Module 5

Vulnerability analysis

2.12.25

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

Index

1 . SmartScanner :

1 . Smart Scanner is an automated vulnerability scanning feature inside OWASP ZAP (Zed Attack Proxy).

2 . It checks your target website for security weaknesses without needing manual configuration.

3 . It detects issues like:

- **1 . XSS (Cross-Site Scripting)**
- **2 . SQL Injection**
- **3 . Broken authentication**
- **4 . Directory listing**
- **5 . Missing security headers**
- **6 . Sensitive data exposure**

4 . Smart Scanner automatically spiders (crawls) all pages it finds all:

- **1 . URLs**
- **2 . Forms**
- **3 . Parameters**

5 . It tests each parameter using pre-built attacks.

6 . Helps find how the web app behaves under malicious input.

7 . Generates security reports and provides a list of:

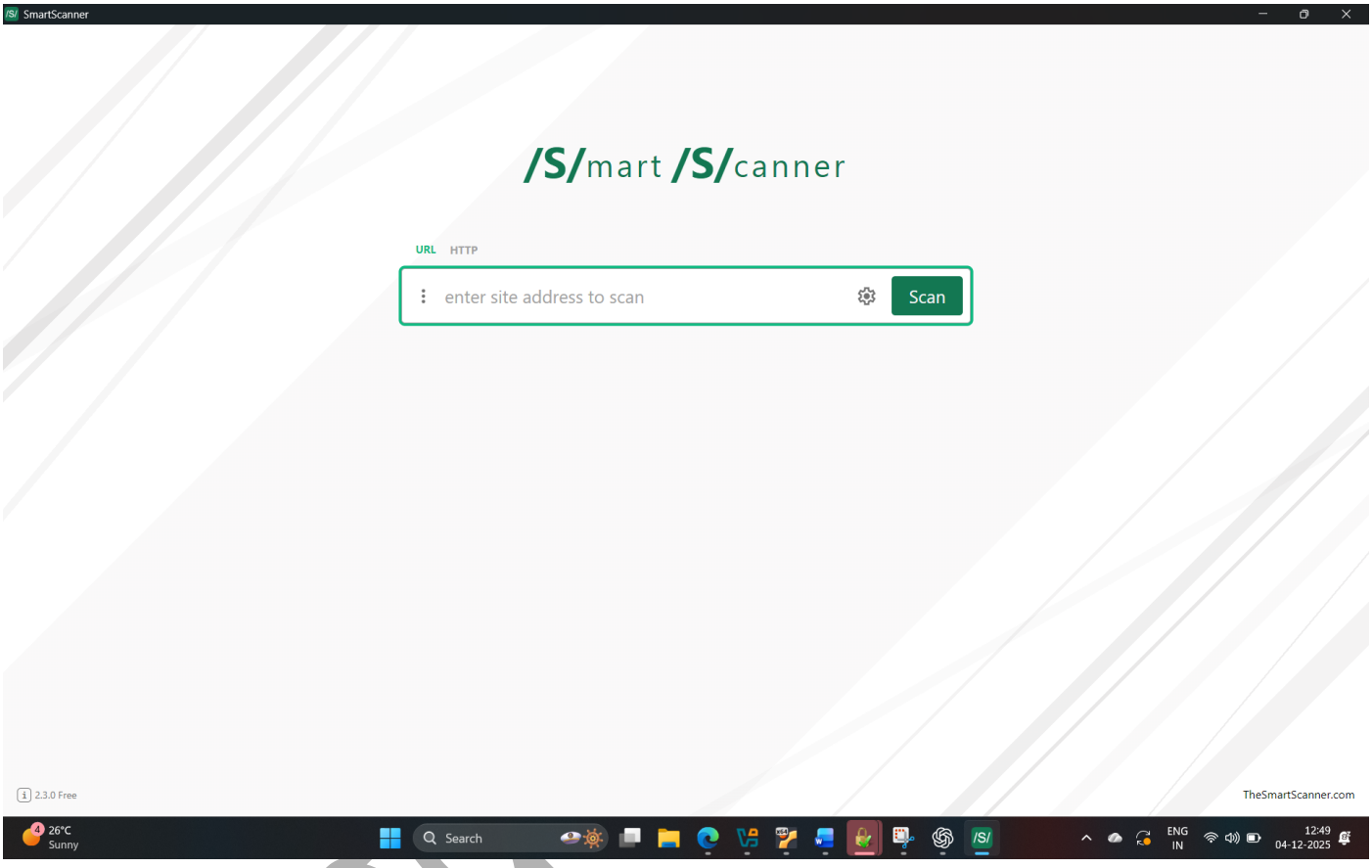
- **1 . Vulnerabilities**
- **2 . Their severity (High, Medium, Low)**
- **3 . Description**
- **4 . Proof of concept**
- **5 . Fix recommendation**

8 . Steps :

1 . install and setup SmartScanner.

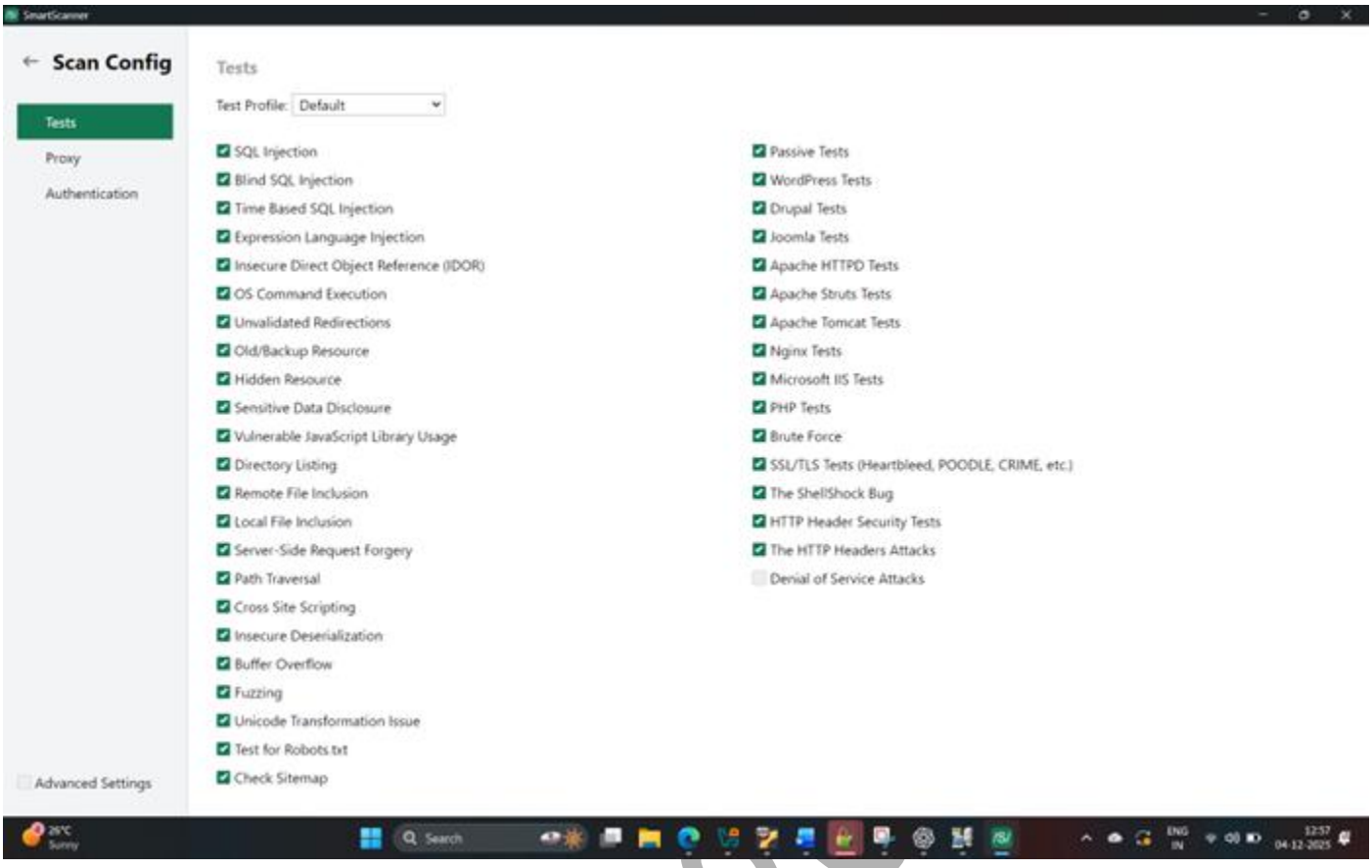
2 . search bar interface will appear then run certifiedhacker.com in the search bar.

3 . then click on the scan .



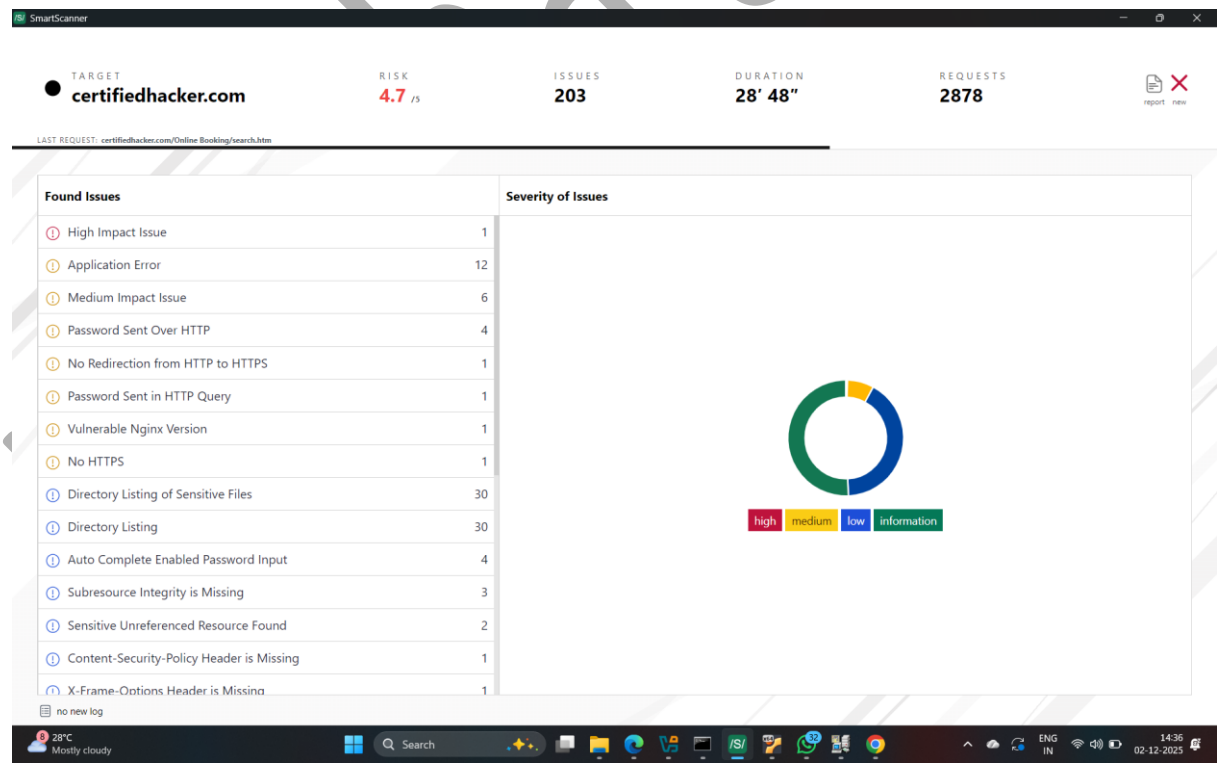
1.1

4 . Then click on the setting icon then various vulnerability checkbox will appear then select which vulnerability you want to check .



1.2

5 . issues/vulnerabilities and severity of issues will start to appear.



1.3

6 . close the SmartScanner.

2 .Nessus :

1 . Vulnerability Scanning Nessus scans systems, servers, and networks to find security weaknesses like misconfigurations, outdated software, weak passwords, etc.

2 . Detects Known Vulnerabilities (CVE) : It identifies vulnerabilities listed in global databases (CVE, CVSS) and tells you their severity levels — Low, Medium, High, Critical.

3 . Generates Detailed Security Reports it provides reports showing vulnerabilities, their impact, affected machines, and recommended fixes.

4 . Helps in Remediation Nessus gives step-by-step guidance to fix the vulnerabilities, helping secure the network faster.

