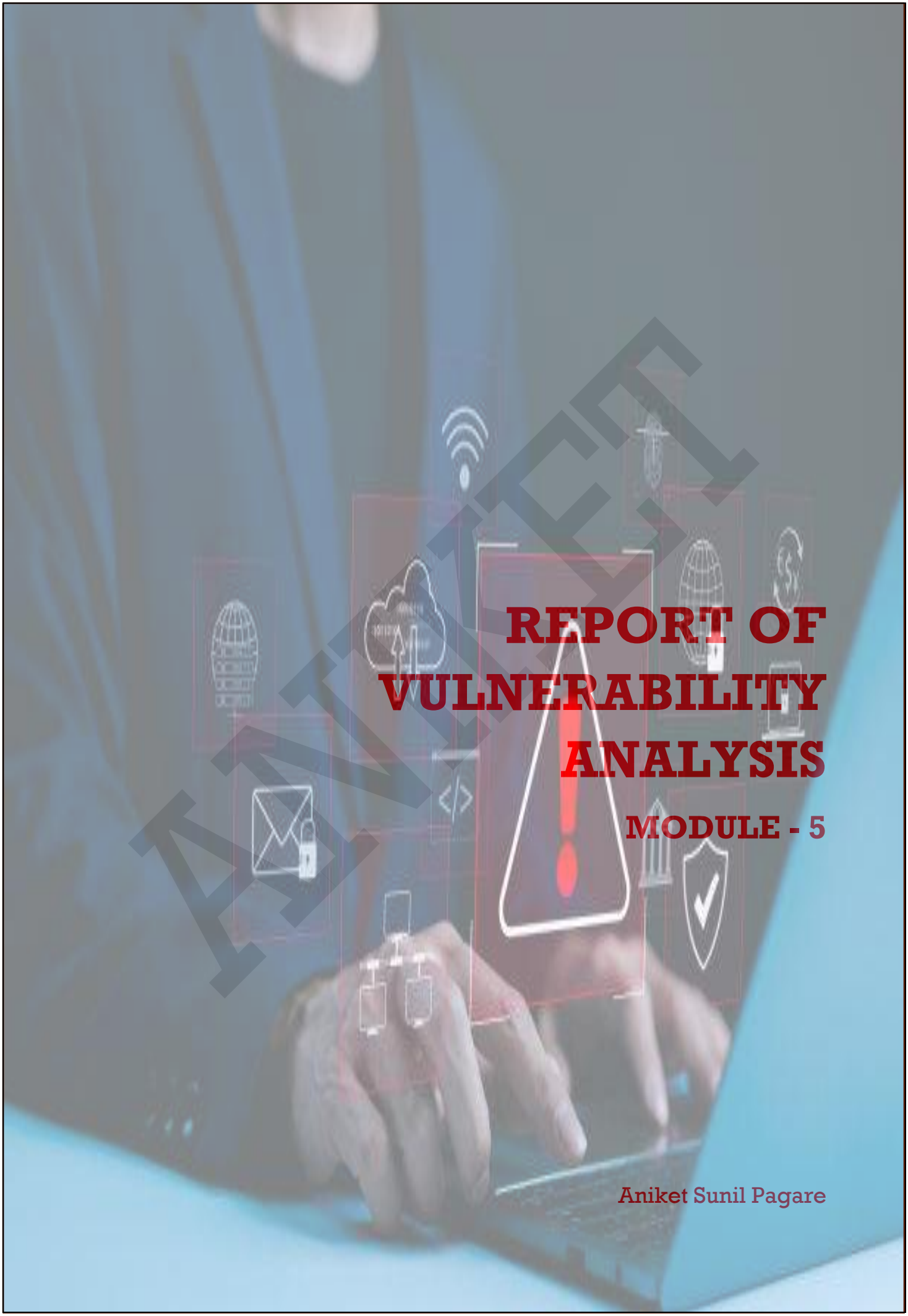


REPORT OF VULNERABILITY ANALYSIS

MODULE - 5

Aniket Sunil Pagare

Table of Contents: Vulnerability Analysis

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Configuration	Default credentials, outdated services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
MBSA	Windows-specific vulnerability scanning
ZAP (OWASP)	Manual + automated web testing
Trivy	Container and cloud scan tool
Qualys SSL Labs	SSL/TLS misconfiguration tester

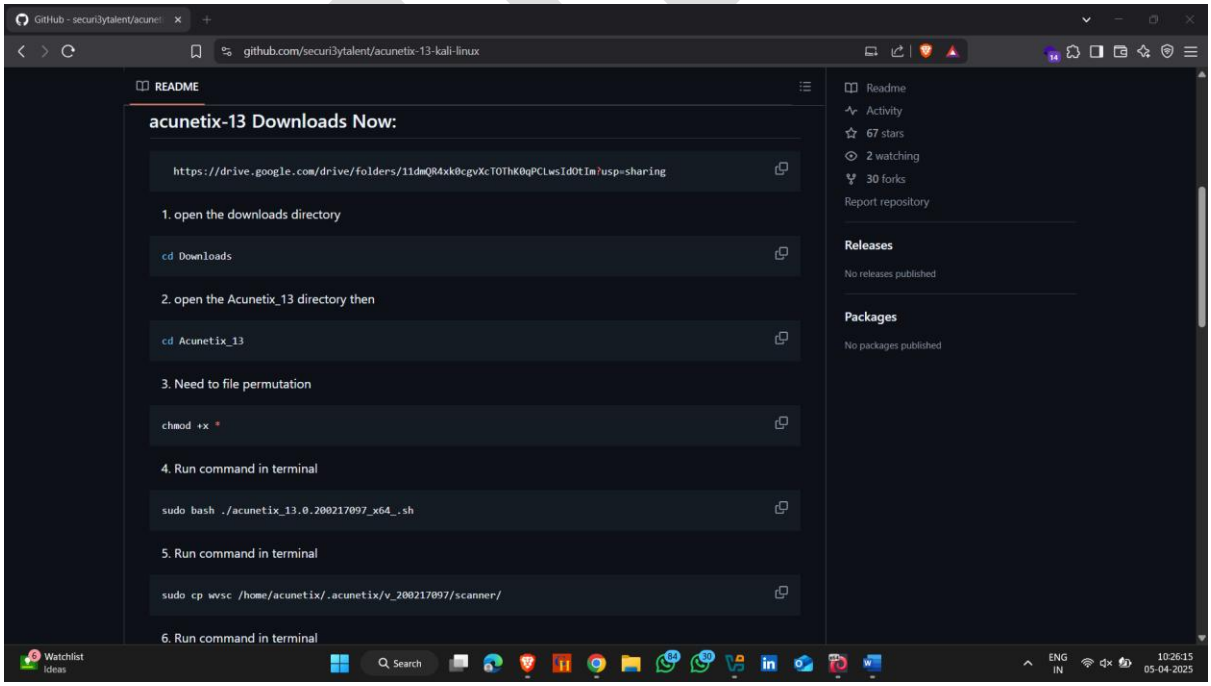
Vulnerability Analysis Using Acunetix

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

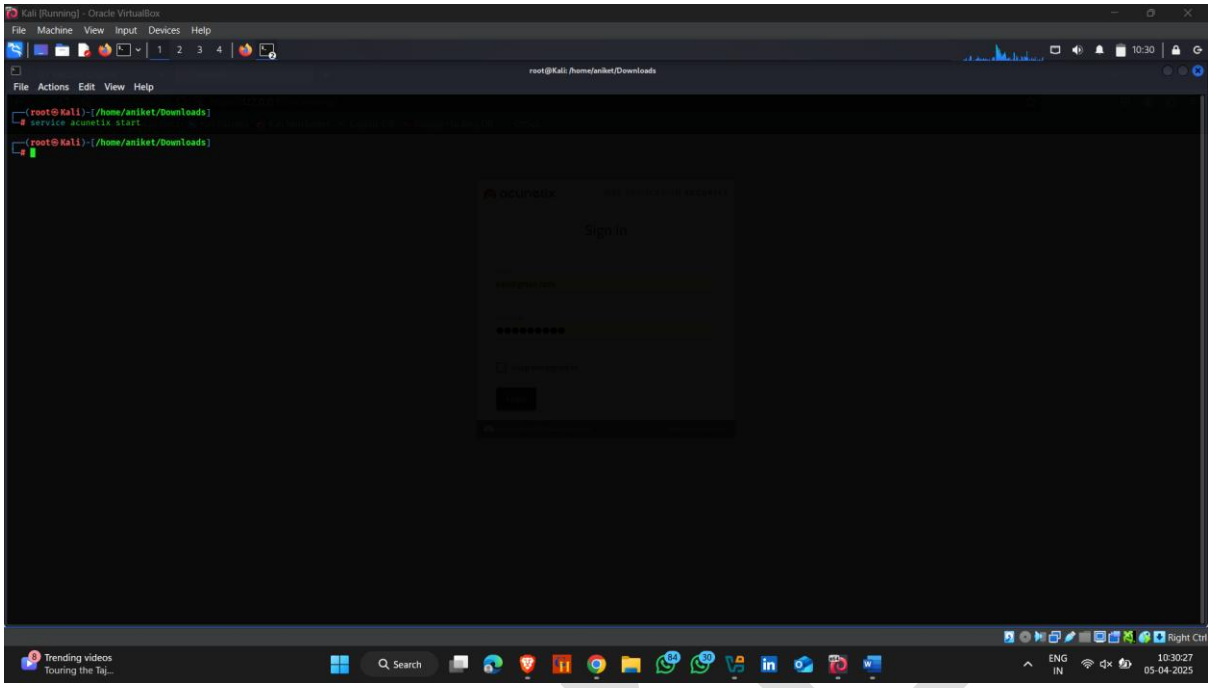
Download link - : https://github.com/securi3ytalent/acunetix-13-kali-linux

How to use it - :

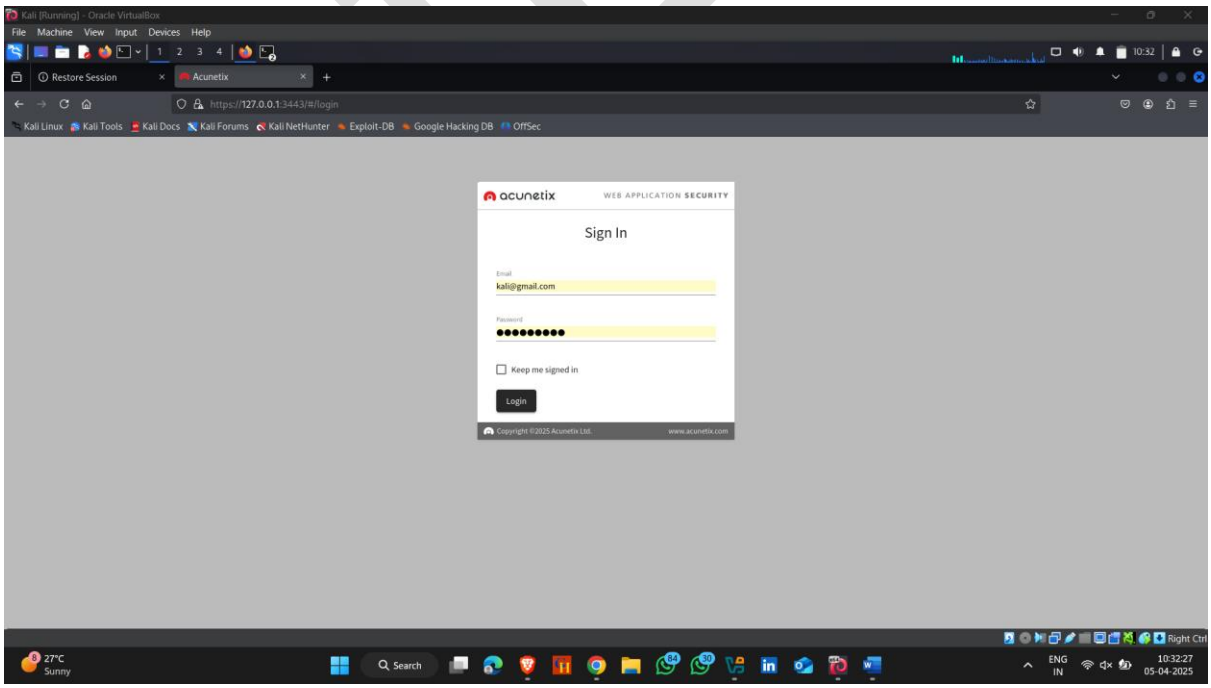
- Step 1 -: Open kali linux / parrot OS
- Step 2 -: type git clone and paste git link
- Step 3 -: copy and paste command one by one



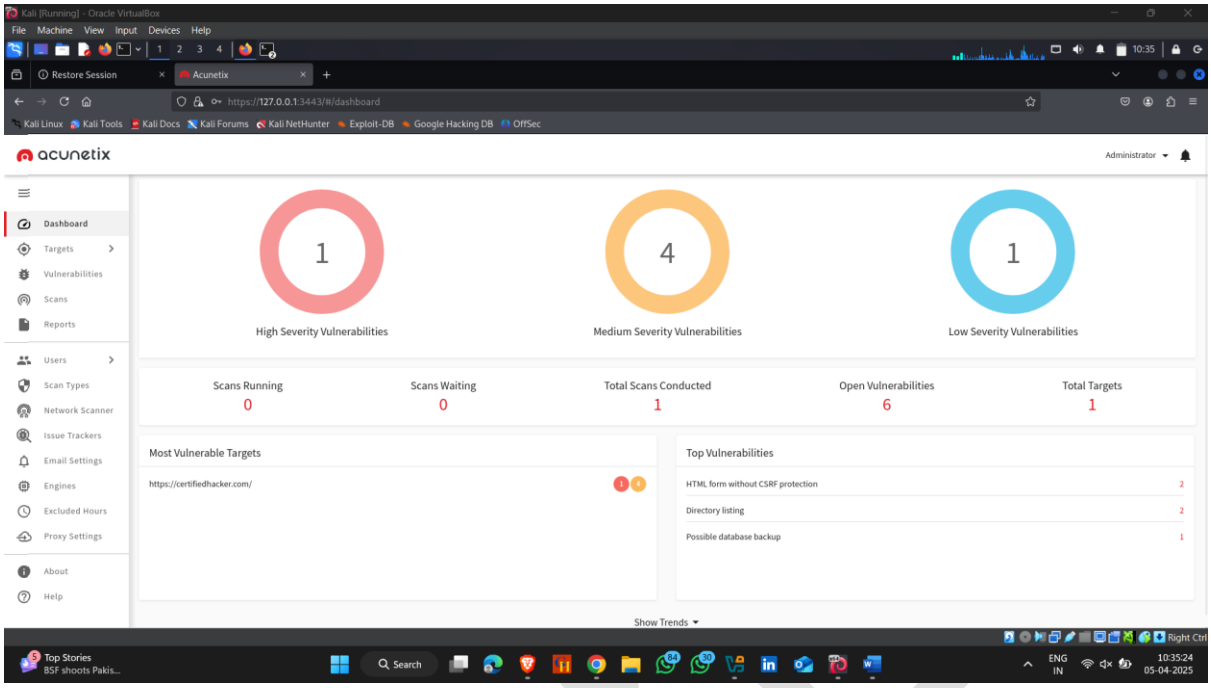
- Start Acunetix using **service acunetix start**



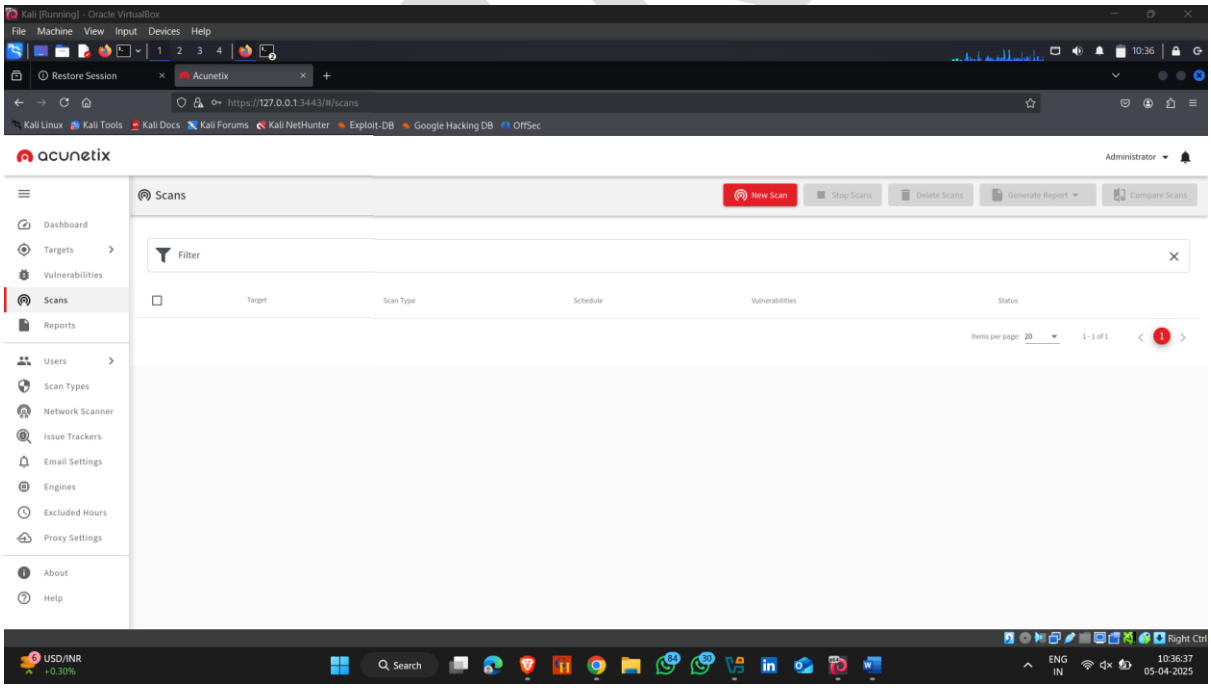
- Now open a firefox and type in url section **https://127.0.0.1:3443**
- Enter email and password that you enter on installation process



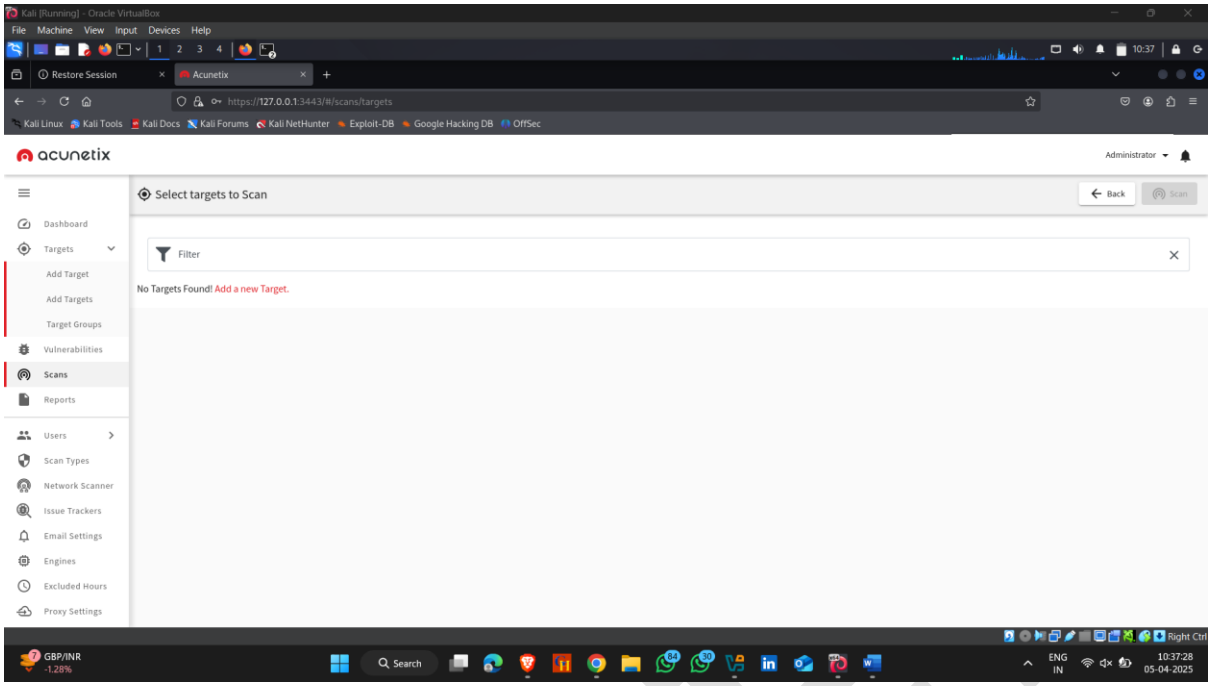
- Successfully login in acunetix



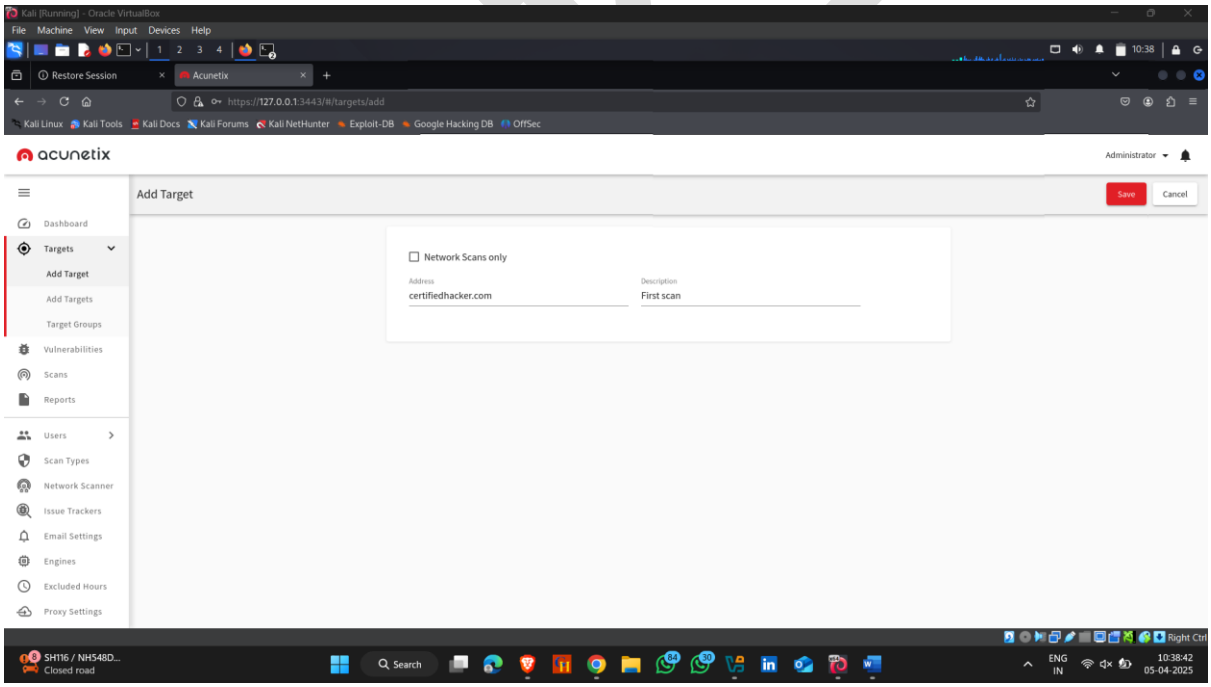
- Then click on scan and then click on new scan



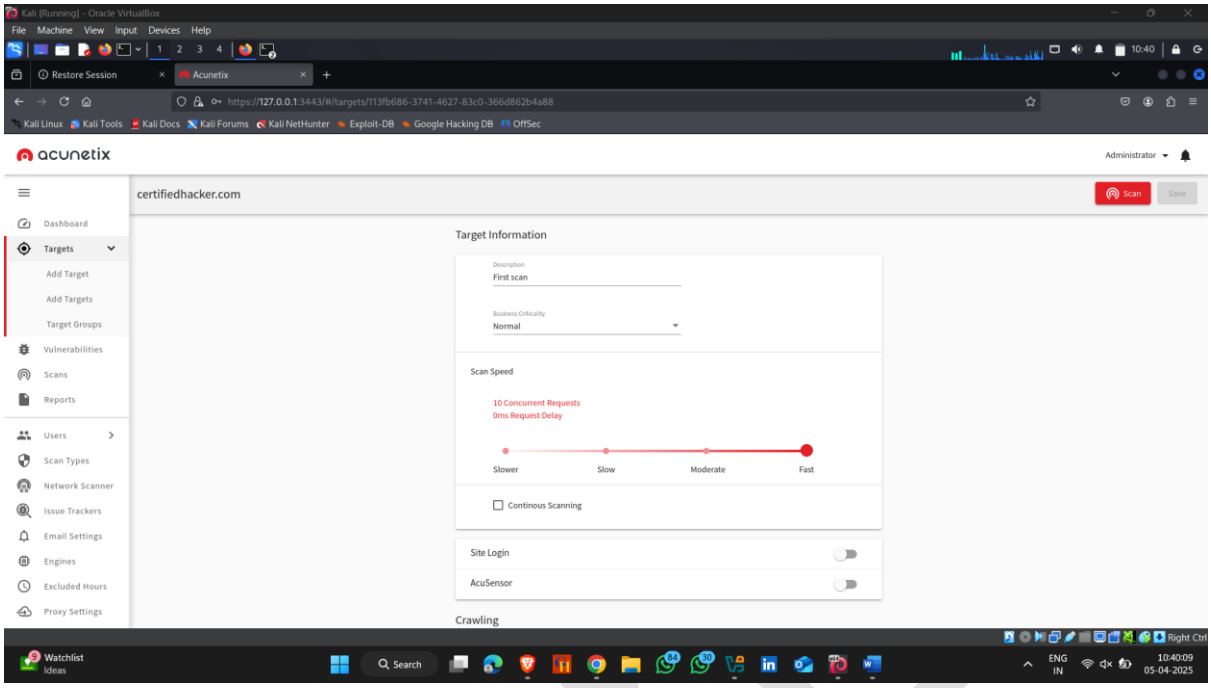
- And then click on **add new target**



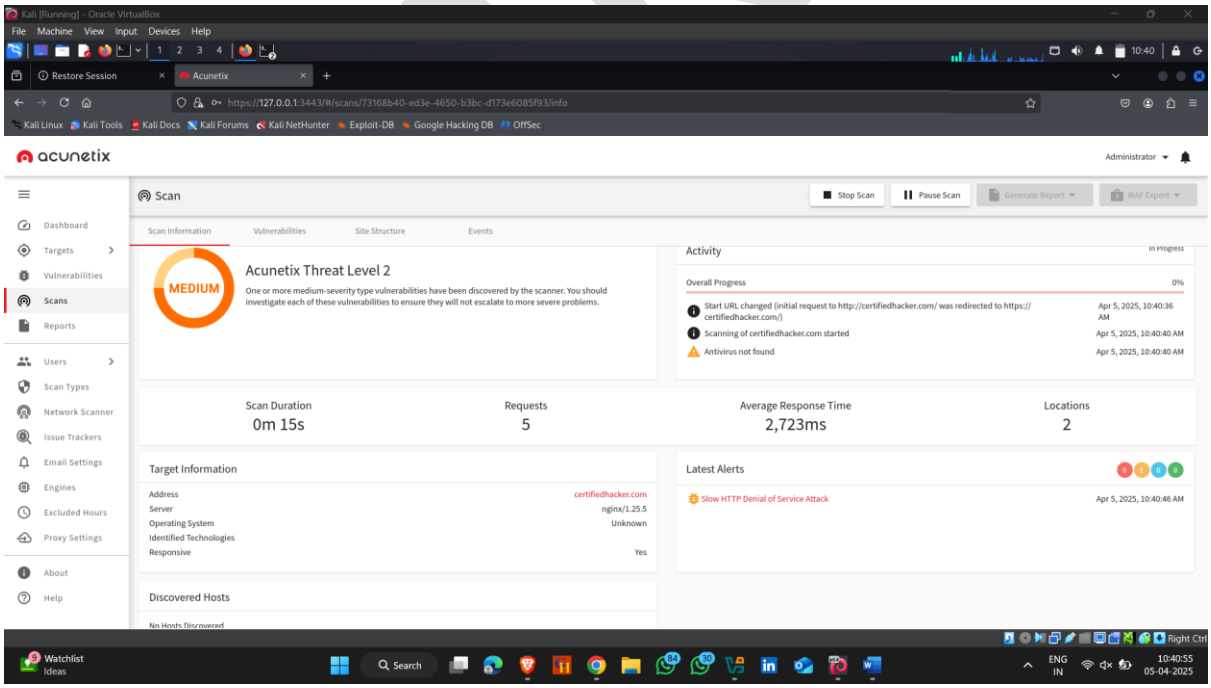
- Enter domain name or website name and click on save



