

Module 5 : Vulnerability Scanning

Definition :

Vulnerability assessment is an examination of the ability of a system or application including current security procedures and controls to withstand and assault vulnerability research is the process of discovering vulnerability and design flaws that leave on OS and its application open to attack or misuse .

Vulnerability scanning in cybersecurity is the process of using automated tools to identify and assess security weaknesses (vulnerabilities) in systems, networks, and applications, allowing organizations to proactively address potential threats before attackers exploit them.

- **What it is:**

Vulnerability scanning involves using software tools to systematically scan IT assets for known weaknesses, including missing security updates, misconfigurations, and exposed secrets.

- **Why it's important:**

- **Proactive Security:** It helps organizations identify and fix vulnerabilities before they are exploited by attackers.
- **Risk Reduction:** By addressing vulnerabilities, organizations can significantly reduce their risk of cyberattacks and data breaches.
- **Compliance:** Many industry regulations and security standards require organizations to conduct regular vulnerability assessments.
- **Data Protection:** Vulnerability scanning demonstrates a commitment to data protection and builds confidence in stakeholders.

- **How it works:** • Vulnerability scanners use a database of known vulnerabilities and security flaws to test systems and networks.
- Scanners can be automated, allowing for regular and efficient scanning of IT assets.

- The results of the scans are used to identify and prioritize vulnerabilities for remediation.
- **Types of vulnerabilities:**
- **Software vulnerabilities:** Bugs, flaws, and weaknesses in software applications.
- **Network vulnerabilities:** Weaknesses in network configurations, protocols, and devices.
- **System vulnerabilities:** Flaws in operating systems, hardware, and other system components.
- **Web application vulnerabilities:** Weaknesses in web applications, such as injection flaws, cross-site scripting (XSS), and insecure configurations.
- **Benefits of vulnerability scanning:**
- **Improved security posture:** By identifying and addressing vulnerabilities, organizations can strengthen their overall security posture.
- **Reduced risk of cyberattacks:** Proactive vulnerability management
- **Compliance with regulations:** Regular vulnerability scanning can help organizations meet compliance requirements.
- **Faster incident response:** Having a clear understanding of vulnerabilities can help organizations respond more quickly to security incidents.
- **Vulnerability Management Lifecycle:**

Vulnerability scanning is the first stage of the broader vulnerability management lifecycle, which also includes vulnerability assessment, remediation, and ongoing monitoring.

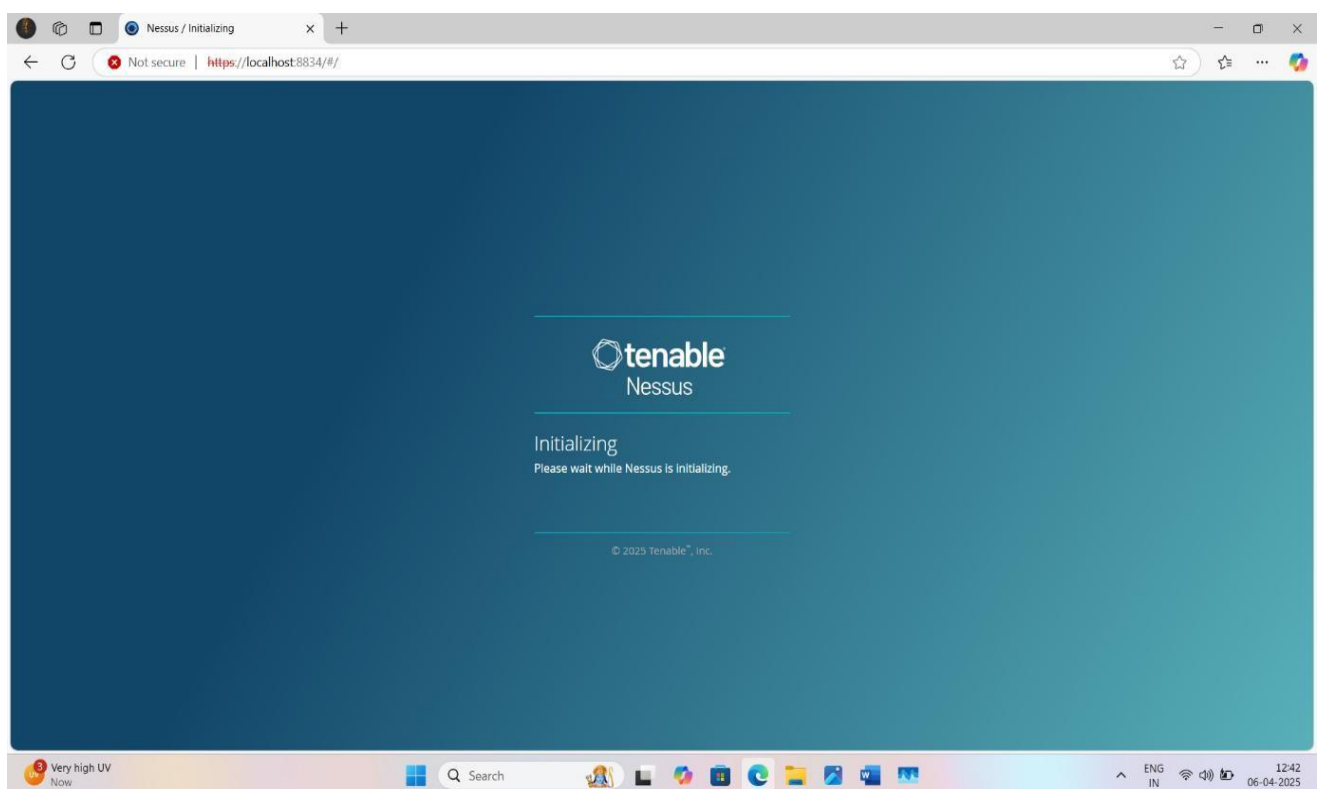
- Here are some tools and their information for do vulnerability scanning .

○ Nessus essential :

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

• USE :

Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner. Limitations: Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance.



• Benefits :