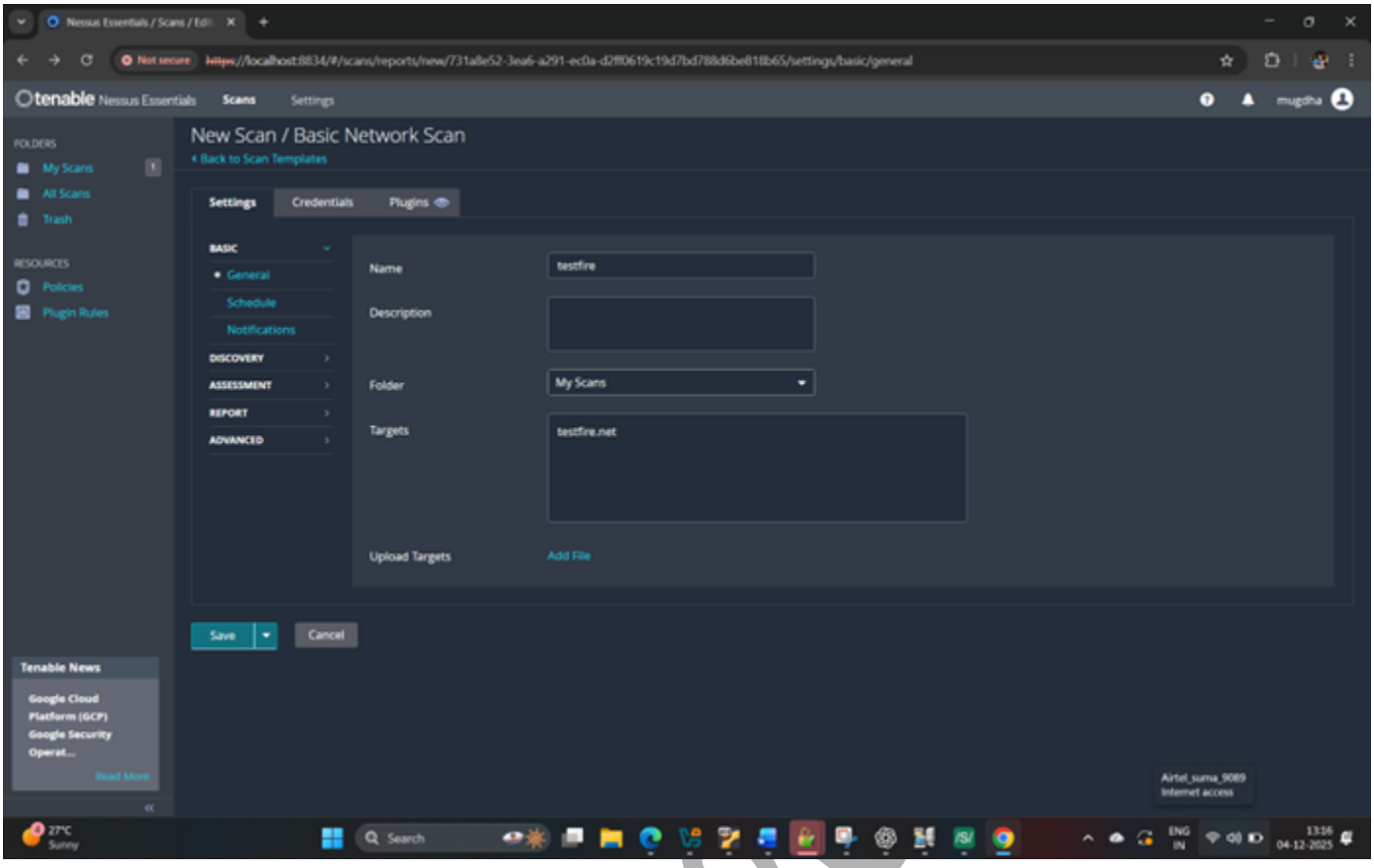
5 . Stepts :

1 . install tenable Nessus.

2 . click on new scan then multiple scanning options will appear here I selected basic network scanning .

3 . then this interface will appear give whatever name you want or here I set it as a testfire.

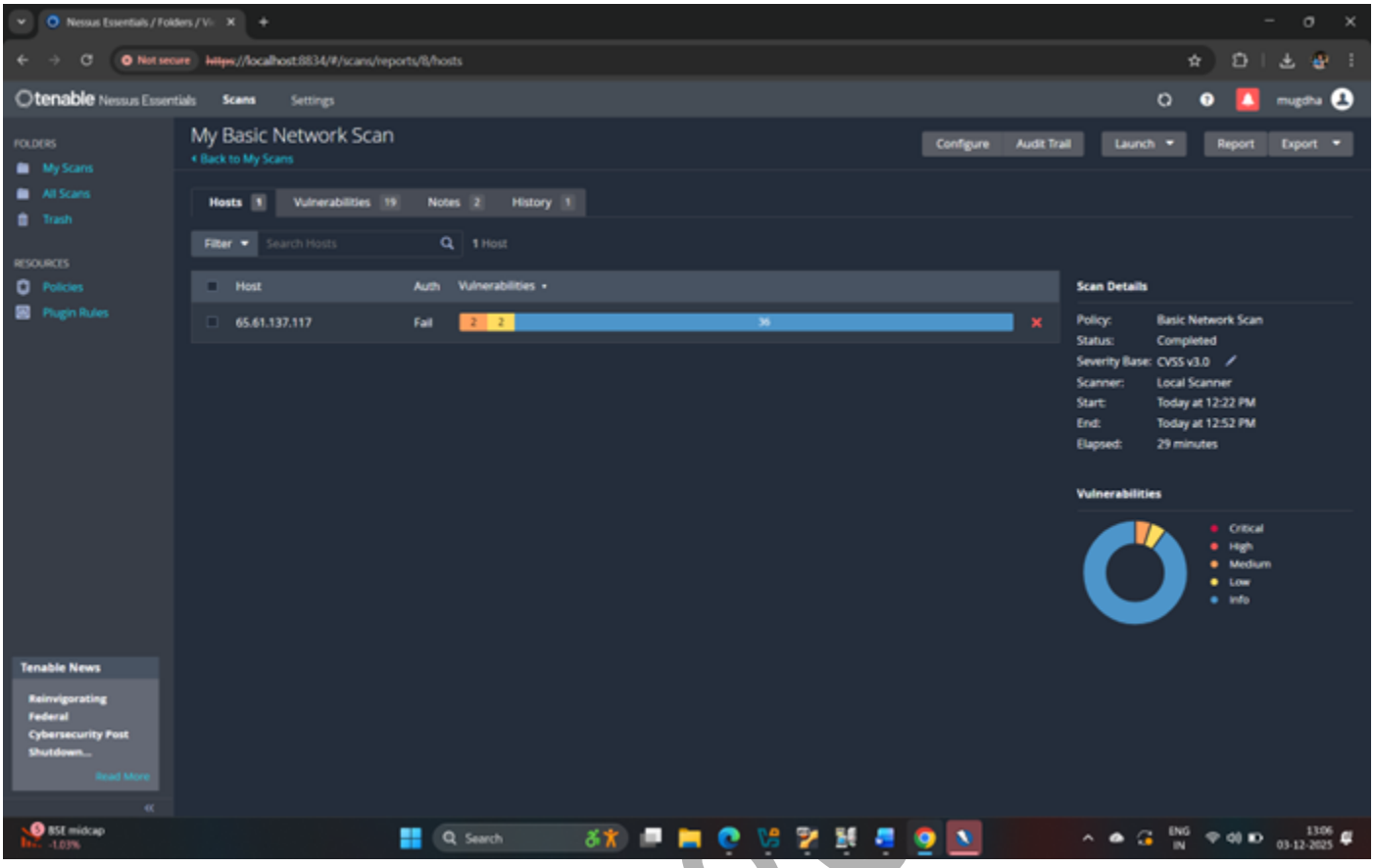
4 . Then in target name give domain name or its ip here I gave domain name as testfire.net



1.1

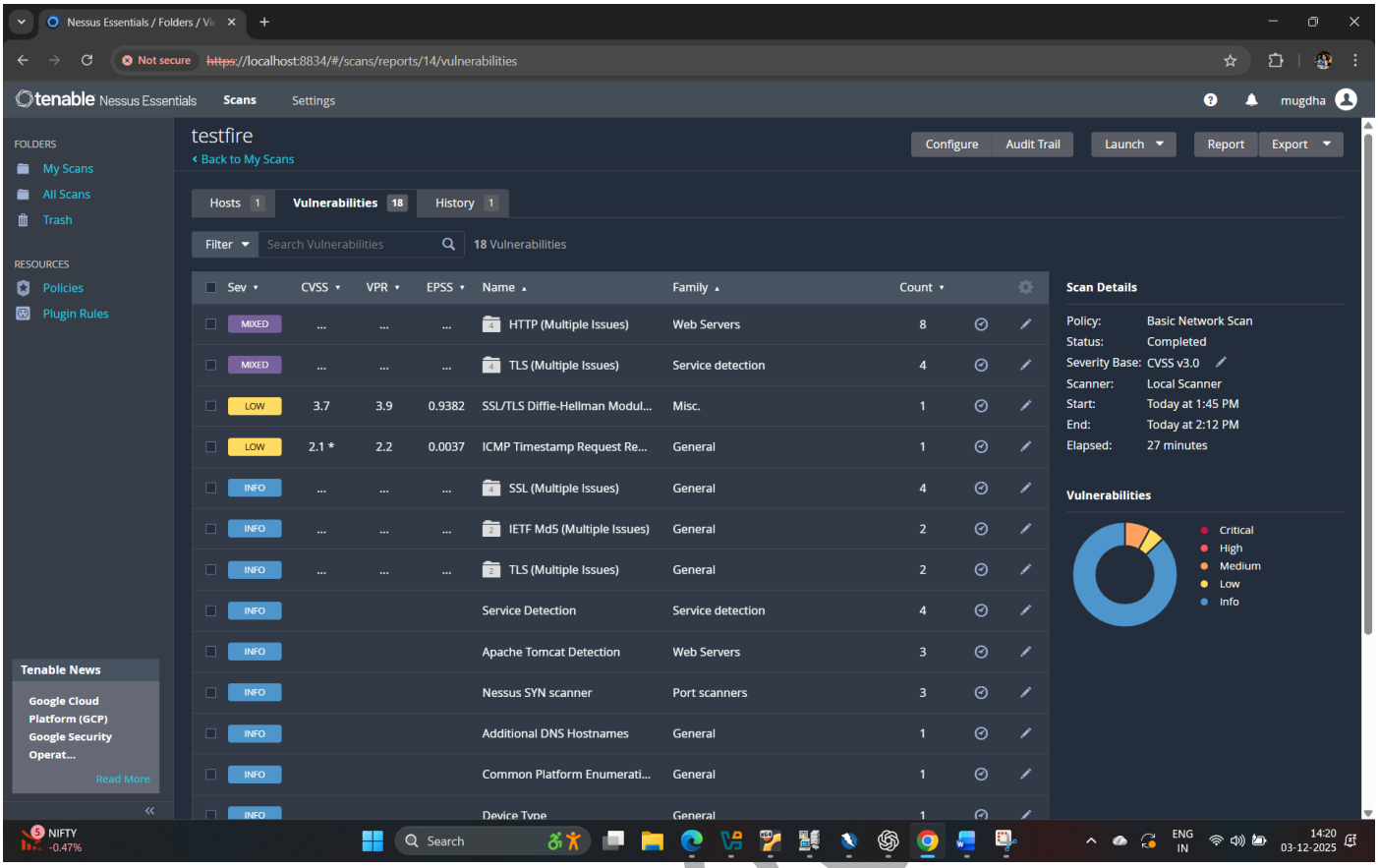
5 . Then launch the scan then scanning interface will appear as it will start scanning.

6 . Here we get the severity of vulnerability as critical high medium low info.