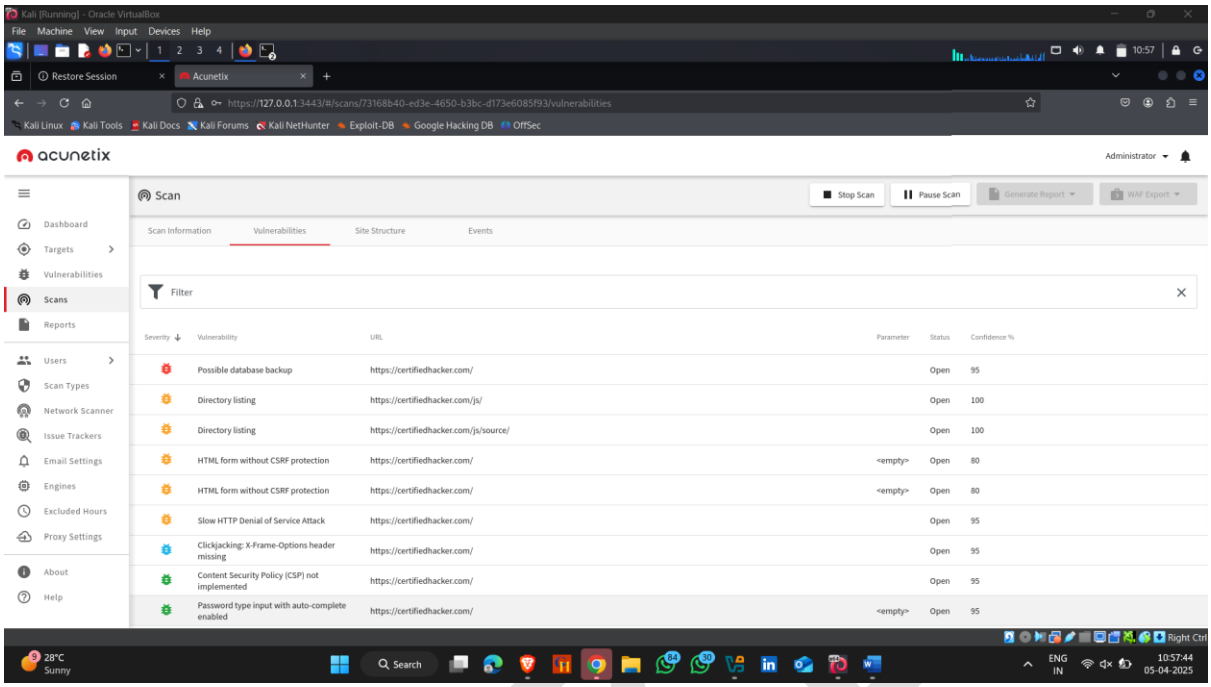
- Click on scan



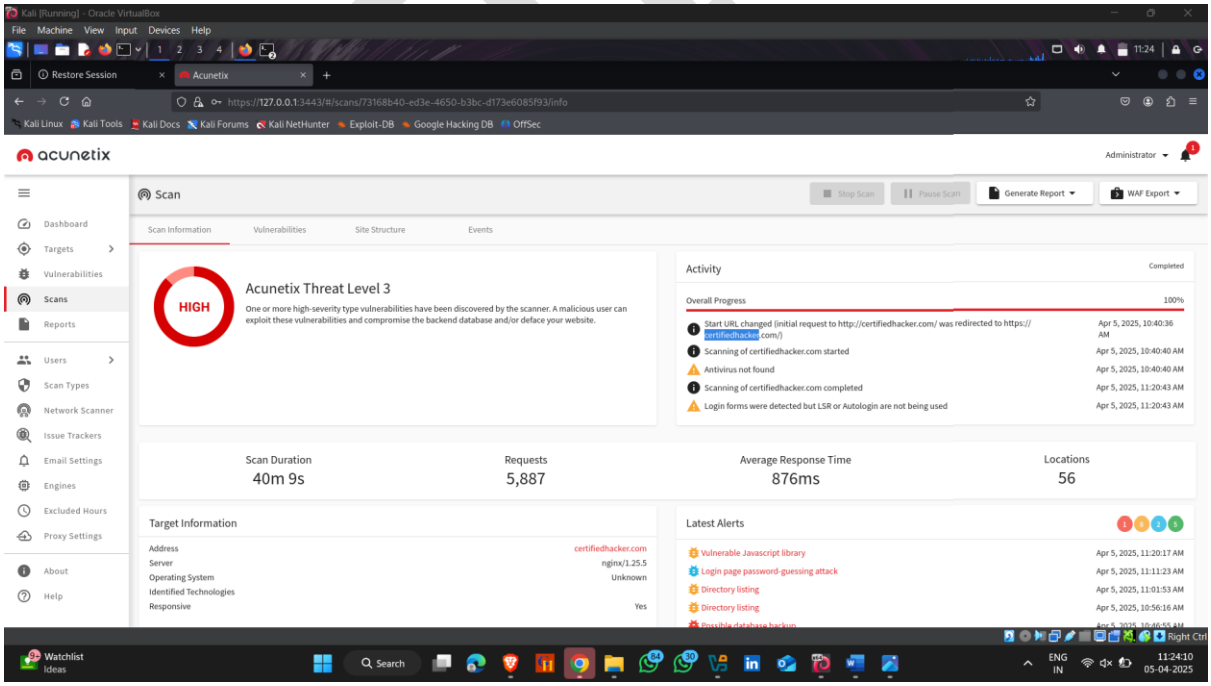
- Here , scanning start



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



- Scan completed



Vulnerability Analysis Using Nikto

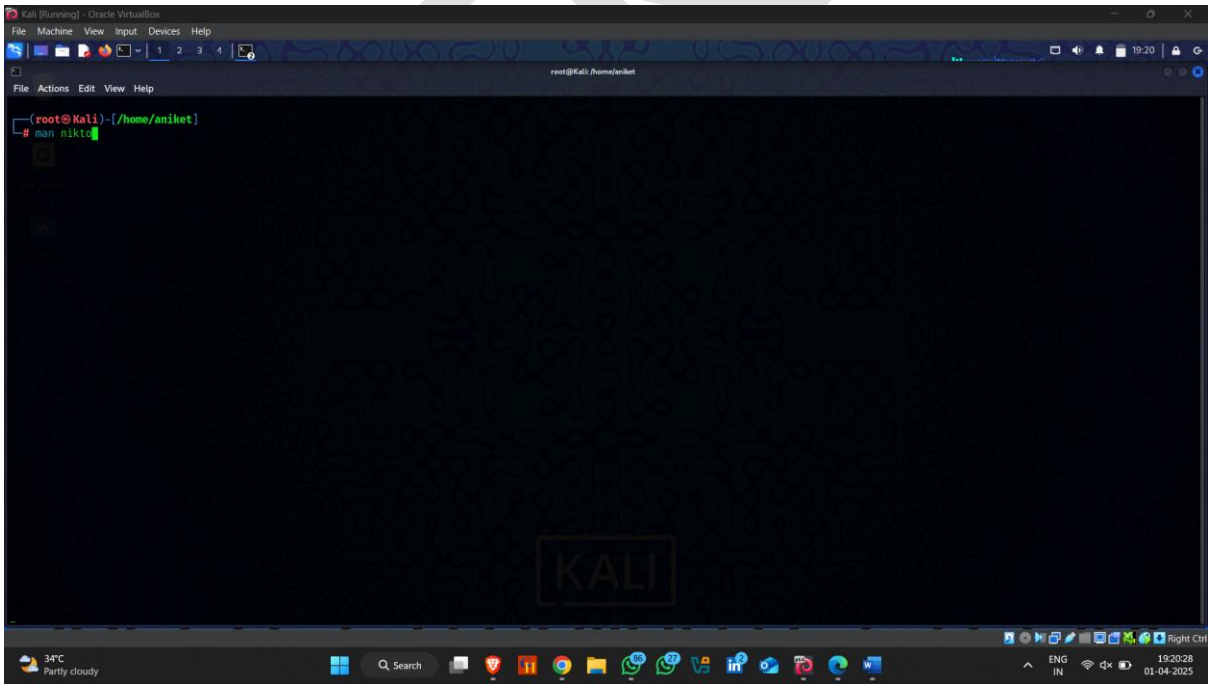
Nikto is an open-source web server scanner used to identify vulnerabilities, misconfigurations, and security issues in web applications.

Cheat Sheet link for Nikto :

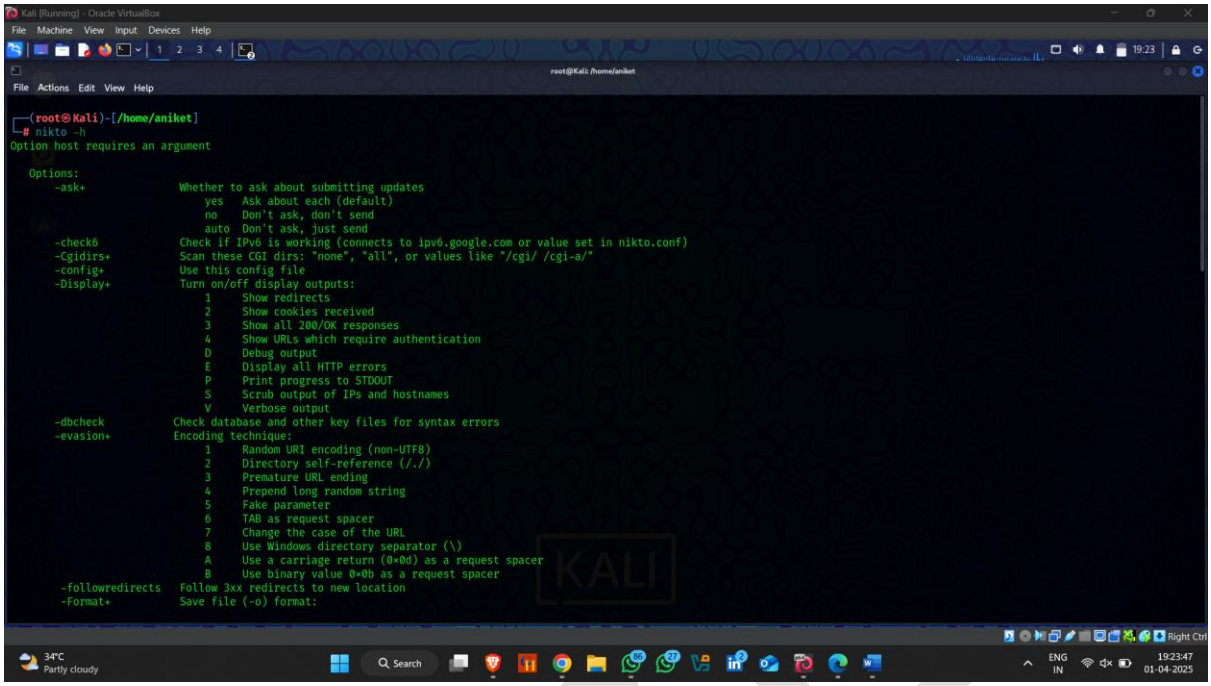
https://cdn.comparitech.com/wp-content/uploads/2019/07/NIkto-Cheat-Sheet.pdf

Common Commands -:

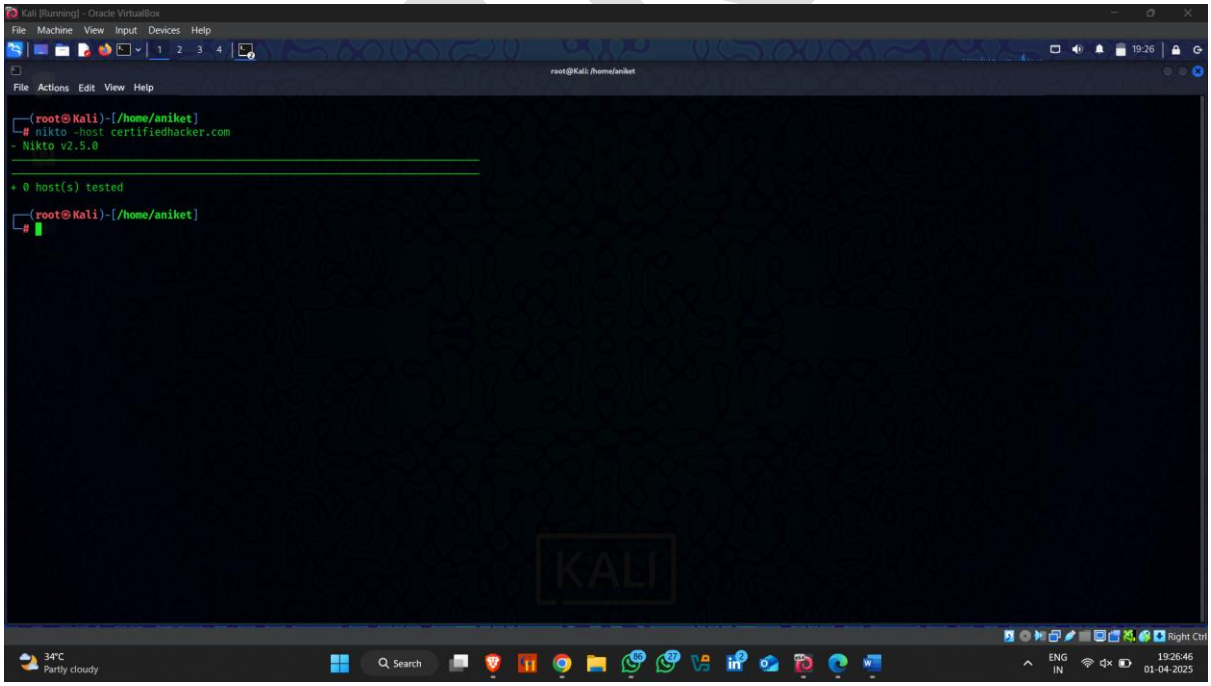
- Man nikto – Details about nikto tool.



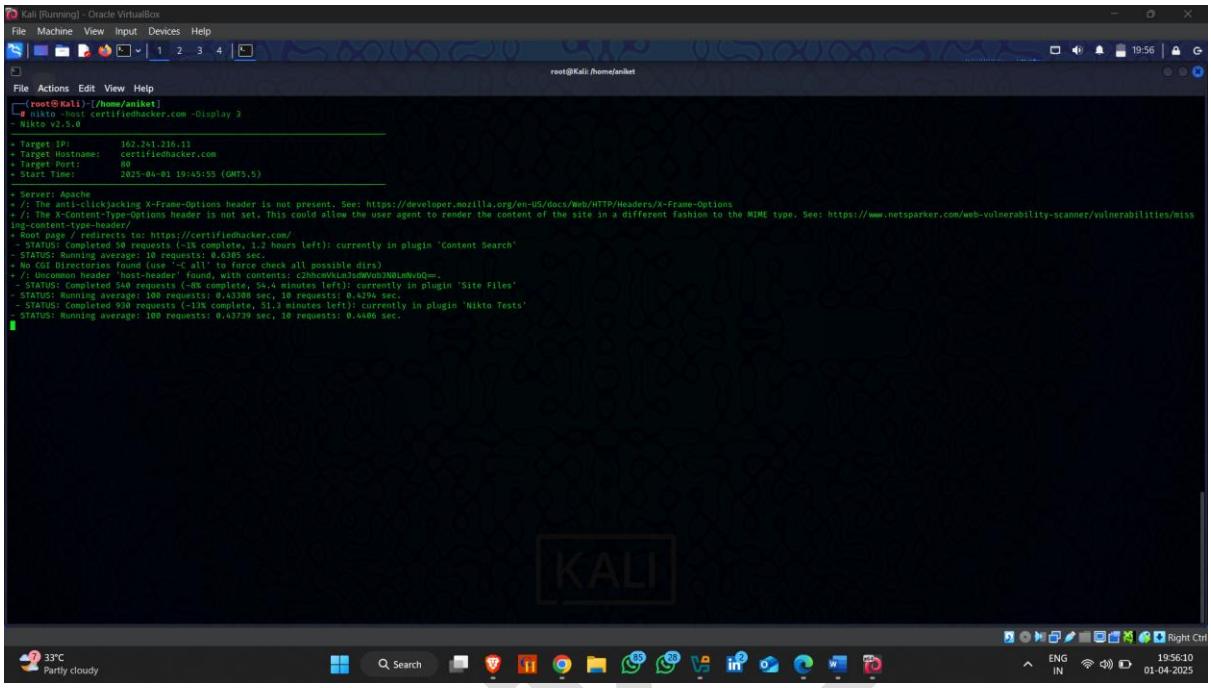
❖ nikto -h – help



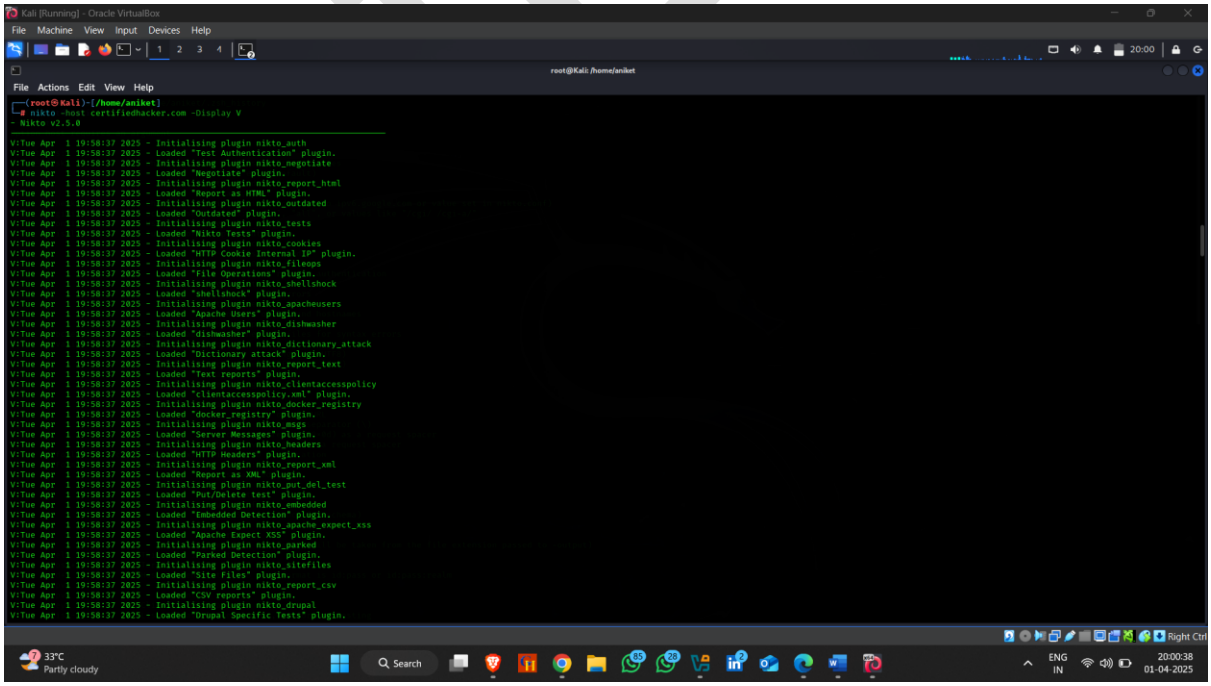
❖ -host – specify a host name or domain name



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



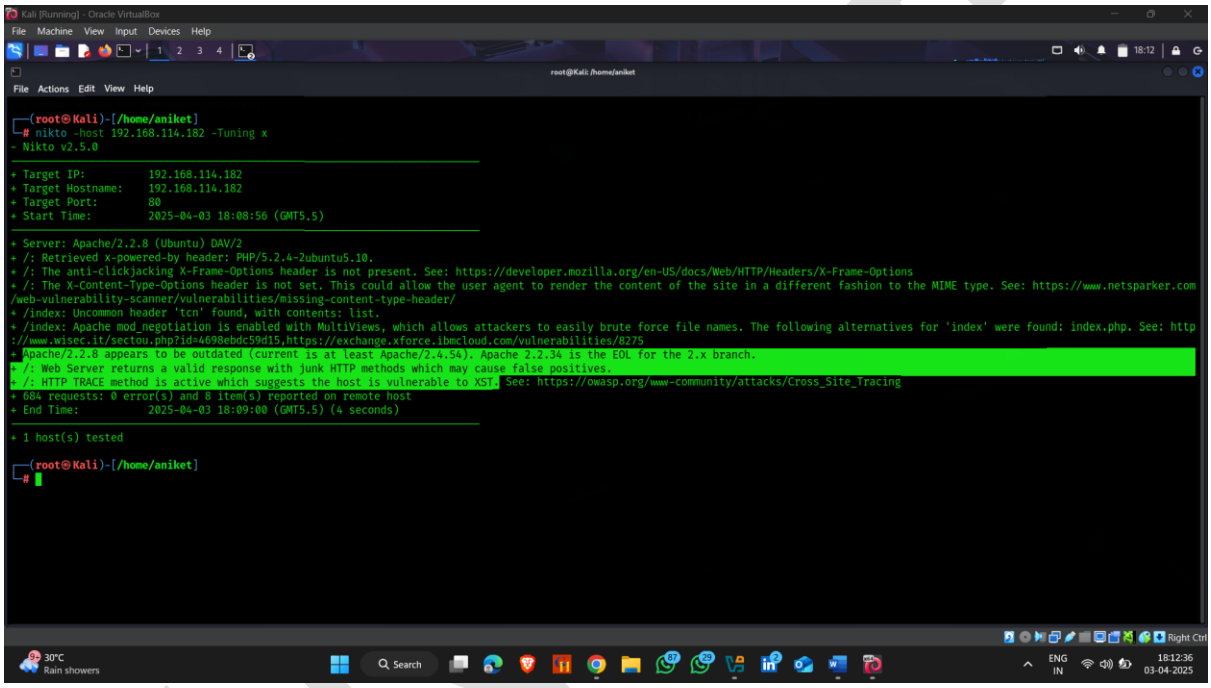
- -Display V – Verbose mode



- 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 .

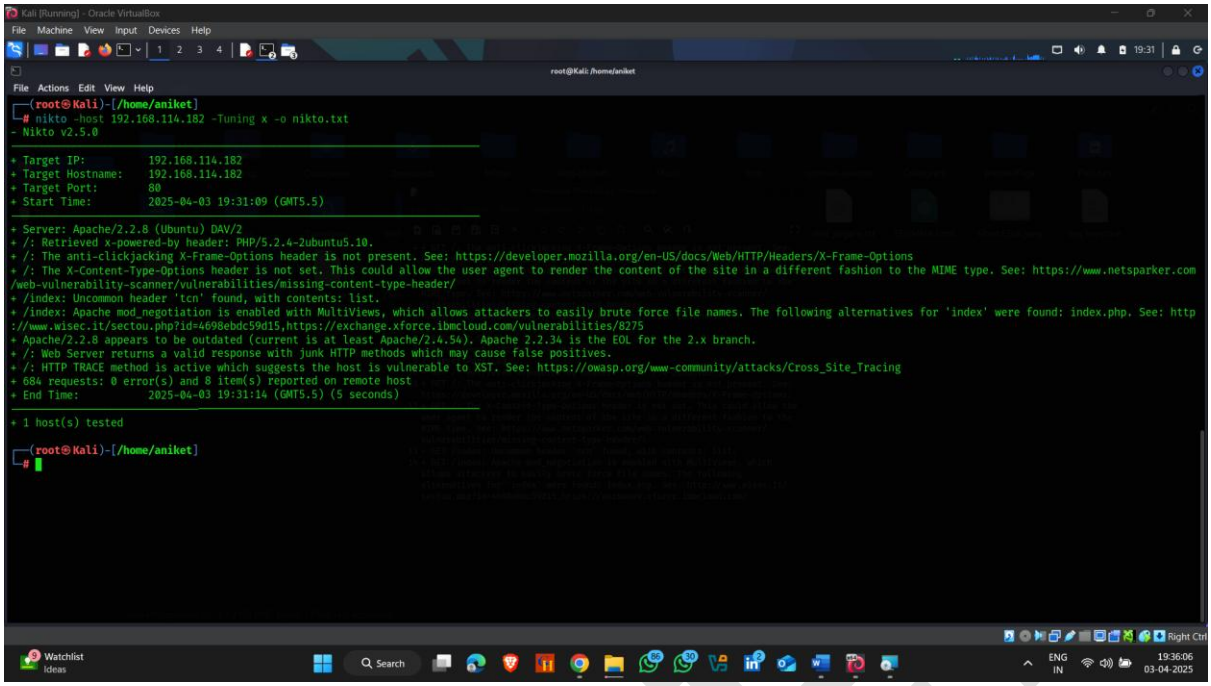


- **You can also generate report using nikto**

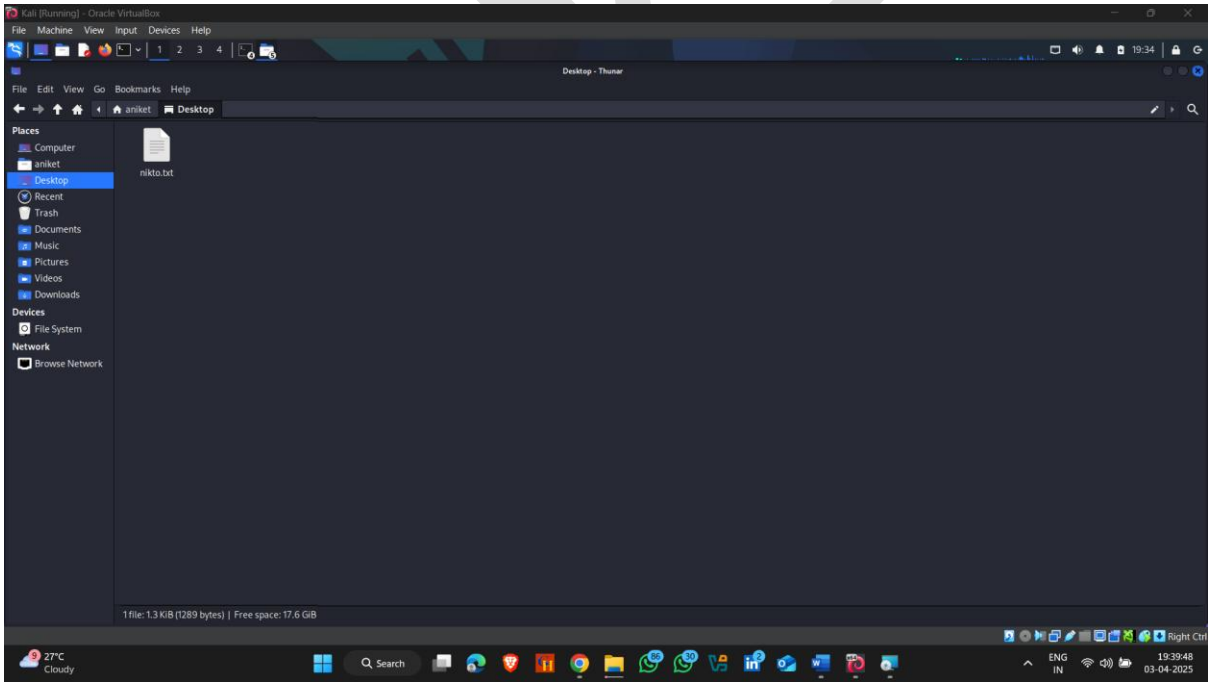
Command – nikto -host <target ip / domain name > -Tuning x