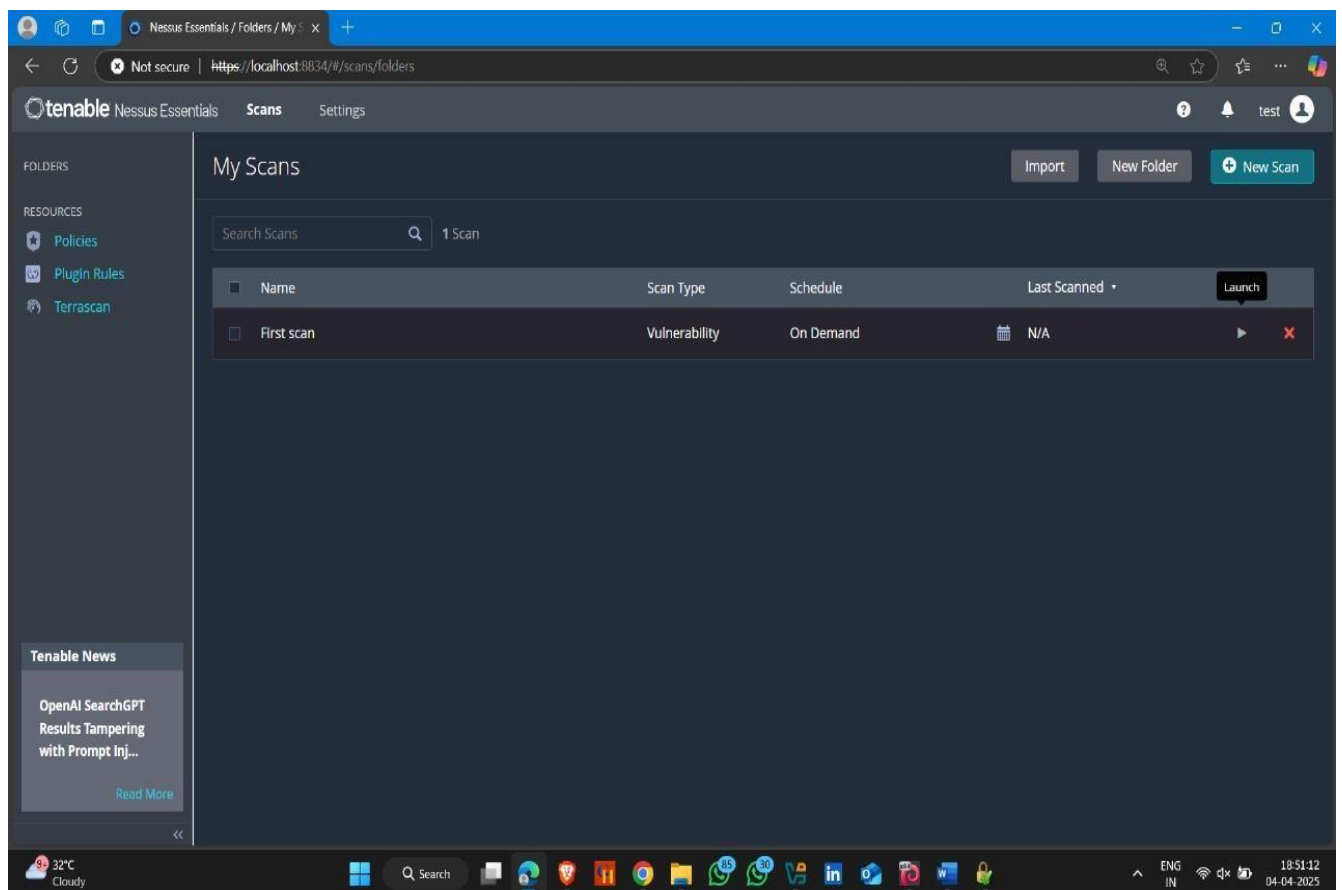
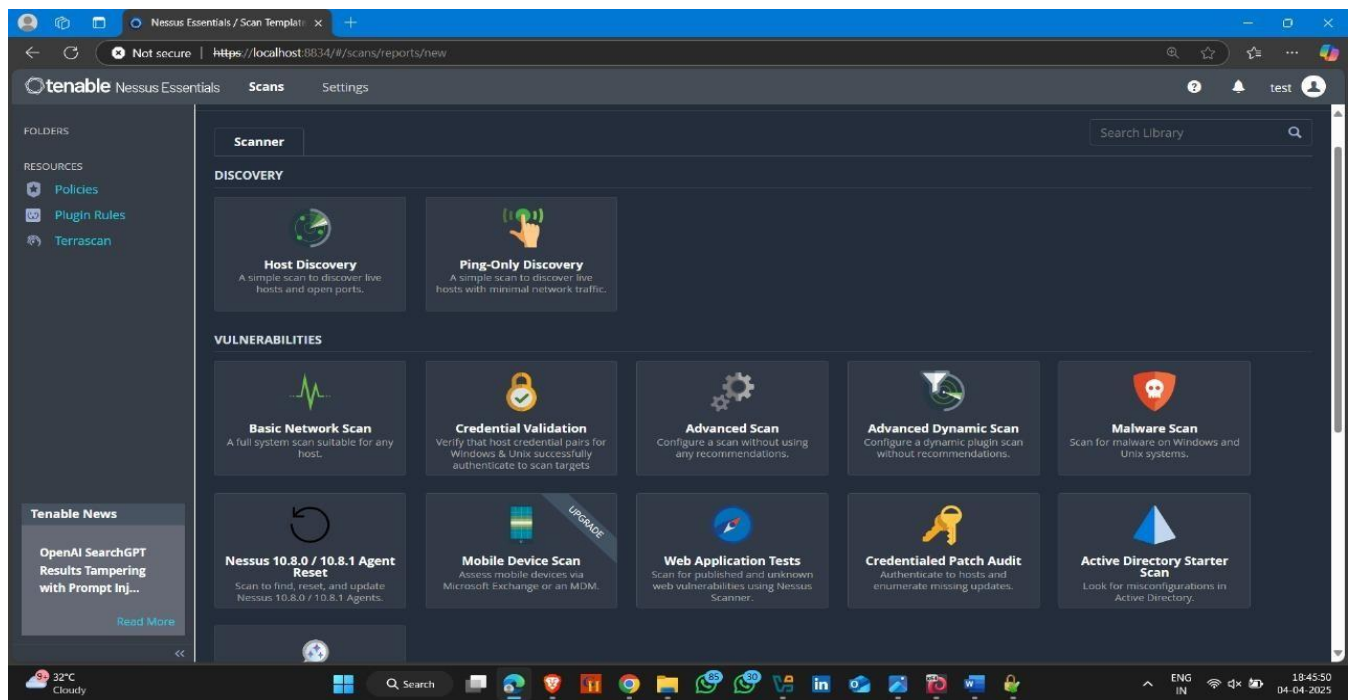
Nessus Pro benefits

- Accurate visibility into your networks. Nessus identifies the vulnerabilities that need attention with high-speed, accurate scanning—and highlights which vulnerabilities should be addressed first.
- The power of the Tenable Zero Day Research team. ...
- The power of Tenable grows with you.

