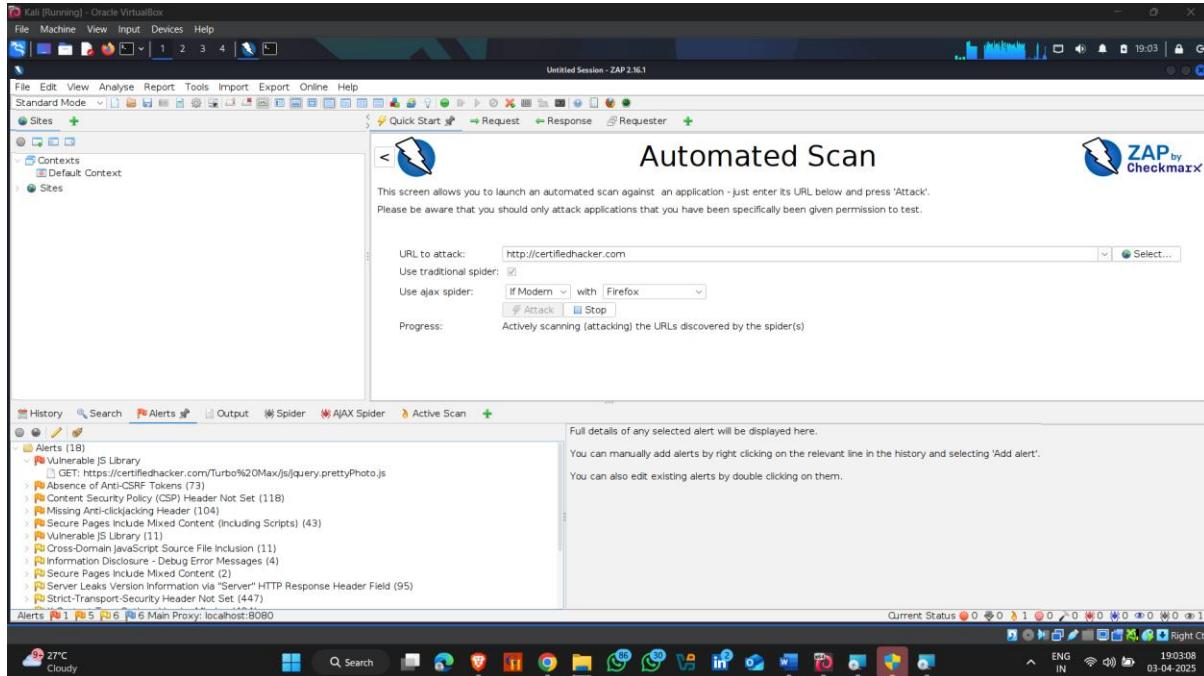
## ❖ Click on automated scan



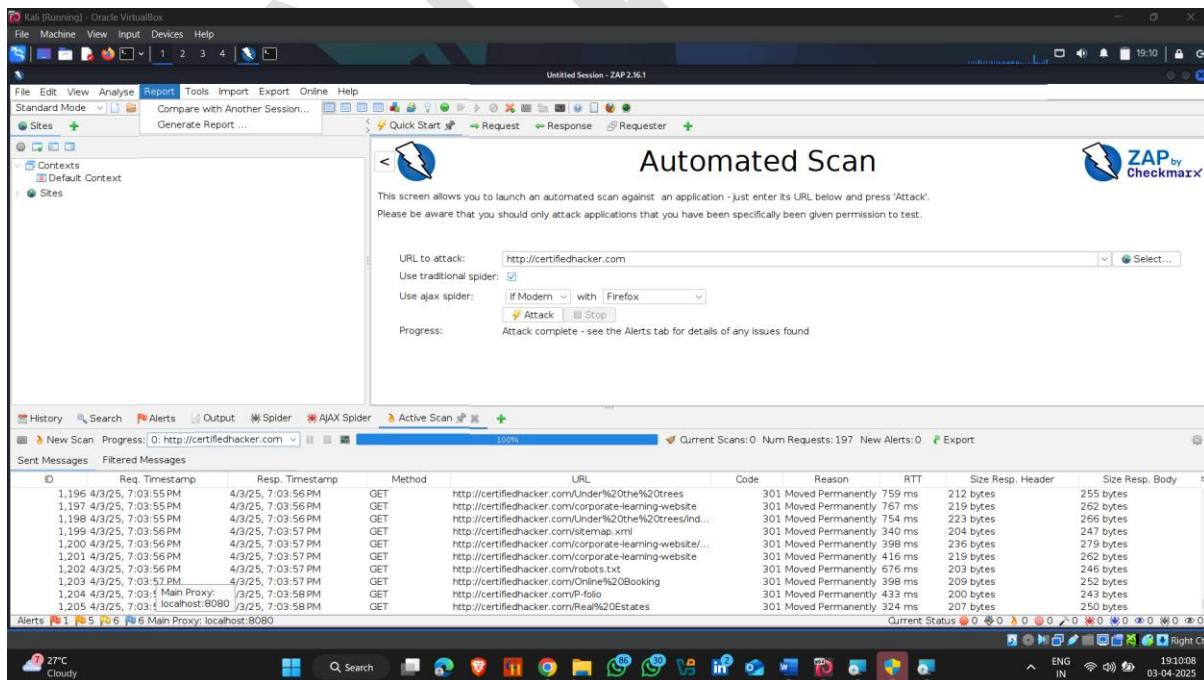
## ❖ Provide domain name , click on use traditional spider checkbox and click on attack



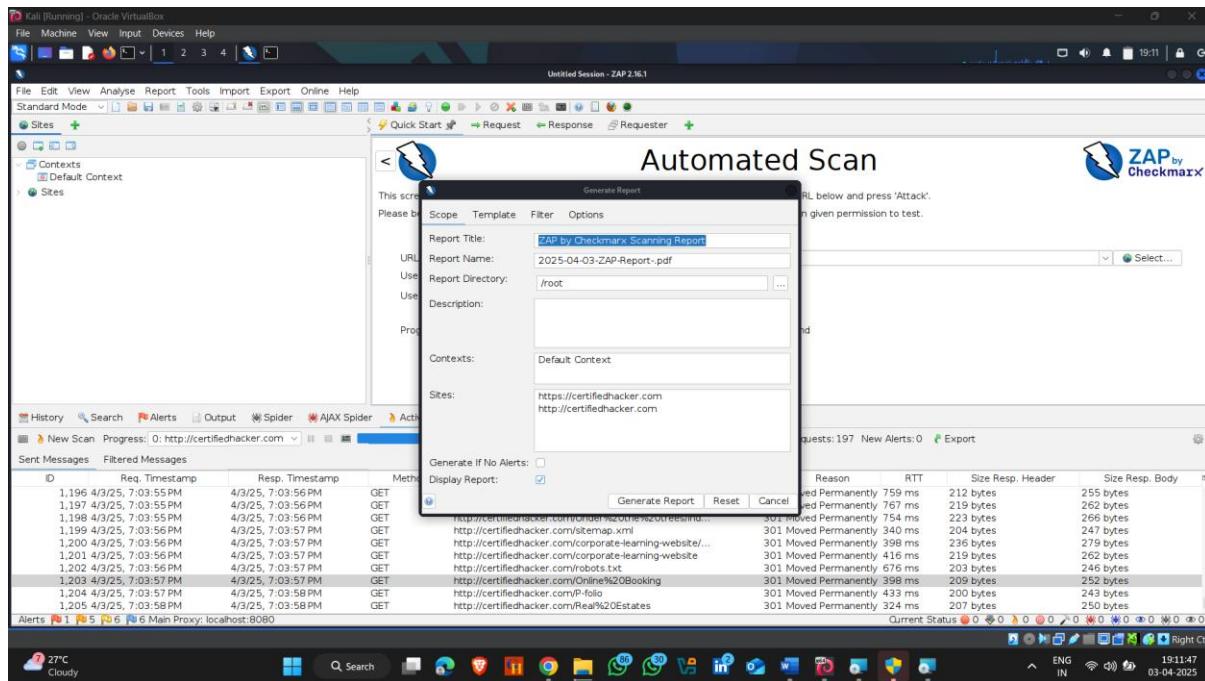
- ❖ If you want to see there is any vulnerability spotted on your target just click on alerts option
- ❖ See our target are vulnerable with many things