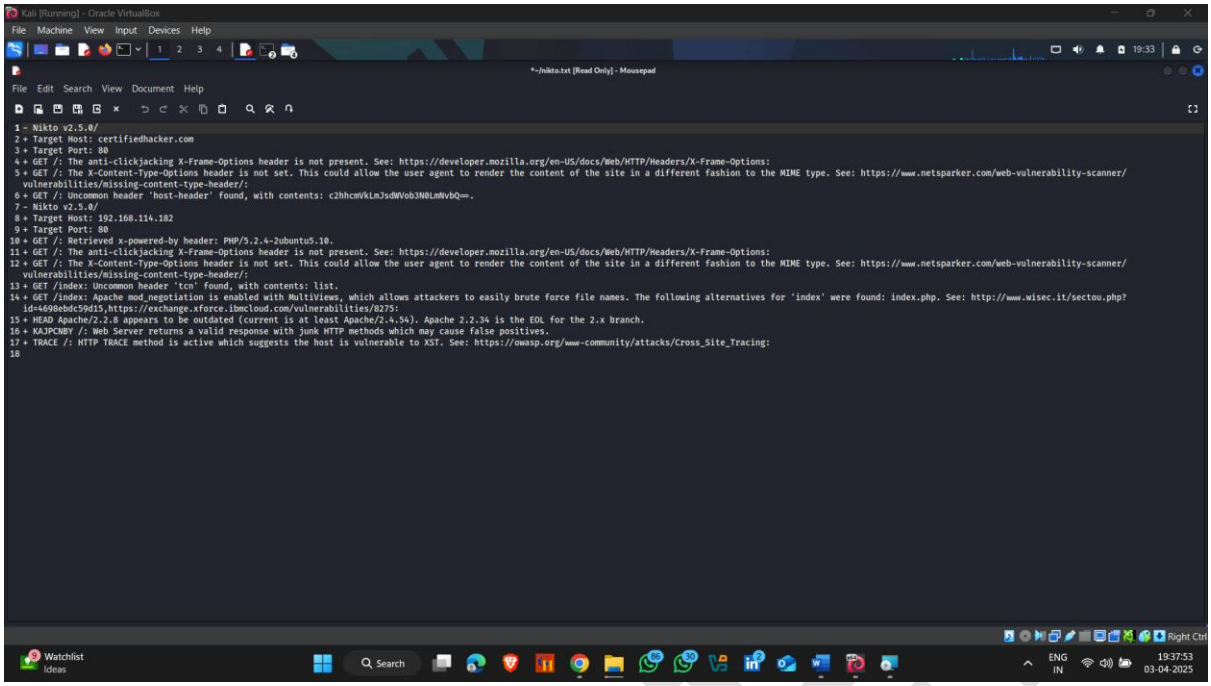
-o filename.txt

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



❖ **Report generate successfully now open it**



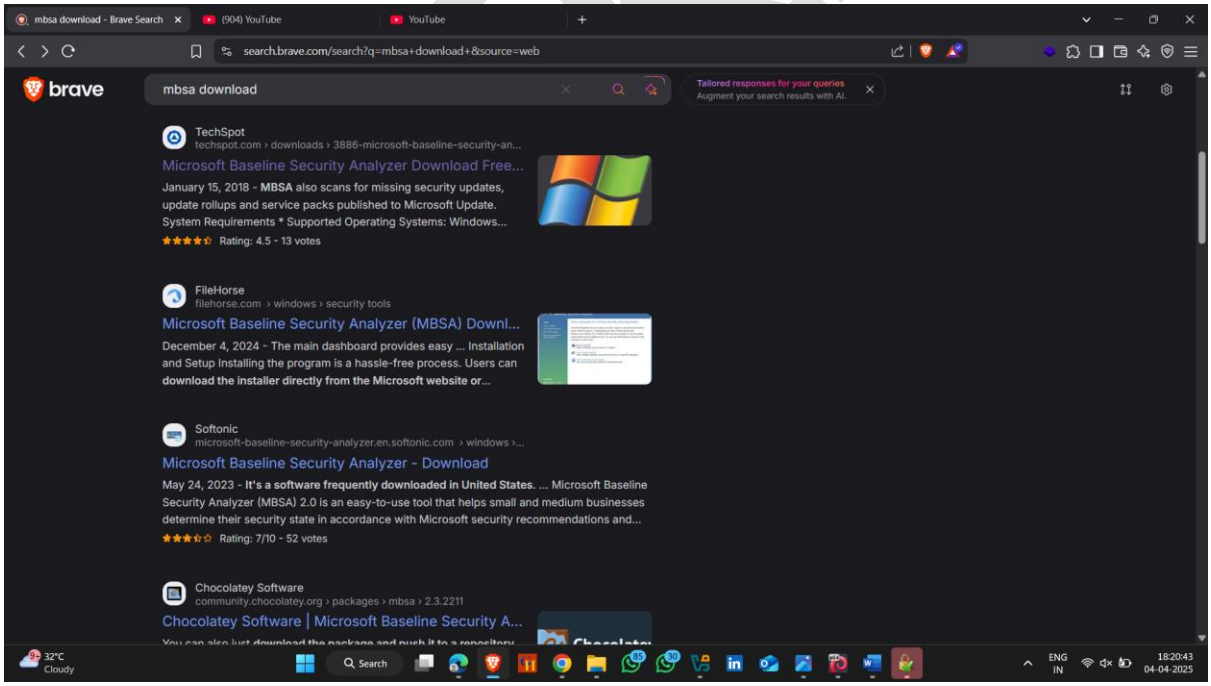

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
*~/nikto.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 - Nikto v2.5.0/
2 + Target Host: certifiedhacker.com
3 + Target Port: 80
4 + GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
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: c2hhcmVkLmJsdWVob3N0LmNvbQ==.
7 - Nikto v2.5.0/
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 + 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/:
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=4698ebdc59d15,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 + KAJPCNBY /: 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:
18
Watchlist
Ideas
Search
ENG
IN
19:37:53
03-04-2025

Vulnerability Analysis Using MBSA (Mircosoft 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.

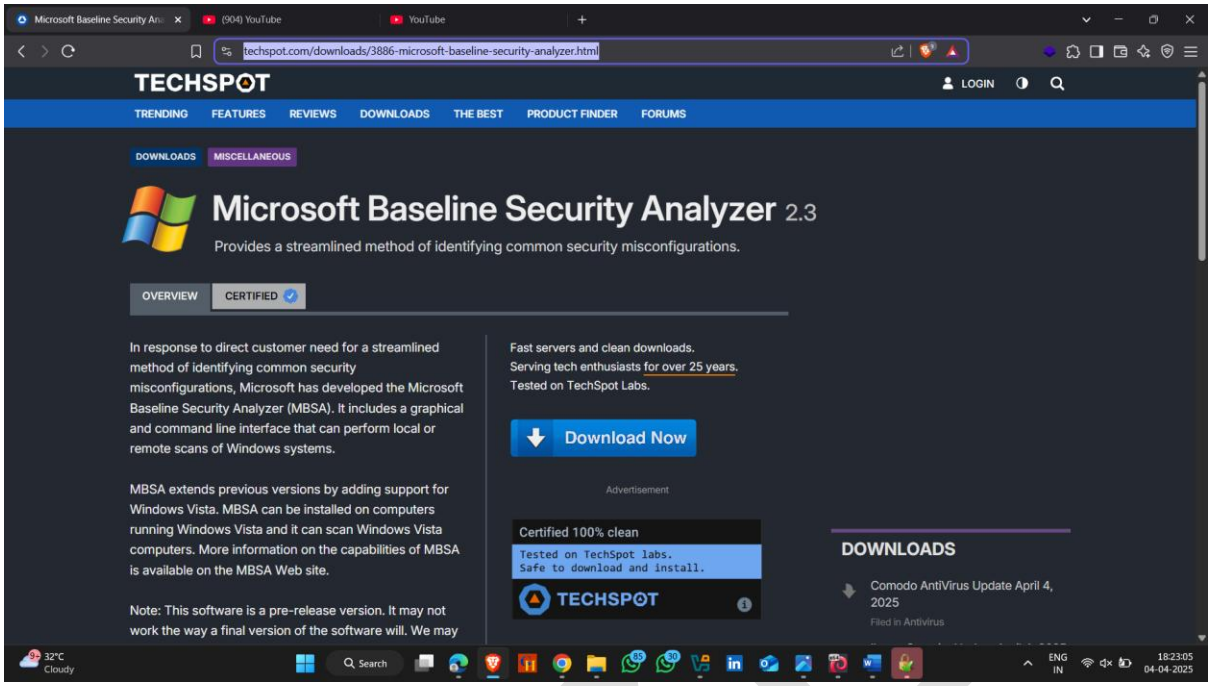
How To Download MBSA

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

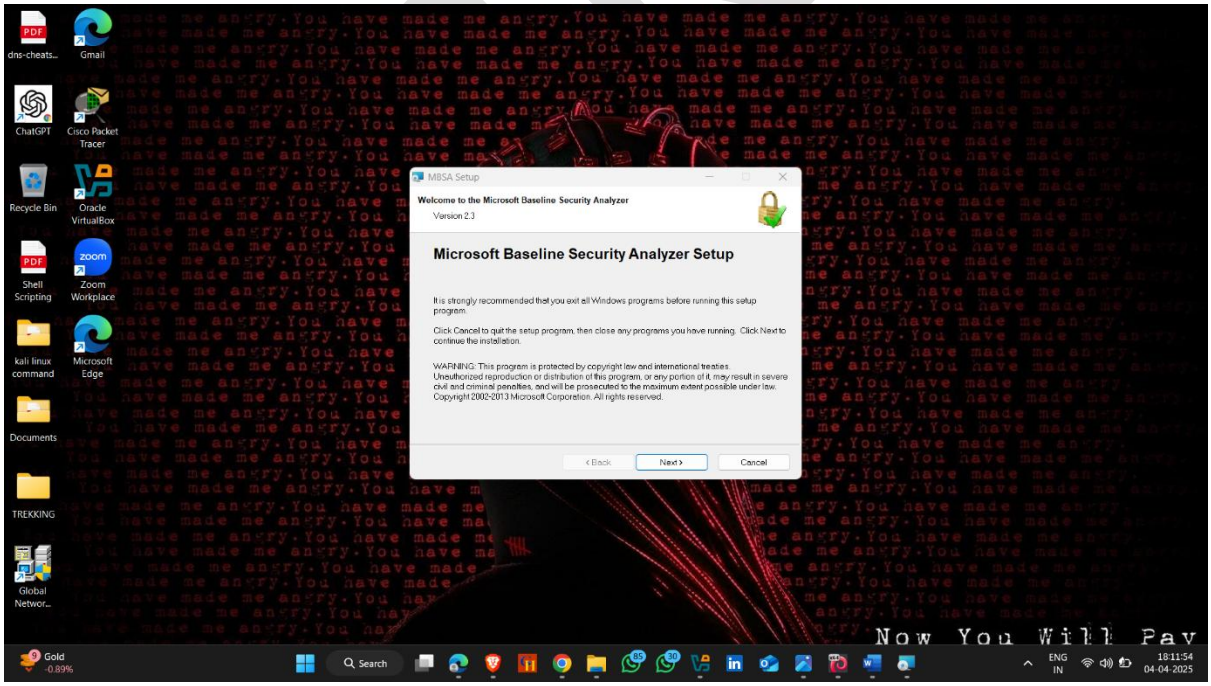


- Click on

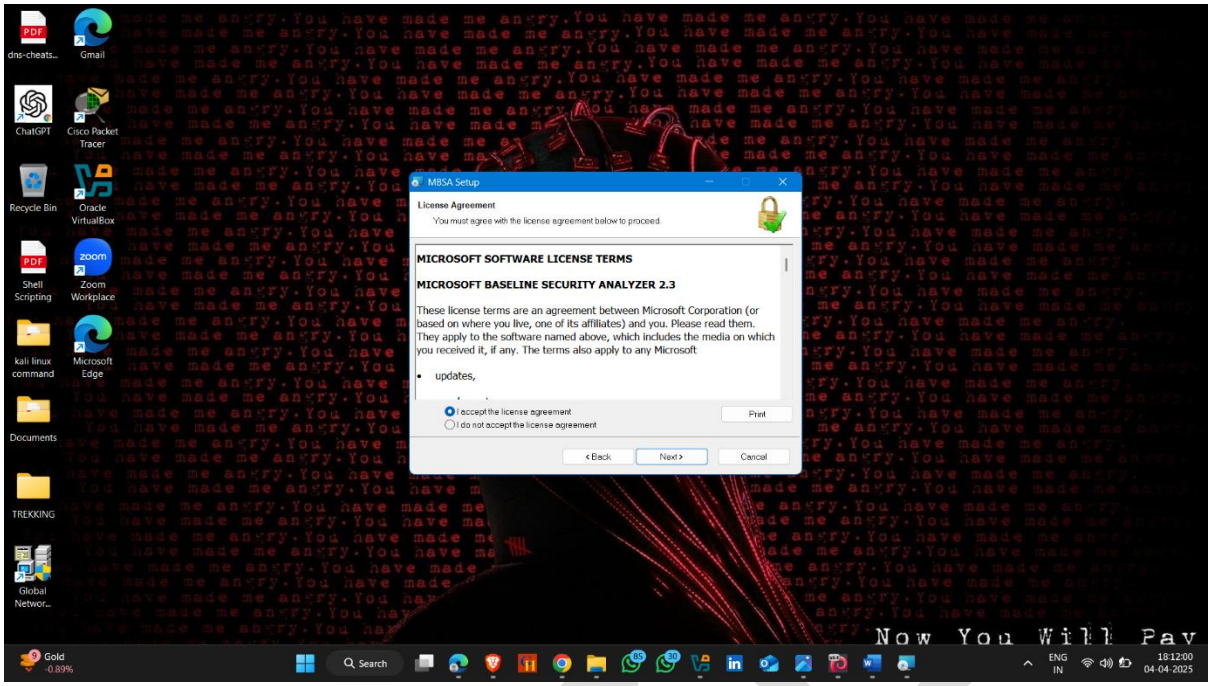
❖ **Download Now**



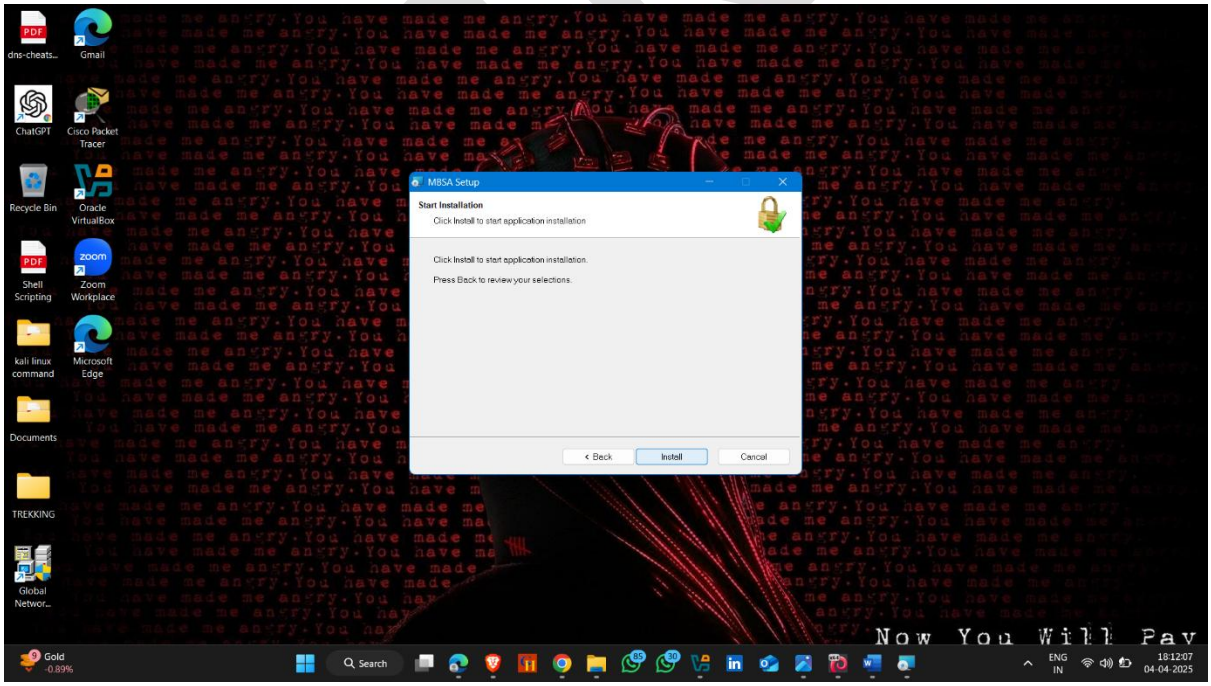
❖ **After Downloading , open the application and click on next**



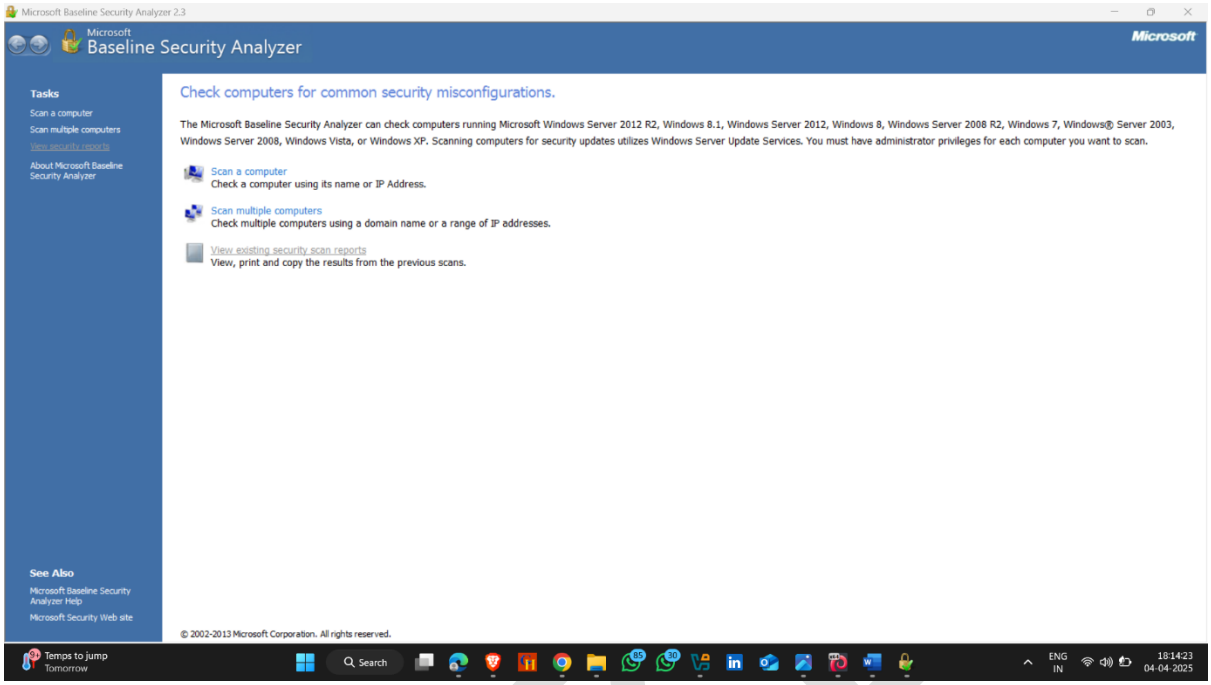
❖ **Accept the license and click next**



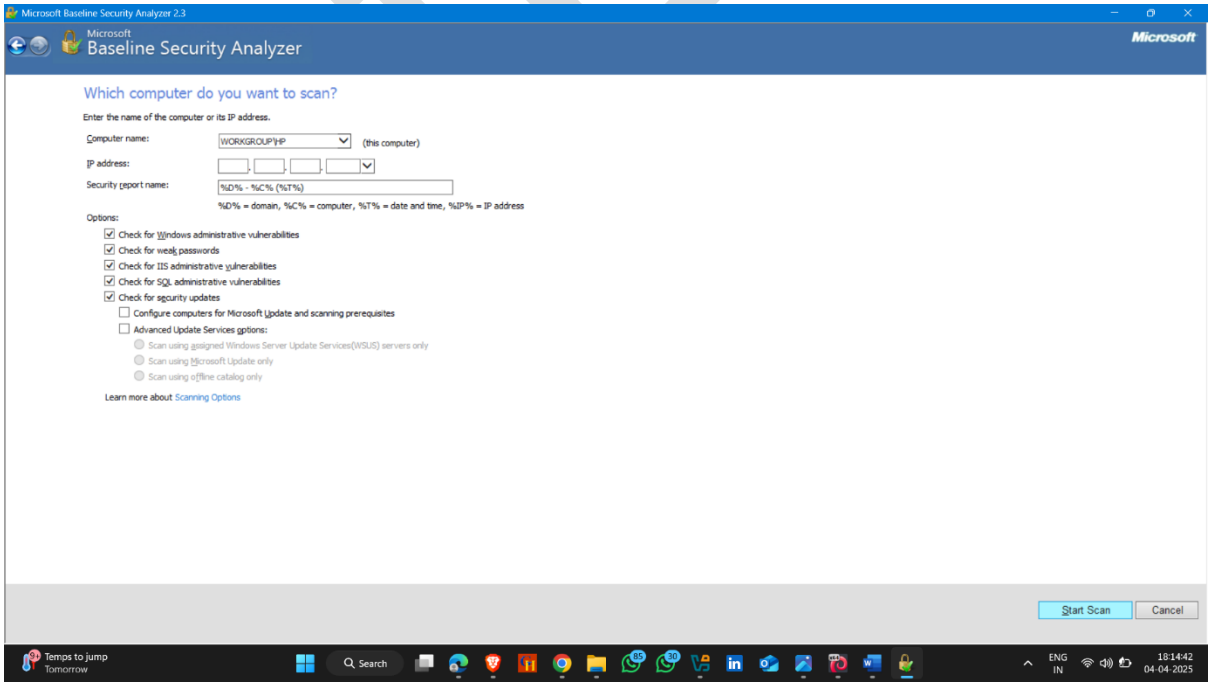
❖ **Click on install**



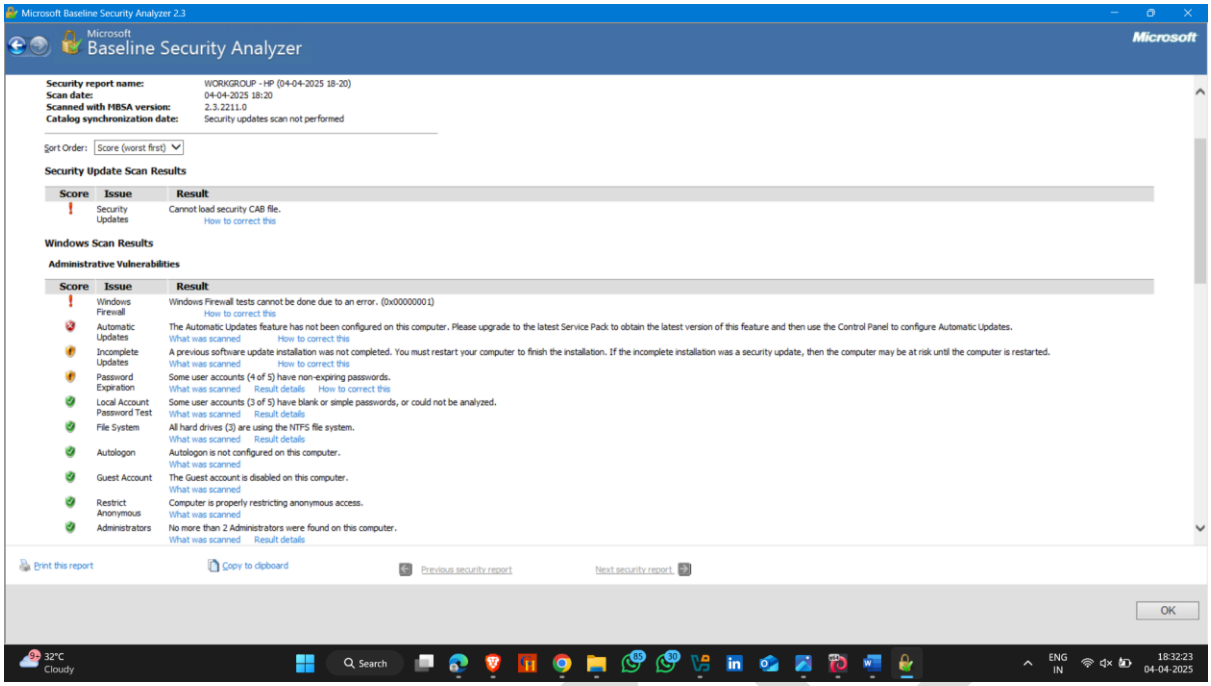
- After successfully install and setup mbsa , open it and **click on scan computer**



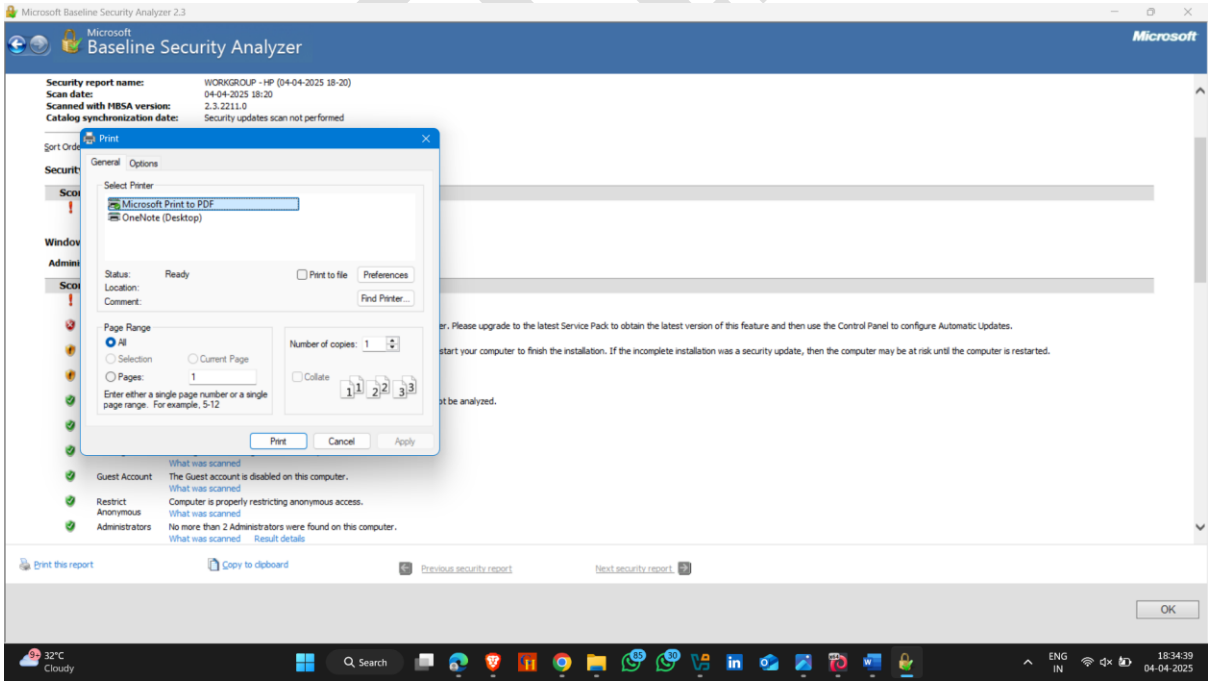
- As you can see MBSA automatically get your system name
- **Click on start scan**



❖ 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.