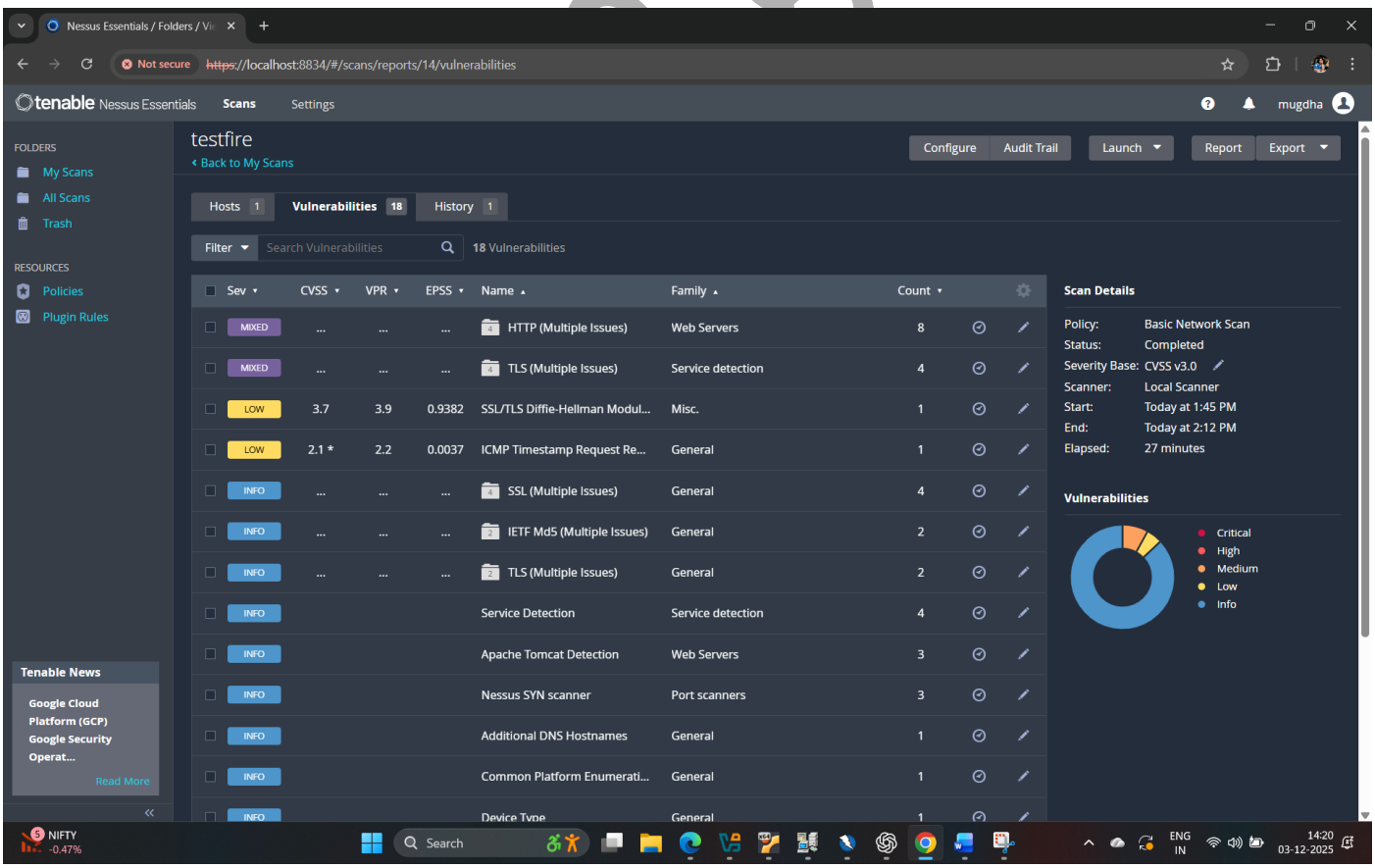


1.2

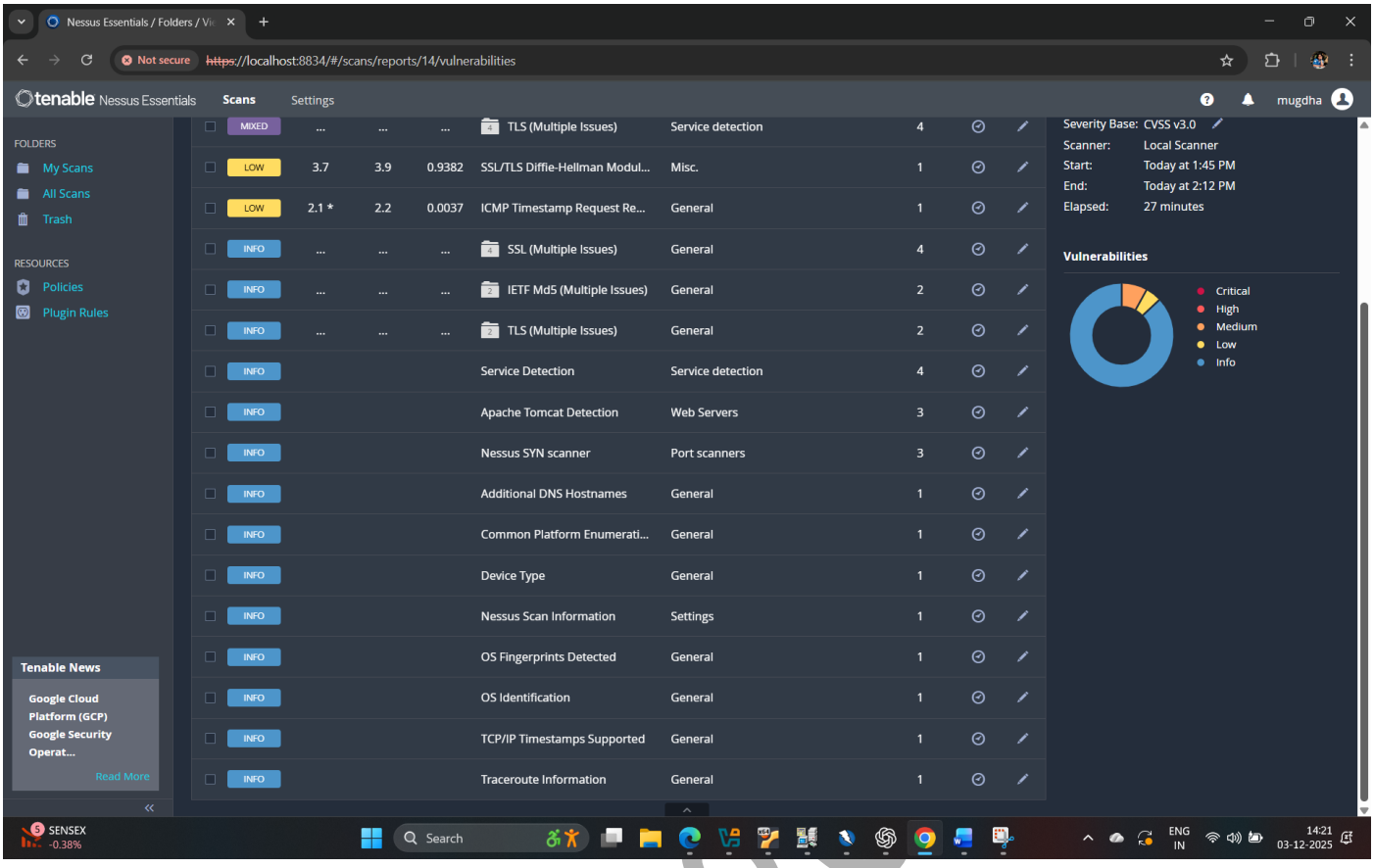
7 . Then click on the vulnerabilities it is showing 18 vulnerabilities as shown below .


Nessus Essentials / Folders / Vi
Not secure https://localhost:8834/#/scans/reports/14/vulnerabilities
tenable Nessus Essentials
Scans
Settings
mugdha
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
testfire
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 18
History 1
Filter
Search Vulnerabilities
18 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED HTTP (Multiple Issues) Web Servers 8
MIXED TLS (Multiple Issues) Service detection 4
LOW 3.7 3.9 0.9382 SSL/TLS Diffie-Hellman Modul... Misc. 1
LOW 2.1 * 2.2 0.0037 ICMP Timestamp Request Re... General 1
INFO SSL (Multiple Issues) General 4
INFO IETF Md5 (Multiple Issues) General 2
INFO TLS (Multiple Issues) General 2
INFO Service Detection Service detection 4
INFO Apache Tomcat Detection Web Servers 3
INFO Nessus SYN scanner Port scanners 3
INFO Additional DNS Hostnames General 1
INFO Common Platform Enumerati... General 1
INFO Device Type General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:45 PM
End: Today at 2:12 PM
Elapsed: 27 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Google Cloud Platform (GCP) Google Security Operat...
Read More
NIFTY -0.47%
Search
ENG IN
14:20 03-12-2025

1.3


Nessus Essentials / Folders / Vi
Not secure https://localhost:8834/#/scans/reports/14/vulnerabilities
tenable Nessus Essentials
Scans
Settings
mugdha
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
testfire
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 18
History 1
Filter
Search Vulnerabilities
18 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED HTTP (Multiple Issues) Web Servers 8
MIXED TLS (Multiple Issues) Service detection 4
LOW 3.7 3.9 0.9382 SSL/TLS Diffie-Hellman Modul... Misc. 1
LOW 2.1 * 2.2 0.0037 ICMP Timestamp Request Re... General 1
INFO SSL (Multiple Issues) General 4
INFO IETF Md5 (Multiple Issues) General 2
INFO TLS (Multiple Issues) General 2
INFO Service Detection Service detection 4
INFO Apache Tomcat Detection Web Servers 3
INFO Nessus SYN scanner Port scanners 3
INFO Additional DNS Hostnames General 1
INFO Common Platform Enumerati... General 1
INFO Device Type General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:45 PM
End: Today at 2:12 PM
Elapsed: 27 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Google Cloud Platform (GCP) Google Security Operat...
Read More
NIFTY -0.47%
Search
ENG IN
14:20 03-12-2025

1.4



1.5

8 . Then close the Nessus.

3 . Zaproxy :

1 . Web Application Vulnerability Scanning :

ZAP automatically scans websites to detect common security issues like SQL Injection, XSS, CSRF, broken authentication, insecure cookies, etc.

2 . Intercepting & Modifying HTTP/HTTPS Traffic:

Through the Proxy, you can capture, inspect, and modify requests/responses between your browser and the server for testing input validation and security controls.

3 . Spidering & Crawling Web Applications:

ZAP maps the entire website structure by crawling all pages, forms, links, and inputs—helping identify attack surfaces.

4 . Active Attacks & Fuzzing:

ZAP can send payloads to test how the server responds. This includes fuzzing parameters, hidden fields, and APIs for weaknesses.

5 . Steps :

1 . install zaproxy then the ineterfacxe will appear as shows in the screenshot

2 . then in the URL attack blank bar type https://www.certifiedhacker.com then click on attack.

3 . It will start searching for vulnerabilities.

4 . following is the step by step explanation of the screenshot

1. **“Automated Scan” Screen**

- **This is the Quick Start feature of ZAP.**
- **It allows you to run a simple automated vulnerability scan by just entering a URL.**
- **It is useful for beginners or quick assessments.**

---

2. “URL to attack” Field

- **You entered https://www.coffeechillaxer.com**
- **ZAP will scan this website for vulnerabilities.**
- **Only scan websites you own or have permission to test.**

3. “Use traditional spider” Option

- **Spider = A crawler that discovers all links/pages of the website.**
- **Traditional spider works for HTML-based websites.**

---

4. “Use AJAX spider” Option

- **AJAX Spider is used for dynamic and JavaScript-heavy websites.**
- **It simulates browser actions to find hidden pages.**
- **You selected Modern Browser → Firefox for scanning.**

---

5. “Attack” Button

- **This launches the Automated Scan:**
  - **First Spidering → Discover URLs**
  - **Then Active Scan → Look for vulnerabilities**

---

6. “Progress: Attack complete – see the Alerts tab...”

- **It means ZAP has finished scanning the website.**
- **All vulnerabilities found are shown under the ‘Alerts’ section below.**

---

7. “Alerts” Section (Bottom Left)

- **This section shows all vulnerabilities found.**
- **Colored icons represent severity:**
  - **High severity**
  - **Medium**
  - **Low**
  - **Informational**
- **Example alerts visible:**
  - **XSS**
  - **CSRF Tokens Missing**

- **Content Security Policy Missing**
- **Cookie Flags missing**

These are security issues discovered on the scanned website.

---

8. “History” Tab (Left Side)

- **Shows all requests ZAP made during the scan.**
- **Helps you manually inspect each HTTP request/response.**

---

9. “Request / Response” Panel (Center Bottom)

- **Displays the selected request and response from the history.**
- **Used by pentesters to review server behavior in detail.**

---

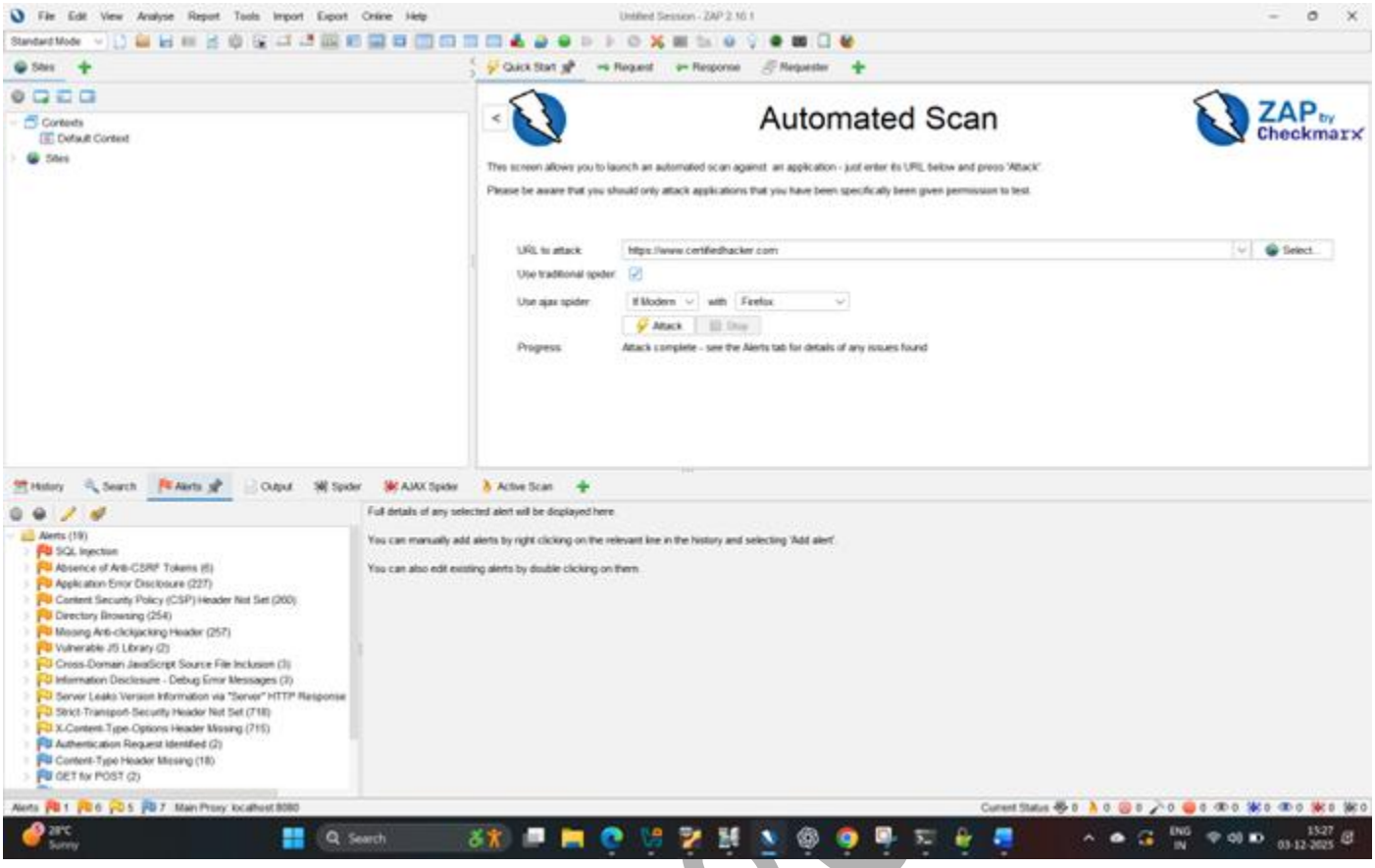
10. “Sites” Tree (Top Left)

- **Lists the website structure discovered during spidering.**
- **Shows all folders, pages, and parameters scanned.**

---

11. “Attack Complete”

- **Means scanning is successfully completed.**
- **Now analyze issues in the Alerts tab.**


Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
https://www.certifiedhacker.com
Select...
Use traditional spider:
Use ajax spider:
with
Firefox
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

4 . Microsoft Baseline Security Analyzer :

1. Checks for Missing Security Updates :

MBSA scans your Windows system and identifies missing Microsoft security patches, updates, and hotfixes to ensure the system is up-to-date.