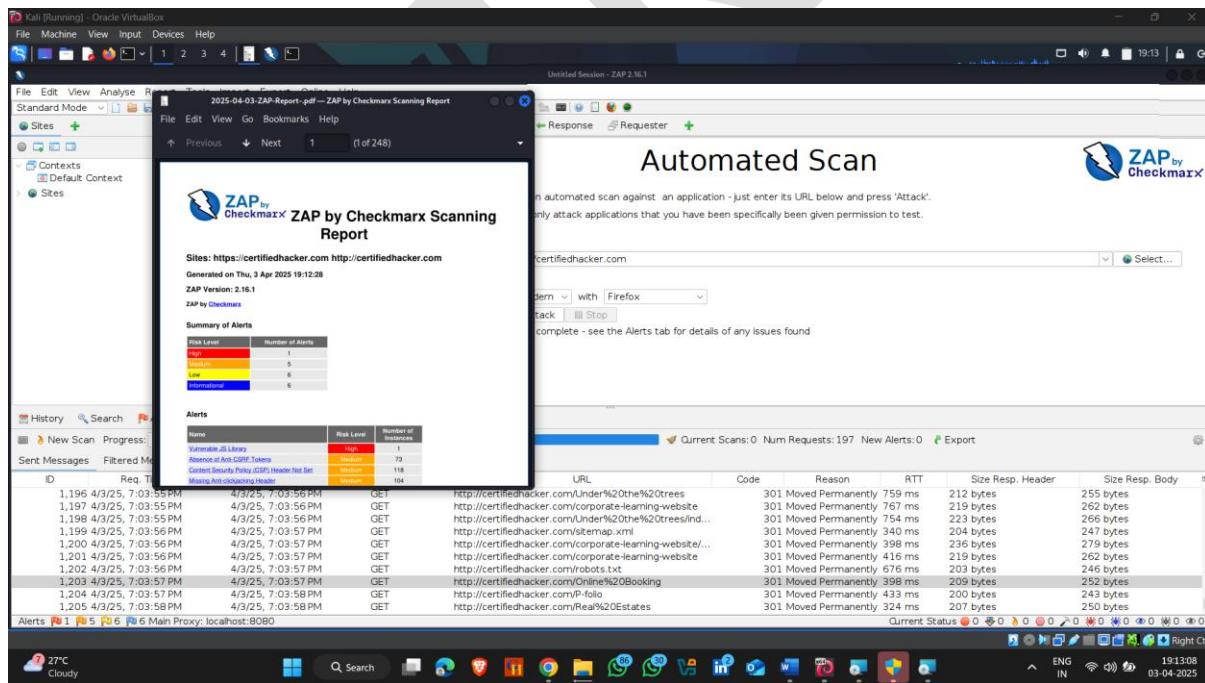
- ❖ Now You can also Generate report
- ❖ Click on report section and click generate report



❖ And click again on generate report



❖ Here You can see the detailed report



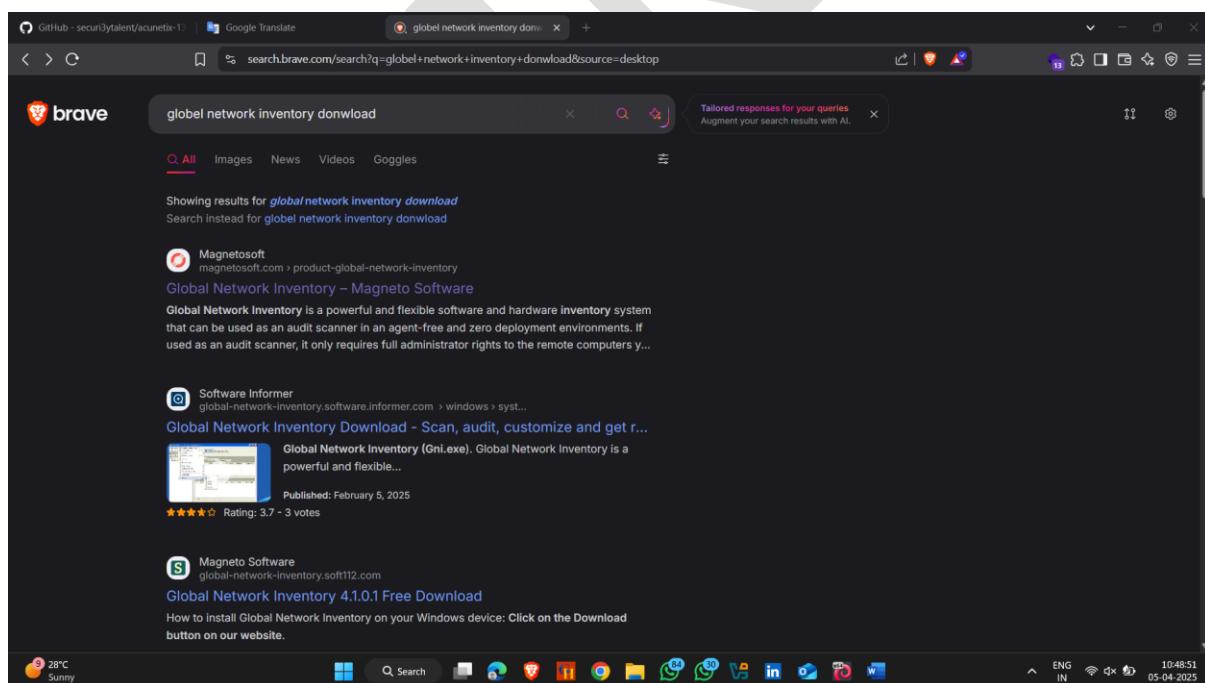
# Vulnerability Analysis Using Global Network Inventory

A Global Network Inventory Application is a software tool used by organizations—especially large enterprises or telecoms—to track, manage, and monitor all the hardware, software, and connections in their global IT and network infrastructure.

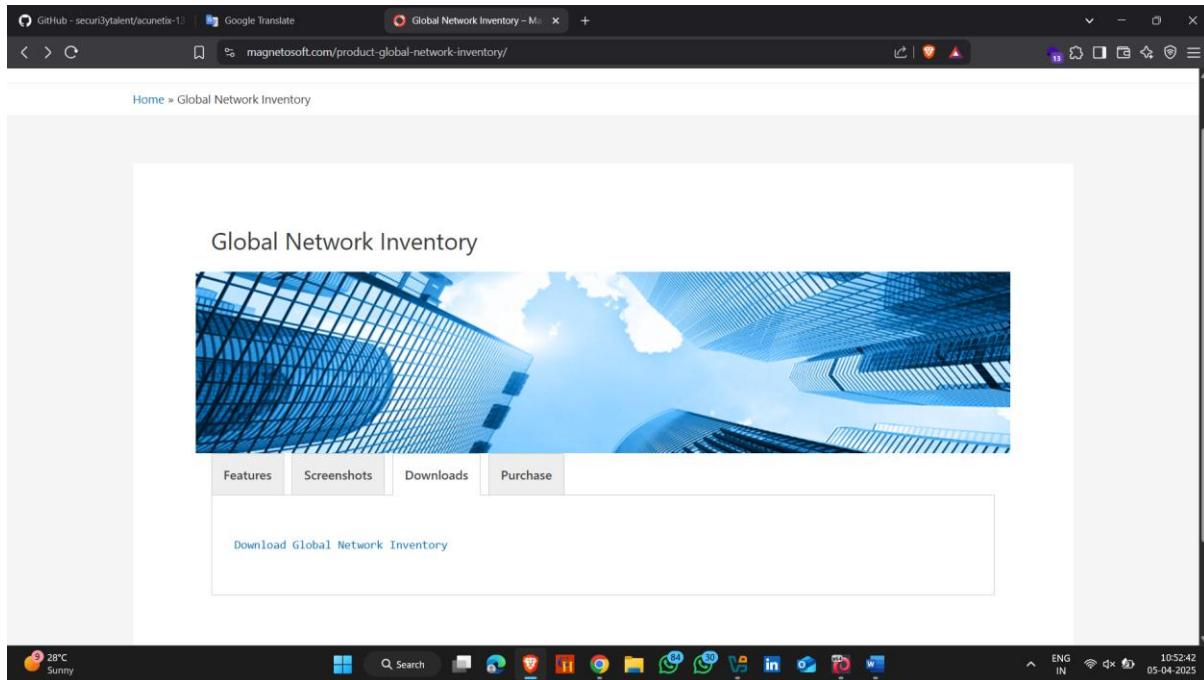
**Download link :-** <https://magnetosoft.com/product-global-network-inventory/>