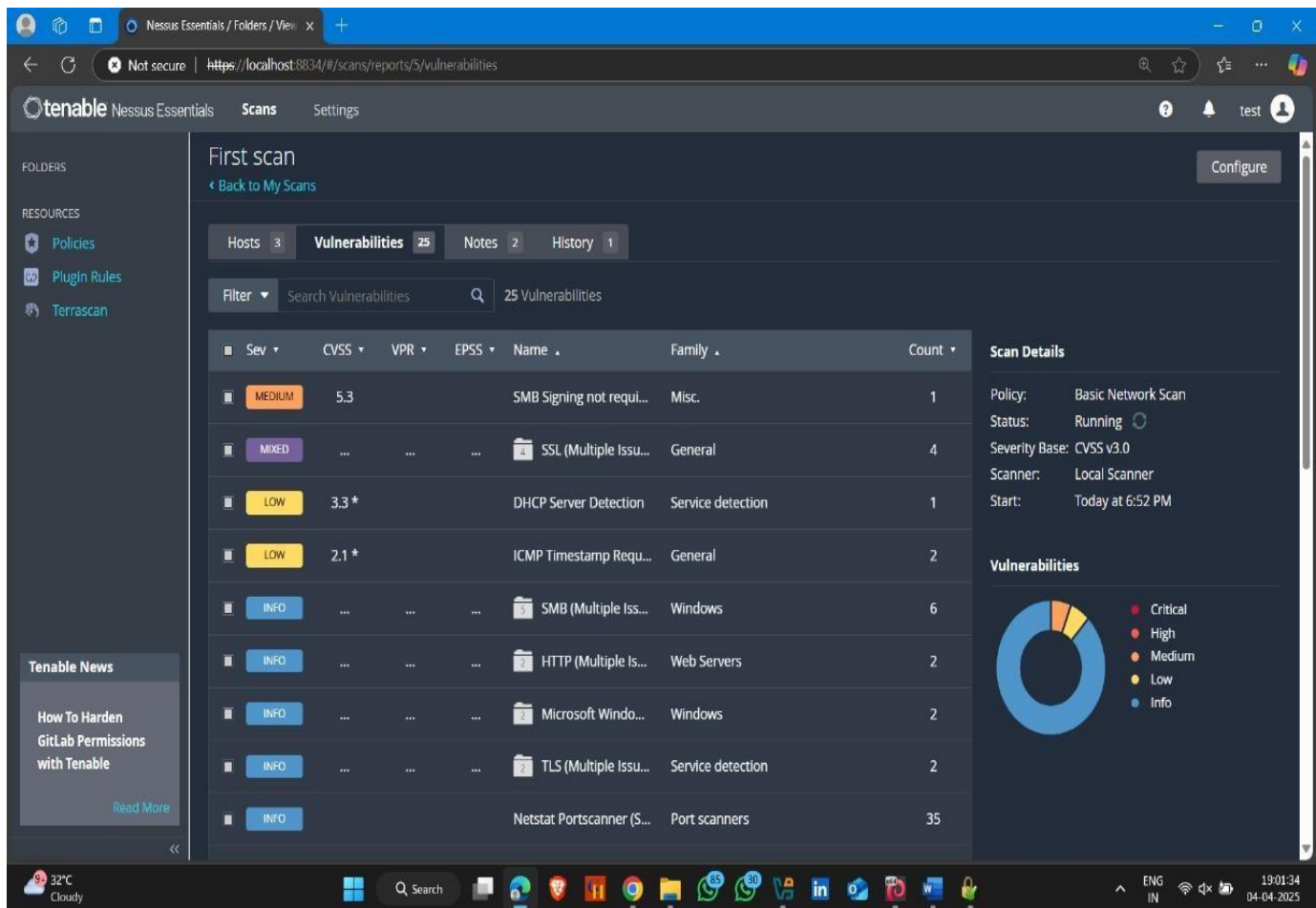
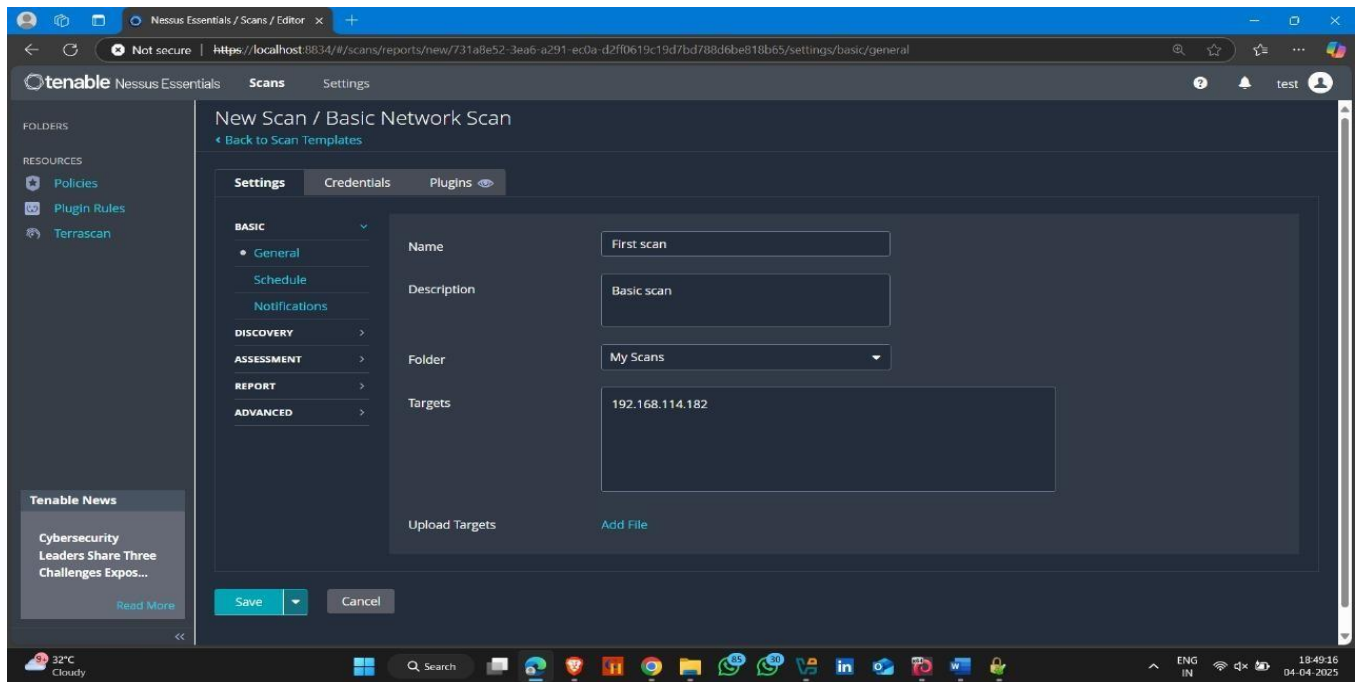
Key Features and Benefits:

- **Vulnerability Detection:** Nessus Essentials helps identify potential security weaknesses in your network, including software flaws, missing patches, and misconfigurations.
- **Prioritization:** It helps you understand which vulnerabilities are most critical and need immediate attention.
- **Proactive Security:** By identifying vulnerabilities before attackers can exploit them, Nessus Essentials enables you to take proactive measures to strengthen your defenses.
- **Compliance Assurance:** It can help ensure your IT infrastructure is compliant with relevant regulatory standards.
- **Detailed Reporting:** Nessus Essentials provides in-depth insights into vulnerabilities, making it easier for teams to understand and address them.
- **Free and Accessible:** Nessus Essentials is free to use, making it an accessible solution for individuals, students, and organizations with limited resources.
- **Tenable Research:** Nessus Essentials leverages the expertise of Tenable Research, which works with the security community to discover new vulnerabilities and provide insights into published vulnerabilities.