2. Detects Common Security Misconfigurations :

It analyzes system settings like password policies, account settings, firewall status, and file shares to find weak or risky configurations.

3. Provides Detailed Vulnerability Reports :

MBSA generates a clear report highlighting vulnerabilities, what caused them, and recommended steps to fix each issue.

4. Helps Maintain Compliance :

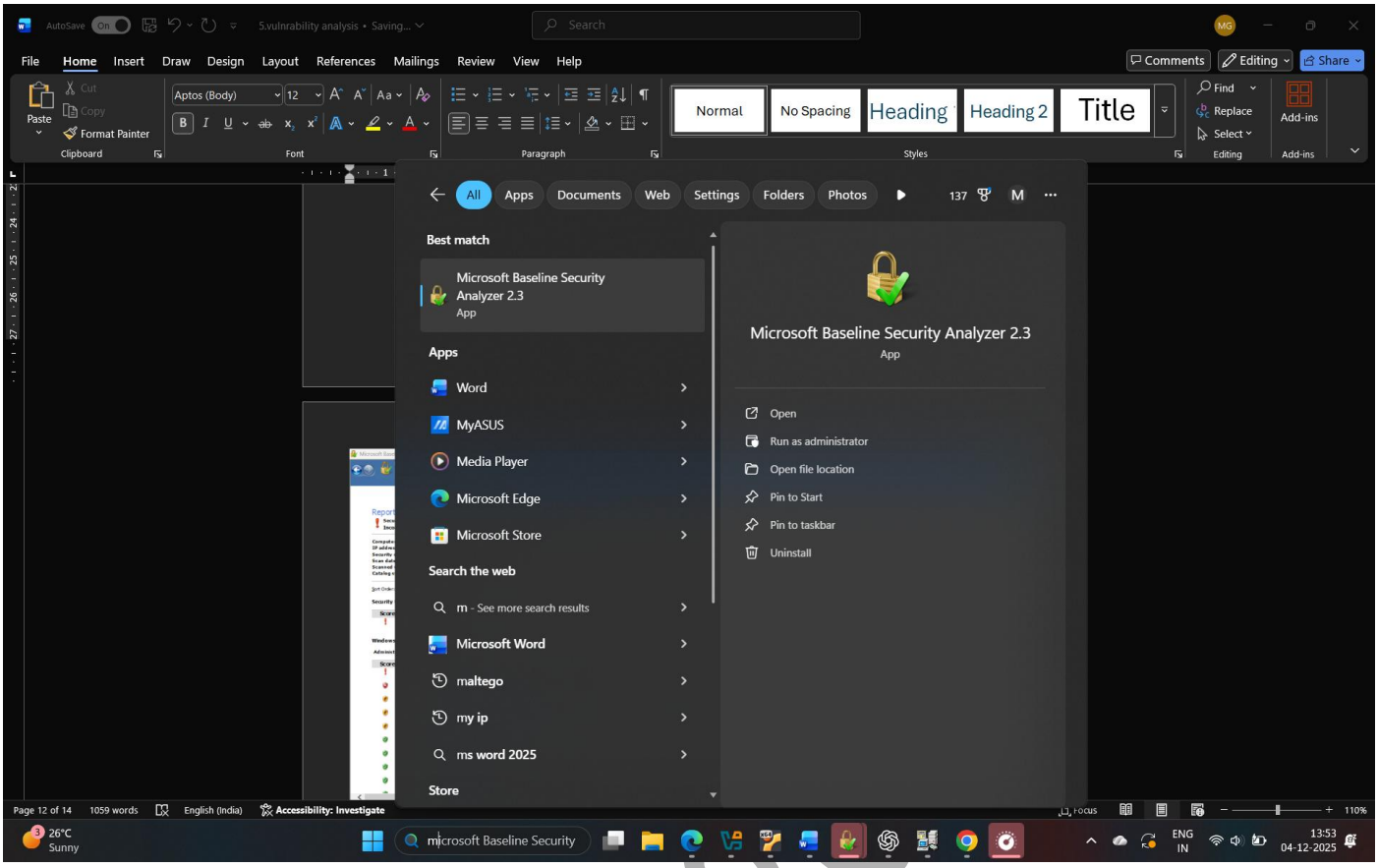
Organizations use MBSA to ensure their systems follow basic Microsoft security best practices, useful for audits and compliance checks.

5. Easy-to-Use Security Tool :

MBSA gives a simple graphical or command-line interface, making it easy even for beginners to check their system security without deep technical skills.

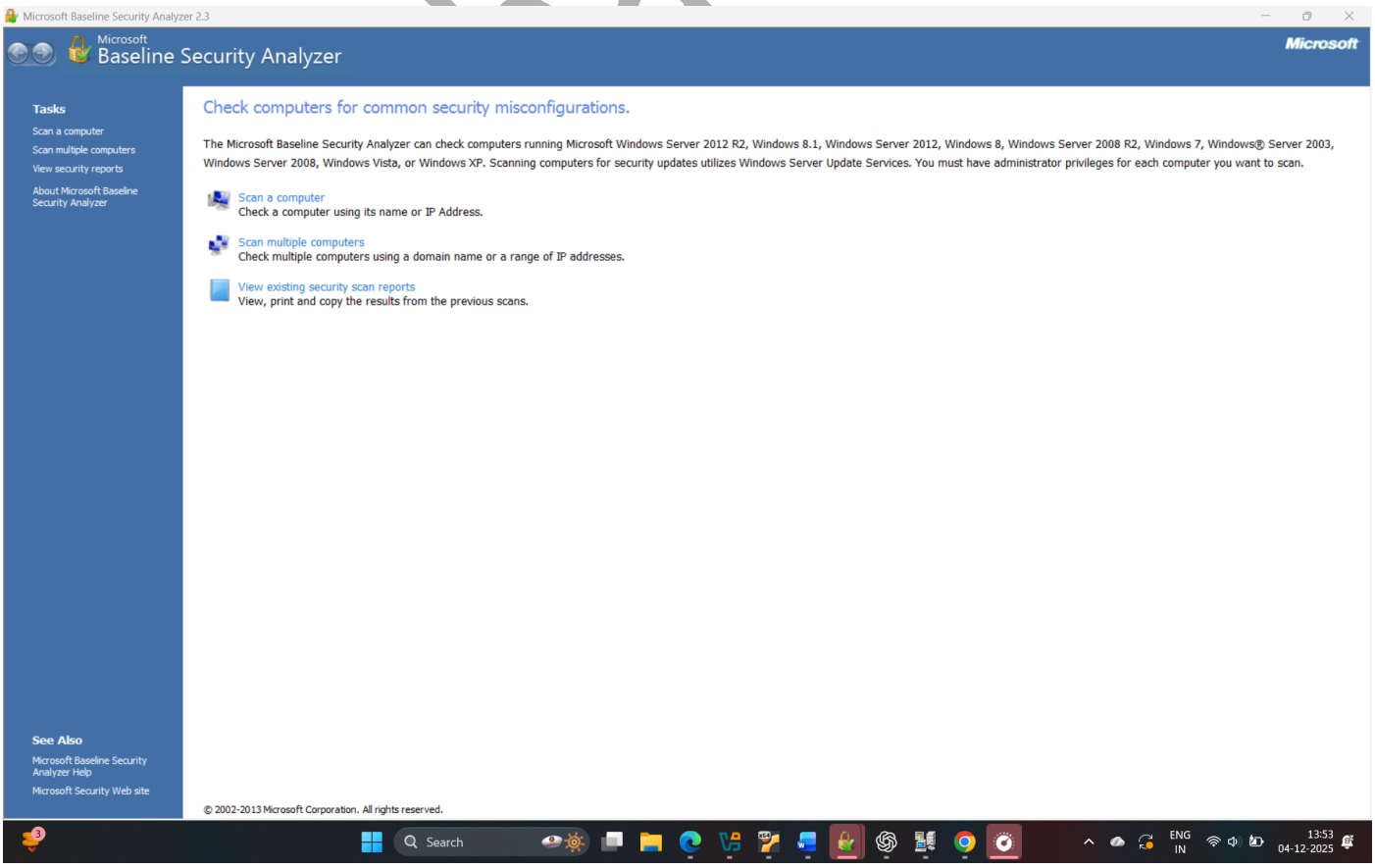
6 : Steps :

1 . click on Microsoft Baseline Security Analyzer.



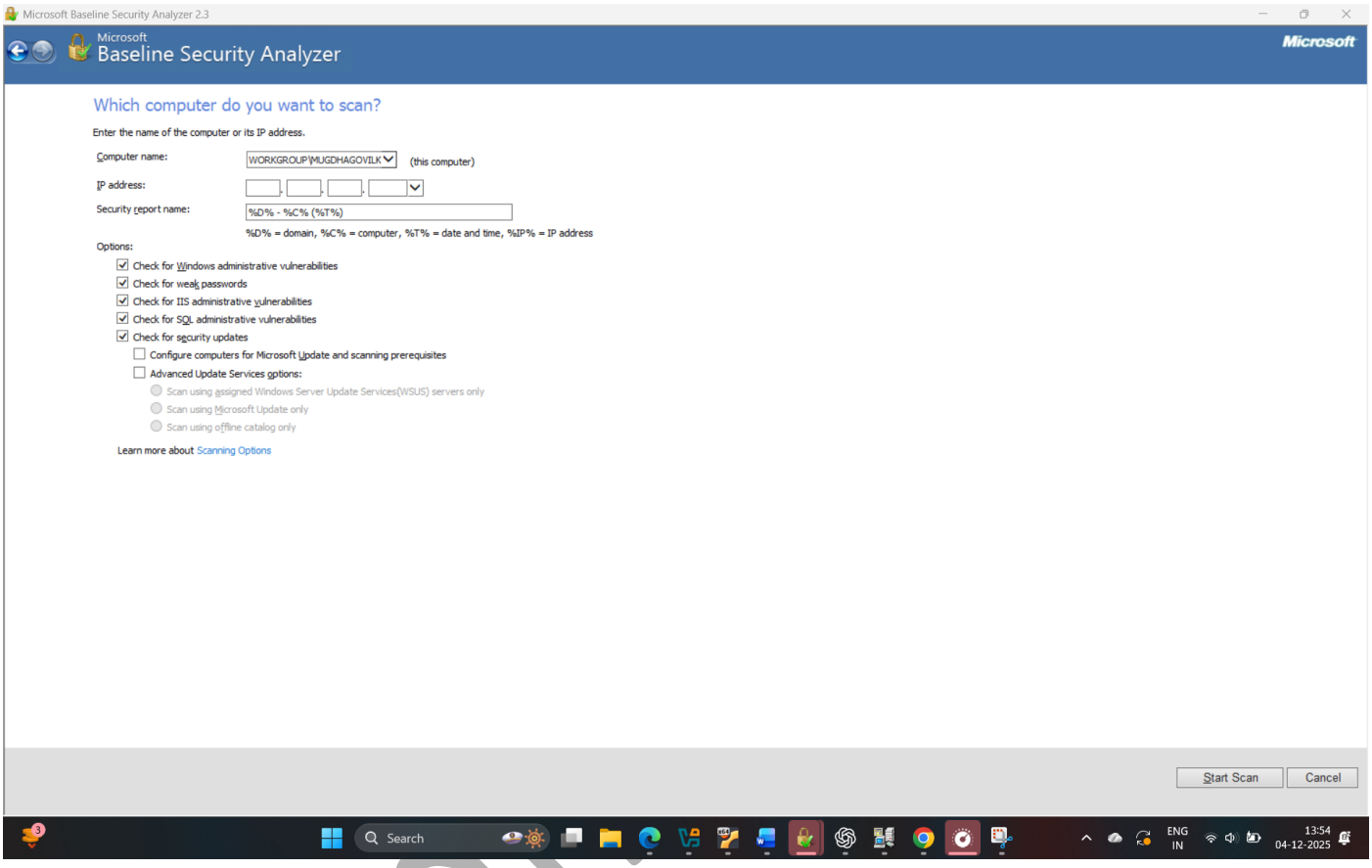
1.1

2 . the click on the scan a computer.