**How to use it - :**

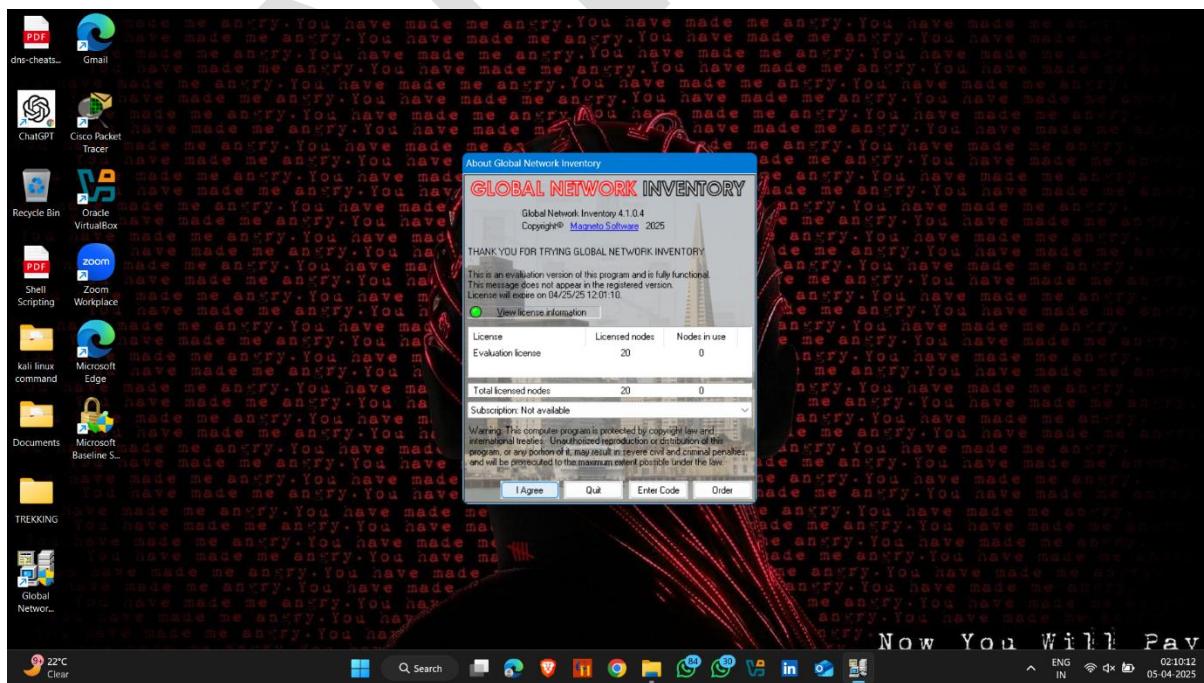
- Step 1 -: open browser
- Step 2 -: search global network inventory download and **click on magnetosoft website**



- Click on Download section and then click on Download Global network inventory

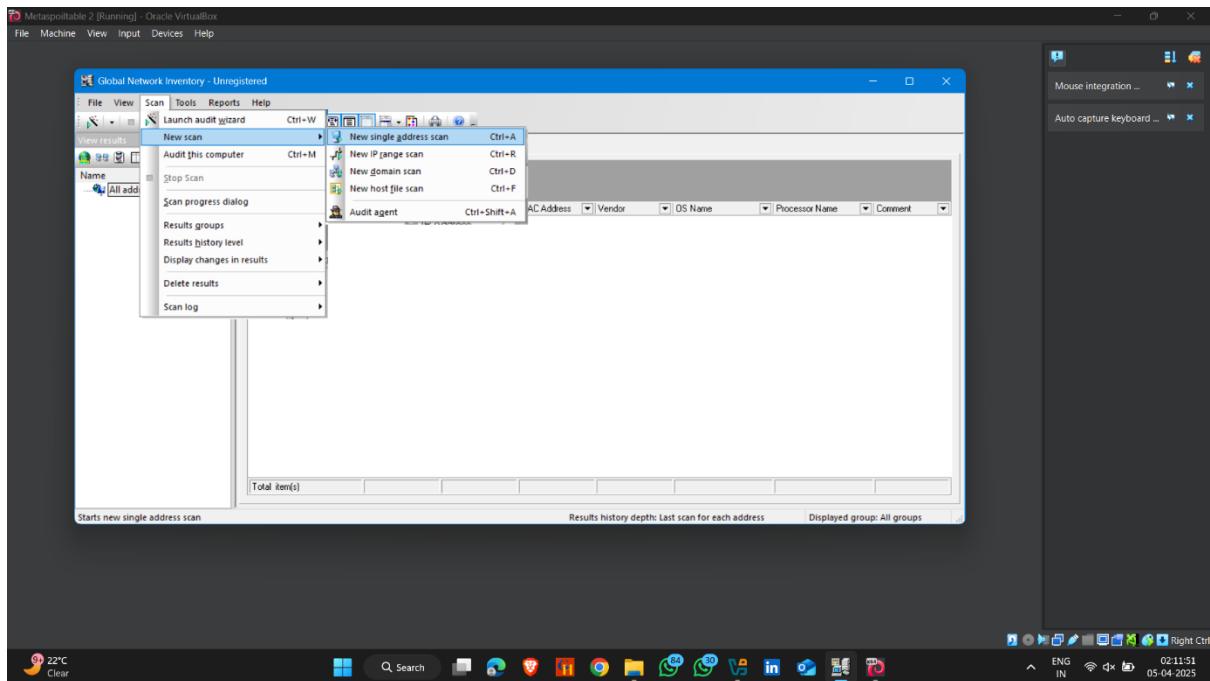


- Install it and setup it
- Here our installation is completed , click on I agree