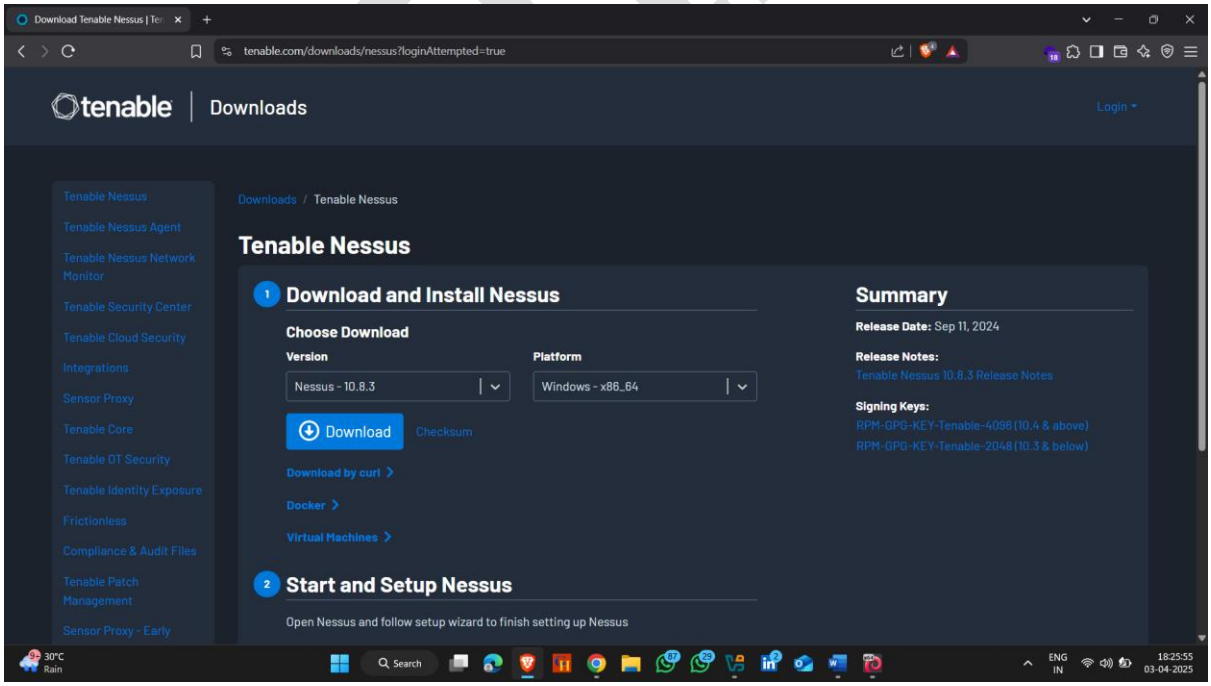
Nessus is a popular vulnerability assessment tool used to scan networks, systems, and applications for security weaknesses. It is developed by Tenable, Inc. and is widely used for penetration testing, compliance auditing, and risk assessment.

Nessus Download Link –

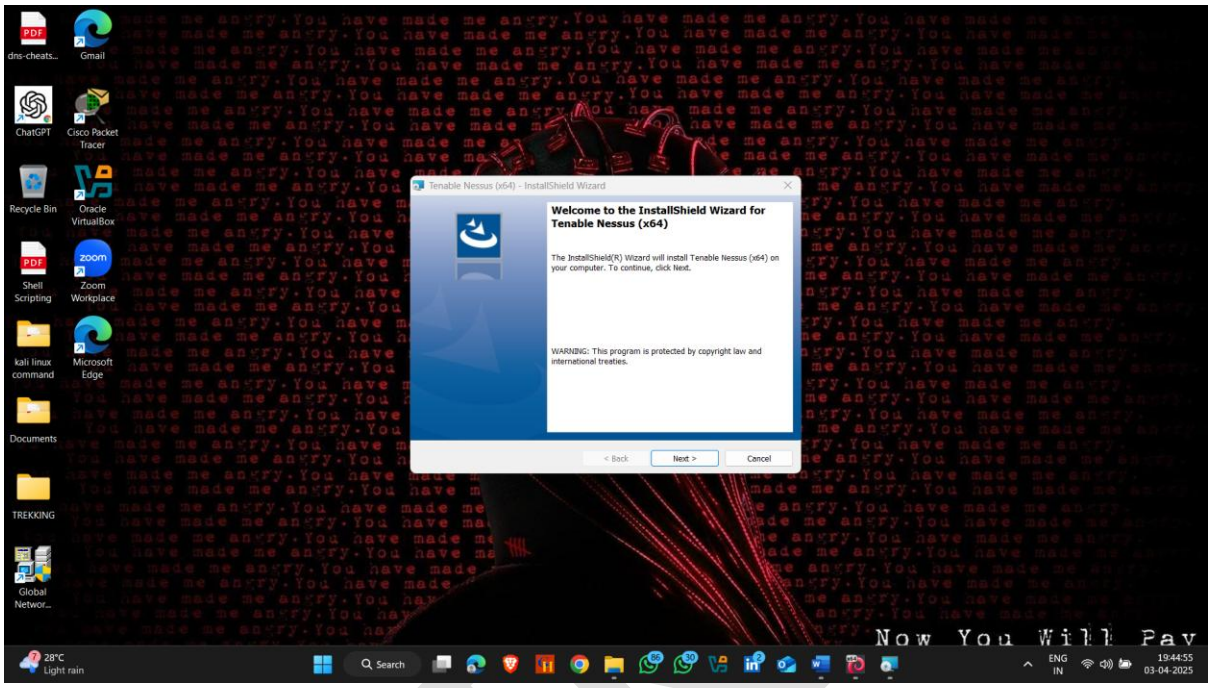
https://www.tenable.com/downloads/nessus?loginAttempted=true

How To Download Nessus –

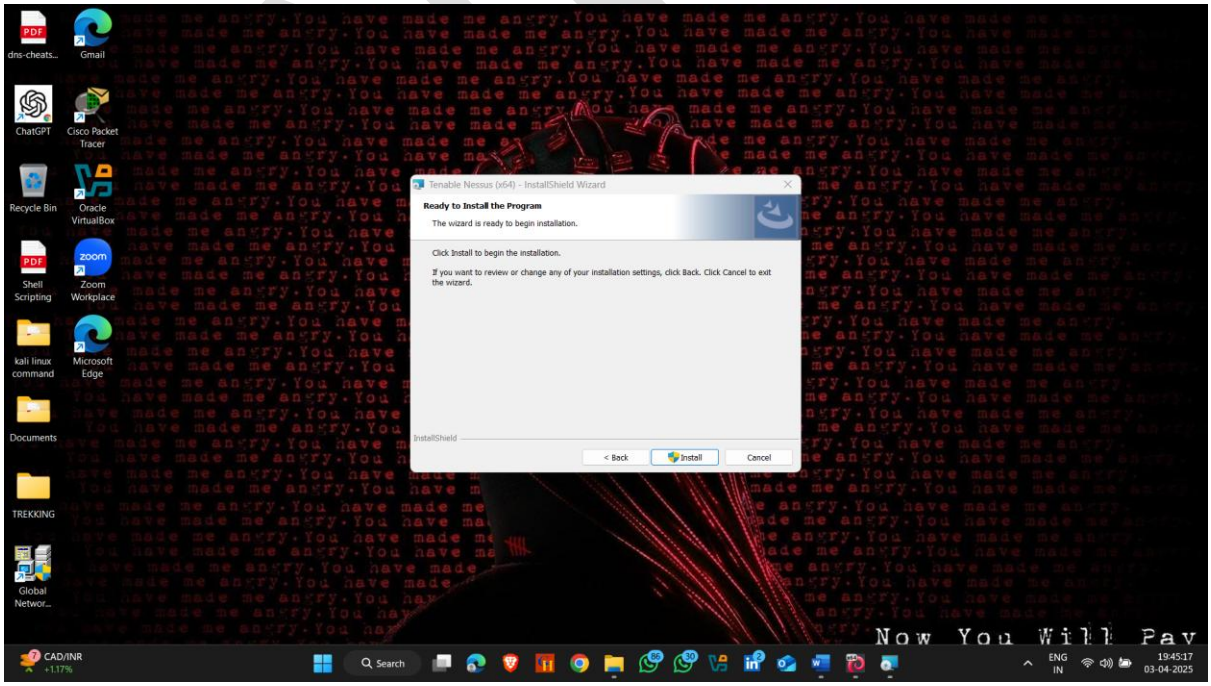
- Open Browser
- Search Nessus Download
- Click first website for official Tenable website and you can redirected to download page



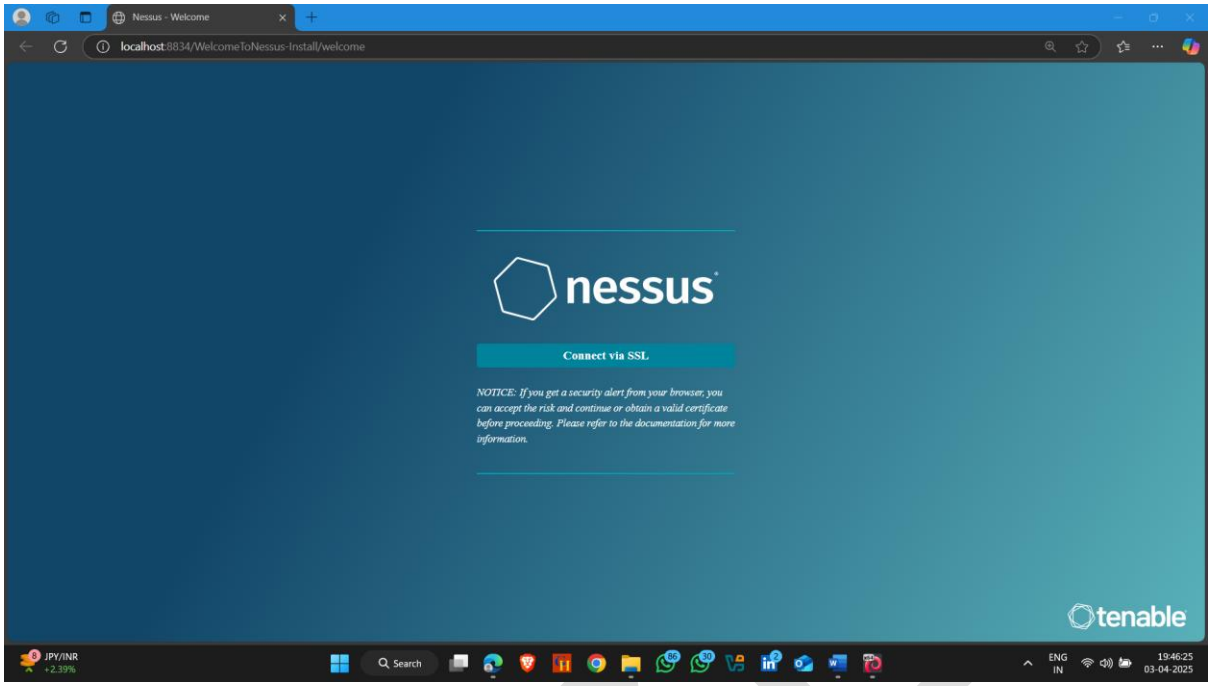
- ❖ Click on Download Button and Download Nessus
- ❖ Open Nessus file /Double click
- ❖ Click on next



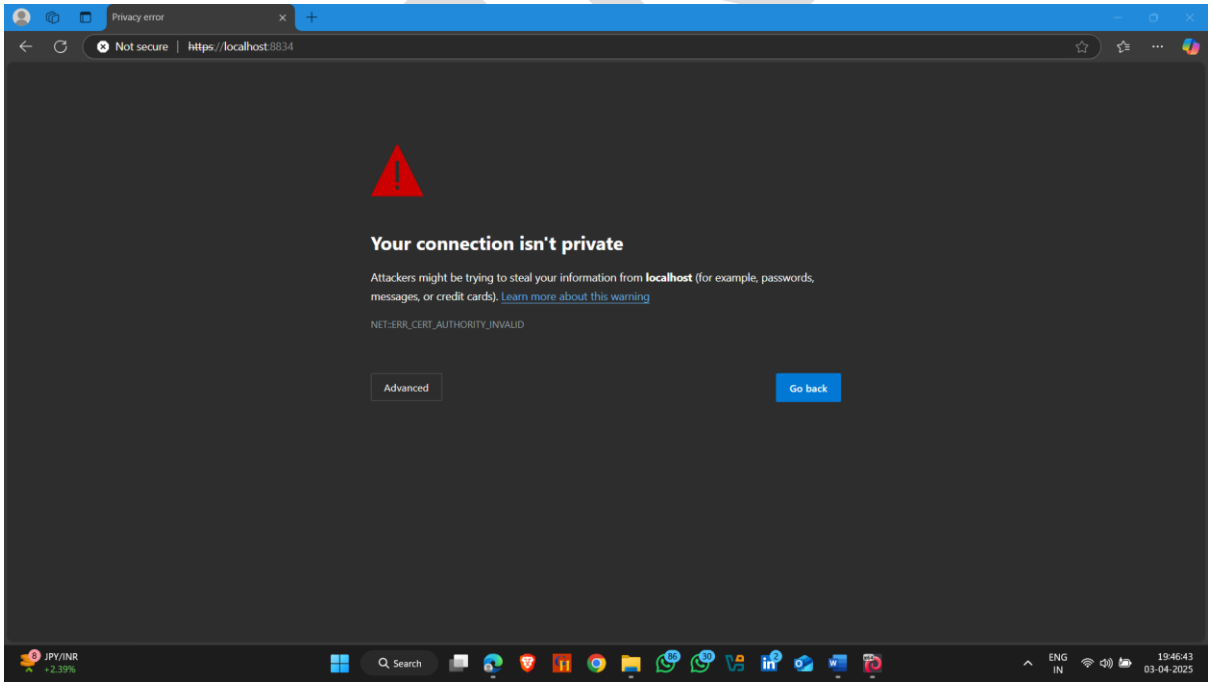
- ❖ Click install



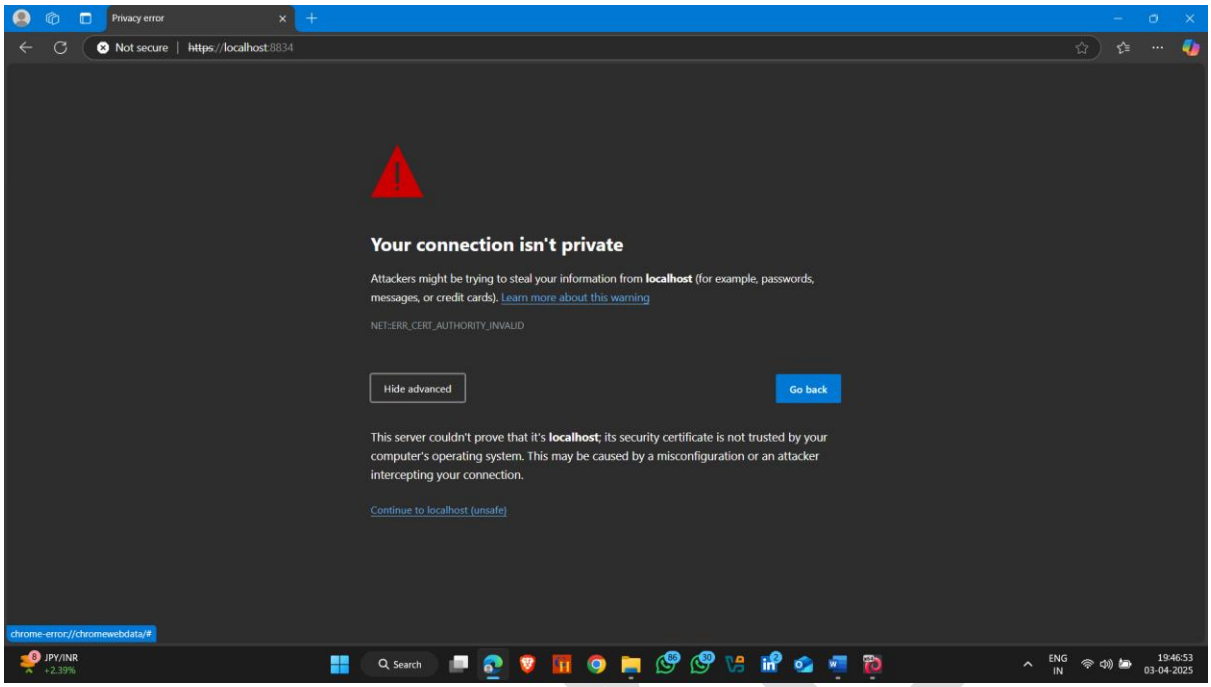
❖ Click on connect via SSL



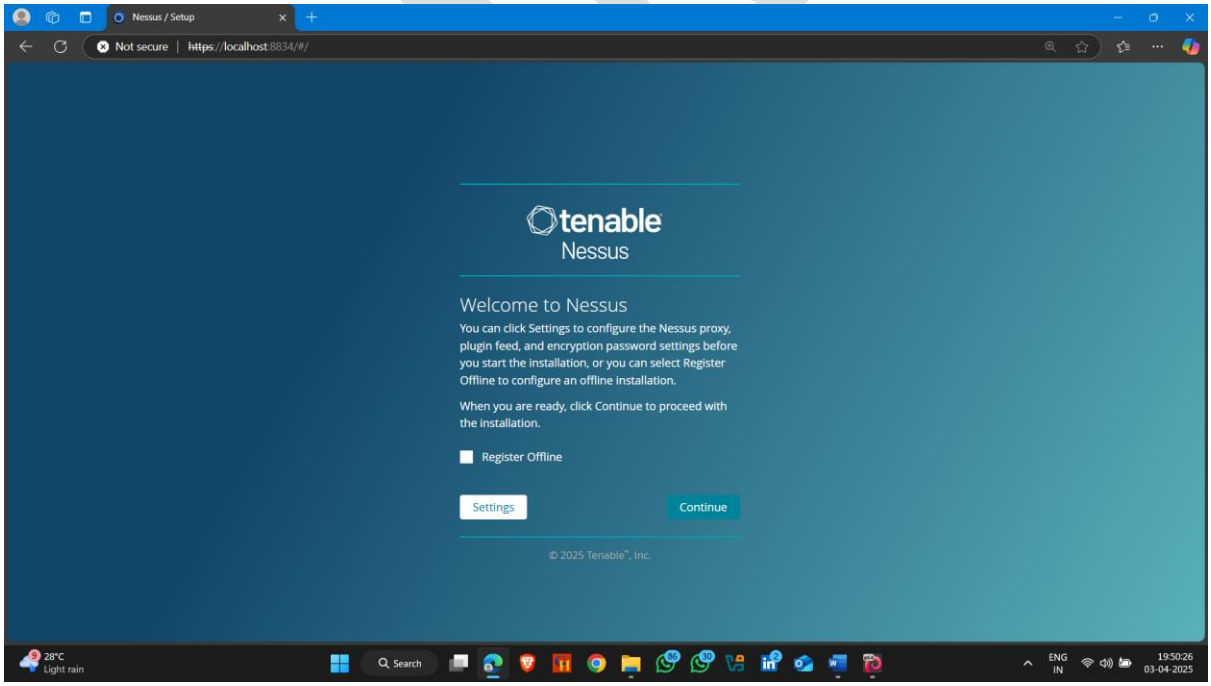
❖ Click on Advance



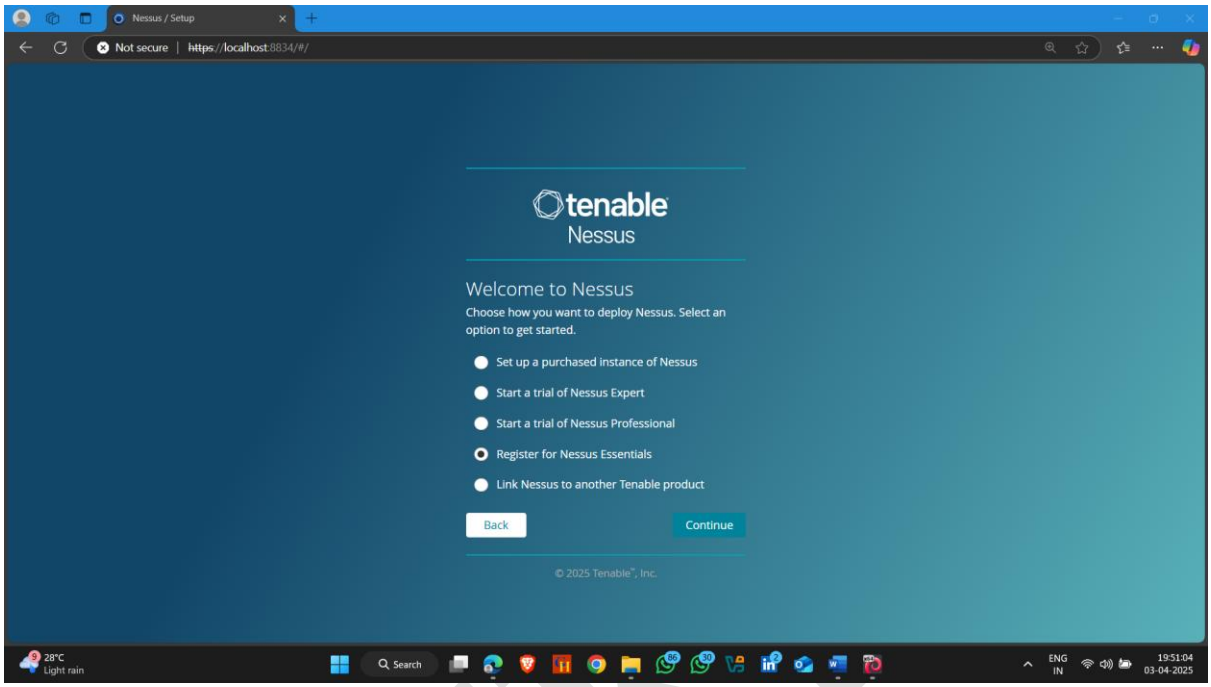
❖ Click continue to localhost(unsafe ⚠)



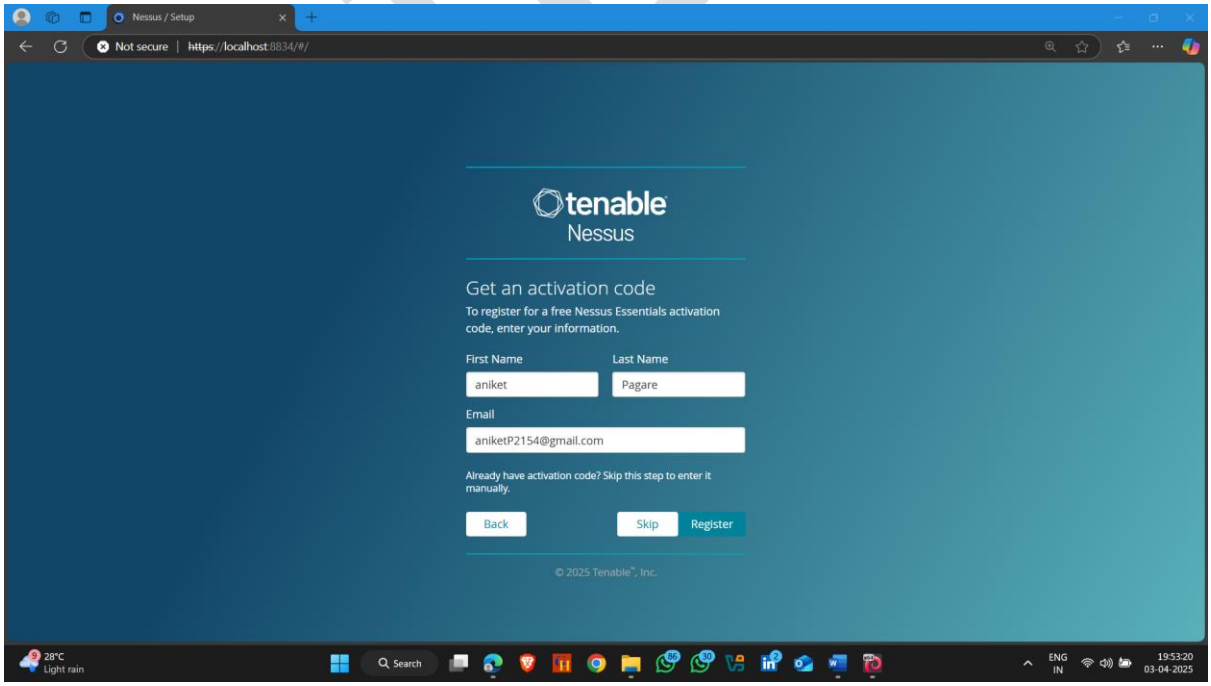
❖ Click on continue



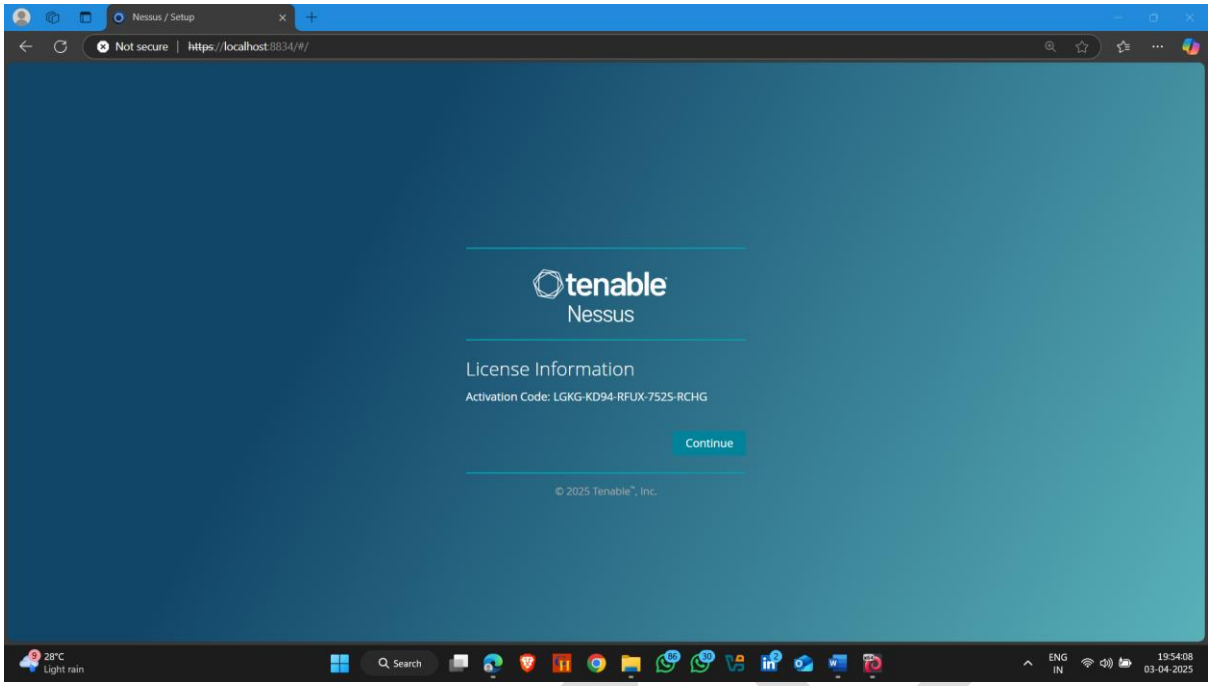
❖ Click on second last option **Register for Nessus Essential** And click Continue



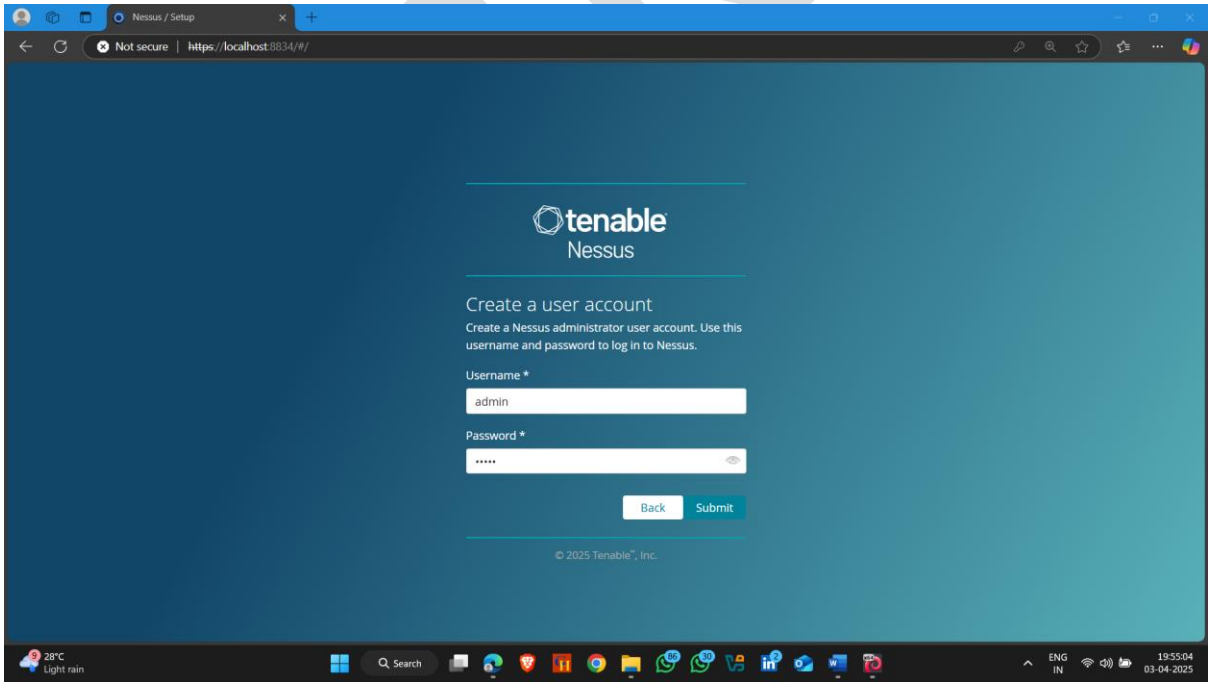
❖ Provide name and other things and click register