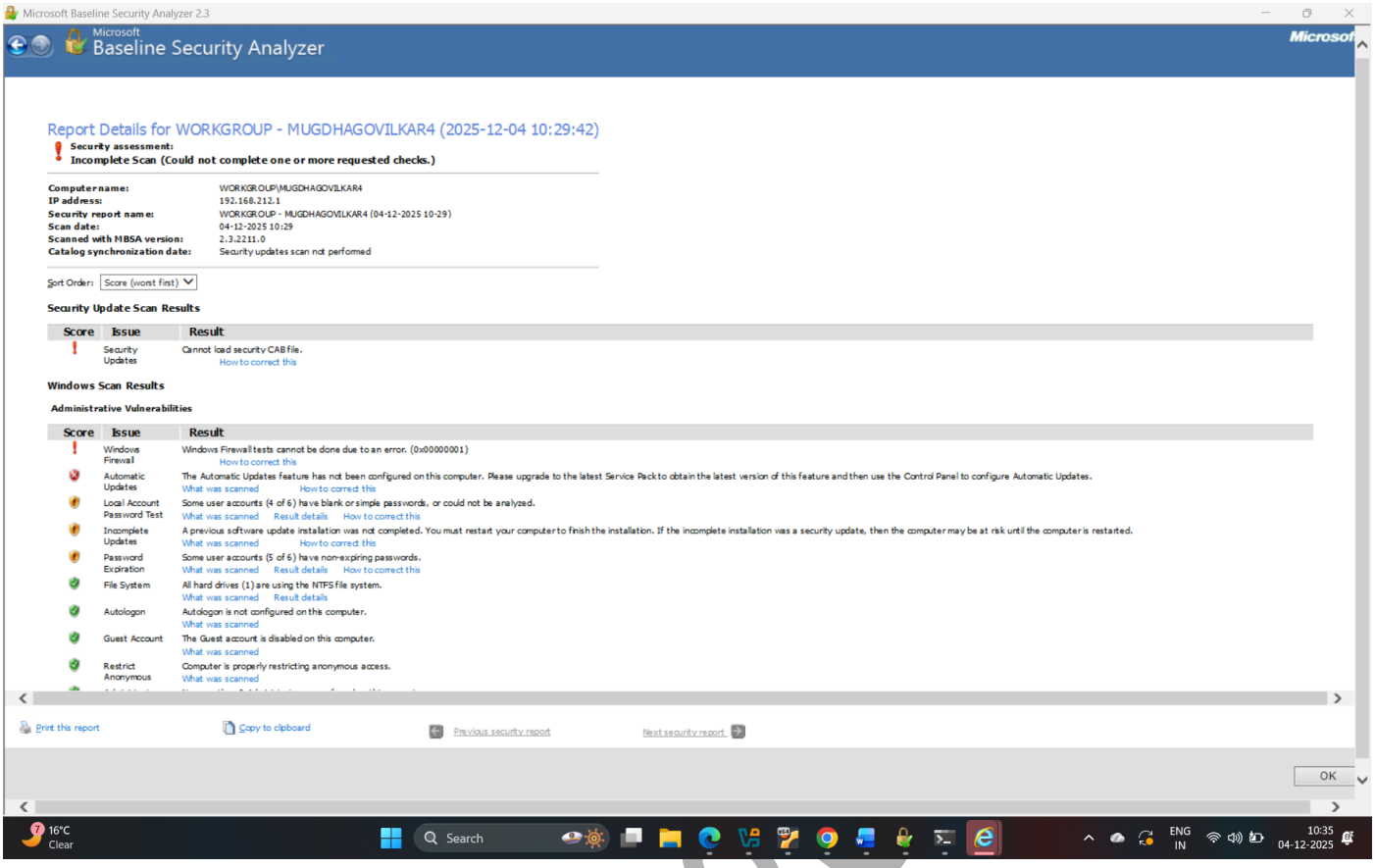
1.2

3 . then click on start scan.

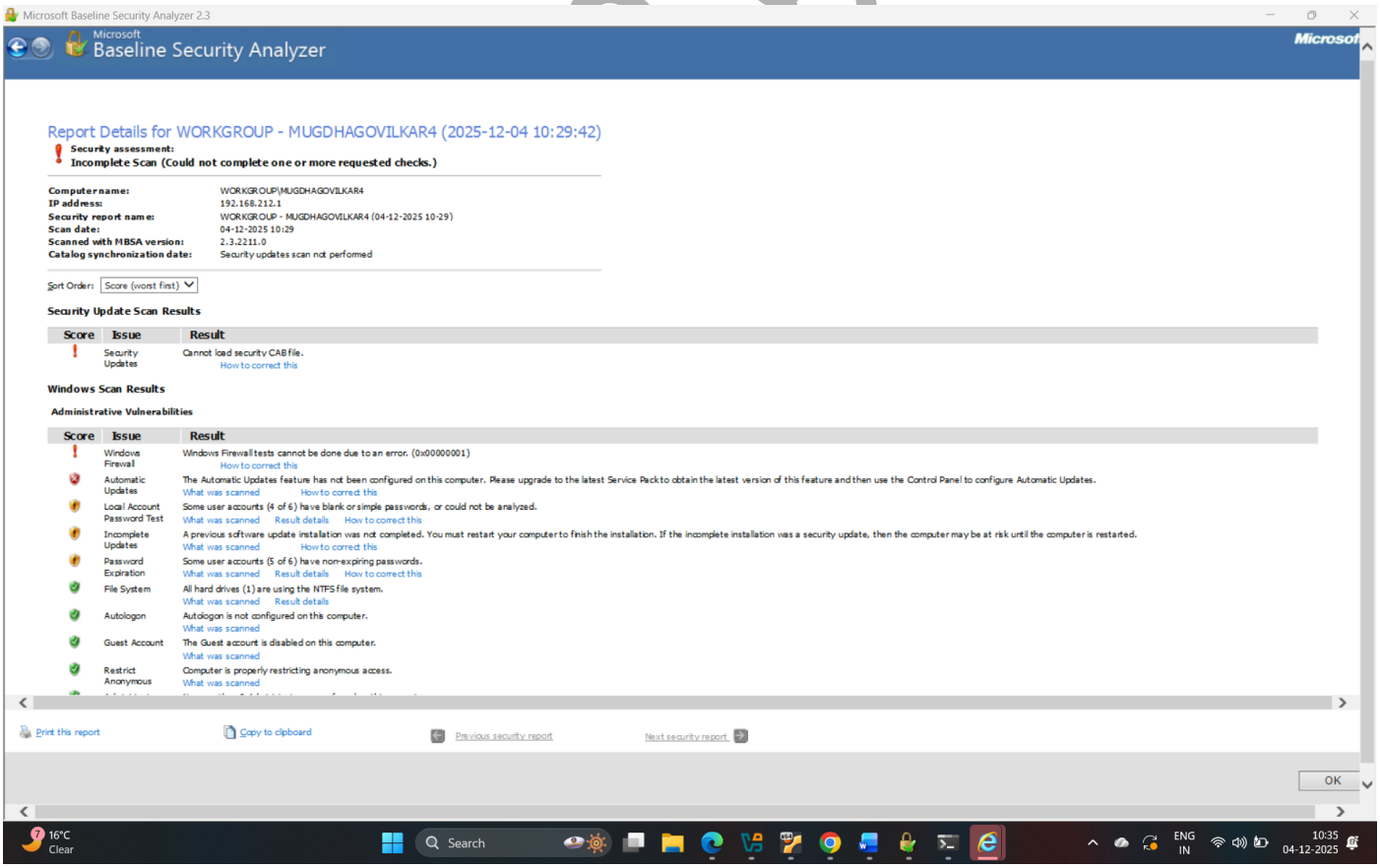


1.3

4 . then following scan will appear


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Report Details for WORKGROUP - MUGDHAGOVILKAR4 (2025-12-04 10:29:42)
Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)
Computer name: WORKGROUP\MUGDHAGOVILKAR4
IP address: 192.168.212.1
Security report name: WORKGROUP - MUGDHAGOVILKAR4 (04-12-2025 10-29)
Scan date: 04-12-2025 10:29
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed
Sort Order: Score (worst first)
Security Update Scan Results
Score Issue Result
Security Updates
Cannot load security CAB file.
How to correct this
Windows Scan Results
Administrative Vulnerabilities
Score Issue Result
Windows Firewall
Windows Firewall tests cannot be done due to an error. (0x00000001)
How to correct this
Automatic Updates
The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.
What was scanned
How to correct this
Local Account Password Test
Some user accounts (4 of 6) have blank or simple passwords, or could not be analyzed.
What was scanned
Result details
How to correct this
Incomplete Updates
A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted.
What was scanned
How to correct this
Password Expiration
Some user accounts (5 of 6) have non-expiring passwords.
What was scanned
Result details
How to correct this
File System
All hard drives (1) are using the NTFS file system.
What was scanned
Result details
Autologon
Autologon is not configured on this computer.
What was scanned
Guest Account
The Guest account is disabled on this computer.
What was scanned
Restrict Anonymous
Computer is properly restricting anonymous access.
What was scanned
Print this report
Copy to clipboard
Previous security report
Next security report
OK
16°C
Clear
Search
ENG
IN
10:35
04-12-2025

1.4


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Report Details for WORKGROUP - MUGDHAGOVILKAR4 (2025-12-04 10:29:42)
Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)
Computer name: WORKGROUP\MUGDHAGOVILKAR4
IP address: 192.168.212.1
Security report name: WORKGROUP - MUGDHAGOVILKAR4 (04-12-2025 10-29)
Scan date: 04-12-2025 10:29
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed
Sort Order: Score (worst first)
Security Update Scan Results
Score Issue Result
Security Updates
Cannot load security CAB file.
How to correct this
Windows Scan Results
Administrative Vulnerabilities
Score Issue Result
Windows Firewall
Windows Firewall tests cannot be done due to an error. (0x00000001)
How to correct this
Automatic Updates
The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.
What was scanned
How to correct this
Local Account Password Test
Some user accounts (4 of 6) have blank or simple passwords, or could not be analyzed.
What was scanned
Result details
How to correct this
Incomplete Updates
A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted.
What was scanned
How to correct this
Password Expiration
Some user accounts (5 of 6) have non-expiring passwords.
What was scanned
Result details
How to correct this
File System
All hard drives (1) are using the NTFS file system.
What was scanned
Result details
Autologon
Autologon is not configured on this computer.
What was scanned
Guest Account
The Guest account is disabled on this computer.
What was scanned
Restrict Anonymous
Computer is properly restricting anonymous access.
What was scanned
Print this report
Copy to clipboard
Previous security report
Next security report
OK
16°C
Clear
Search
ENG
IN
10:35
04-12-2025

1.5

5 . after getting the result close the tab.

5 . Nikto:

1 . Web Server Vulnerability Scanning :

Nikto scans web servers to find security vulnerabilities, such as outdated software versions, misconfigurations, or insecure files.

2 . Detection of Dangerous Files & Directories :

It identifies sensitive files, exposed directories, backup files, admin panels, and other items that should not be publicly visible.

3 . Checks for Outdated Server Components :

Nikto compares the web server against a large database to detect:

- **Old Apache/IIS/Nginx versions**
- **Deprecated modules**
- **Vulnerable plugins**

4 . Misconfiguration Identification :

Nikto alerts if the server has misconfigurations like:

- **Directory indexing enabled**
- **Improper HTTP methods allowed (PUT/DELETE)**
- **Missing security headers**

5 . Fast and Easy Recon Tool :

Nikto is simple to run and provides quick results, making it useful for:

- **Penetration testing**
- **Initial reconnaissance**
- **Bug bounty assessments**

6 . Steps :

1 . open kali terminal.

2 . then click on application in left upper corner then search nikto it is a inbuilt tool in kali linuz click on it

3 . run nikto -host <target domain name> here we take testfire.net as a target domain name.

4 . result will start appearing

5 . following is the meaning of the following screenshot :

1. Target Information

- **Target IP: 65.61.137.117**
- **Target Hostname: testfire.net**
- **Port: 80 (HTTP)**
  This tells you which website Nikto is scanning for vulnerabilities.

---

2. Server Details

- **Server: Apache-Coyote/1.1**
  This shows the web server software running on the target site.
  Identifying server type helps understand what vulnerabilities might exist.

---

3. Security Headers Missing

- **X-Frame-Options header not present**
  → Website may be vulnerable to clickjacking.
- **X-Content-Type-Options header not set**
  → Browser may misinterpret file types (possible MIME-type vulnerability).

These are web security best practices that are missing.

---

4. Scan Status Progress

- **Shows messages like:**
  - **“Completed 180 requests (3% complete, 49 hours left)”**

- **“Running average: 36.14891 sec per request”**
  Nikto sends many web requests.
  This part shows how much of the scan is done and estimated time remaining.

---

5. Errors During Scan

- **ERROR: Error limit reached – giving up**
- **getaddrinfo problems (Temporary failure in name resolution)**
  This means:
- **The website sometimes did not respond or**
- **DNS failed to resolve the hostname**
  So Nikto stopped the scan early because too many errors occurred.