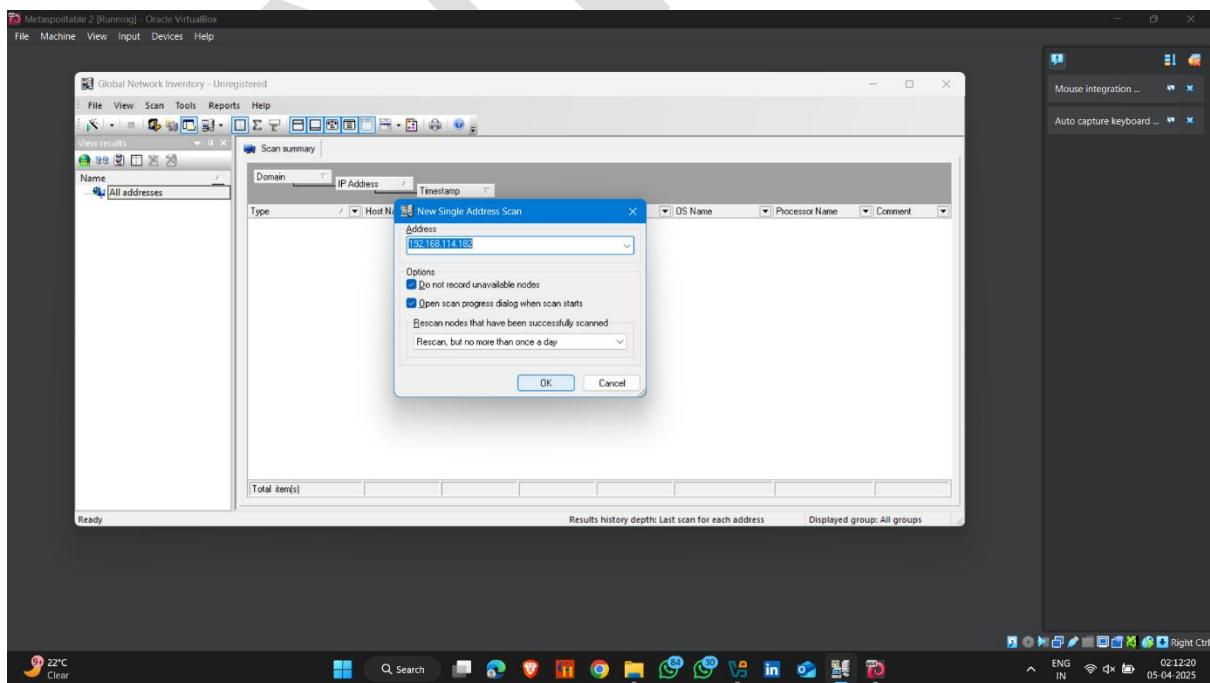


- Then click on scan option , new scan and new single address scan

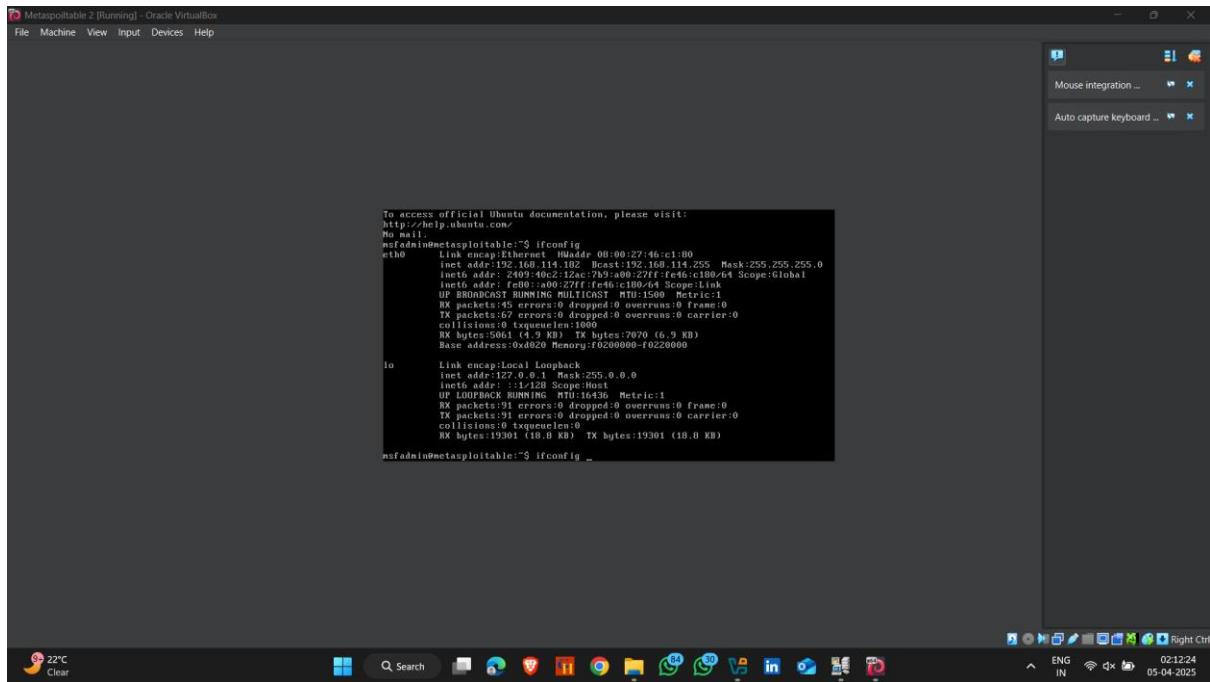
**Note :- you can also scan ip ranges , domain scan**



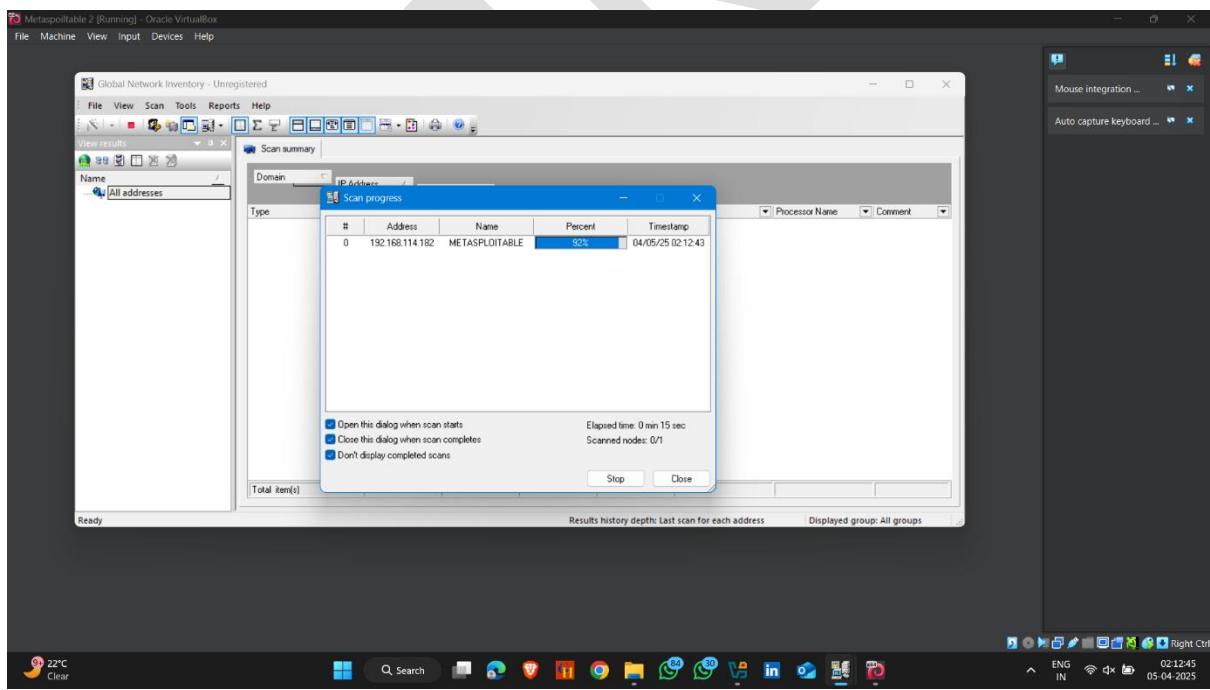
- Enter target ip address and click ok



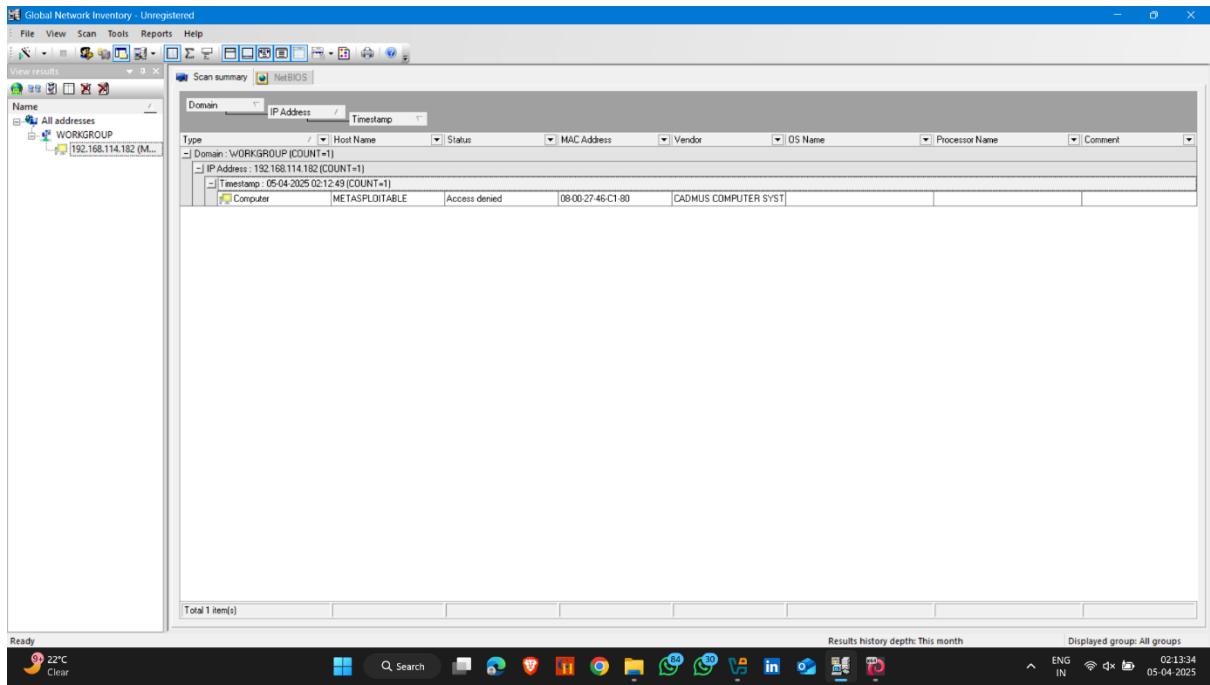
- In my case , I'm using metasploitable 2 as a target machine