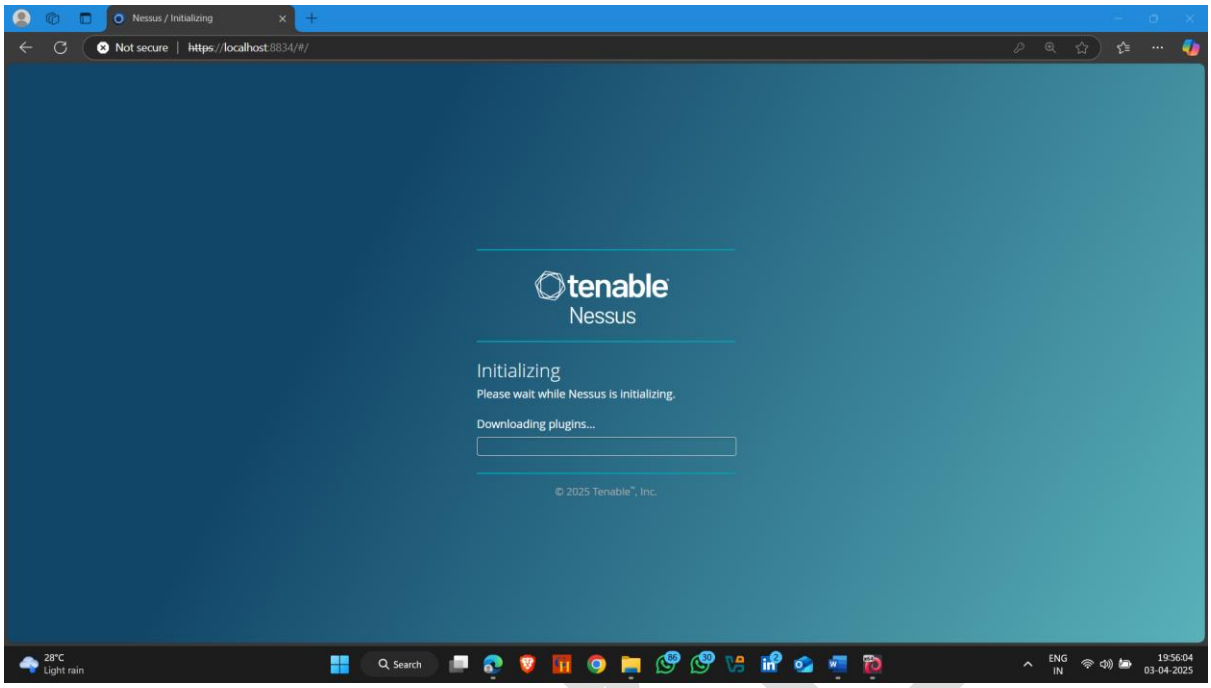
❖ Click on continue



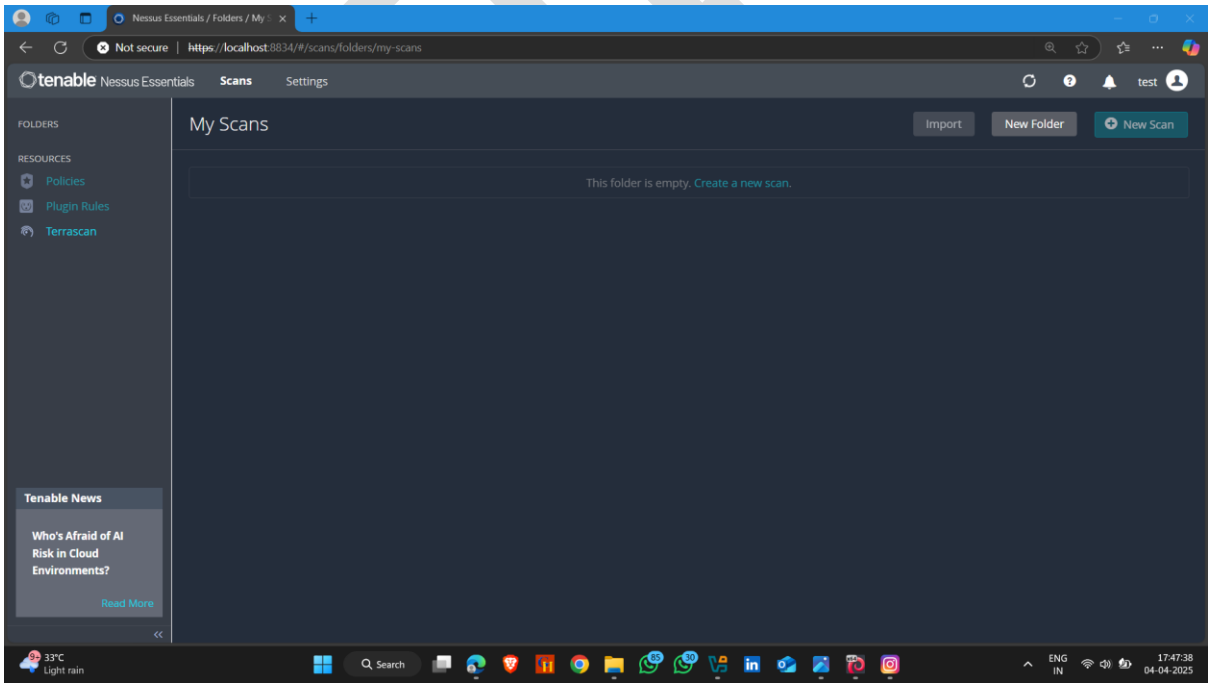
❖ Provide username and password and submit



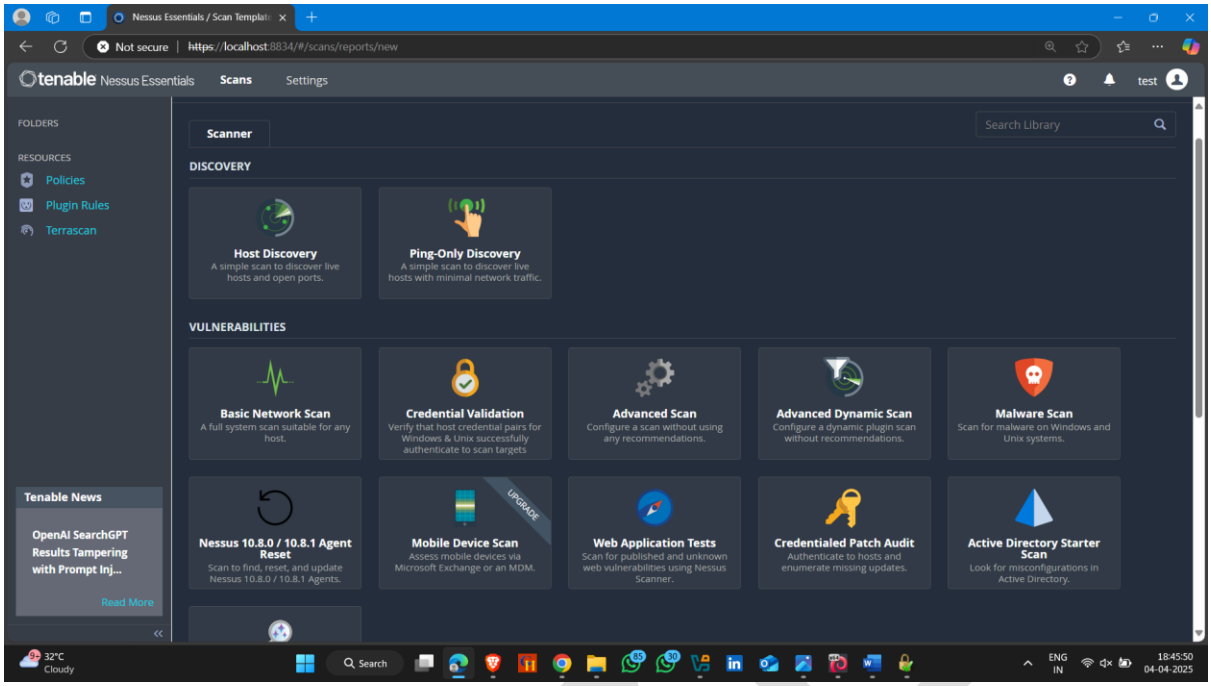
❖ **Wait** ⚠️



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

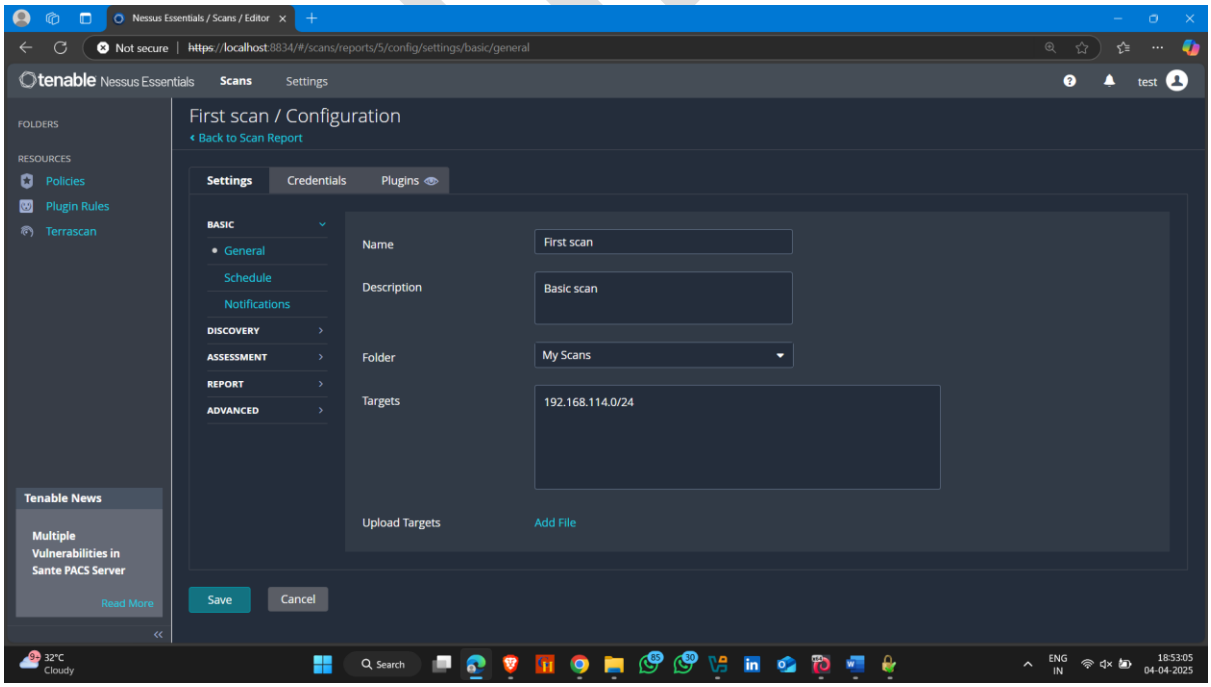


❖ Click on Basic network scan

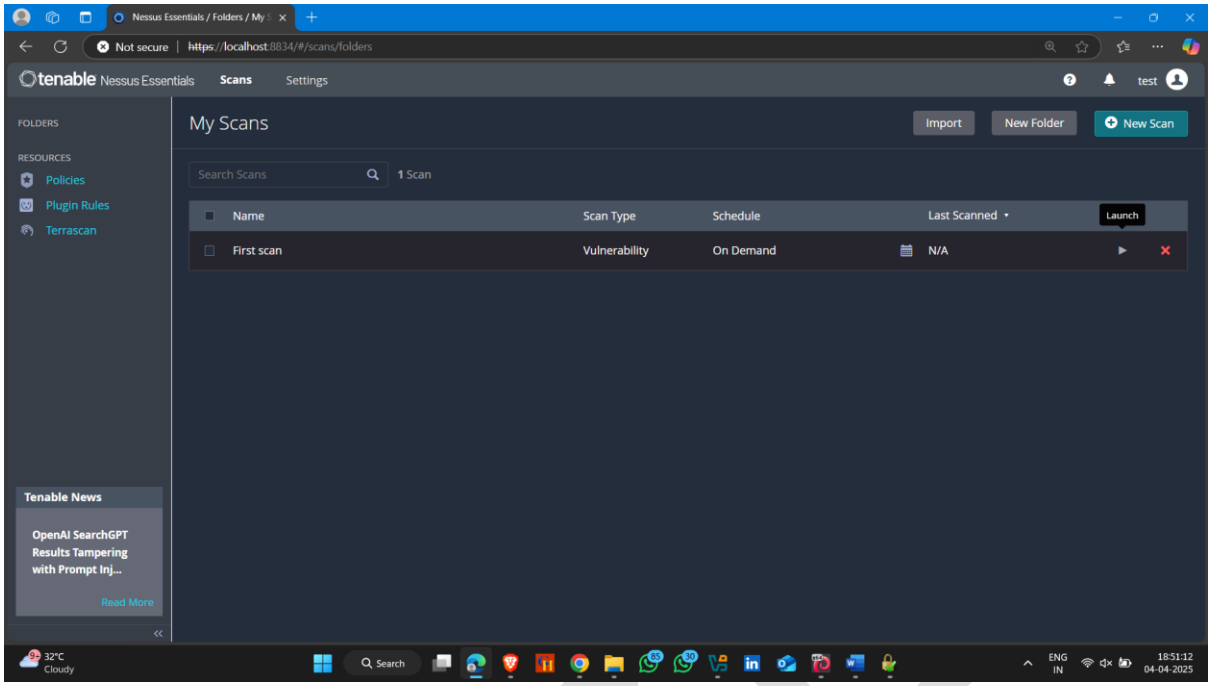


❖ Provide target

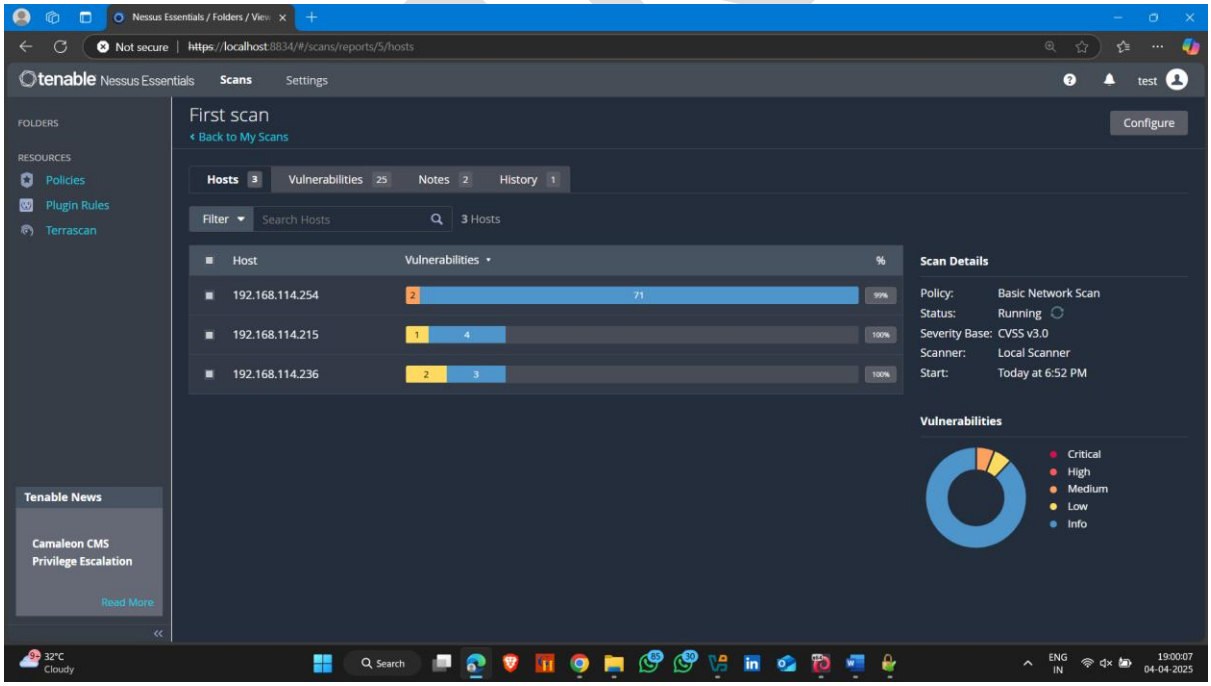
Note – In my case , I'm scan Entire network , you can also scan a entire network as well as single ip address its all depend on you



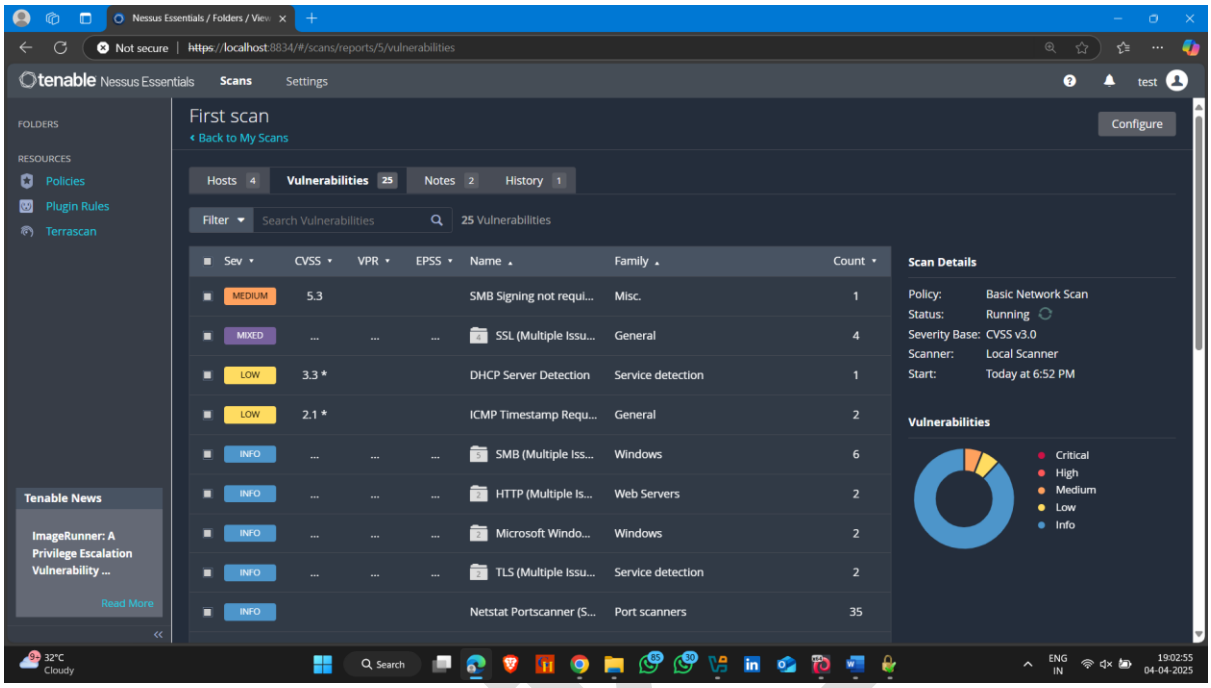
❖ Click on save and then click on launch