---

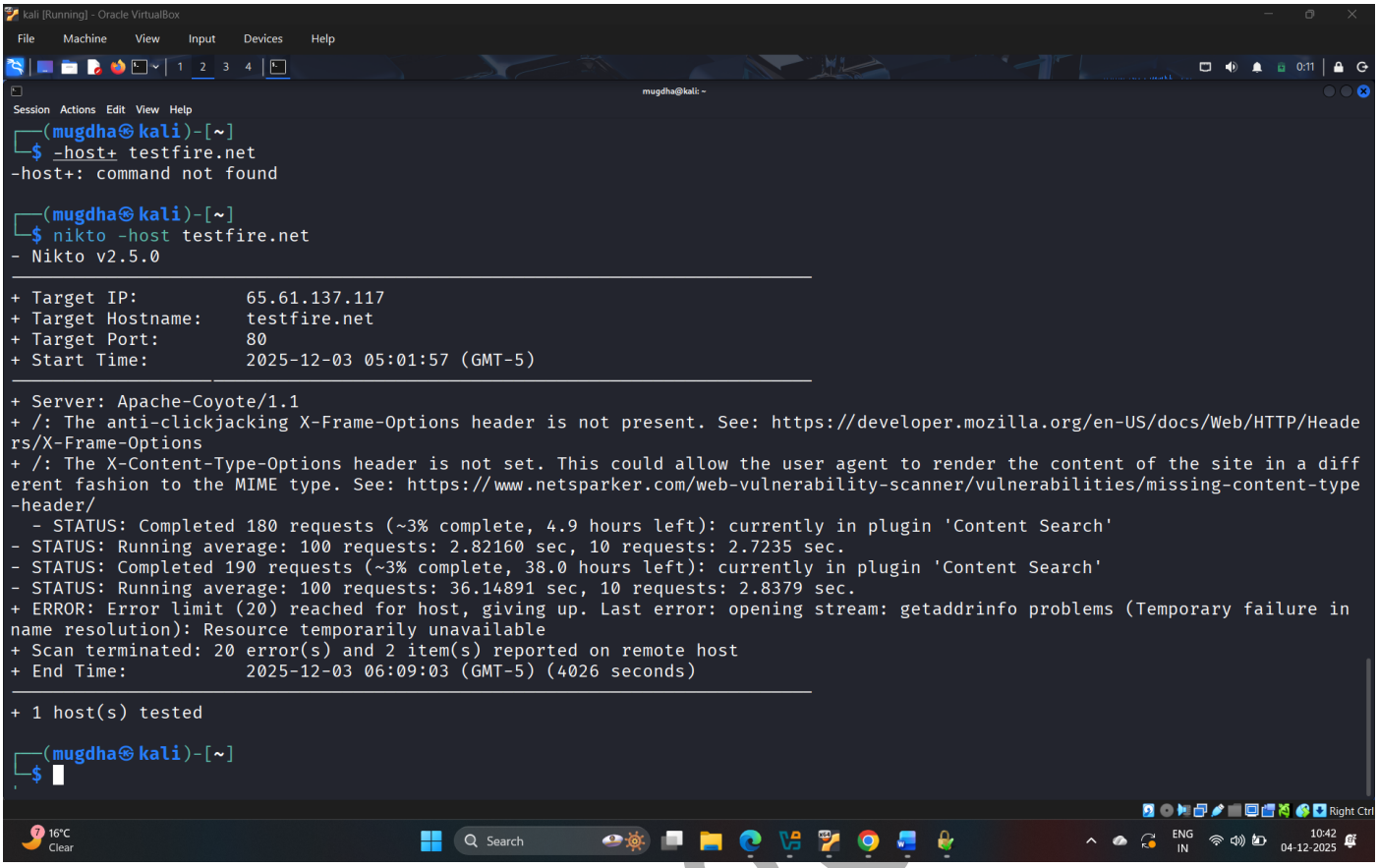
6. Scan Summary

- **Scan terminated**
- **20 error(s) and 2 item(s) reported on remote host**
  This means:
- **Nikto found 2 issues (vulnerabilities or misconfigurations)**
- **The rest were errors due to the server or network, not vulnerabilities.**

---

7. Final Result

- **1 host tested**
  Only testfire.net was scanned.


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mugdha@kali: ~
Session Actions Edit View Help
┌──(mugdha㉿kali)-[~]
└─$ -host+ testfire.net
-host+: command not found
┌──(mugdha㉿kali)-[~]
└─$ nikto -host testfire.net
- Nikto v2.5.0
+ Target IP: 65.61.137.117
+ Target Hostname: testfire.net
+ Target Port: 80
+ Start Time: 2025-12-03 05:01:57 (GMT-5)
+ Server: Apache-Coyote/1.1
+ /: 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/
- STATUS: Completed 180 requests (~3% complete, 4.9 hours left): currently in plugin 'Content Search'
- STATUS: Running average: 100 requests: 2.82160 sec, 10 requests: 2.7235 sec.
- STATUS: Completed 190 requests (~3% complete, 38.0 hours left): currently in plugin 'Content Search'
- STATUS: Running average: 100 requests: 36.14891 sec, 10 requests: 2.8379 sec.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time: 2025-12-03 06:09:03 (GMT-5) (4026 seconds)
+ 1 host(s) tested
┌──(mugdha㉿kali)-[~]
└─$
Right Ctrl
16°C Clear
Search
ENG IN
10:42 04-12-2025

6 . Vulnerability Analisys using nmap :

1. Port Scanning (Identify Open Ports) :

Nmap helps you discover which ports are open on a target system.
Open ports indicate possible entry points an attacker can use.

2. Service & Version Detection :

Nmap detects what services are running (HTTP, SSH, FTP, SMB, etc.) and their versions.
Knowing this helps identify outdated or vulnerable services.

3. OS Detection (Identify Operating System) :

Nmap can detect the target OS, including version and device type.
This information helps security testers find OS-specific vulnerabilities.

4. Vulnerability Detection Using NSE Scripts :

Nmap's Nmap Scripting Engine (NSE) has scripts that check for:

- **Weak configurations**
- **Known CVEs**
- **Misconfigurations**
- **Default credentials**
  This makes Nmap a lightweight vulnerability scanner.

5. Network Mapping & Attack Surface Discovery :

Nmap helps understand the network structure, live hosts, and exposed services.
This allows security analysts to measure the attack surface before deeper testing.

6 . Steps :

1 . open kali linux terminal.

2 . run sudo su for user privileges and then type passwork

3 . then run nmap -A -T4 -Pn certifiedhacker.com

4 . Result will start appearing as shown below

5 . Explanation of the Screenshot :

1. Command Used:

nmap -A -Pn certificedhacker.com

- **-A → Enables aggressive scan (OS detection, version detection, traceroute, scripts).**
- **-Pn → Treats host as *online* even if ping fails (skips host discovery).**

---

2. Host is Up

Nmap confirms the target 162.241.216.11 is reachable.
This means the server is responding to probes even though ping was disabled.

---

3. No Open Ports / Ports Ignored

The output shows:

Not shown: 1000 filtered ports

- **This means all 1000 common ports are filtered (likely blocked by firewall).**
- **No open services were detected.**

---

4. OS Detection Failed

Nmap message:

Too many fingerprints match this host to give specific OS details

- **This happens when the firewall blocks OS detection probes.**
- **Nmap cannot confidently determine the operating system.**

---

5. Traceroute Result

Traceroute using ICMP shows only:

1 30

- **It means the route to the target is blocked or hidden after the first hop.**
- **Firewall or ISP may be filtering ICMP packets.**

---

6. Final Result Summary

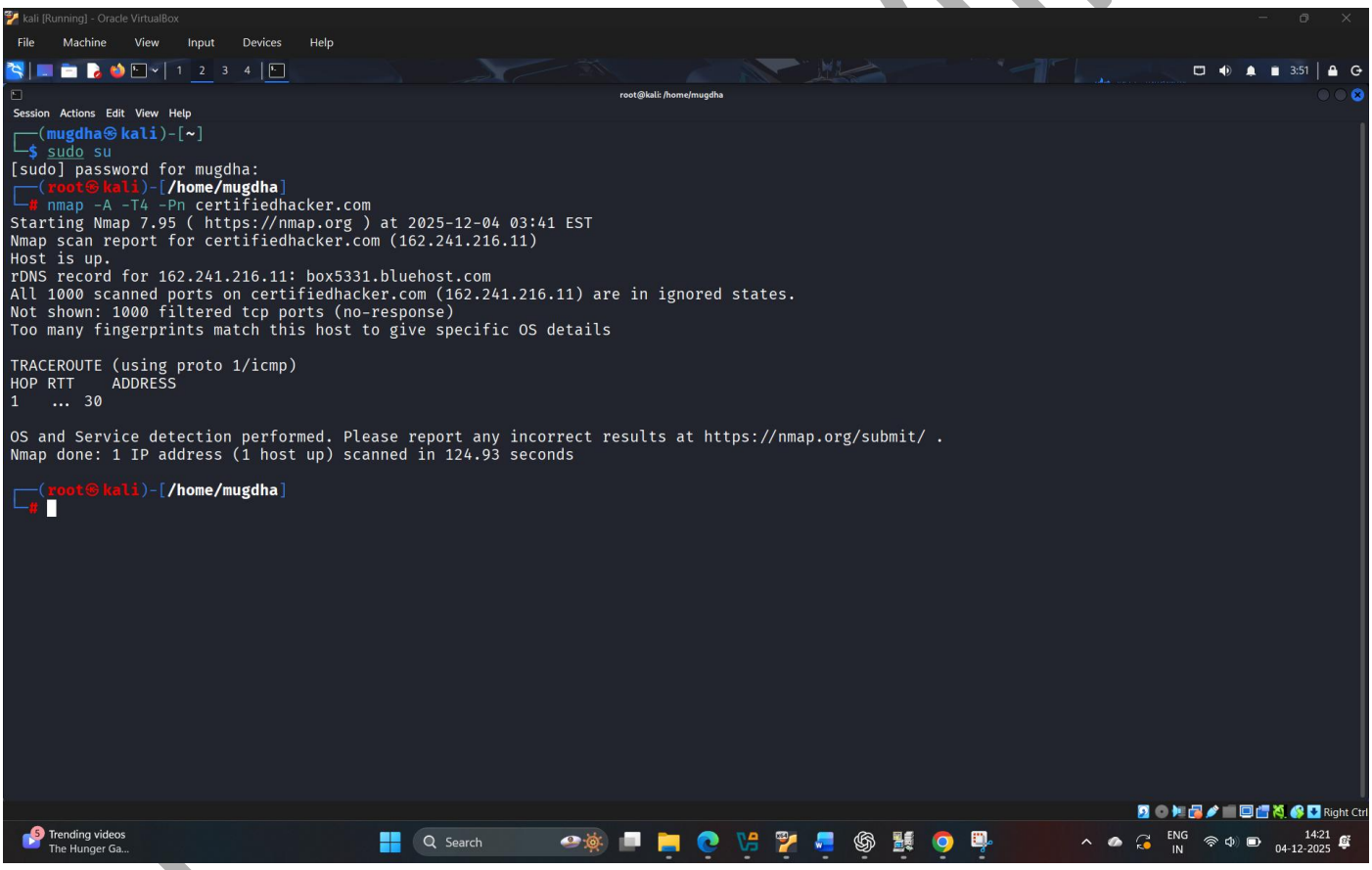
- **1 host scanned.**
- **No open ports found.**
- **OS detection unsuccessful.**
- **Host likely uses strong firewall and filtering rules.**

---

7. Scan Time

scanned in 124.93 seconds

- **Aggressive scan + firewall filtering makes the scan slow.**



7 . Global Network Inventory :

1 . Device Discovery :

Automatically finds all computers, servers, network devices, and peripherals connected to your network.

2 . Hardware Inventory :

Collects detailed information about hardware components such as CPU, RAM, storage, motherboard, printers, etc.

3 . Software Inventory :

Lists installed software on every system and helps identify outdated, unauthorized, or vulnerable applications.

4 . Network Management & Monitoring :

Helps administrators track devices, monitor system status, and maintain an organized view of the entire network.

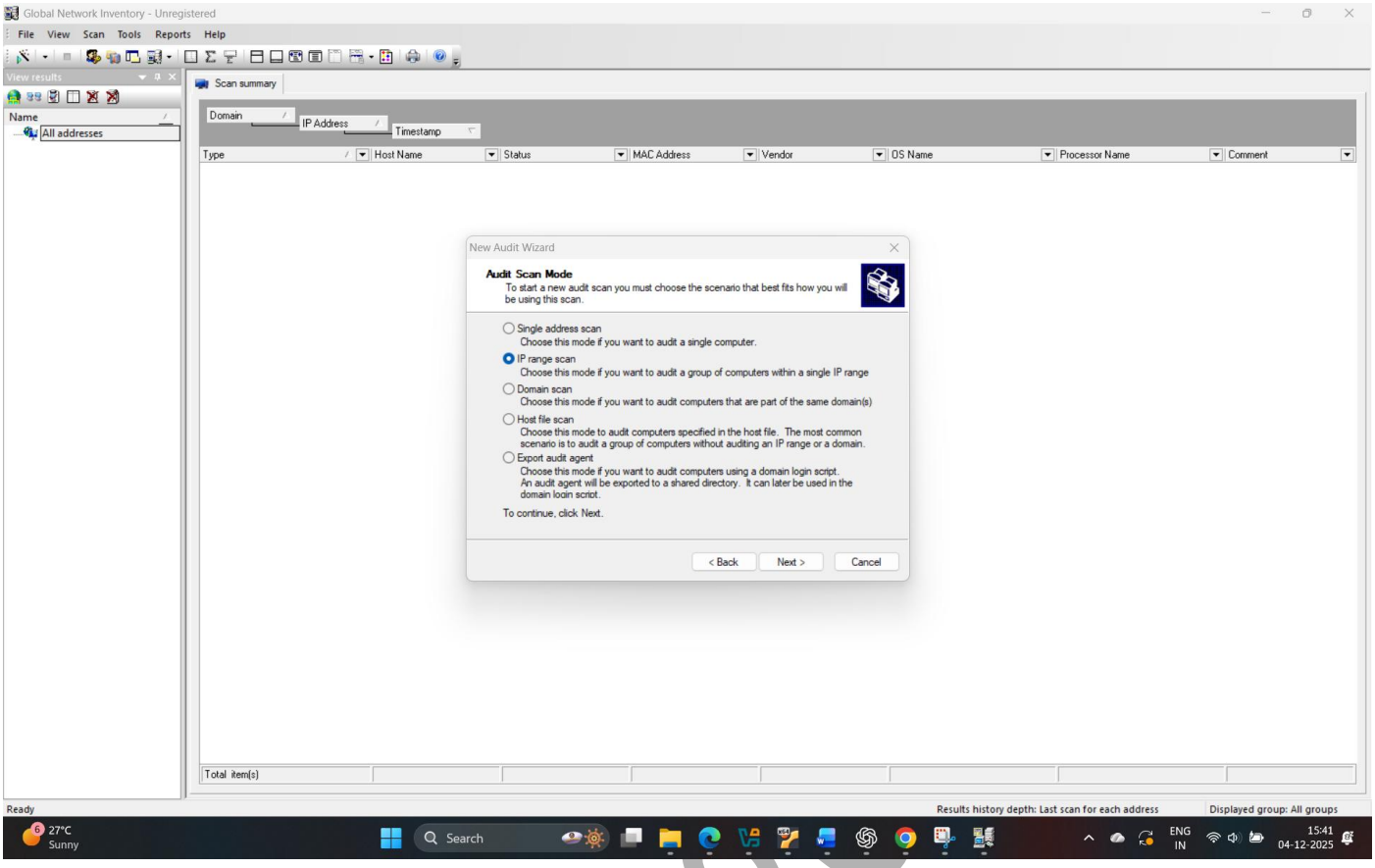
5 . Reporting & Compliance :

Generates detailed inventory reports for audits, compliance checks, asset management, and IT documentation.