Name : kunal Jawale



Name : kunal Jawale



Name : kunal Jawale

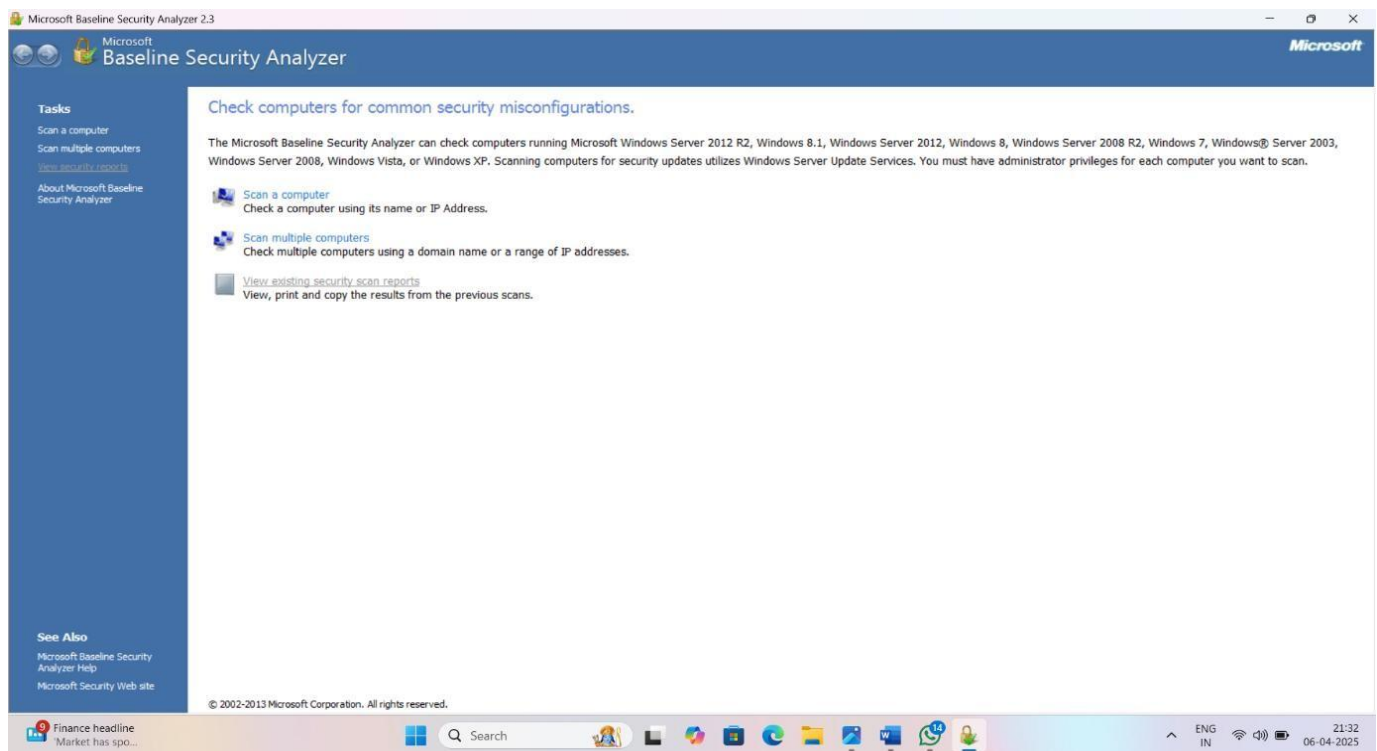
- **No time limit for usage**
- **Access to the Nessus training curriculum**
- **Community Engagement**

○ MBSA scan : (Microsoft baseline security analyzer)

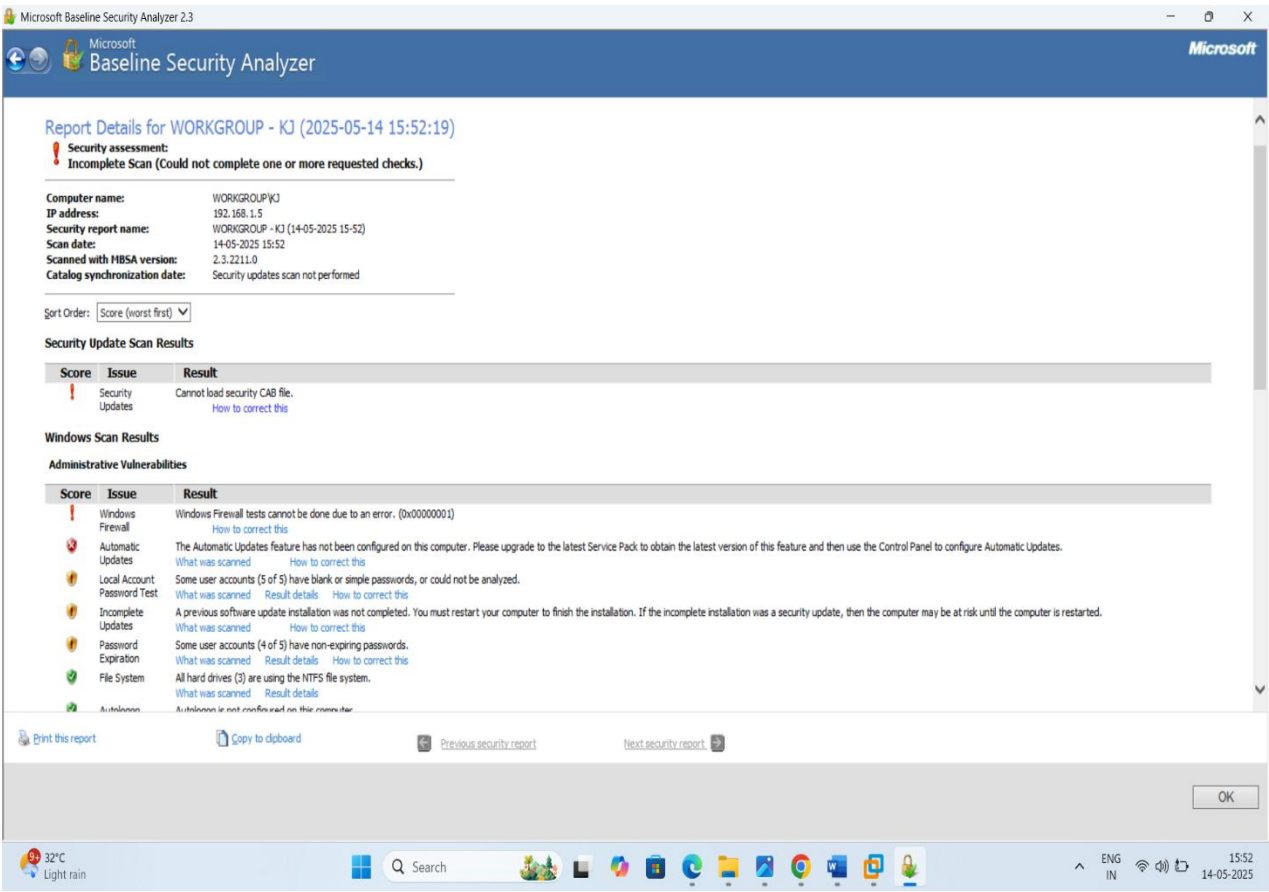
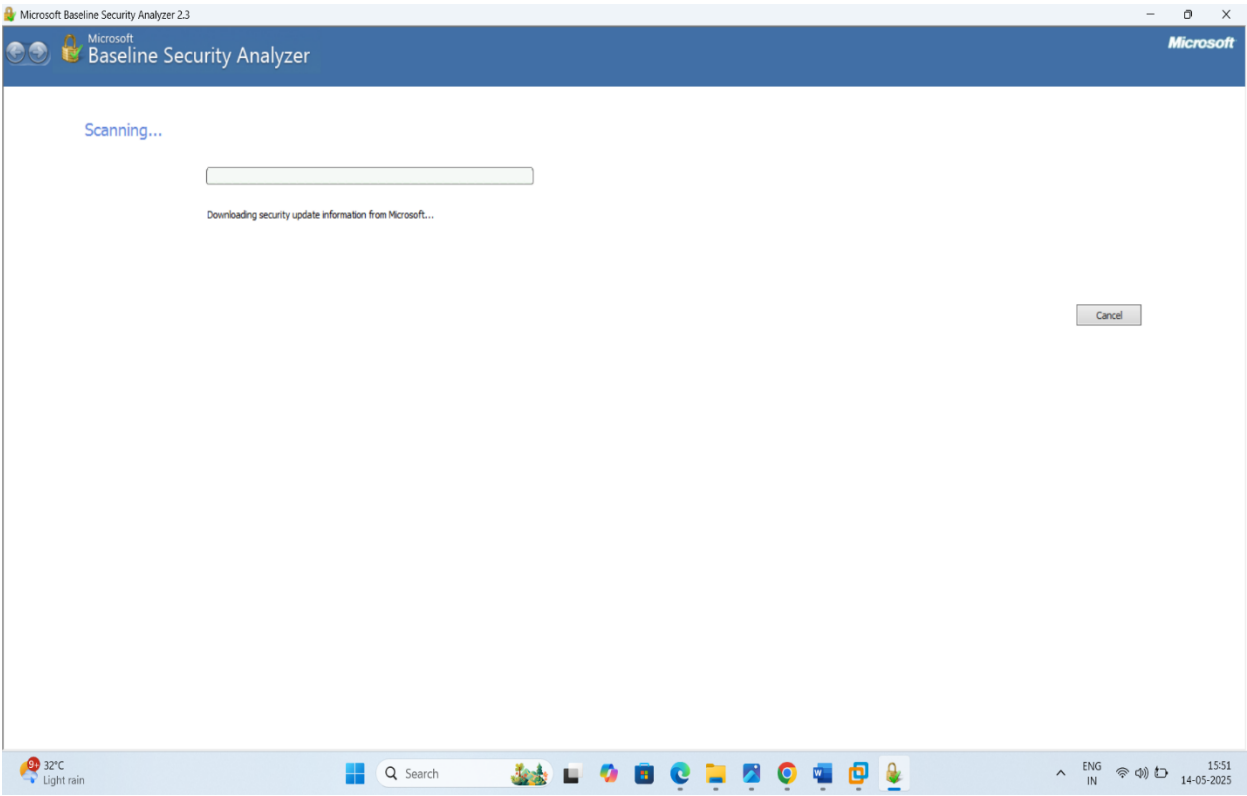
The Microsoft Baseline Security Analyzer (MBSA) is a software tool that helps determine the security of your Windows computer based on Microsoft's security recommendations.