❖ Here , scanning start

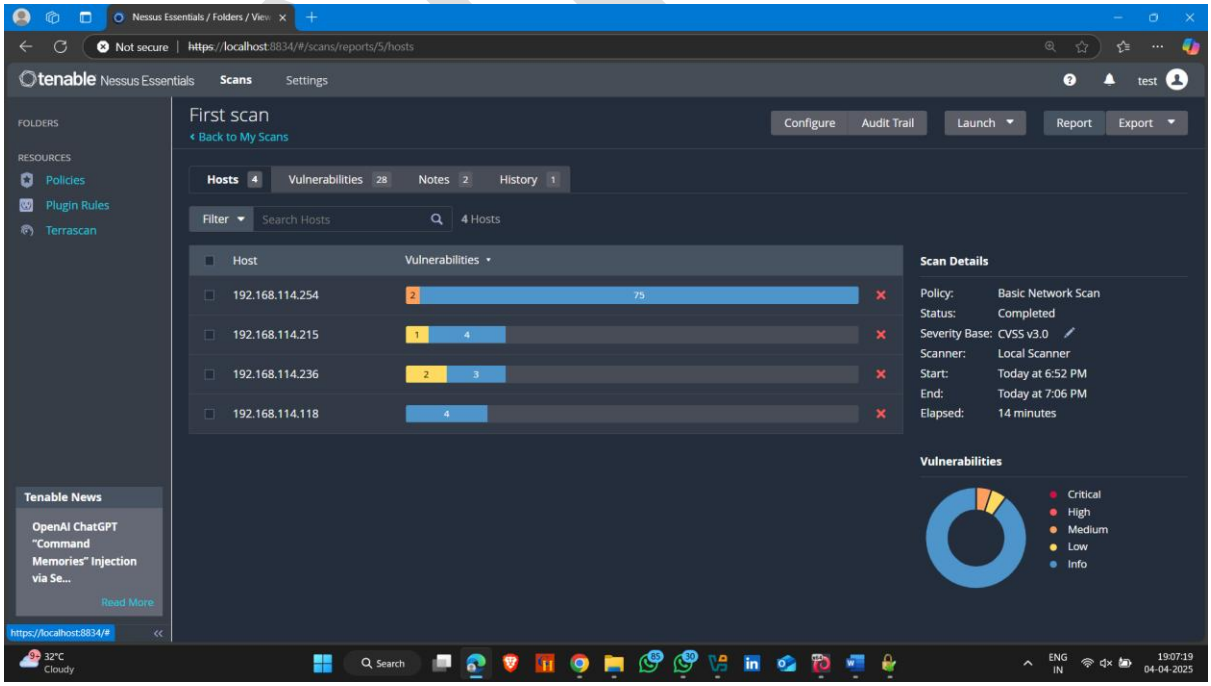


❖ You can also check vulnerabilities , just click on vulnerabilities section

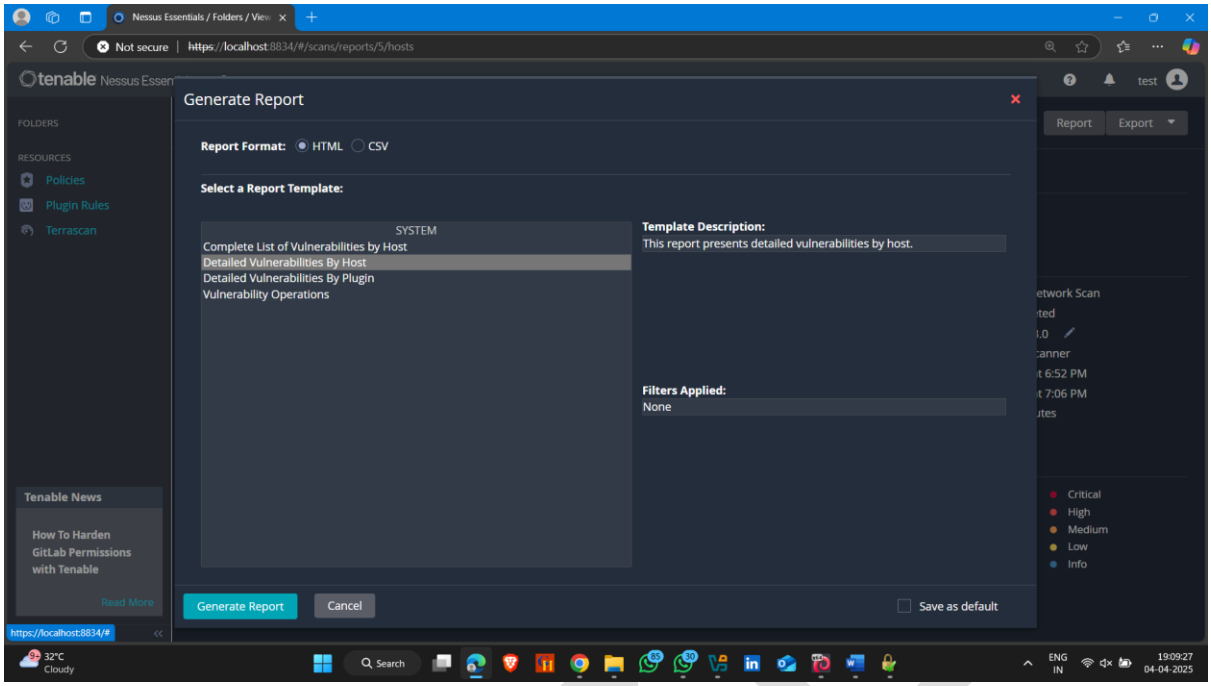


❖ **Now generate a report using Nessus**

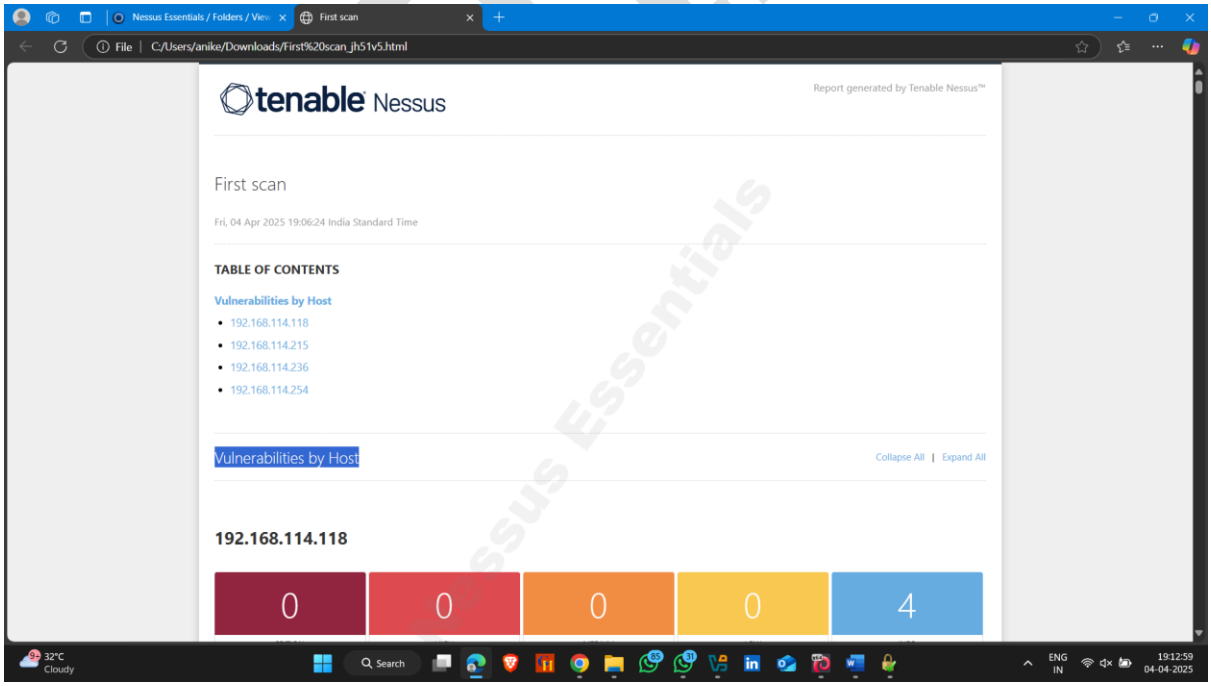
❖ **Click on report (top right side)**



❖ Here , you see different different report option



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

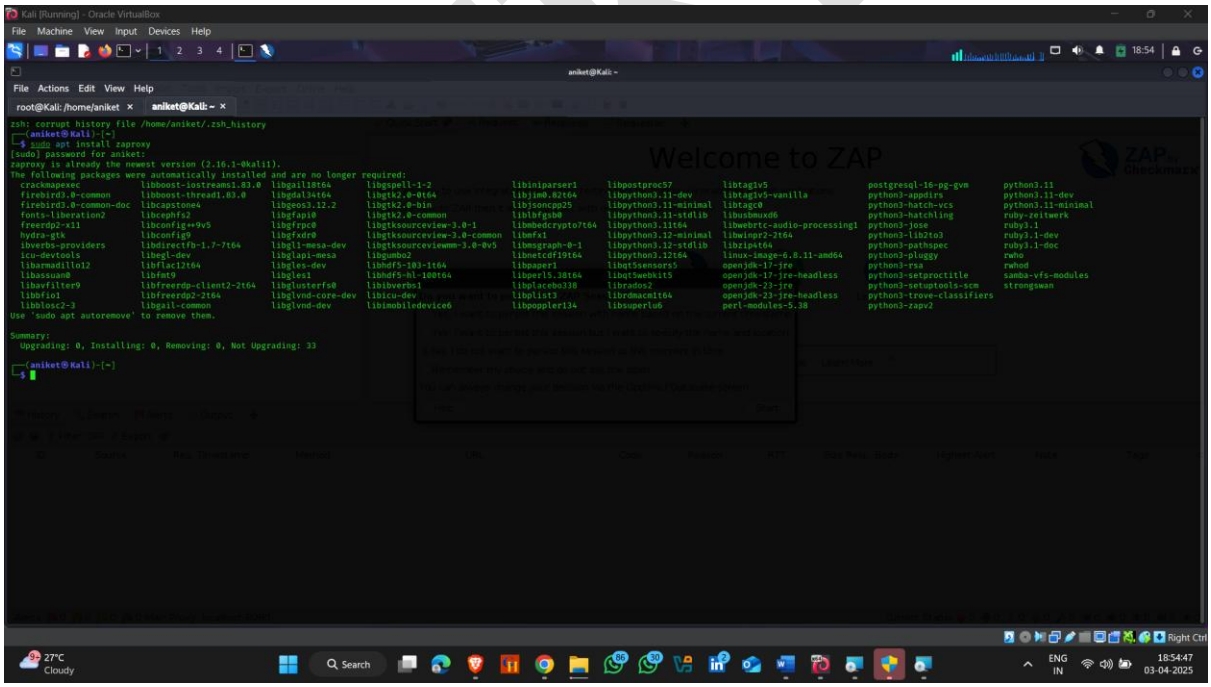


Vulnerability Analysis Using Checkmarx ZAP

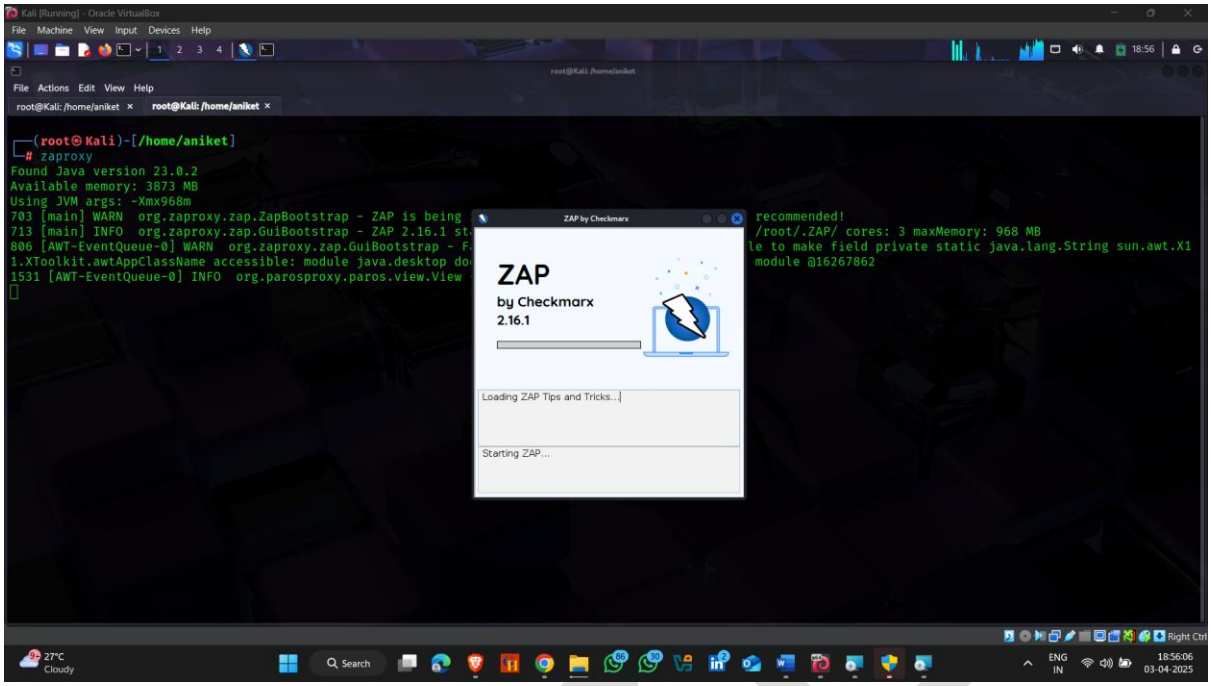
ZAP (Zed Attack Proxy) is a dynamic application security testing tool published under the Apache License. It allows users to manipulate all of the traffic that passes through it, including HTTPS encrypted traffic, when used as a proxy server.

How to use it –

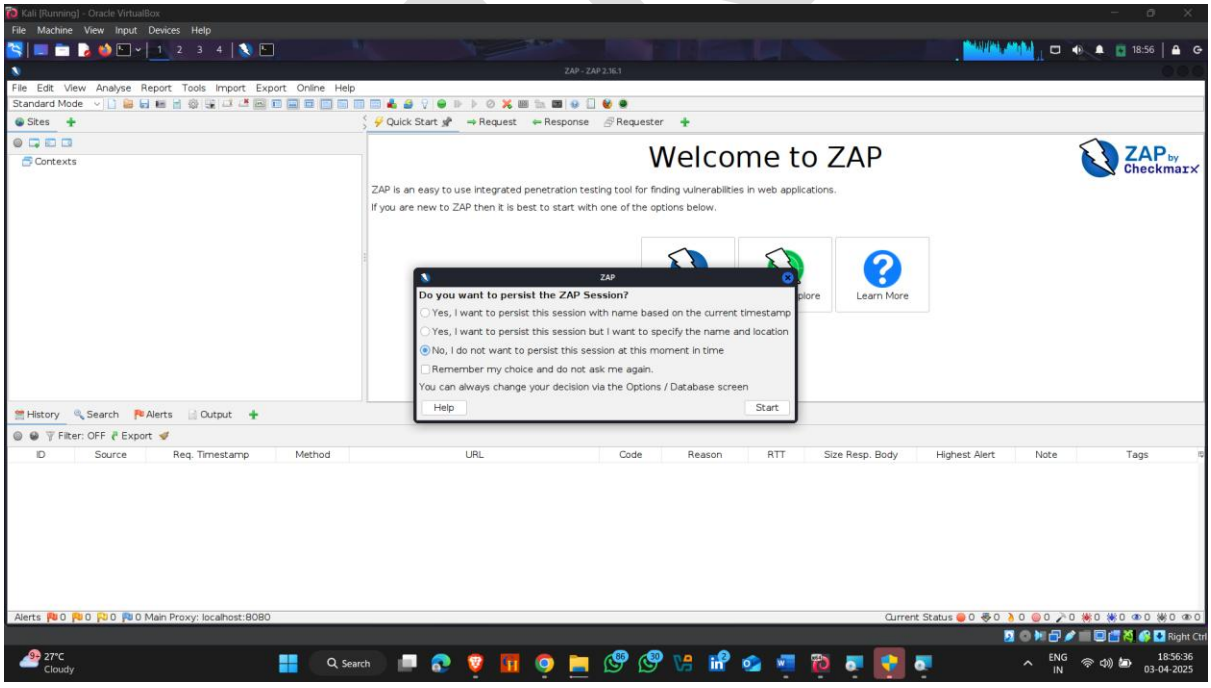
- Open kali Linux / Parrot OS
- Open Terminal And **type sudo apt install zaproxy**



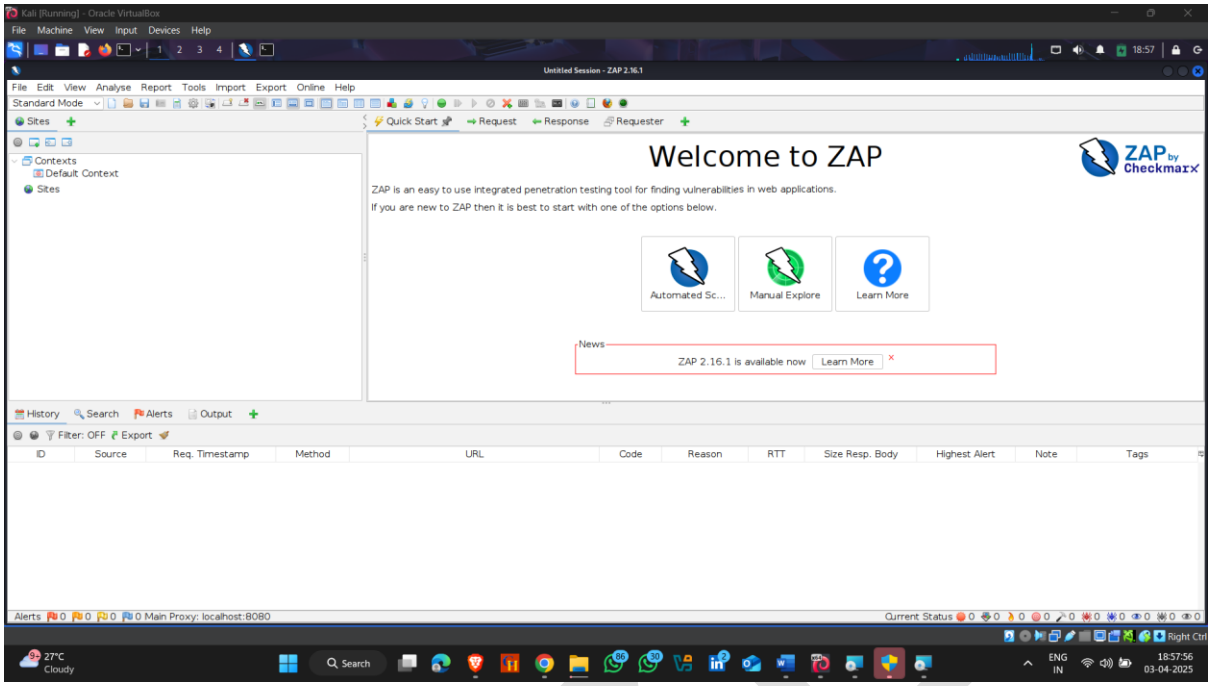
❖ **Then type zaproxy**



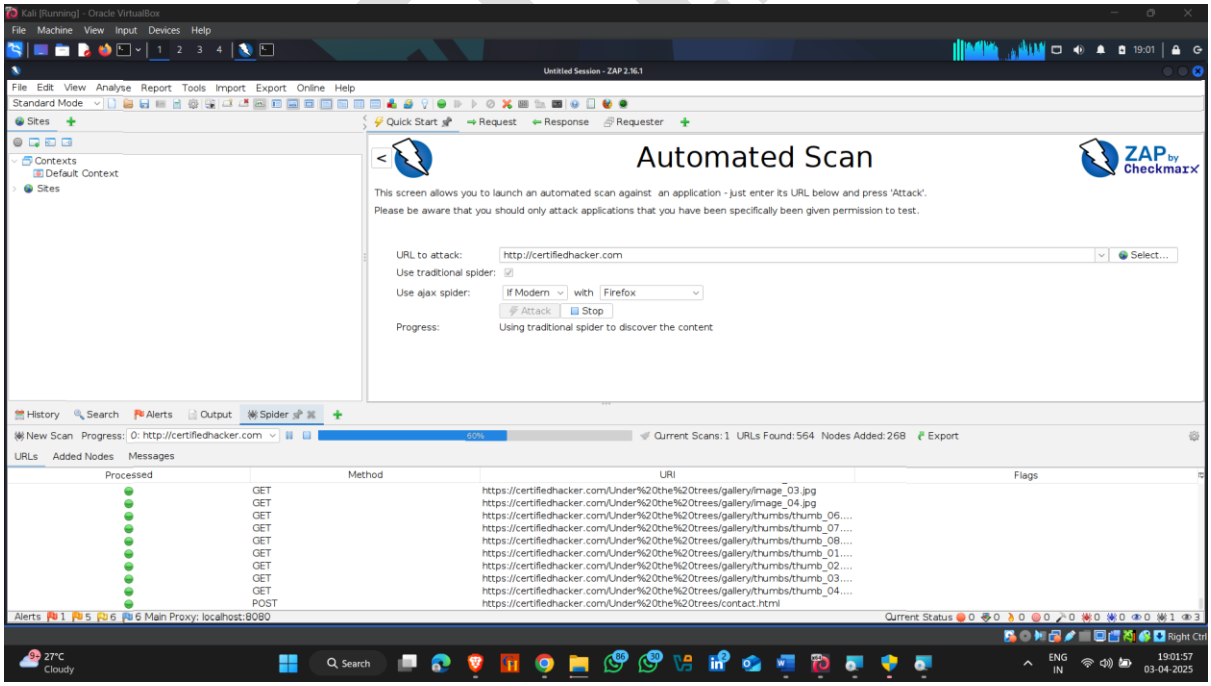
❖ Select **third option** and click on **start**



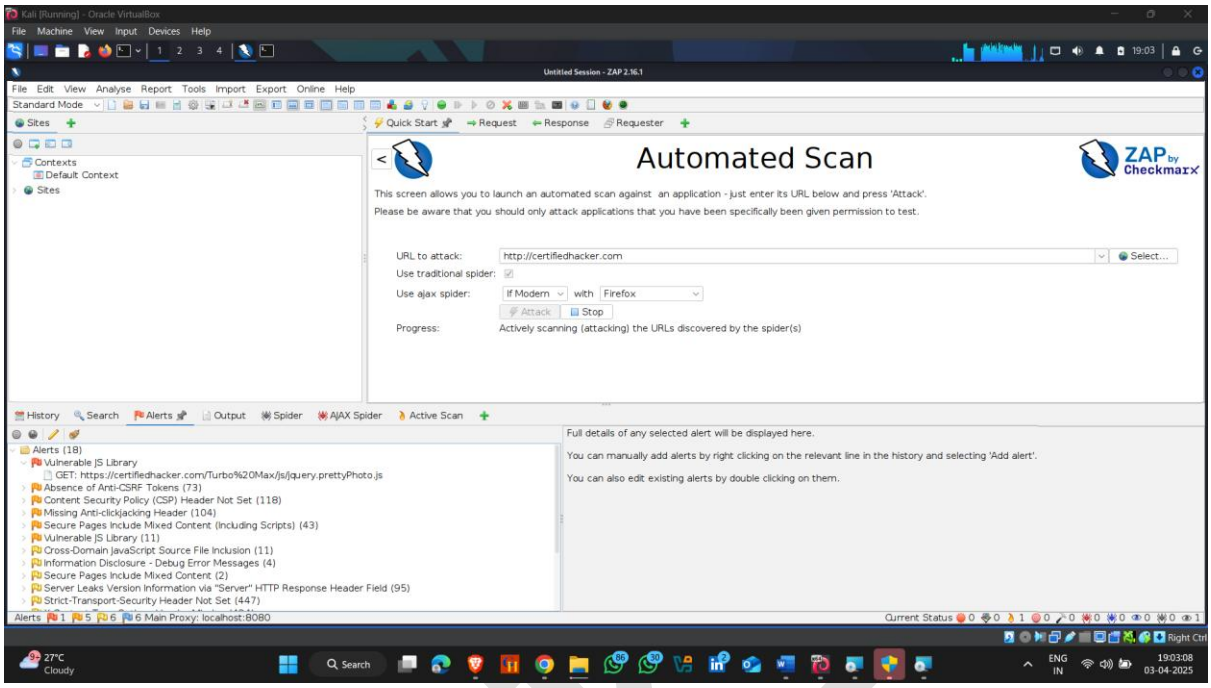
❖ **Click on automated scan**



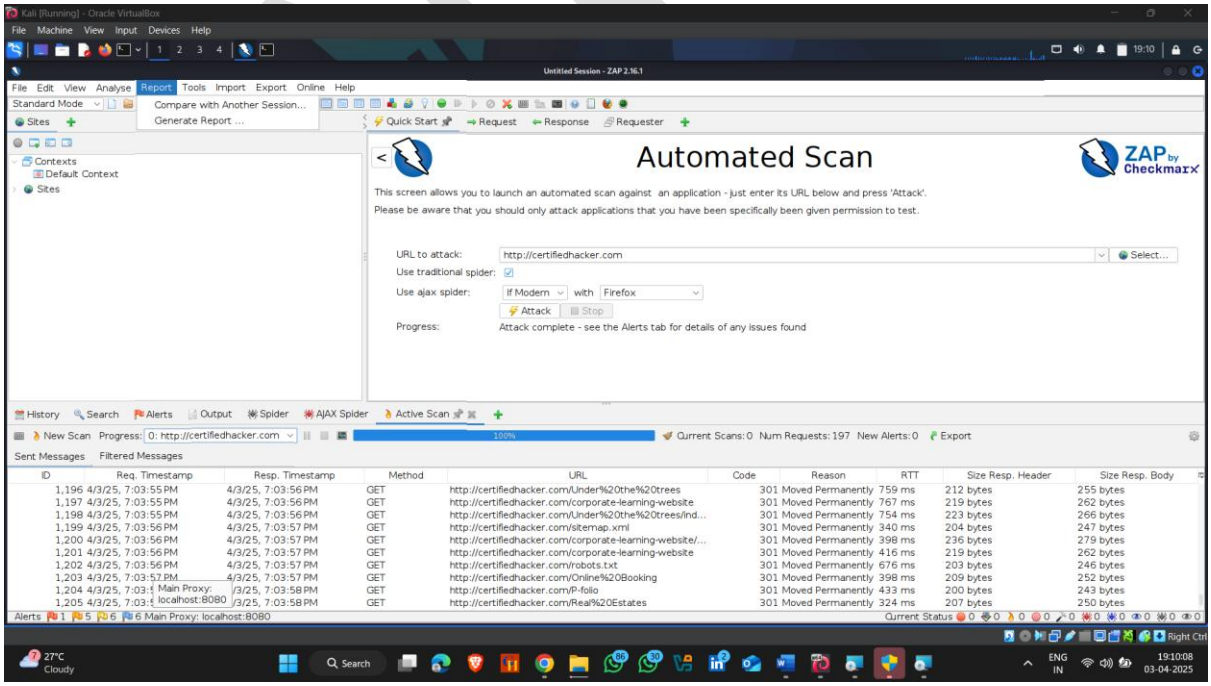
❖ Provide **domain name** , click on **use traditional spider checkbox** and click on **attack**



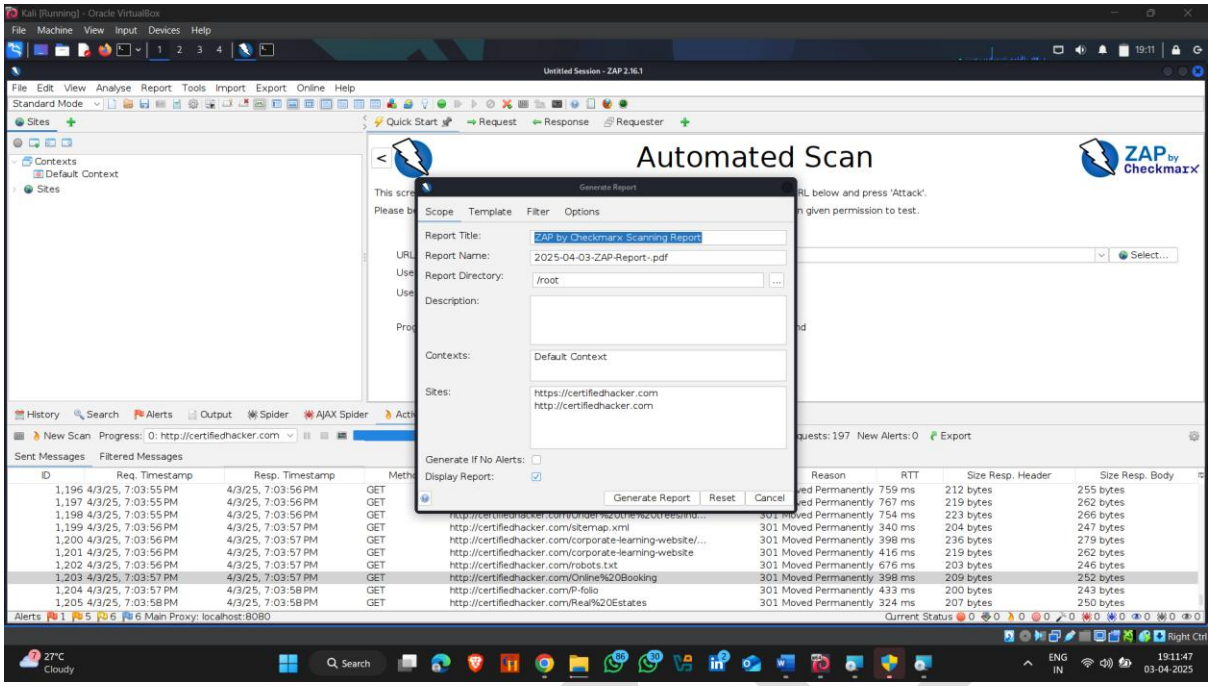
- If you want to see there is any vulnerability spotted on your target **just click on alerts option**
- See our target are vulnerable with many things



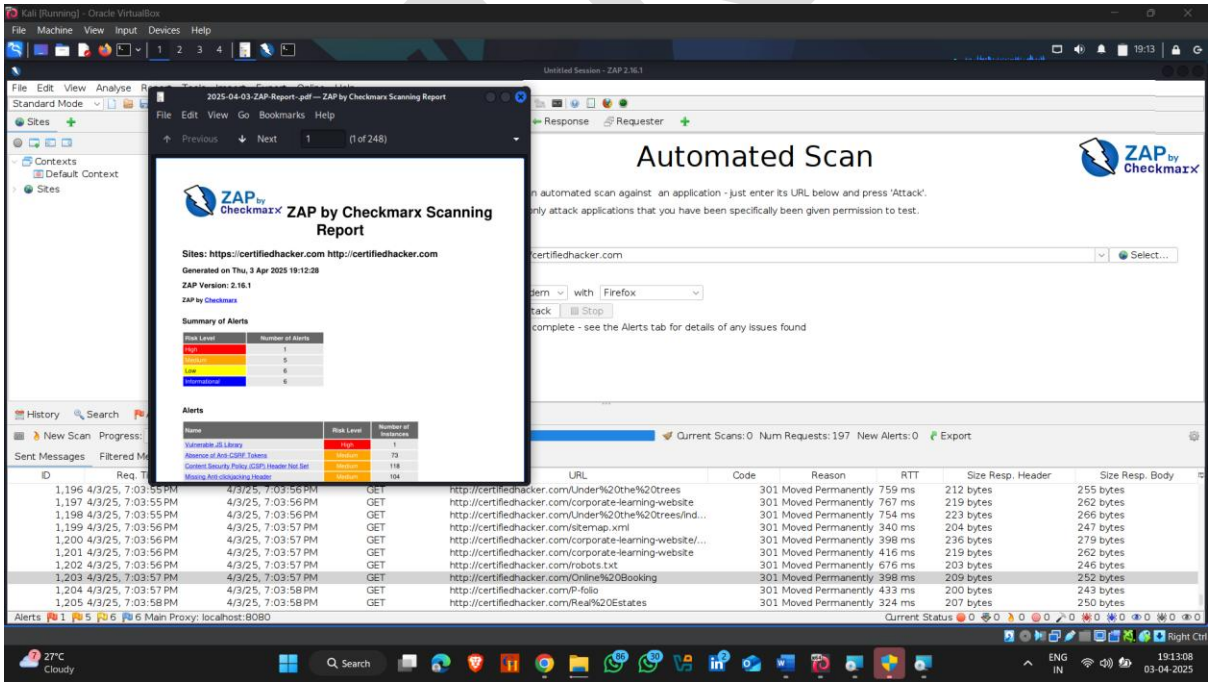
- **Now You can also Generate report**
- **Click on report section and click generate report**



❖ And click again on **generate report**



❖ Here You can see the detailed report



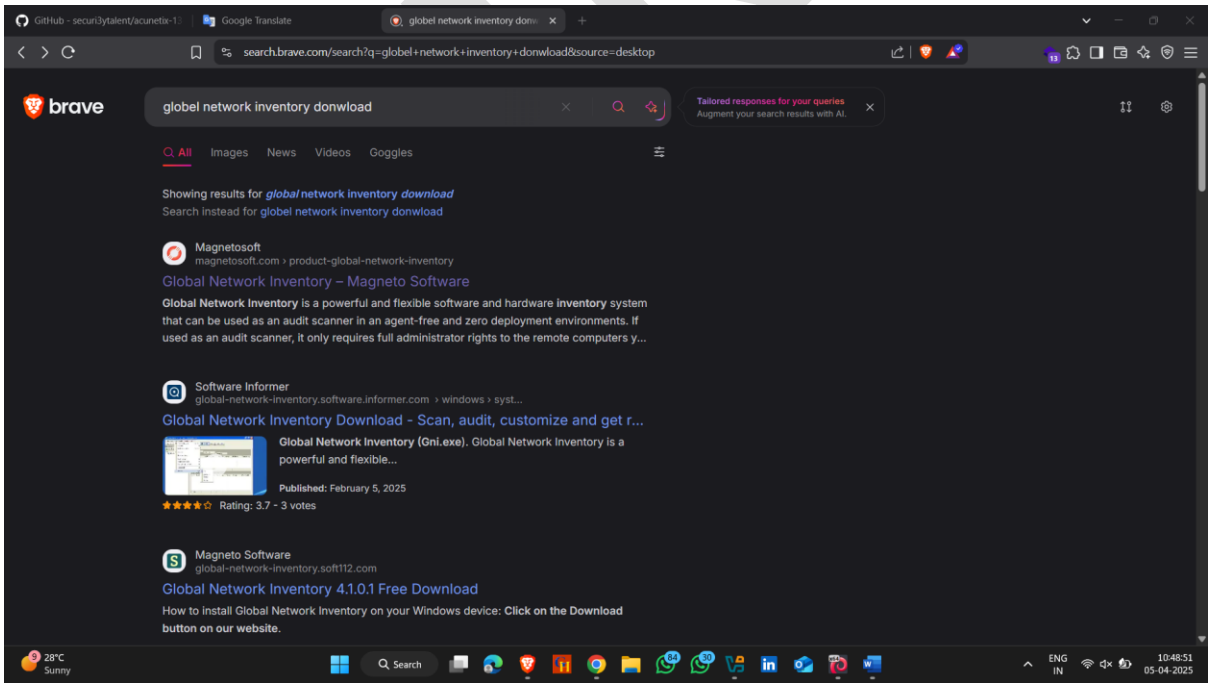
Vulnerability Analysis Using Globel Network Inventory

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.