6 . Steps :

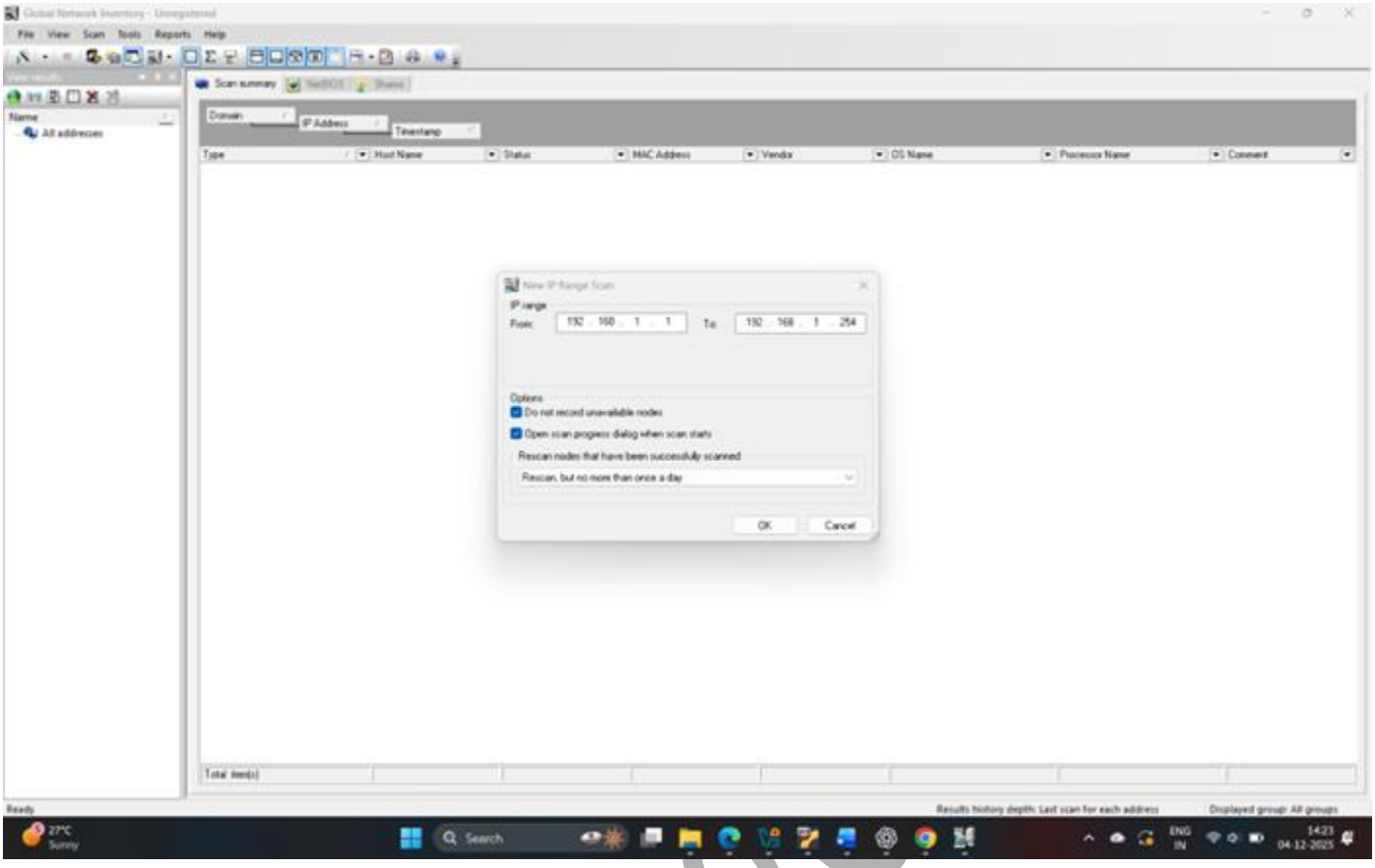
1 . install Global Network Inventory.

2 . run it then we will select ip scan



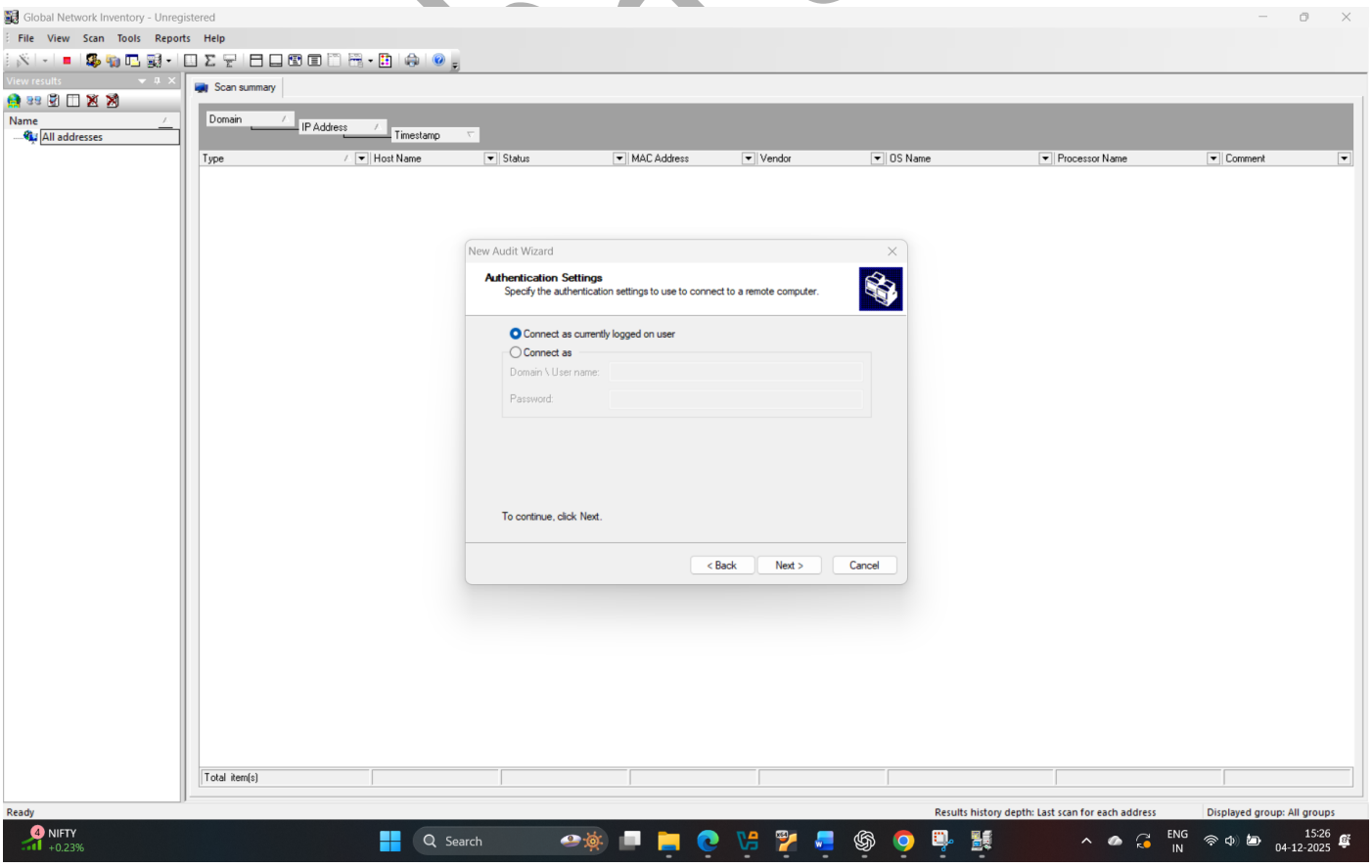
1.1

3 . Then set the range here we set the whole /24 range that is 192.168.1.1 to 192.168.1.254.



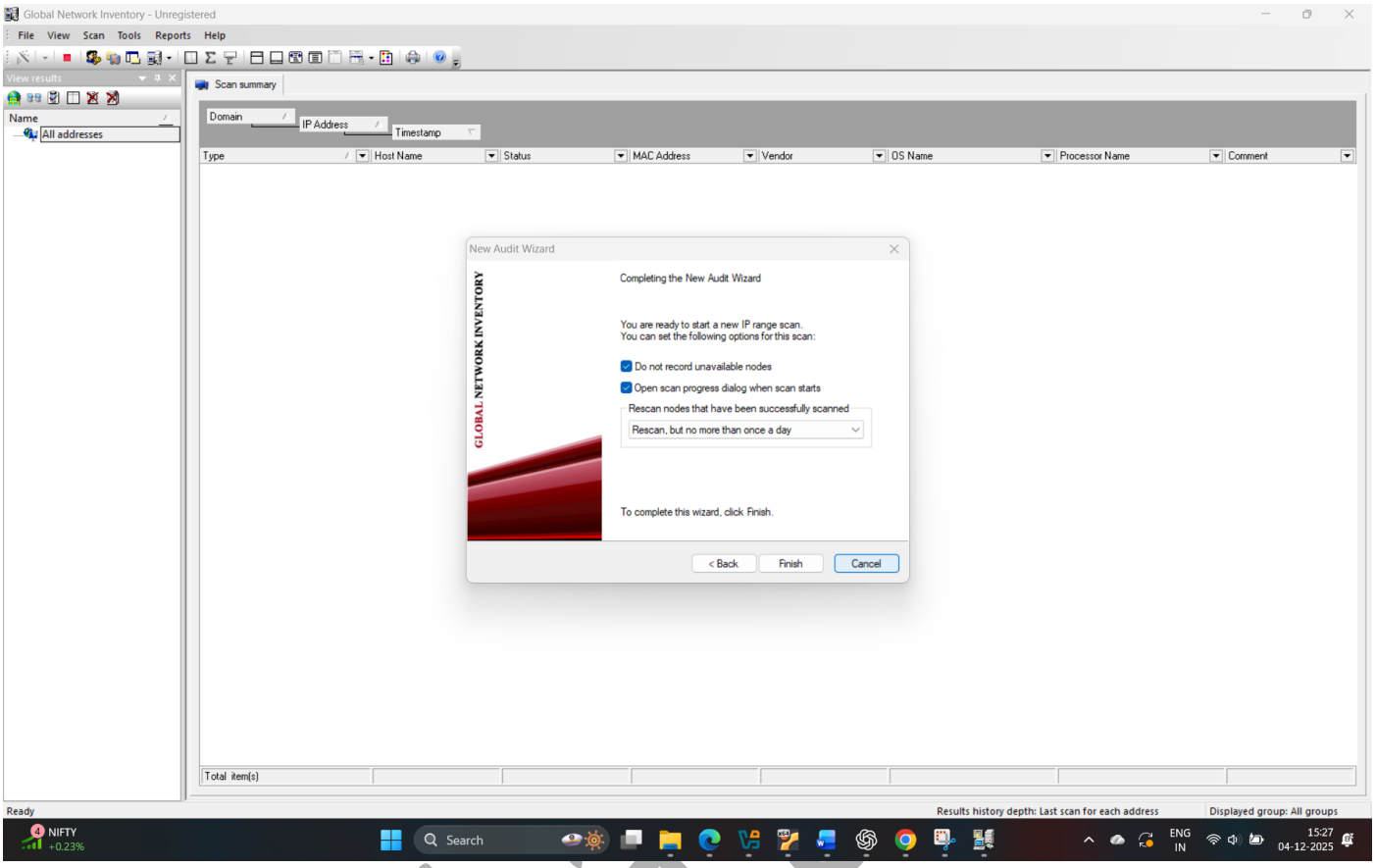
1.2

4 . Then select connect as currently logged on user.