Purpose :

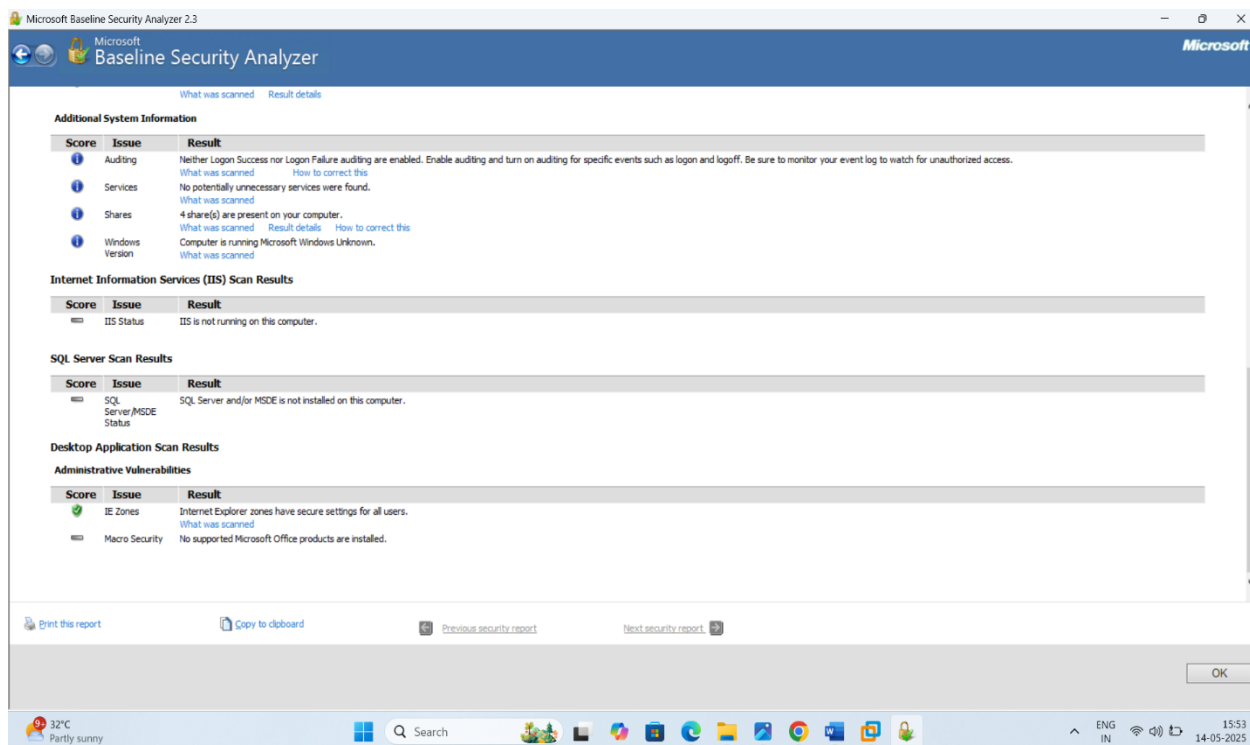
Microsoft Baseline Security Analyzer (MBSA) checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server. MBSA also scans a computer for insecure configuration settings.



Name : kunal Jawale



Name : kunal Jawale



Here is my laptop scanning report

Benefits :

The Microsoft Baseline Security Analyzer (MBSA), while an older tool, offers benefits like identifying missing security updates and misconfigurations, helping organizations improve their security posture and comply with security recommendations.

Key Benefits of Using MBSA:

- **Identifies Missing Updates and Patches:**

MBSA scans for missing security updates, update rollups, and service packs available from Microsoft Update, helping ensure systems are patched against known vulnerabilities.

- **Detects Security Misconfigurations:**

MBSA also scans for insecure configuration settings on Windows, IIS, and SQL Server, allowing for proactive remediation of potential weaknesses.

- **Provides Remediation Guidance:**

MBSA offers specific suggestions and instructions on how to address identified security vulnerabilities, making it easier to improve security.

- **Easy to Use:**

MBSA is designed to be easy for IT professionals to use, even in small and medium-sized businesses, to assess their security state.

Compliance Tool:

MBSA can be used as a compliance tool to ensure that all security updates are deployed to a managed environment.

- **Free Tool:**

MBSA is a free tool provided by Microsoft, making it accessible to organizations of all sizes.

- **Automated Scanning:**

MBSA can scan one or more computers by domain, IP address range, or other grouping, making it easy to automate vulnerability scans.

- **Detailed Reporting:**

MBSA provides detailed reports on vulnerabilities and their severity levels, allowing for better prioritization of security efforts.