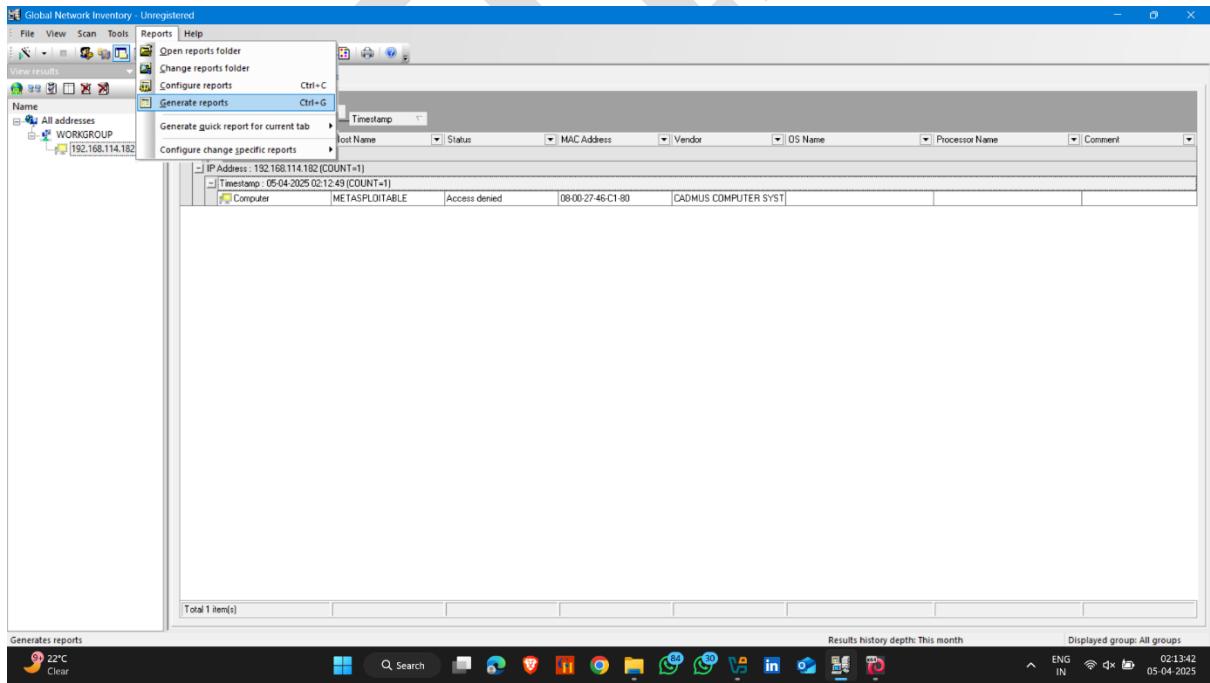
- Here scanning start



- Scan Completed



- Now you can also generate of scanning report , just click on report (navigation bar ) and then generate report



- Now you see the report



A screenshot of a Windows desktop showing a web browser window titled "Scan\_summary\_main\_04.05.25.htm". The browser is displaying a network scan report from "Global Network Inventory". The report shows one item in the "Scan summary" table:

Type	Host Name	Status	MAC Address	Vendor	OS Name	Processor Name	Comment
Domain	WORKGROUP (COUNT=1)						
IP Address	192.168.114.182 (COUNT=1)						
Timestamp	05-04-2025 02:12:49 (COUNT=1)						
<hr/>							
	Computer	METASPLITABLE	Access denied	08-00-27-46-C1-80	CADMUS COMPUTER SYSTEMS		
Total 1 item(s)							

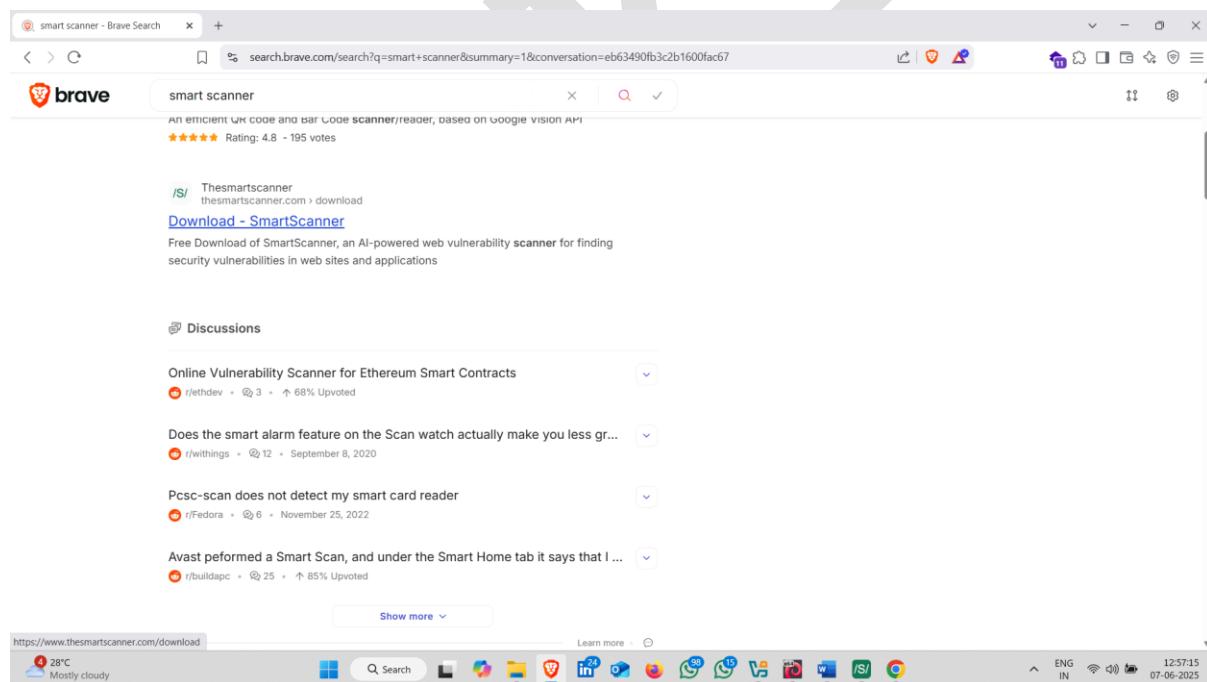
The browser address bar shows the full URL: "File | C:/Program%20Files%20(x86)/Magneto%20Software/GlobalNetworkInventory/Reports/Scan\_summary\_main\_04.05.25.htm". The taskbar at the bottom of the screen includes icons for File Explorer, Edge, and various system status indicators like battery level and date/time.