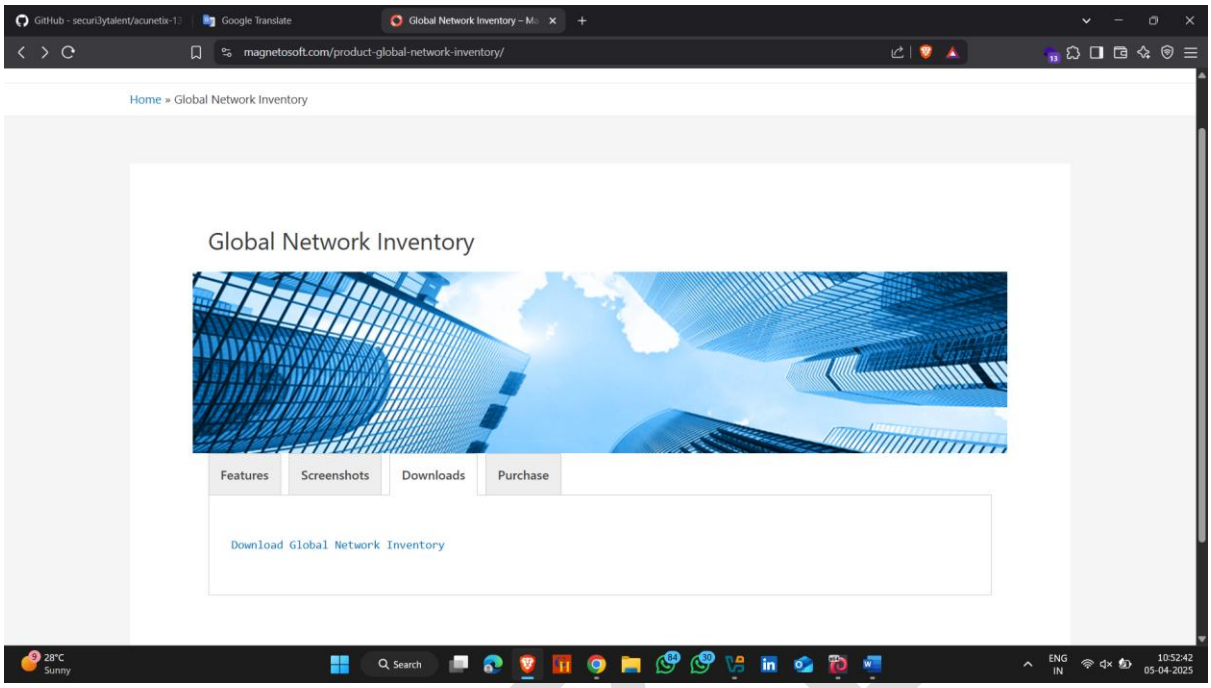
Download link -: https://magnetosoft.com/product-global-network-inventory/

How to use it – :

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

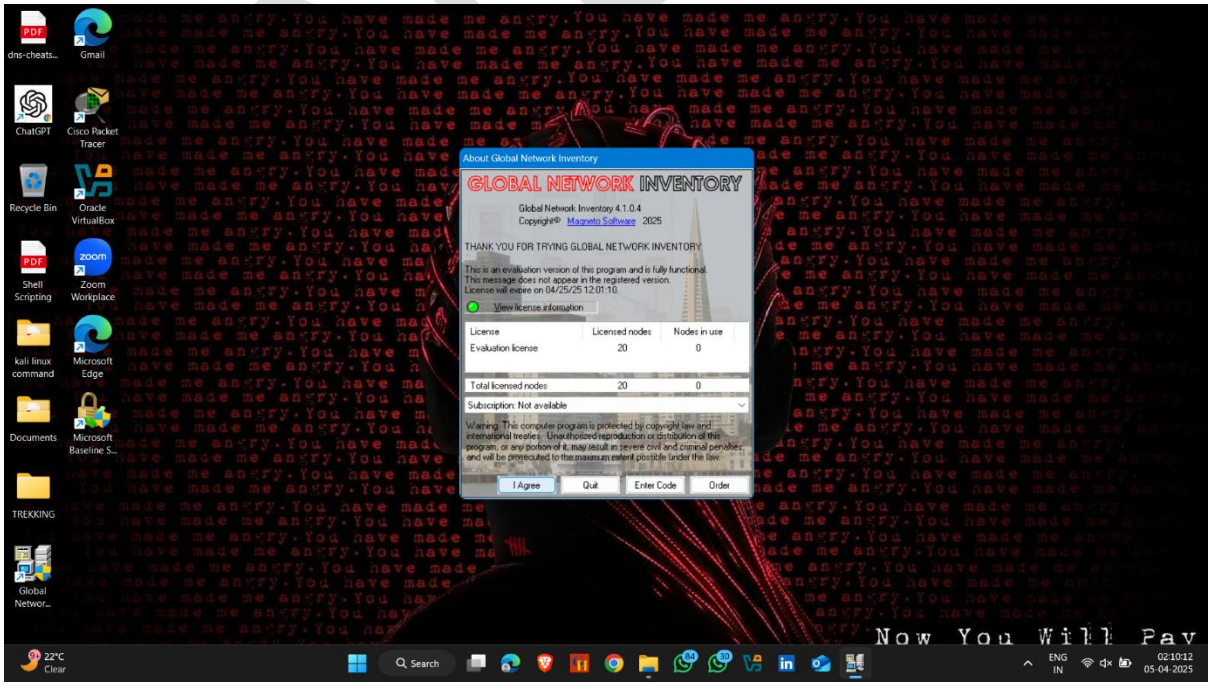


- Click on Donwload section and then **click on Download Globel network inventory**



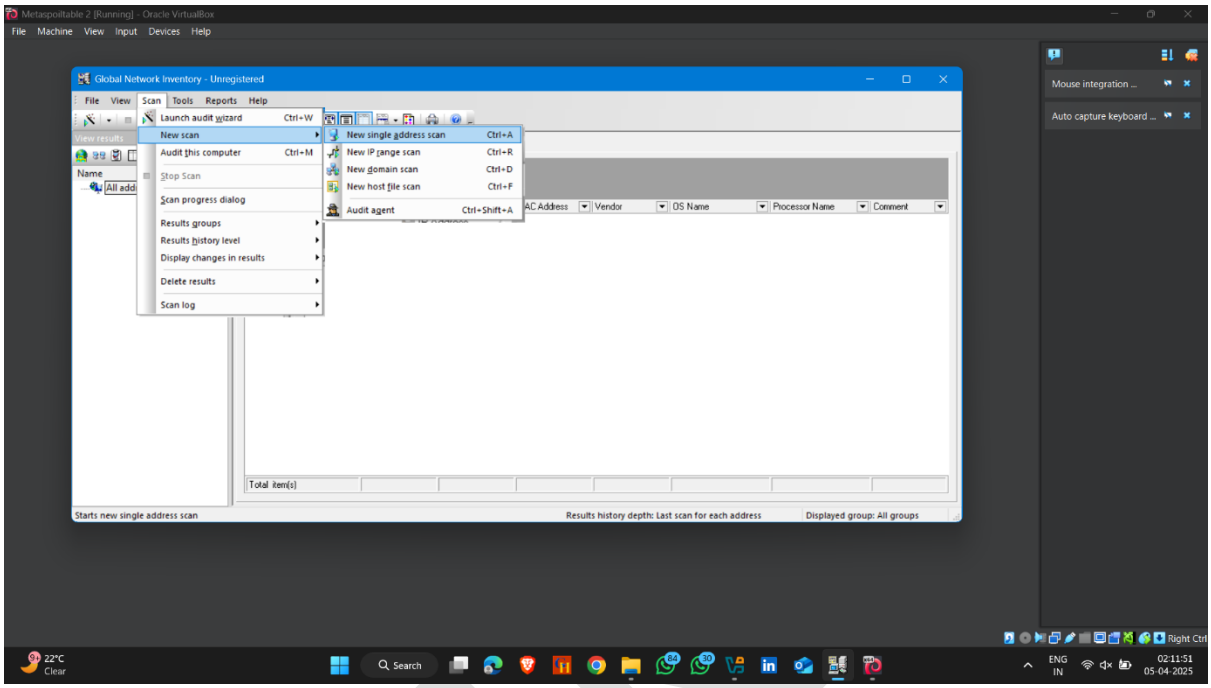
- **Install it and setup it**

- Here our installation is completed , **click on I agree**

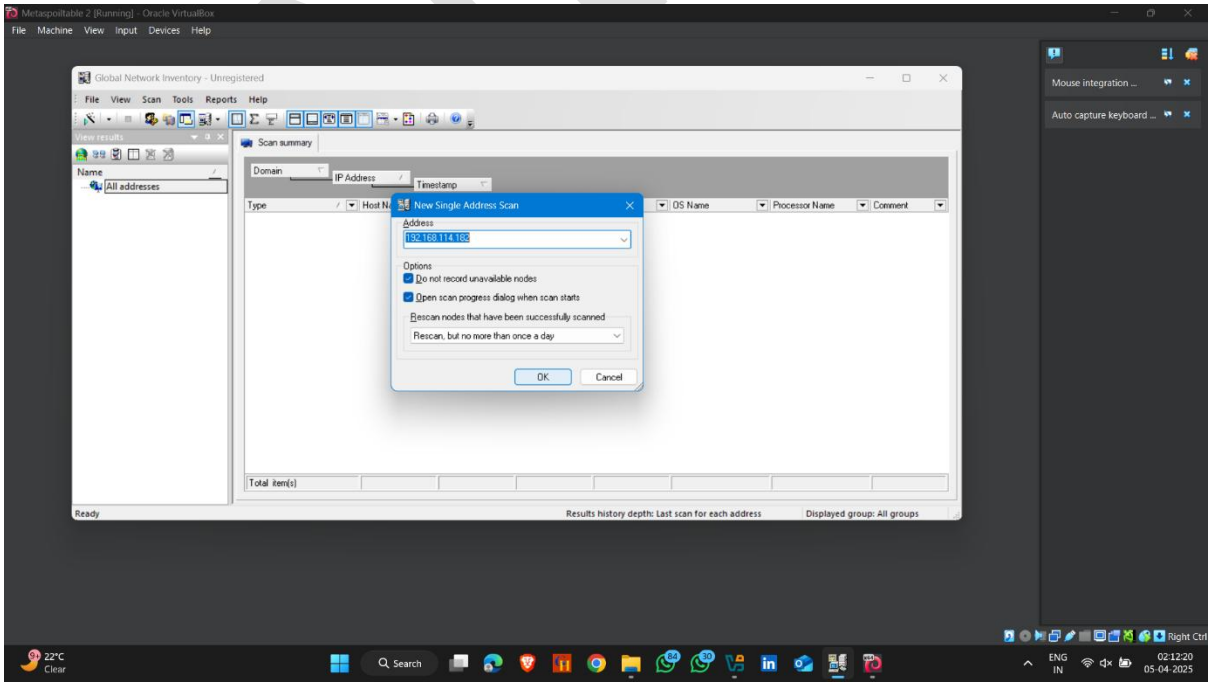


- Then click on scan option , new scan and new single address scan

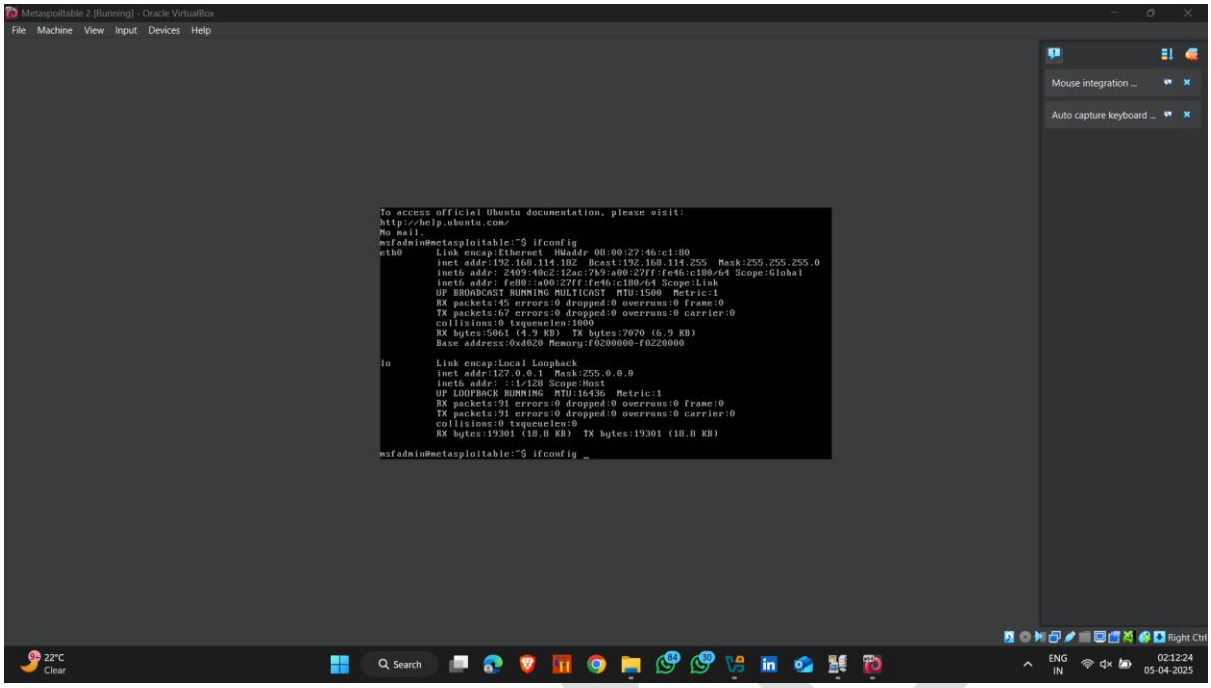
Note -: you can also scan ip ranges , domain scan



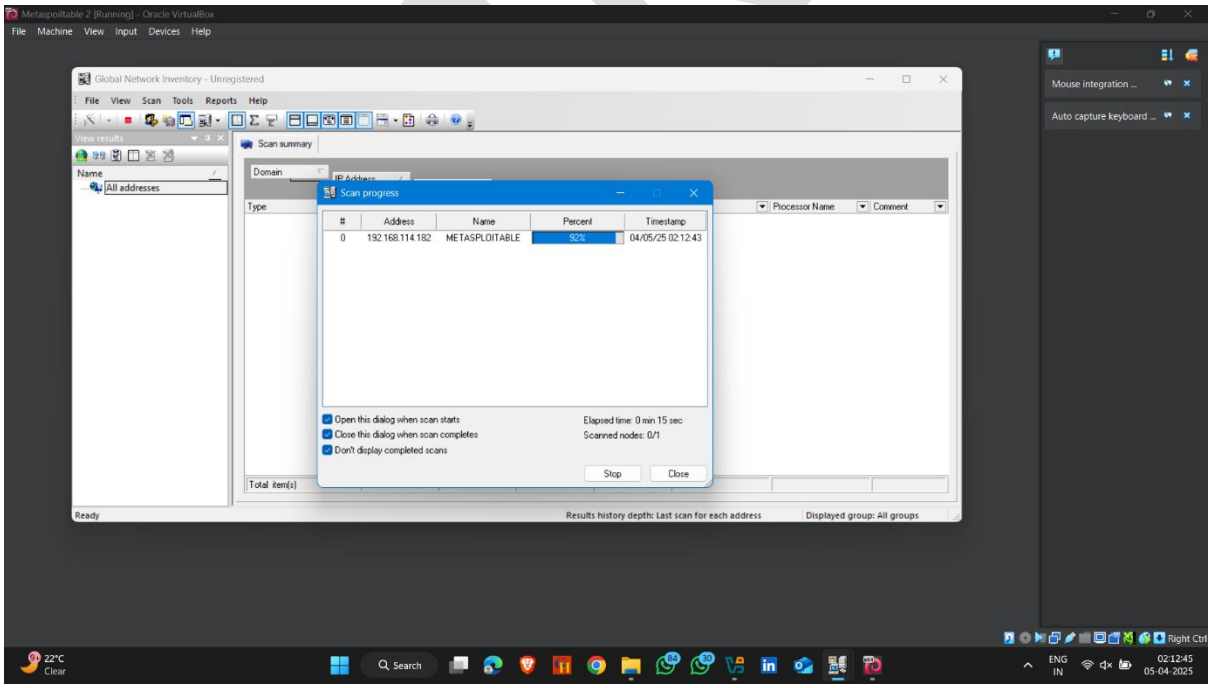
- Enter target ip address and click ok



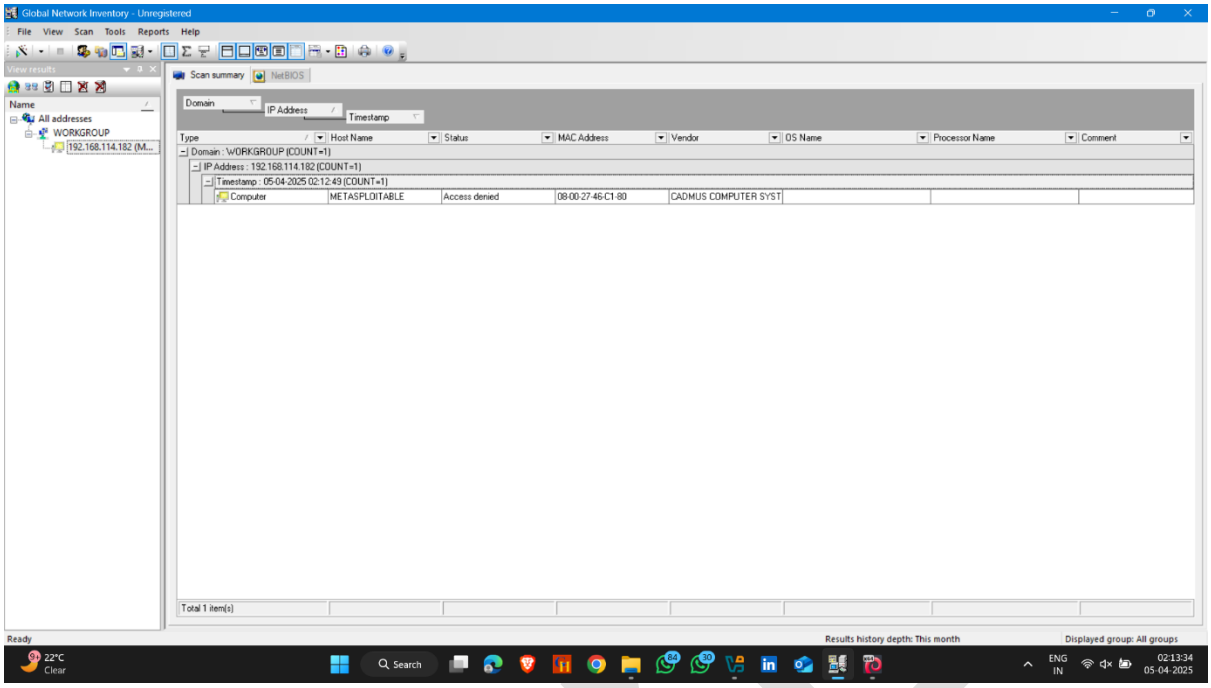
- **In my case , I'm using metasploitable 2 as a target machine**



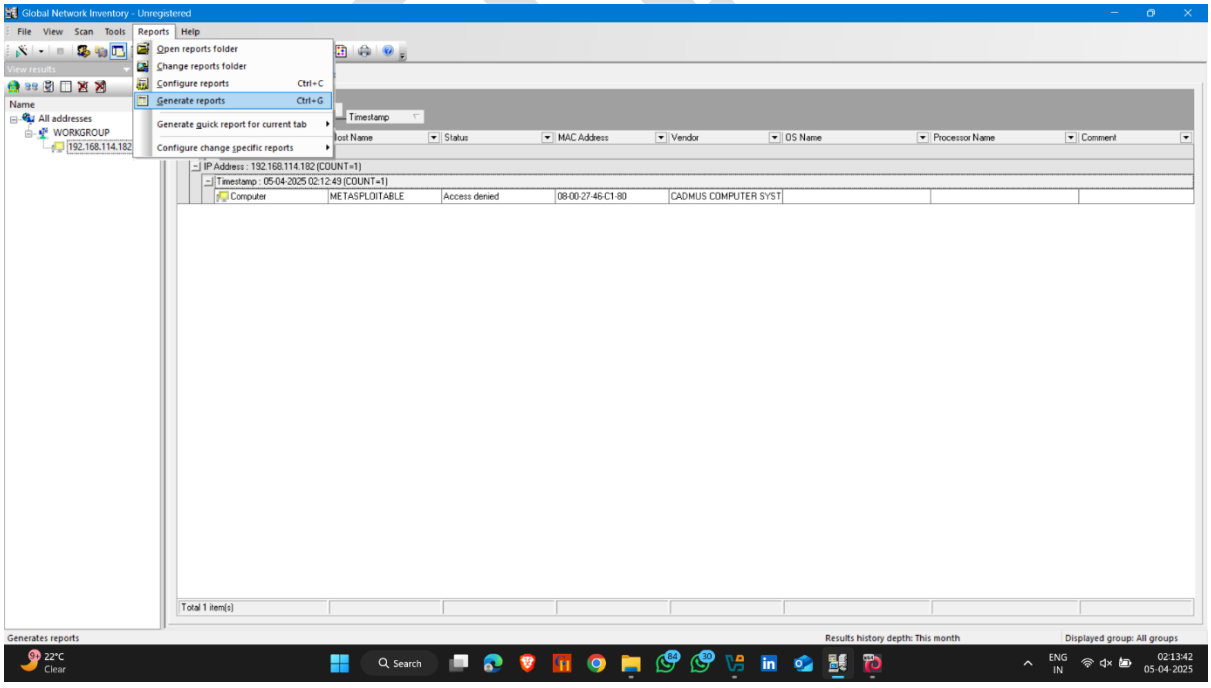
- Here scanning start



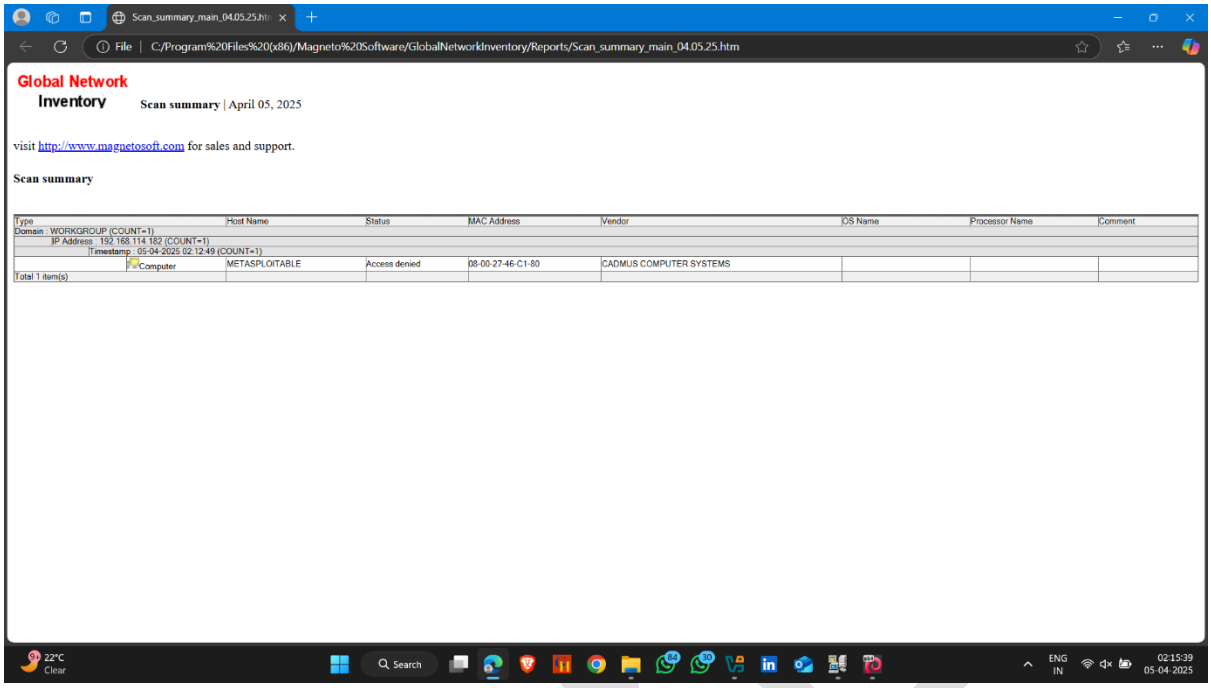
- **Scan Completed**



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



- Now you see the report

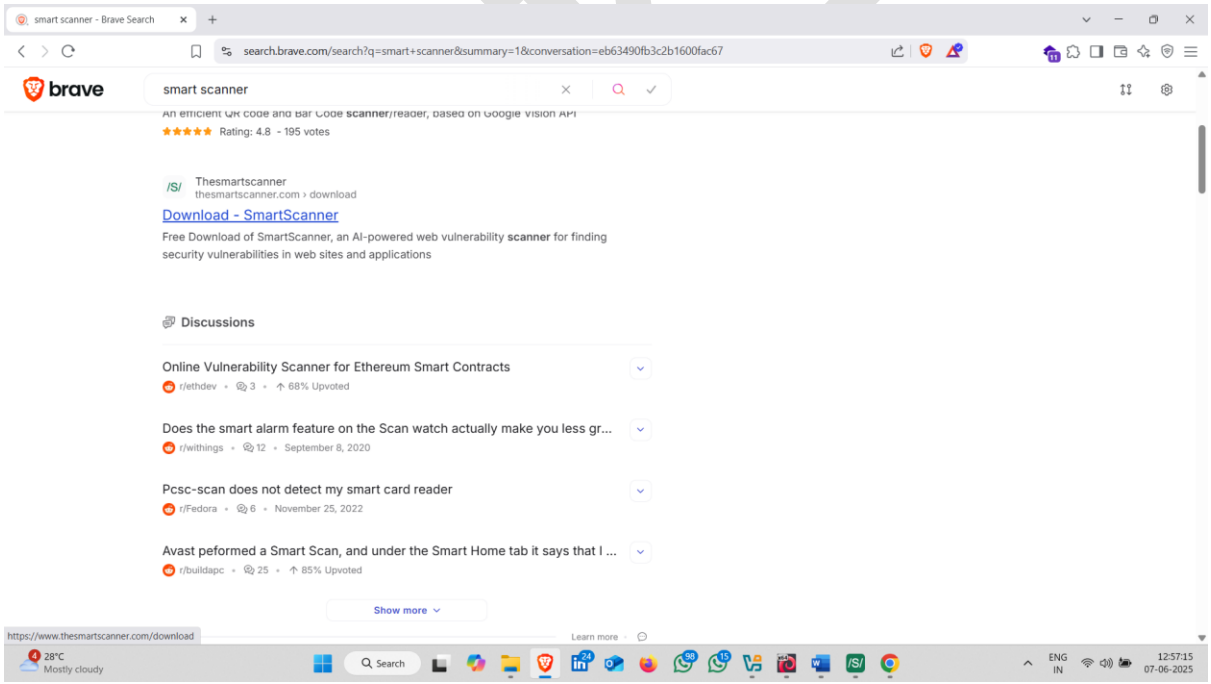


Vulnerability Analysis Using Smart Scanner

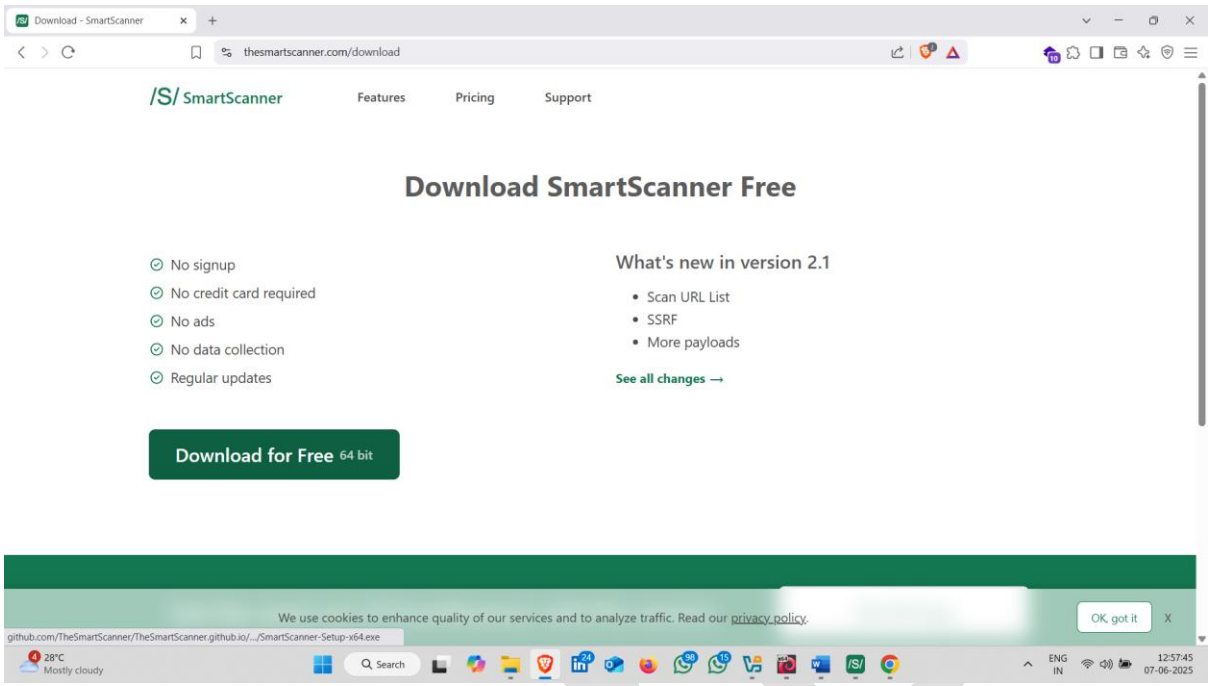
A **Smart Scanner** is an **intelligent vulnerability scanning tool or feature** that uses advanced techniques like automation, machine learning, or heuristic analysis to **efficiently detect security vulnerabilities** in systems, networks, or applications — with **greater accuracy, speed, and context-awareness**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