- **Integrates with Microsoft Management Products:**

MBSA is built on the Windows Update Agent and Microsoft Update infrastructure, ensuring consistency with other Microsoft management products.

- **Legacy Tool:**

While MBSA is an older tool, it can still be useful for organizations that primarily use Windows-based systems and need a free, easy-to-use tool for assessing security.

o Openvas :

Integrating OpenVAS with Kali Linux provides cybersecurity professionals with a powerful, open-source vulnerability scanning tool, enabling comprehensive assessment of network security by identifying and prioritizing vulnerabilities.

Here's a breakdown of the benefits:

Enhanced Vulnerability Assessment:

- **Comprehensive Scanning:**

OpenVAS can scan both unauthenticated and authenticated systems, testing a wide range of protocols and services.

- **Detailed Reporting:**

OpenVAS generates detailed reports outlining detected vulnerabilities, severity levels, and remediation recommendations, facilitating effective risk management.

- **Automated Scanning:**

OpenVAS supports automated scanning, allowing for regular and scheduled vulnerability assessments, ensuring ongoing security monitoring.

- **Customization:**

OpenVAS offers a powerful internal programming language, allowing for the implementation of custom vulnerability tests.

- **Actionable Data:**

OpenVAS helps prioritize vulnerabilities based on risk, enabling security teams to focus on the most critical issues first.

- **Open Source:**

Being open-source, OpenVAS is free to use and allows for community contributions and customization.

- **Integration with Kali Linux:**

Kali Linux, a popular penetration testing distribution, provides a preconfigured environment for installing and using OpenVAS, streamlining the setup process.

- **Continuous Updates:**

OpenVAS benefits from continuous updates to its vulnerability database (NVT), ensuring it stays current with the latest threats.

- **Remediation Tasks:**

OpenVAS can assist with remediation tasks by providing detailed information about vulnerabilities and recommended fixes.

- **Scalability:**

OpenVAS is designed to handle large-scale scans, making it suitable for organizations with extensive networks.

- **Security Professionals Tool:**

OpenVAS is a network scanning tool designed for cyber security professionals.