# Vulnerability Analysis Using Smart Scanner

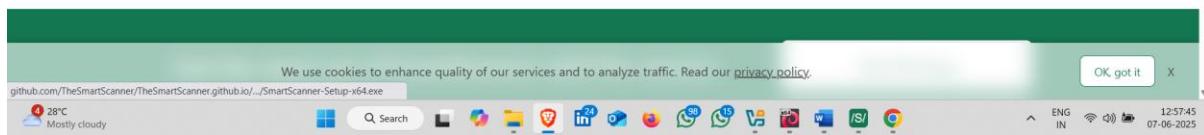
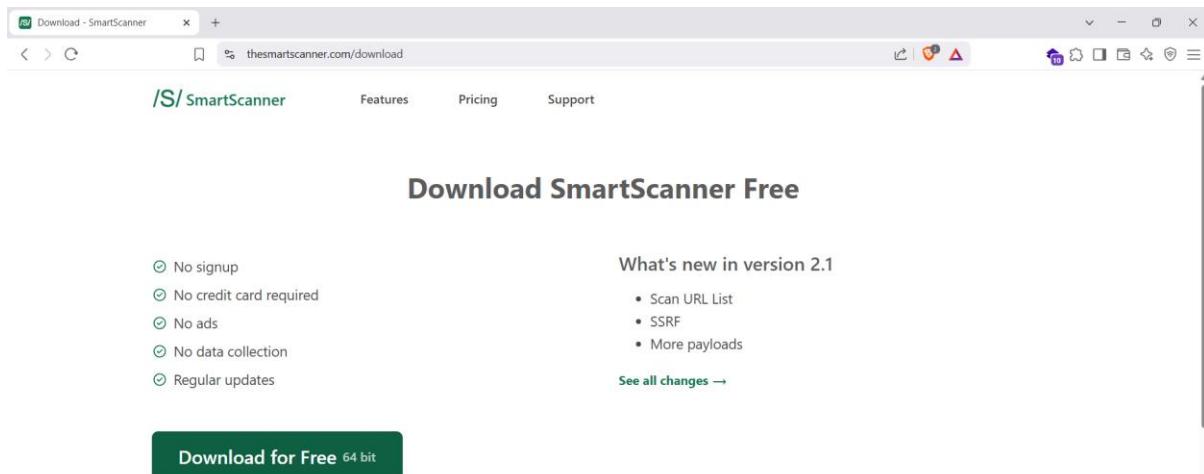
A **Smart Scanner** is an **intelligent vulnerability scanning tool or feature** that uses advanced techniques like automation, machine learning, or heuristic analysis to **efficiently detect security vulnerabilities** in systems, networks, or applications — with **greater accuracy, speed, and context-awareness** compared to traditional scanners.

How to download it :-

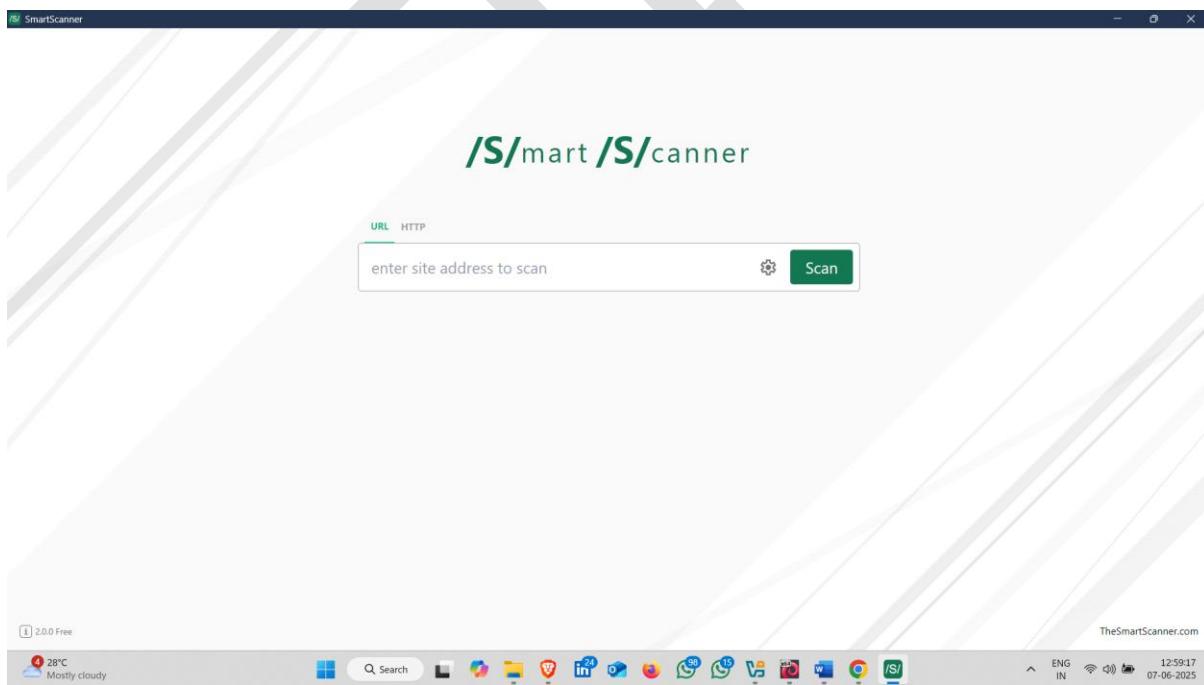
- Open Browser and search smart scanner
- Click on official Website