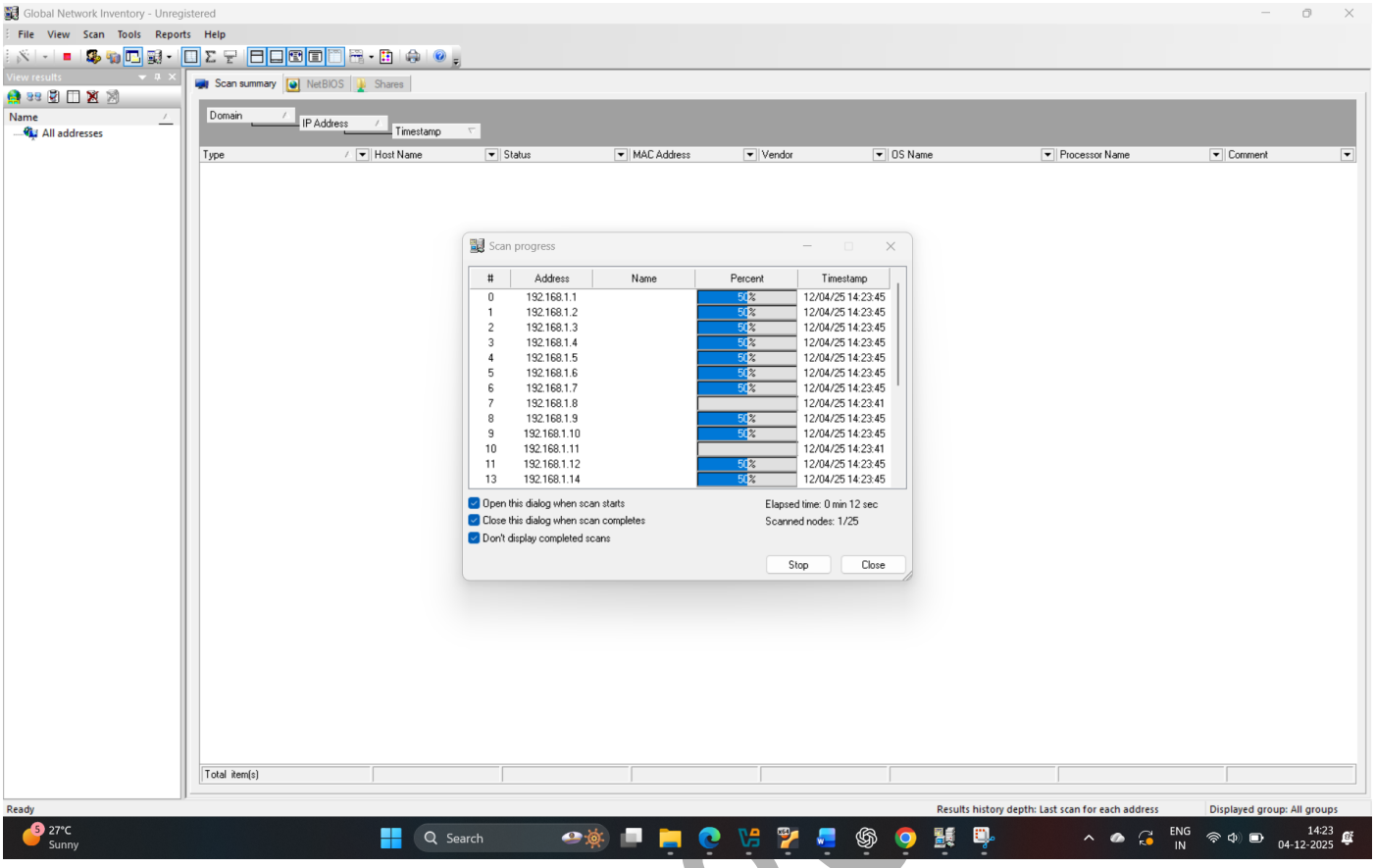
1.3

5 . Then click on the finish



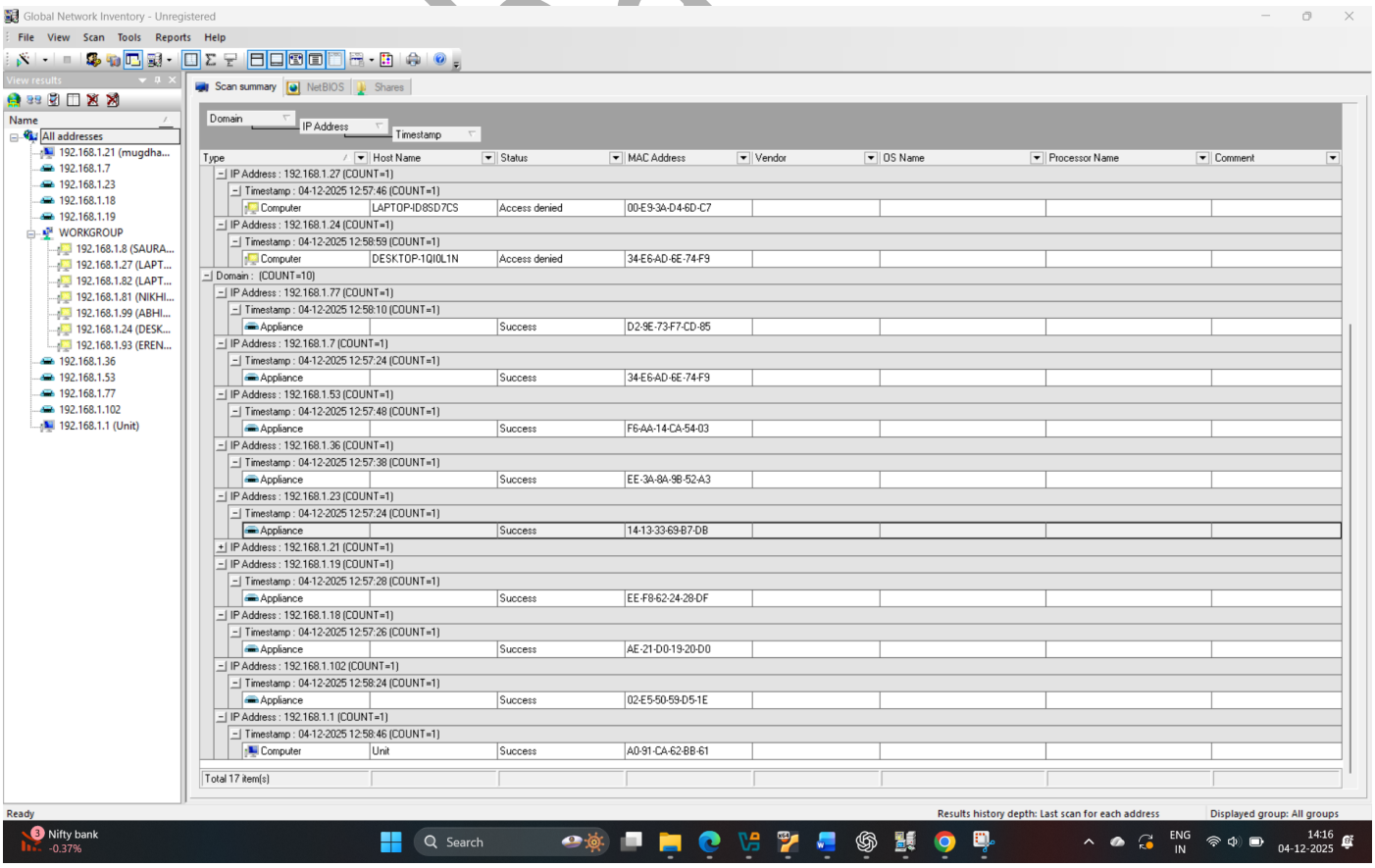
1.4

6 . It will start scanning.

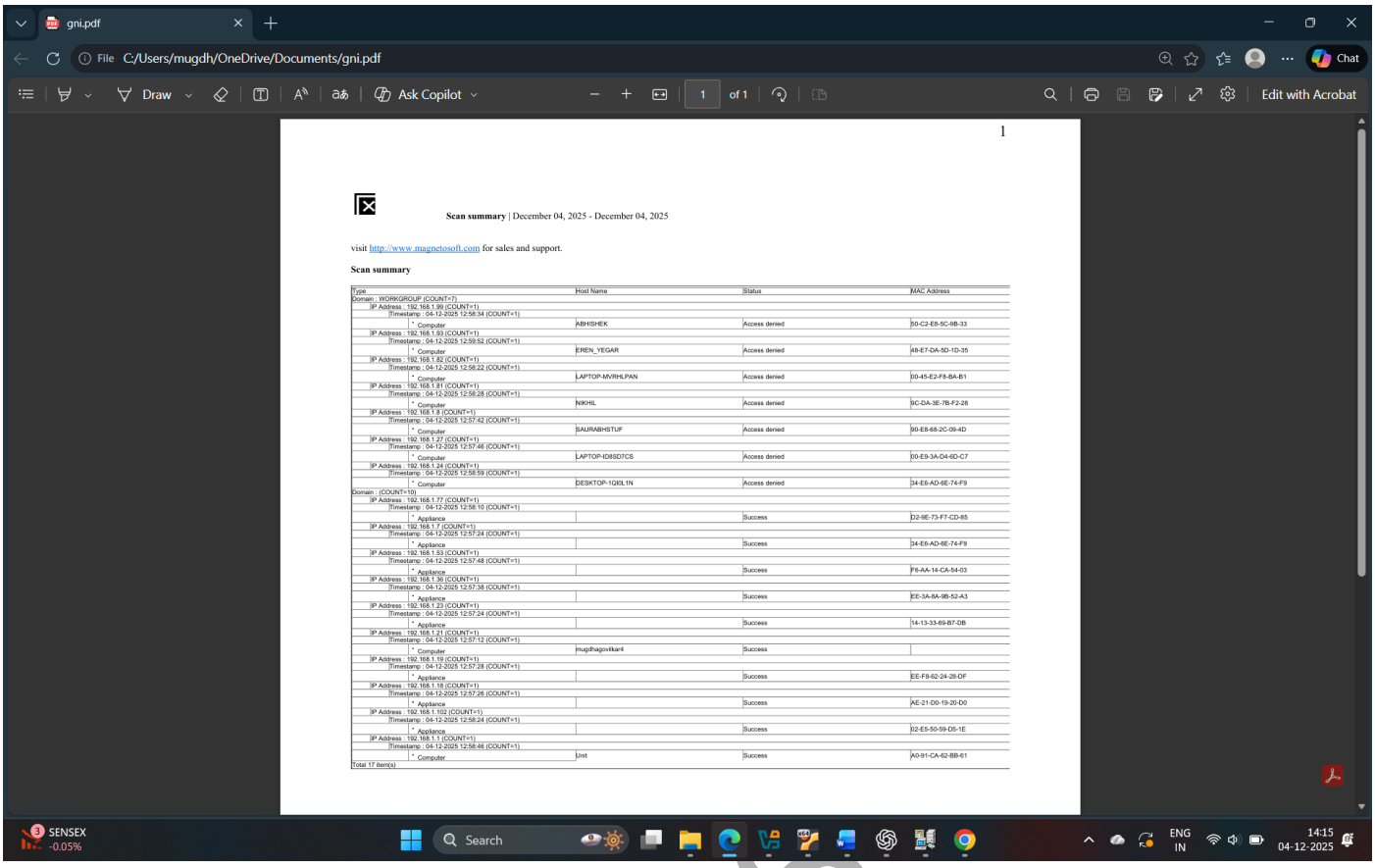


1.5

7 . This is the result .



1.6


gni.pdf
File C:/Users/mugdh/OneDrive/Documents/gni.pdf
Chat
Draw
Ask Copilot
1
of 1
Edit with Acrobat
1
Scan summary | December 04, 2025 - December 04, 2025
visit http://www.magnetosoft.com for sales and support.
Scan summary
Type | Host Name | Status | MAC Address
Domain : WORKGROUP (COUNT=7)
IP Address : 192.168.1.99 (COUNT=1)
Timestamp : 04-12-2025 12:58:34 (COUNT=1)
Computer | ABHISHEK | Access denied | 50-C2-E8-5C-9B-33
IP Address : 192.168.1.93 (COUNT=1)
Timestamp : 04-12-2025 12:59:52 (COUNT=1)
Computer | EREN_YEGAR | Access denied | 48-E7-DA-5D-1D-35
IP Address : 192.168.1.82 (COUNT=1)
Timestamp : 04-12-2025 12:58:22 (COUNT=1)
Computer | LAPTOP-MVRHLPAN | Access denied | 00-45-E2-F8-BA-B1
IP Address : 192.168.1.81 (COUNT=1)
Timestamp : 04-12-2025 12:58:28 (COUNT=1)
Computer | NIKHIL | Access denied | 9C-DA-3E-7B-F2-28
IP Address : 192.168.1.8 (COUNT=1)
Timestamp : 04-12-2025 12:57:42 (COUNT=1)
Computer | SAURABHSTUF | Access denied | 90-E8-68-2C-09-4D
IP Address : 192.168.1.27 (COUNT=1)
Timestamp : 04-12-2025 12:57:46 (COUNT=1)
Computer | LAPTOP-ID8SD7CS | Access denied | 00-E9-3A-D4-6D-C7
IP Address : 192.168.1.24 (COUNT=1)
Timestamp : 04-12-2025 12:58:59 (COUNT=1)
Computer | DESKTOP-1QI0L1N | Access denied | 34-E6-AD-6E-74-F9
Domain : (COUNT=10)
IP Address : 192.168.1.77 (COUNT=1)
Timestamp : 04-12-2025 12:58:10 (COUNT=1)
Appliance | | Success | D2-9E-73-F7-CD-85
IP Address : 192.168.1.7 (COUNT=1)
Timestamp : 04-12-2025 12:57:24 (COUNT=1)
Appliance | | Success | 34-E6-AD-6E-74-F9
IP Address : 192.168.1.53 (COUNT=1)
Timestamp : 04-12-2025 12:57:48 (COUNT=1)
Appliance | | Success | F6-AA-14-CA-54-03
IP Address : 192.168.1.36 (COUNT=1)
Timestamp : 04-12-2025 12:57:38 (COUNT=1)
Appliance | | Success | EE-3A-8A-9B-52-A3
IP Address : 192.168.1.23 (COUNT=1)
Timestamp : 04-12-2025 12:57:24 (COUNT=1)
Appliance | | Success | 14-13-33-69-B7-DB
IP Address : 192.168.1.21 (COUNT=1)
Timestamp : 04-12-2025 12:57:12 (COUNT=1)
Computer | mugdhagovilkar4 | Success |
IP Address : 192.168.1.19 (COUNT=1)
Timestamp : 04-12-2025 12:57:28 (COUNT=1)
Appliance | | Success | EE-F8-62-24-28-DF
IP Address : 192.168.1.18 (COUNT=1)
Timestamp : 04-12-2025 12:57:26 (COUNT=1)
Appliance | | Success | AE-21-D0-19-20-D0
IP Address : 192.168.1.102 (COUNT=1)
Timestamp : 04-12-2025 12:58:24 (COUNT=1)
Appliance | | Success | 02-E5-50-59-D5-1E
IP Address : 192.168.1.1 (COUNT=1)
Timestamp : 04-12-2025 12:58:46 (COUNT=1)
Computer | Unit | Success | A0-91-CA-62-BB-61
Total 17 item(s)
SENSEX -0.05%
Search
ENG IN
14:15 04-12-2025

1.7