How to download it -:

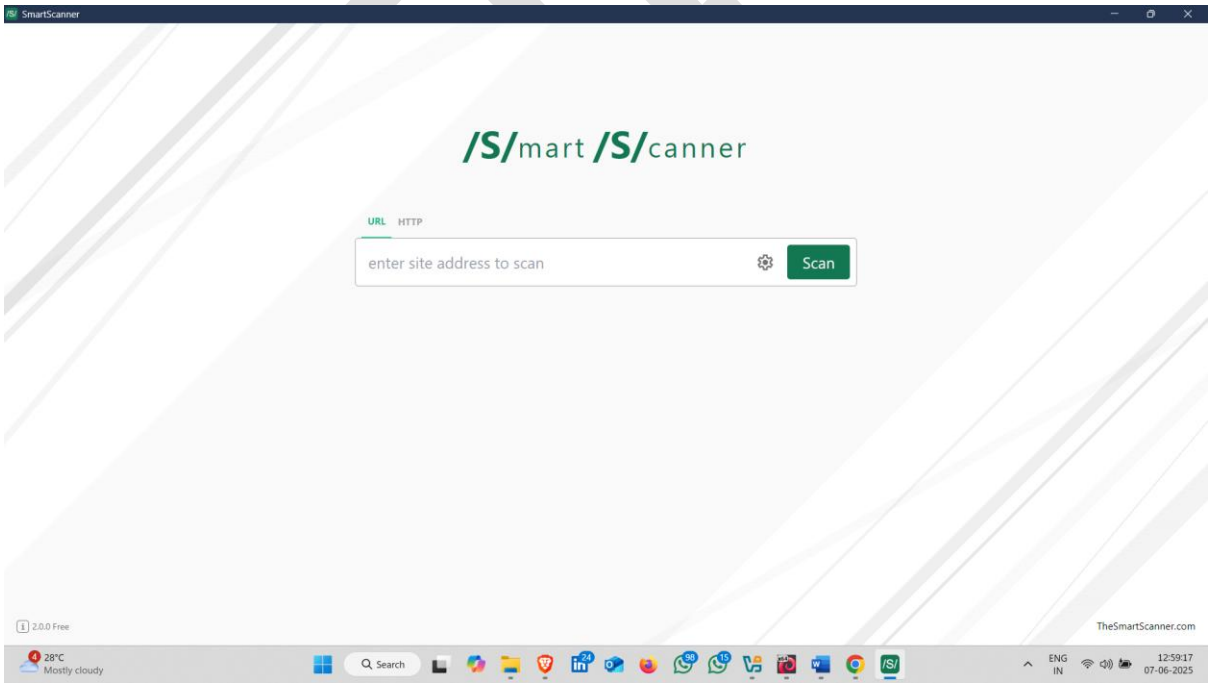
- Open Browser and search smart scanner
- Click on official Website



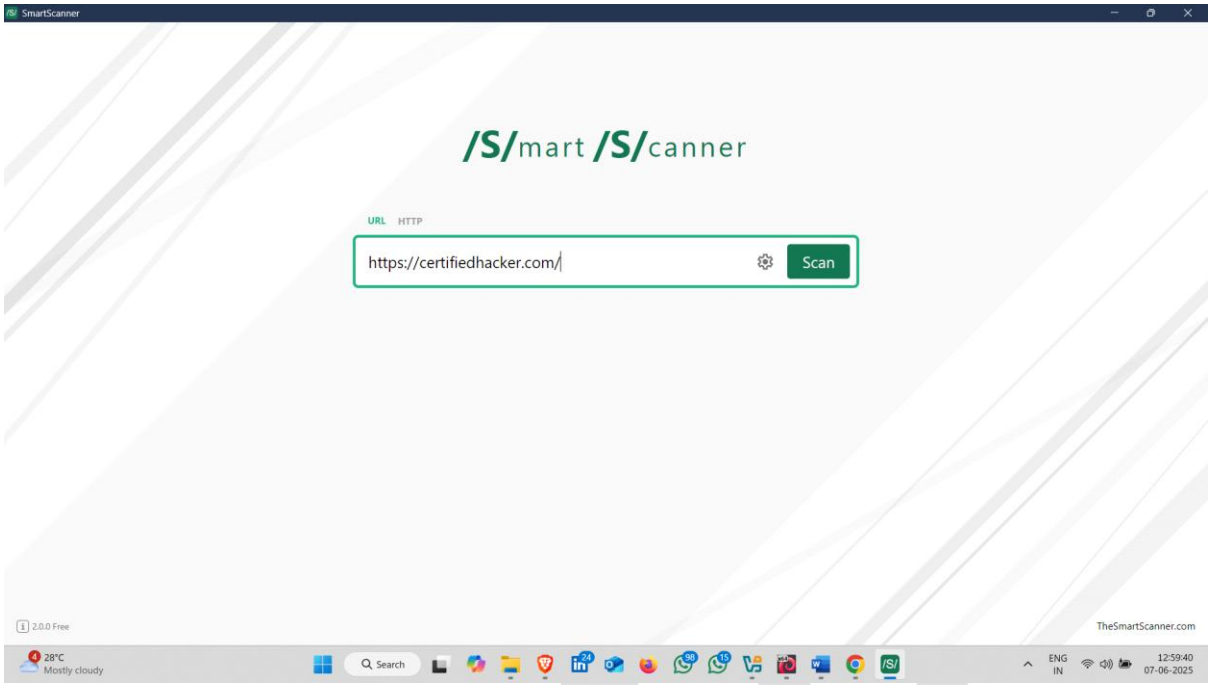
- Click on Download for free 👇



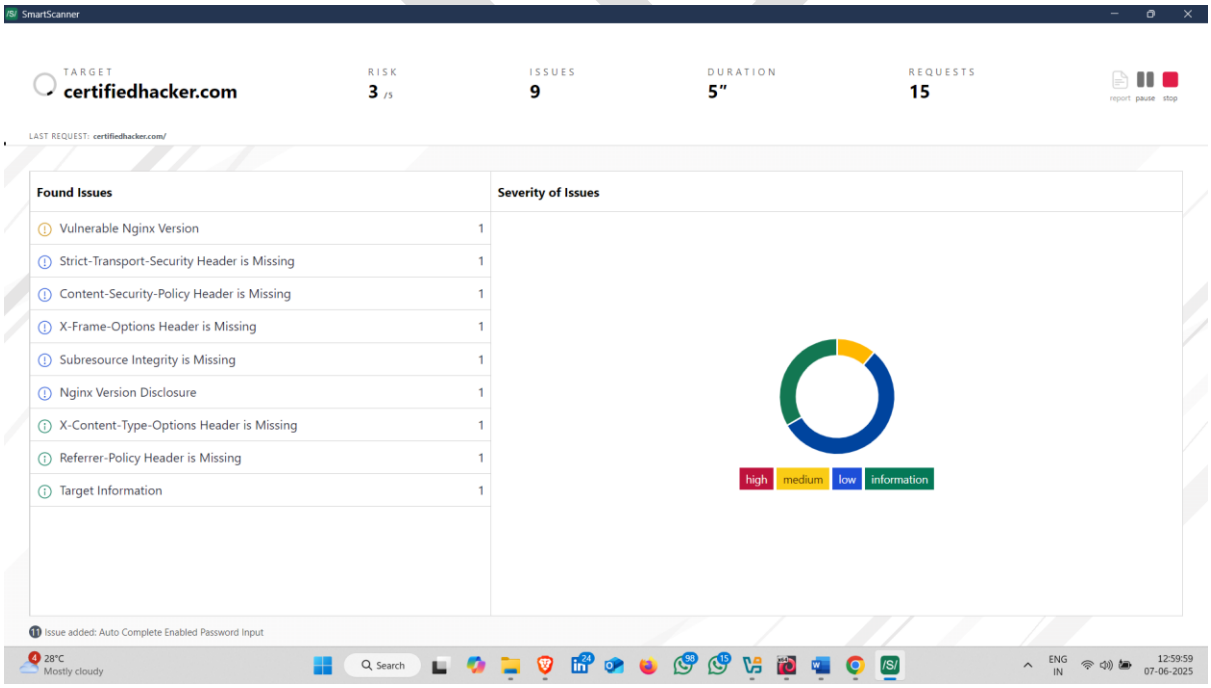
- After Downloading the app open and setup it -:
- Now enter the website that you want to scan



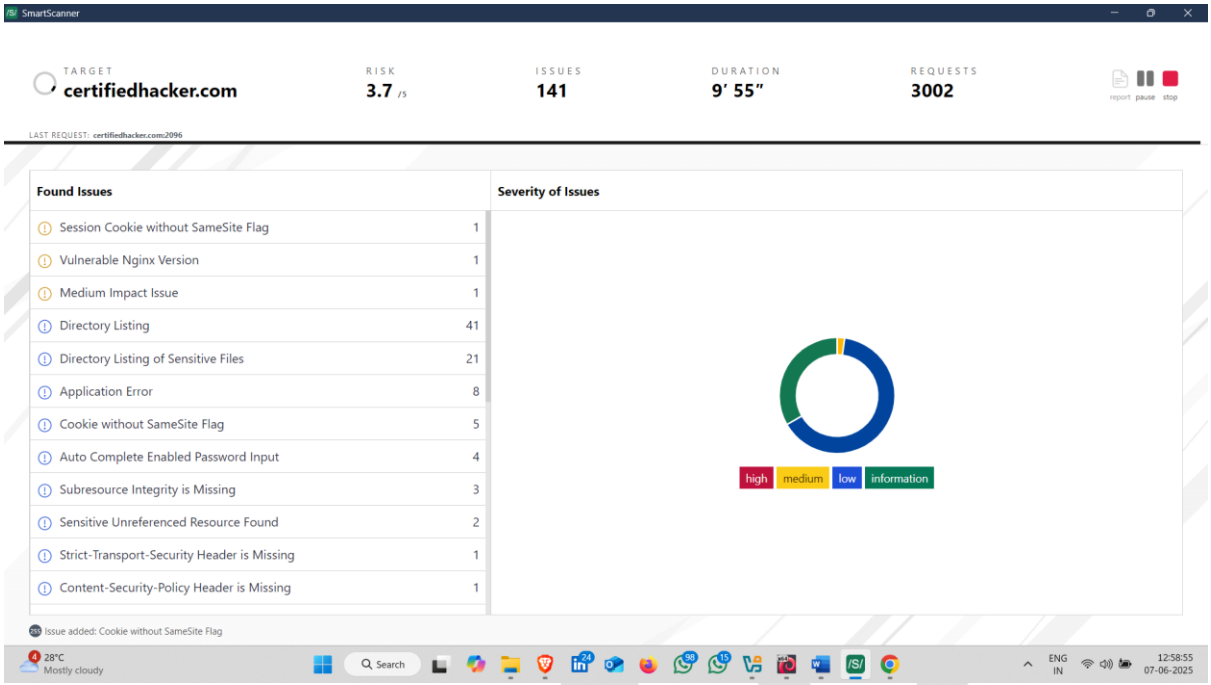
- Now click on Scan



- 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)** 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)

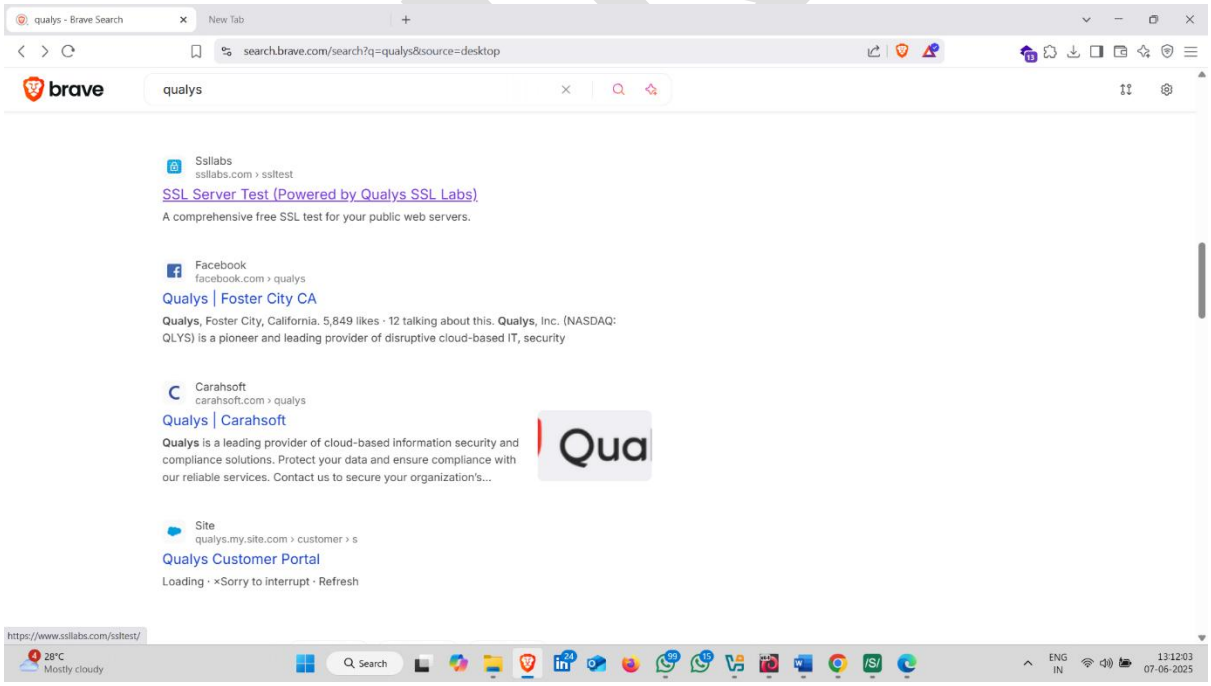
- **DROWN** (SSLv2 usage in TLS servers)
- **Logjam** (weak Diffie-Hellman parameters)
- **RC4 cipher usage** (insecure and deprecated)
- **Export-grade ciphers** (weak for modern use)

🔍 10. Scan Depth:

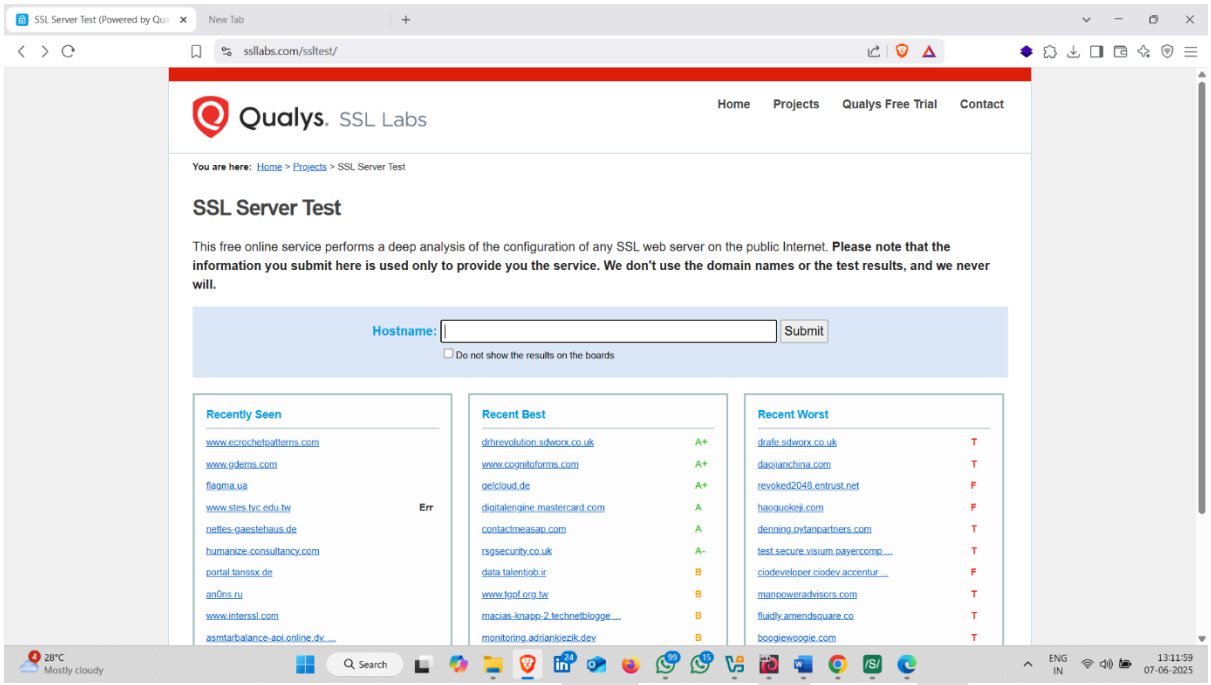
The tool simulates how different browsers and devices (e.g., IE on XP, Chrome on Android, Safari on Mac) interact with the server to identify handshake compatibility issues.

How to use it -:

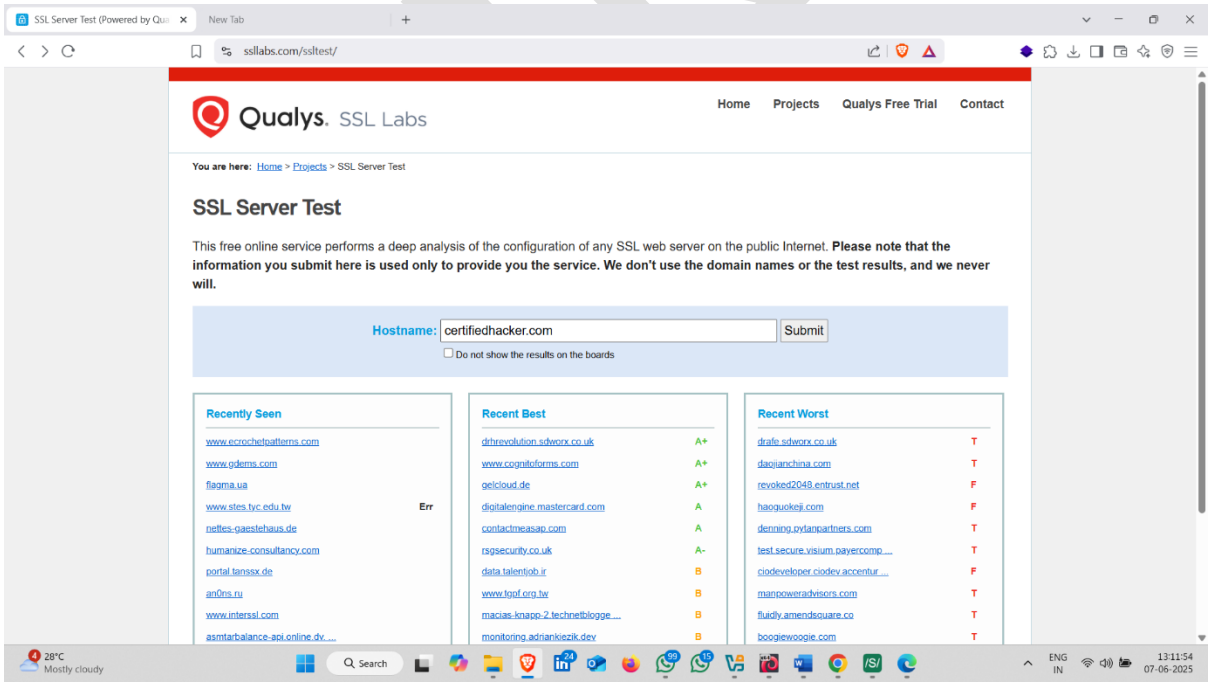
- Open Browser and Search Qualys Ssl Labs
- Click on ssllabs Official Website 👇



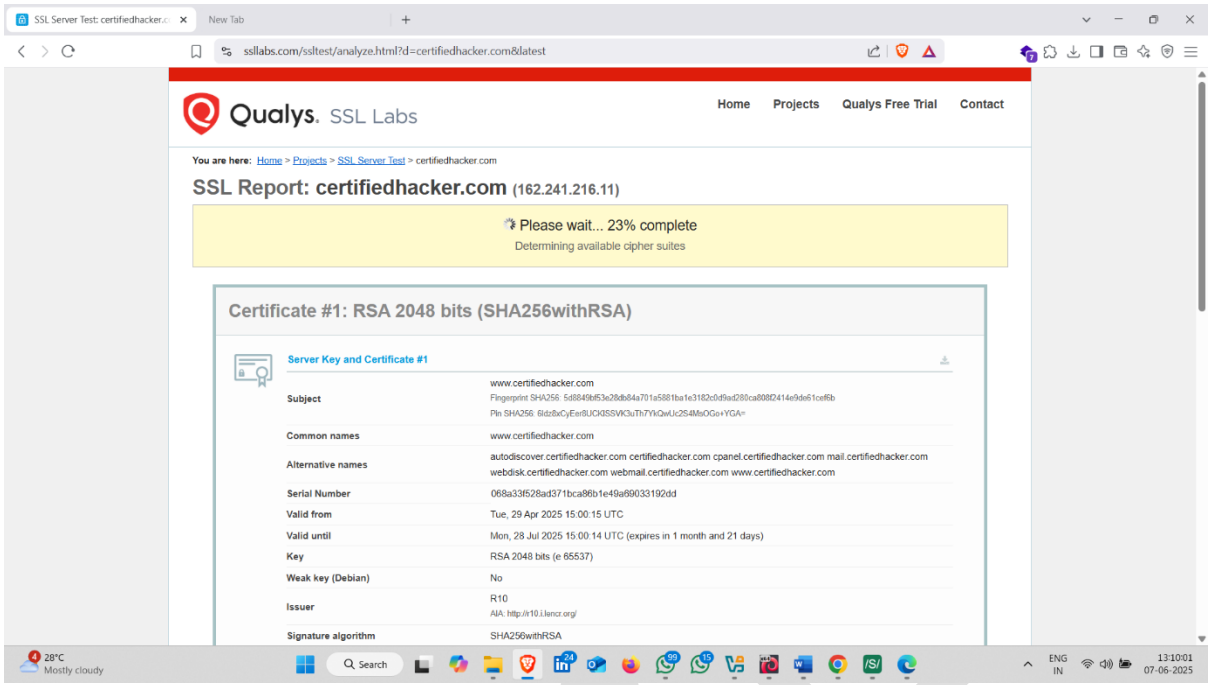
- Provide a URL for scanning



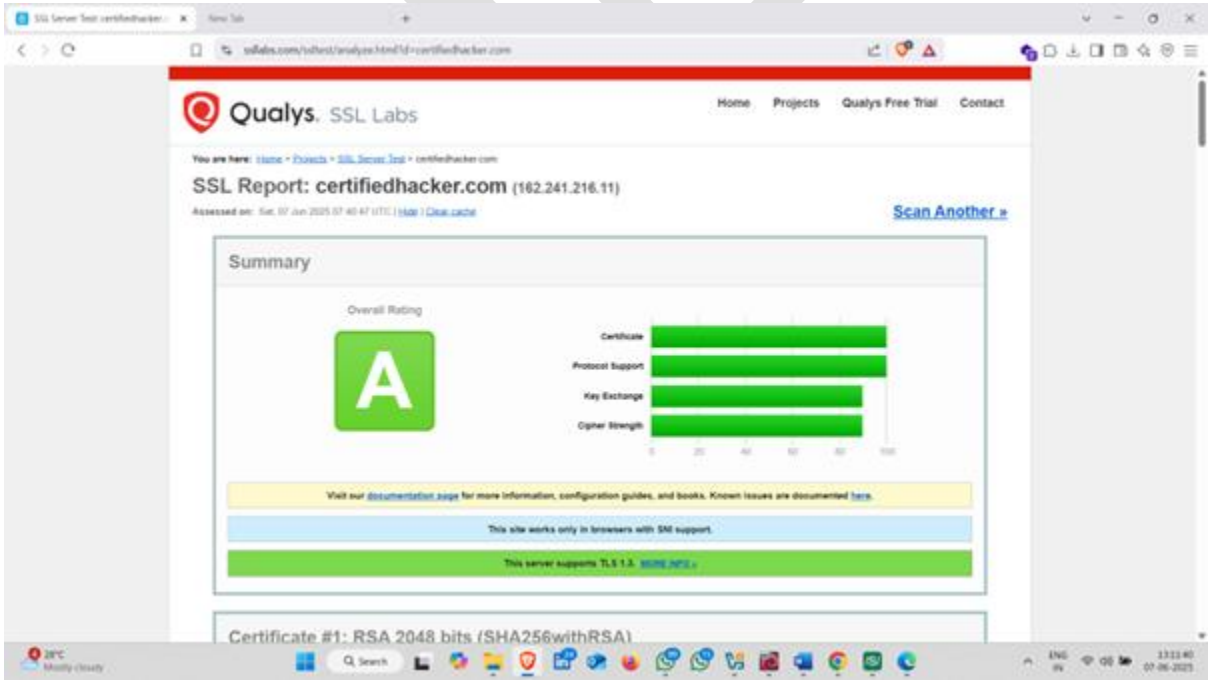
- Click on Submit



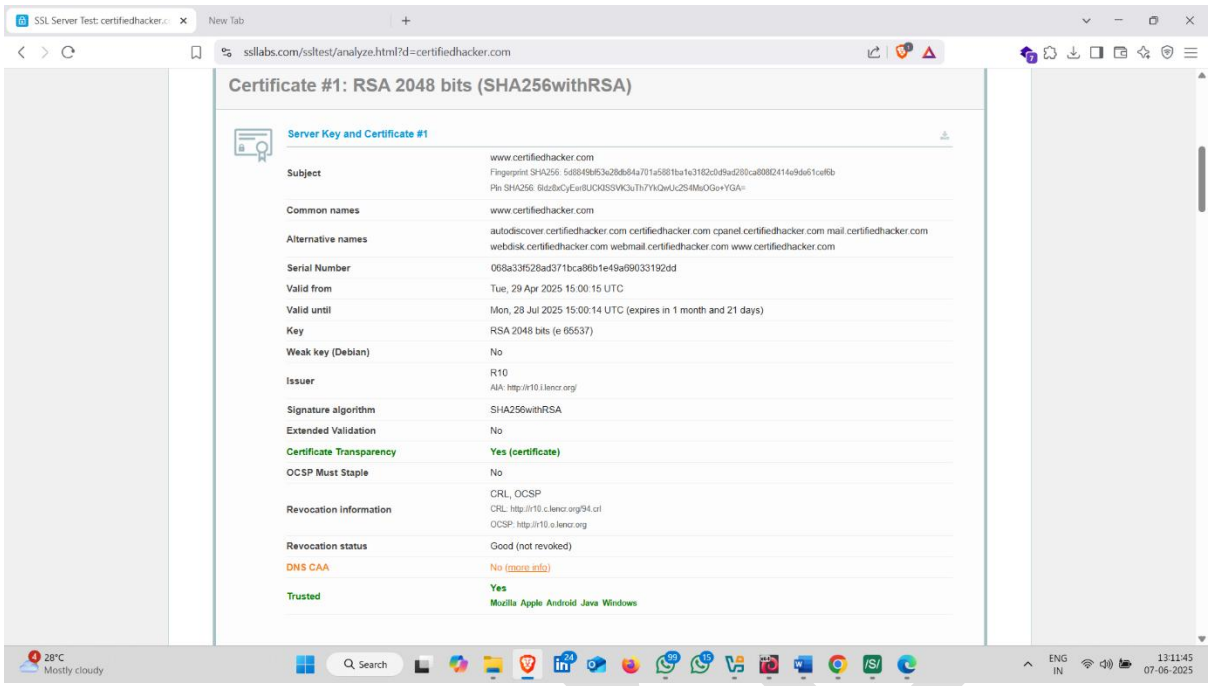
- Scanning Started



- Scan Completed 👇



- Result ✅ 👇



THANK YOU