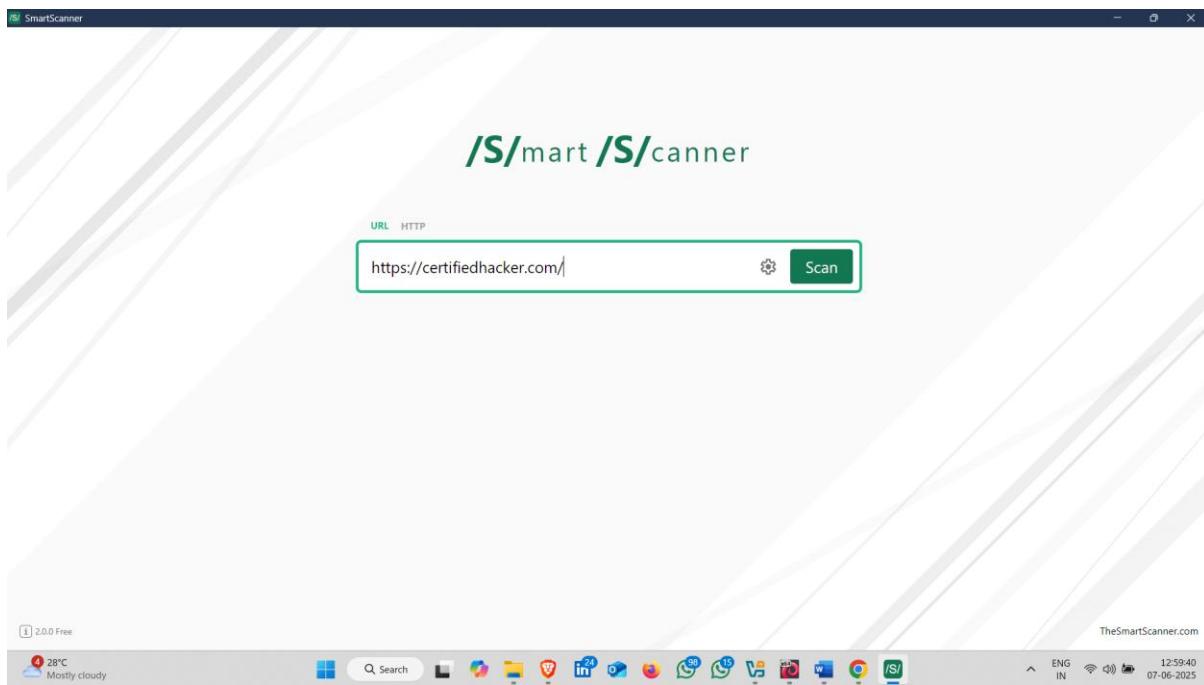
- Click on Download for free 



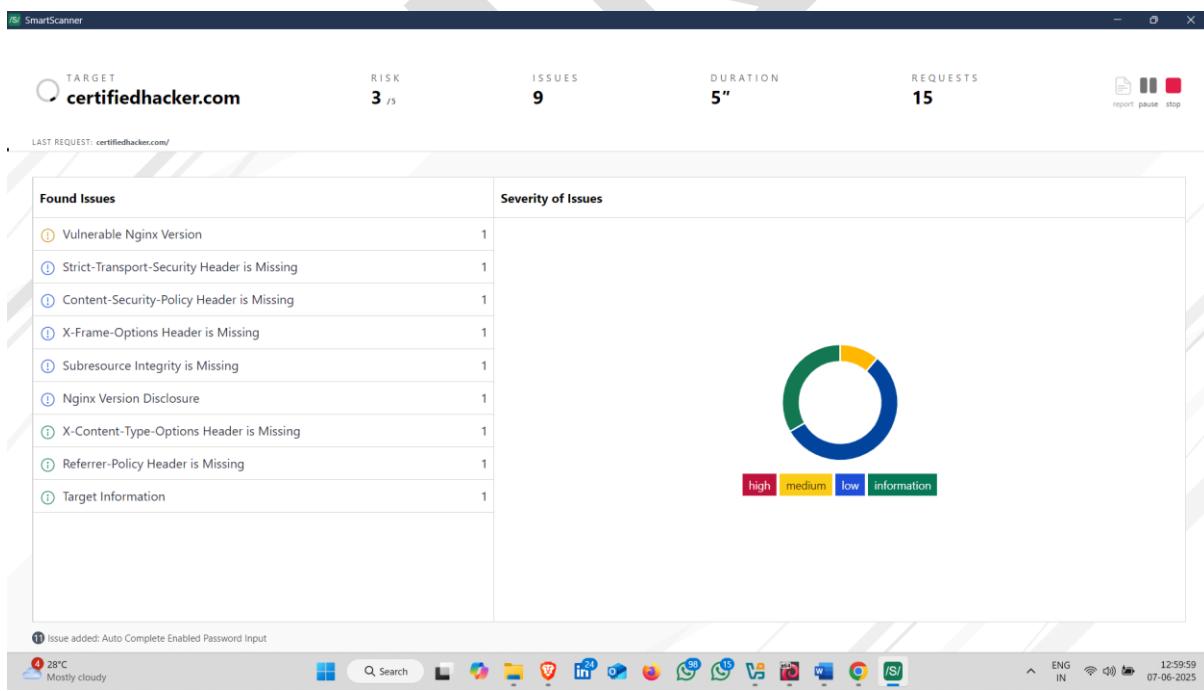
- After Downloading the app open and setup it :-
- Now enter the website that you want to scan



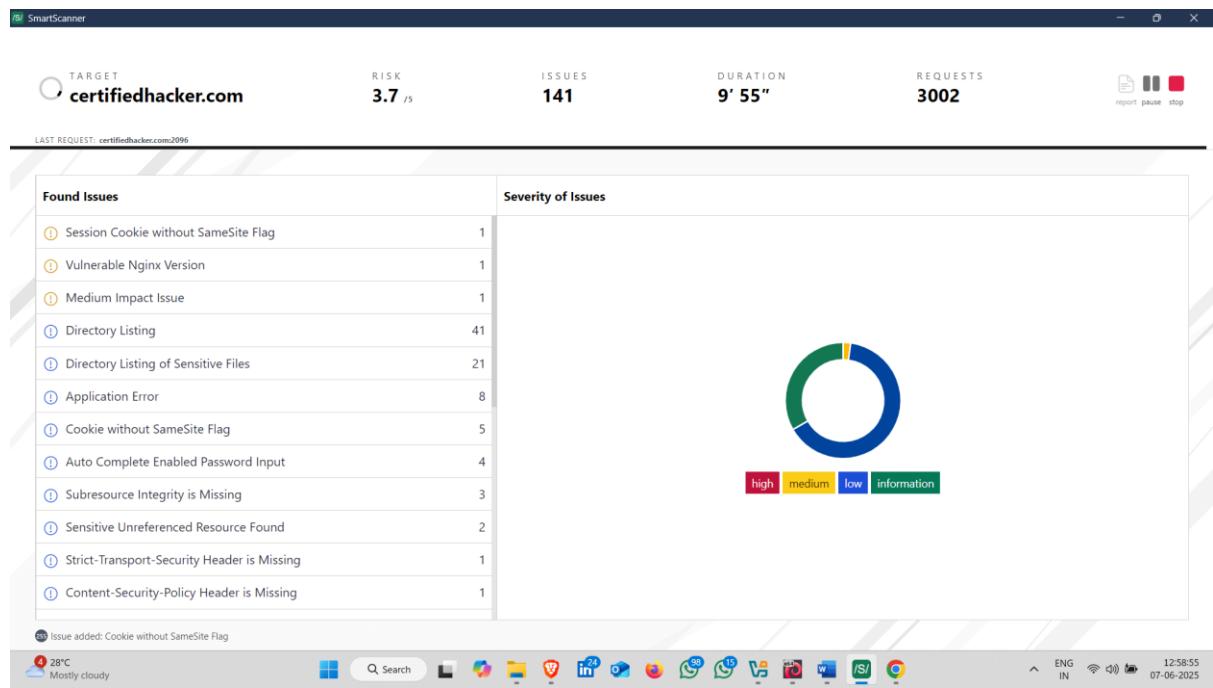
- Now click on Scan



- It Started the scanning 



## • Finding the Vulnerability



# Vulnerability Analysis Using Qualys SSL Labs

## 1. What is Qualys SSL Labs?

Qualys SSL Labs is a **free, public online tool** offered by Qualys to test and analyze the **SSL/TLS configuration** of web servers.

---

## 2. Purpose of SSL Labs Scanning:

Its goal is to help organizations, administrators, and researchers identify **weaknesses, misconfigurations, and outdated cryptographic settings** in HTTPS websites.

---

## 3. Website URL:

The official tool is available at: <https://www.ssllabs.com/ssltest/>

---

## 4. What It Tests:

It tests how well a server implements **SSL/TLS encryption**, focusing on certificates, protocols, key exchange, cipher strength, and known vulnerabilities.

---

## 5. Input Required:

You simply enter a **domain name** (e.g., [www.example.com](http://www.example.com)) and start the scan — no installation or account is required.

---

## 6. Who Uses It:

Used by **ethical hackers, web admins, developers, auditors, and security professionals** for SSL configuration auditing.

---

## 7. Key Features of SSL Labs Scanner:

- Checks for **certificate validity, expiration, chain trust**
  - Verifies **support for TLS versions (1.0 to 1.3)**
  - Analyzes **supported cipher suites** and encryption strength
  - Detects **insecure renegotiation** and weak key exchange
  - Checks for **HTTP Strict Transport Security (HSTS)**
  - Looks for known SSL/TLS vulnerabilities (e.g., **Heartbleed, POODLE, BEAST**)
  - Supports **forward secrecy** testing
  - Shows whether **OCSP Stapling** is enabled
  - Tests **server preference order**
  - Measures **response time and handshake simulations**
  - Rates the server with an **overall grade (A+ to F)**
- 

## 8. Grading System:

- **A+** = Perfect configuration with strong ciphers, latest protocols, HSTS, and no known issues
  - **A** = Strong configuration but missing HSTS or other small issues
  - **B-D** = Moderate to weak configurations
  - **F** = Major vulnerabilities or expired certificates
  - **T** = Test failed or timed out
- 

## 9. Vulnerabilities It Detects:

- **Heartbleed** (OpenSSL flaw leaking memory)
- **POODLE** (SSLv3 protocol downgrade attack)
- **BEAST** (CBC block cipher weakness)
- **CRIME** (compression attack)

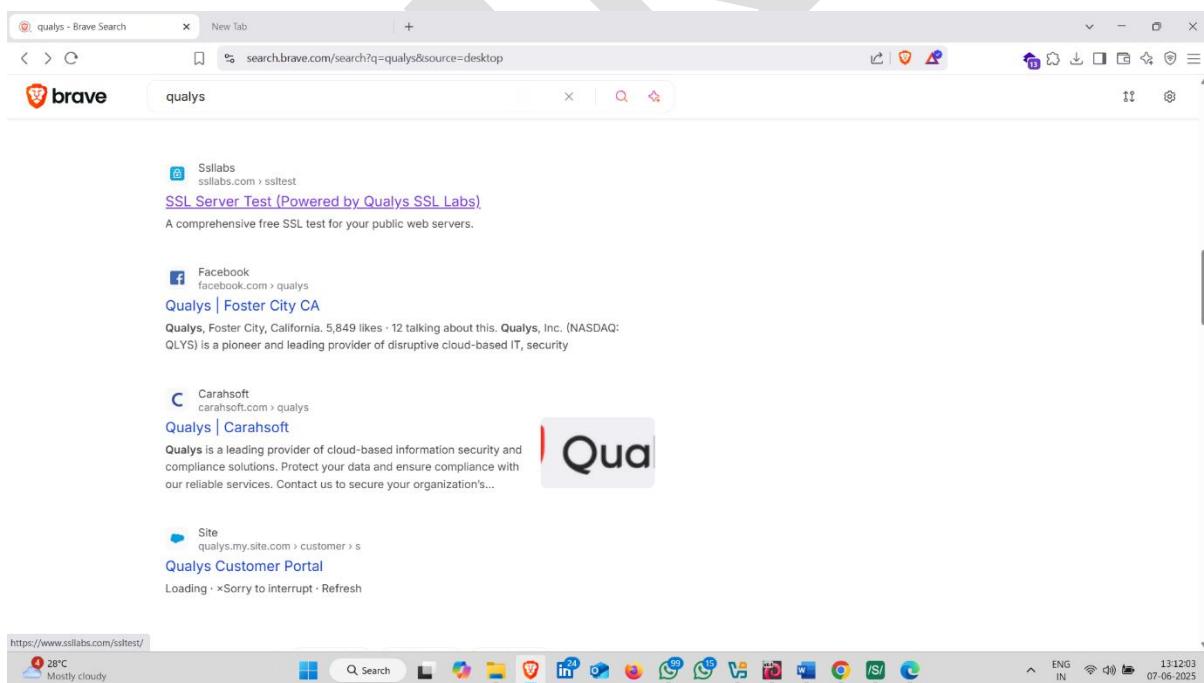
- **DROWN** (SSLv2 usage in TLS servers)
  - **Logjam** (weak Diffie-Hellman parameters)
  - **RC4 cipher usage** (insecure and deprecated)
  - **Export-grade ciphers** (weak for modern use)
- 

## 10. Scan Depth:

The tool simulates how different browsers and devices (e.g., IE on XP, Chrome on Android, Safari on Mac) interact with the server to identify handshake compatibility issues.

### How to use it :-

- Open Browser and Search Qualys Ssl Labs
- Click on ssllabs Official Website 



- Provide a URL for scanning

**SSL Server Test**

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname:  Submit  Do not show the results on the boards

Recently Seen	Recent Best	Recent Worst
<a href="#">www.ecrochetpatterns.com</a>	<a href="#">dthreevolution.sdworx.co.uk</a> A+	<a href="#">drafe.sdworx.co.uk</a> T
<a href="#">www.qdems.com</a>	<a href="#">www.cognitiforms.com</a> A+	<a href="#">daojianchina.com</a> T
<a href="#">fligma.us</a>	<a href="#">gelicloud.de</a> A+	<a href="#">revoked2048.entrust.net</a> F
<a href="#">www.stes.tyc.edu.tw</a>	<a href="#">digitalengine.mastercard.com</a> A	<a href="#">haoguokei.com</a> F
<a href="#">nettes-gaestehaus.de</a>	<a href="#">contactmeasap.com</a> A	<a href="#">denning.pytampartners.com</a> T
<a href="#">humanize-consultancy.com</a>	<a href="#">rssecurity.co.uk</a> A-	<a href="#">test.secure.viavum.payercomp..._</a> T
<a href="#">portal.tanssok.de</a>	<a href="#">data.talentjob.ir</a> B	<a href="#">ciodeveloper.ciodev.accentur...</a> F
<a href="#">an0ns.ru</a>	<a href="#">www.tgof.org.tw</a> B	<a href="#">manpoweradvisors.com</a> T
<a href="#">www.intersal.com</a>	<a href="#">macias-knapo-2.technetblogge..._</a> B	<a href="#">fluidly.amendsquare.co</a> T
<a href="#">asmtarbalance-api.online.dv...</a>	<a href="#">monitoring.adriankezik.dev</a> B	<a href="#">boogiewoogie.com</a> T

- Click on Submit

**SSL Server Test**

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname:  Submit  Do not show the results on the boards

Recently Seen	Recent Best	Recent Worst
<a href="#">www.ecrochetpatterns.com</a>	<a href="#">dthreevolution.sdworx.co.uk</a> A+	<a href="#">drafe.sdworx.co.uk</a> T
<a href="#">www.qdems.com</a>	<a href="#">www.cognitiforms.com</a> A+	<a href="#">daojianchina.com</a> T
<a href="#">fligma.us</a>	<a href="#">gelicloud.de</a> A+	<a href="#">revoked2048.entrust.net</a> F
<a href="#">www.stes.tyc.edu.tw</a>	<a href="#">digitalengine.mastercard.com</a> A	<a href="#">haoguokei.com</a> F
<a href="#">nettes-gaestehaus.de</a>	<a href="#">contactmeasap.com</a> A	<a href="#">denning.pytampartners.com</a> T
<a href="#">humanize-consultancy.com</a>	<a href="#">rssecurity.co.uk</a> A-	<a href="#">test.secure.viavum.payercomp..._</a> T
<a href="#">portal.tanssok.de</a>	<a href="#">data.talentjob.ir</a> B	<a href="#">ciodeveloper.ciodev.accentur...</a> F
<a href="#">an0ns.ru</a>	<a href="#">www.tgof.org.tw</a> B	<a href="#">manpoweradvisors.com</a> T
<a href="#">www.intersal.com</a>	<a href="#">macias-knapo-2.technetblogge..._</a> B	<a href="#">fluidly.amendsquare.co</a> T
<a href="#">asmtarbalance-api.online.dv...</a>	<a href="#">monitoring.adriankezik.dev</a> B	<a href="#">boogiewoogie.com</a> T

- Scanning Started

A screenshot of a web browser displaying the Qualys SSL Labs report for `certifiedhacker.com`. The page shows a progress bar indicating "Please wait... 23% complete" and "Determining available cipher suites". Below this, a detailed view of "Certificate #1: RSA 2048 bits (SHA256withRSA)" is shown, listing various certificate details such as subject, common names, alternative names, serial number, validity period, key type, issuer, and signature algorithm. The browser interface includes a taskbar at the bottom with various application icons.

- Scan Completed 🎉

A screenshot of a web browser displaying the Qualys SSL Labs report for `certifiedhacker.com`, showing the completed scan results. The report is titled "SSL Report: certifiedhacker.com (162.241.216.11)". It includes a summary section with an overall rating of "A" and four green bars representing "Certificate", "Protocol Support", "Key Exchange", and "Cipher Strength". Below this, there are sections for "Documentation", "Browser Support", and "TLS 1.3 Support". The browser interface includes a taskbar at the bottom with various application icons.

- **Result**  



A screenshot of a Microsoft Edge browser window displaying the SSL Labs test results for a certificate. The title bar shows 'SSL Server Test: certifiedhacker.com' and the address bar shows 'sslabs.com/sslttest/analyze.html?d=certifiedhacker.com'. The main content area is titled 'Certificate #1: RSA 2048 bits (SHA256withRSA)'. The table below provides detailed information about the certificate:

Server Key and Certificate #1	
Subject	www.certifiedhacker.com Fingerprint SHA256: 5fb849b53c28dbd4a701a5881ba1e3182c0d9ad280ca8002414e9de61cefb Pfx SHA256: 0d2d8c4cEa8UUC0BSSVK3t7YQnUJ23MeOGvYGA-
Common names	www.certifiedhacker.com
Alternative names	autodiscover.certifiedhacker.com certifiedhacker.com cpanel.certifiedhacker.com mail.certifiedhacker.com webdisk.certifiedhacker.com webmail.certifiedhacker.com www.certifiedhacker.com
Serial Number	068a33f528a371bc89b1e49a69033192dd
Valid from	Tue, 29 Apr 2025 15:00:15 UTC
Valid until	Mon, 28 Jul 2025 15:00:14 UTC (expires in 1 month and 21 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R10 AIA: http://r10.clenz.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://r10.clenz.org/94.crl OCSP: http://r10.clenz.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

**THANK YOU**