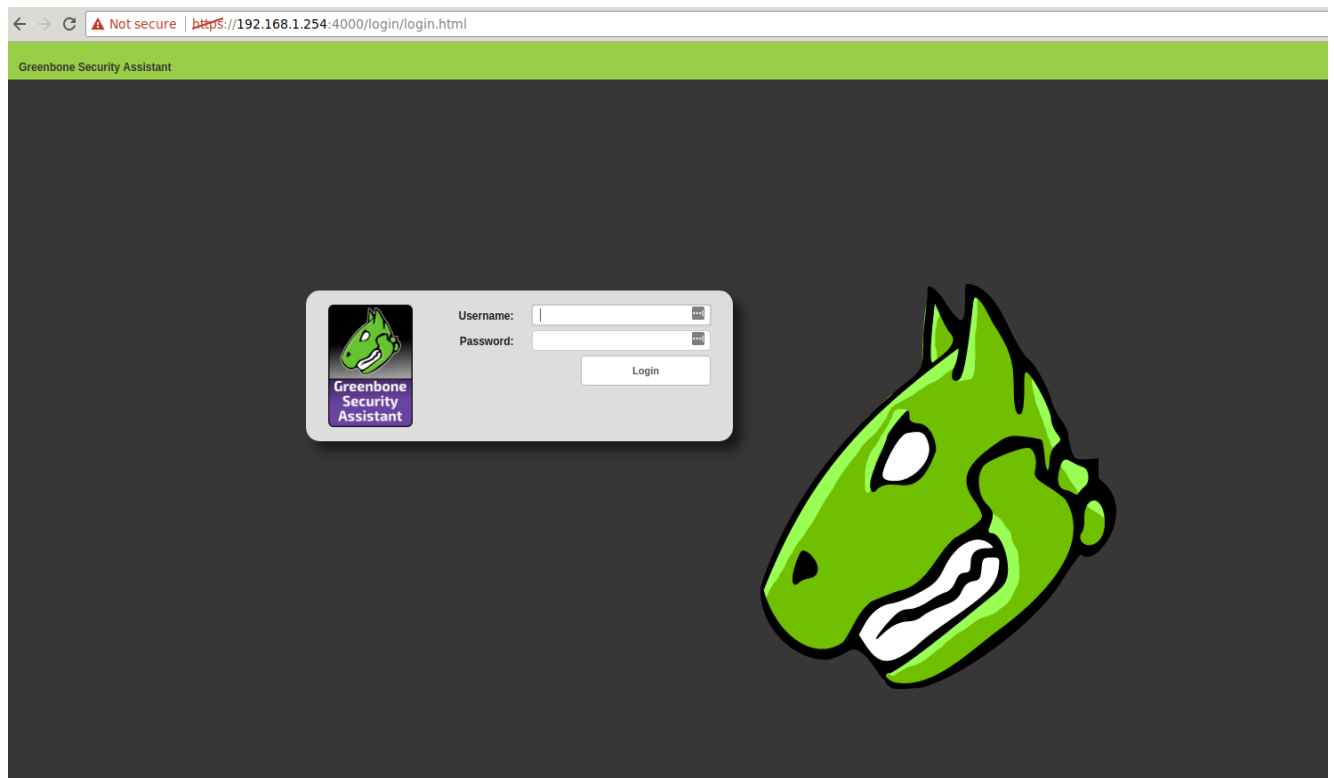
- **Vulnerability Management:**

Name : kunal Jawale

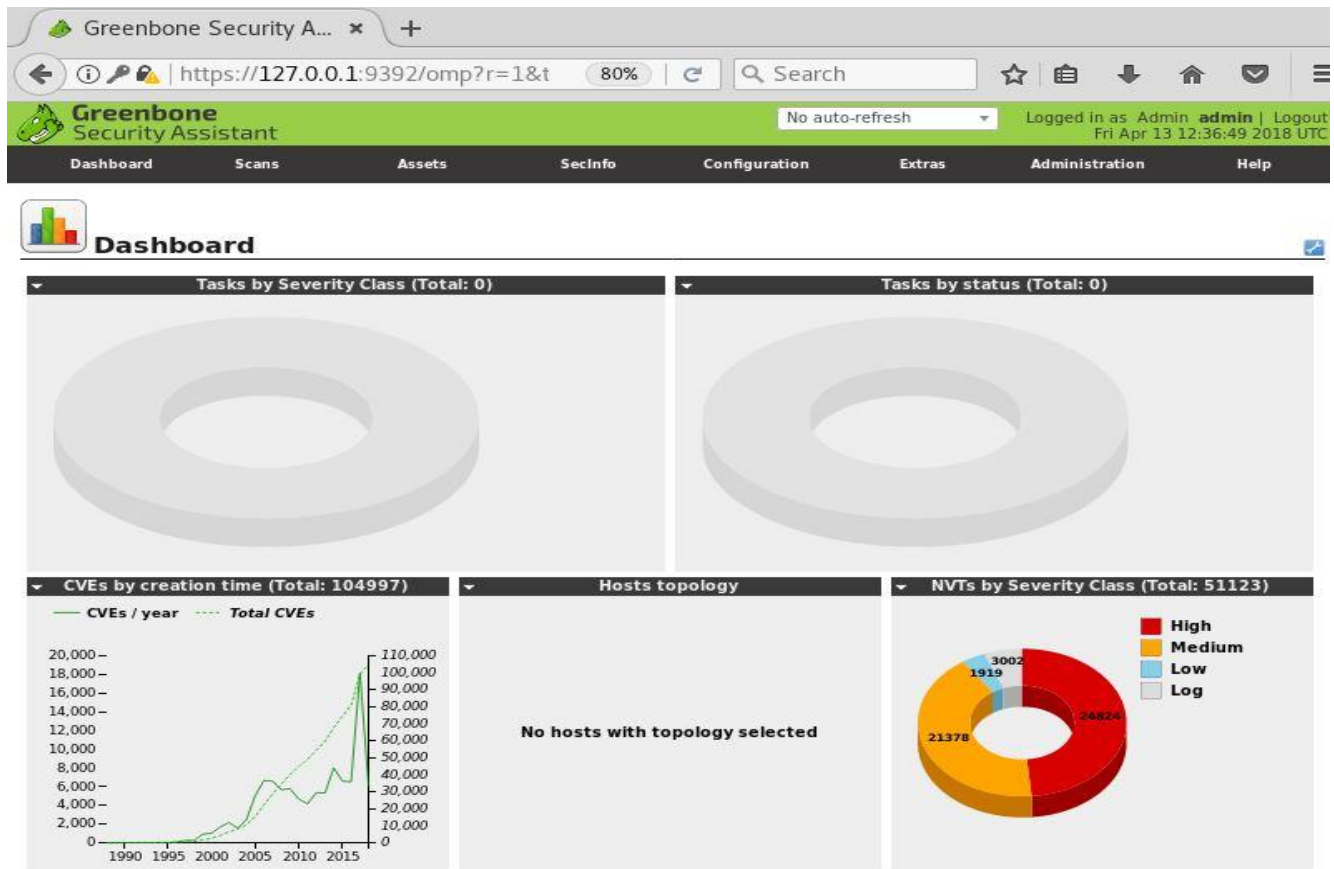
OpenVAS supports vulnerability management, including scan automation, GVMD, SCAP, and CERT feed updates.

Multiple Scanning Techniques:

OpenVAS employs various techniques, including network scanning, service enumeration, and vulnerability checks, to comprehensively assess the security posture of the target environment.



Name : kunal Jawale



Name : kunal Jawale

Greenbone Security Assistant

Logged in as Admin admin | Logout
Tue Aug 13 00:50:14 2013 UTC

Scan Management

Asset Management

SecInfo Management

Configuration

Extras

Administration

Help

Tasks (total: 0) No auto-refresh Apply overrides


Filter:


Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		

(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)

Welcome dear new user!

To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon  any time later on.


For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon .

Quick start: Immediately scan an IP address

IP address or hostname:

For this short-cut I will do the following for you:



































1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the details icon  and review the results collected so far.

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net

Report: Results 1 - 100 of 102 (total: 233) PDF 78 %

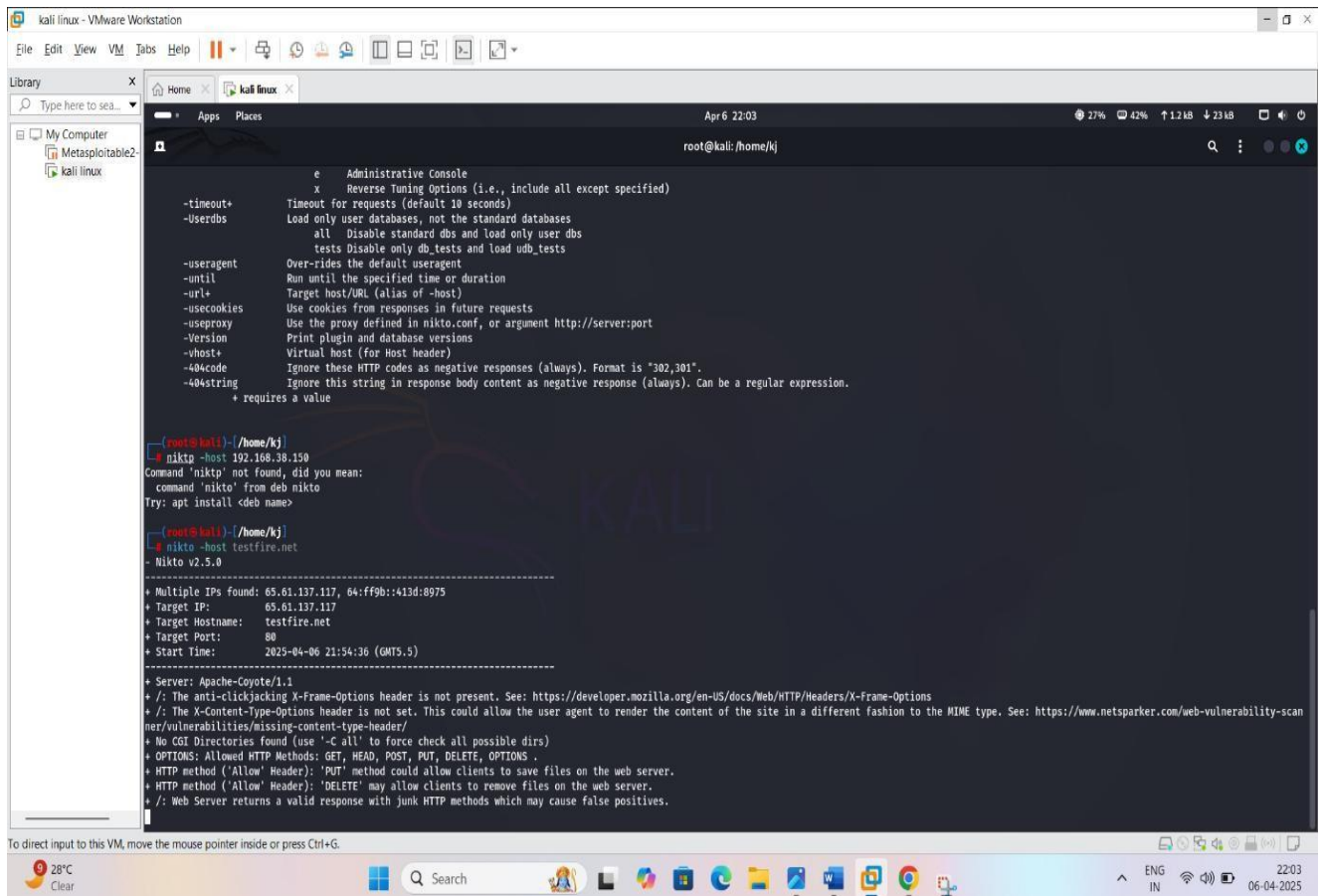
Filter:

Vulnerability	Severity	QoD	Host	Location	Actions
X Server	10.0 (High)	80%	192.168.56.101	6000/tcp	 
PostgreSQL weak password	9.0 (High)	99%	192.168.56.101	5432/tcp	 
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	192.168.56.101	5432/tcp	 
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.56.101	80/tcp	 
phpinfo() output accessible	7.5 (High)	80%	192.168.56.101	80/tcp	 
ProFTPD Long Command Handling Security Vulnerability	6.8 (Medium)	80%	192.168.56.101	2121/tcp	 
PostgreSQL Multiple Security Vulnerabilities	6.8 (Medium)	80%	192.168.56.101	5432/tcp	 
phpMyAdmin Bookmark Security Bypass Vulnerability	6.5 (Medium)	80%	192.168.56.101	80/tcp	 
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	 
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	 
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability	6.0 (Medium)	80%	192.168.56.101	5432/tcp	 
http TRACE XSS attack	5.8 (Medium)	99%	192.168.56.101	80/tcp	 
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability	5.5 (Medium)	80%	192.168.56.101	5432/tcp	 
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.56.101	25/tcp	 
/doc directory browsable ?	5.0 (Medium)	80%	192.168.56.101	80/tcp	 
TikiWiki CMS/Groupware Input Sanitation Weakness Vulnerability	5.0 (Medium)	80%	192.168.56.101	80/tcp	 
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.56.101	22/tcp	 

Name : kunal Jawale

○ Nikto :

Nikto is an open source (GPL) web server scanner that performs vulnerability scanning against web servers for multiple items, including dangerous files and programs. Nikto checks for outdated versions of web server software.



```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2
kali linux
Apr 6 22:03
root@kali: /home/kj
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdbs Load only user databases, not the standard databases
all Disable standard dbs and load only user dbs
tests Disable only db_tests and load udb_tests
-useragent Over-rides the default useragent
-until Run until the specified time or duration
-url+ Target host/URL (alias of -host)
-usecookies Use cookies from responses in future requests
-useproxy Use the proxy defined in nikto.conf, or argument http://server:port
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
-404code Ignore these HTTP codes as negative responses (always). Format is "302,301".
-404string Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value

root@kali: /home/kj
nikto -host 192.168.38.150
Command 'niktp' not found, did you mean:
command 'nikto' from deb nikto
Try: apt install <deb name>

root@kali: /home/kj
nikto -host testfire.net
- Nikto v2.5.0

+ Multiple IPs found: 65.61.137.117, 64:ff9b::413d:8975
+ Target IP: 65.61.137.117
+ Target Hostname: testfire.net
+ Target Port: 80
+ Start Time: 2025-04-06 21:54:36 (GMT5.5)

+ 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
```

Benefits :

By analysing server configuration items, HTTP server options, and installed web servers and software, Nikto provides invaluable insights into potential security flaws. Furthermore, its ability to perform version-specific checks on a wide range of servers ensures that no vulnerability goes unnoticed.

Main features:

-
- Nikto is free to use, open source and frequently updated.
- Can be used to scan any web server (Apache, Nginx, Lighttpd, Litespeed, etc.)
- Scans against 6,700+ known vulnerabilities and version checks for 1,250+ web servers (and growing)
- Scans for configuration-related issues such as open index directories.

Zaproxy :

OWASP ZAP (Zed Attack Proxy) is a powerful, free, and opensource penetration testing tool that's included in Kali Linux, offering benefits like easy web application vulnerability identification, active and passive scanning, and flexible usage for various skill levels.

Here's a more detailed look at the benefits of using OWASP ZAP within Kali Linux:

Key Benefits:

- **Web Application Vulnerability Testing:**

ZAP is designed specifically for testing web applications, helping identify vulnerabilities before they can be exploited.

- **Easy to Use:**

ZAP is designed to be user-friendly, making it suitable for developers, functional testers, and experienced penetration testers alike.

- **Active and Passive Scanning:**

ZAP offers both active and passive scanning capabilities, allowing for thorough vulnerability detection.

- **Intercept and Modify Traffic:**

ZAP acts as a "manipulator-in-the-middle proxy," allowing you to intercept, inspect, and modify traffic between your browser and the web application.

- **Automated and Manual Testing:**

ZAP supports both automated vulnerability scanning and manual testing, providing flexibility for different testing scenarios.

- **WebSockets Support:**

Name : kunal Jawale

ZAP can also scan and analyze WebSockets, which are increasingly used in modern web applications and can introduce security vulnerabilities.

Open-Source and Flexible:

ZAP is open-source, meaning its code can be examined, and anyone can contribute to its development.

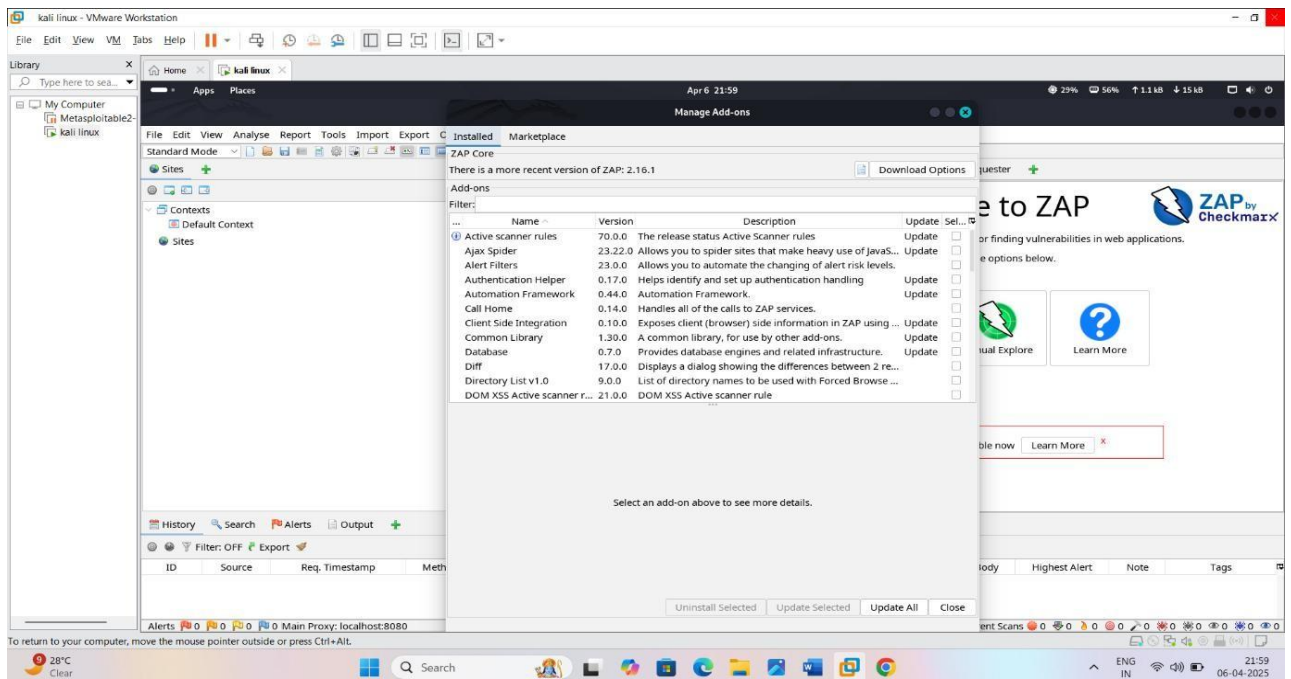
- **Cross-Platform:**

ZAP is available for multiple operating systems, including Kali Linux, Windows, and macOS.

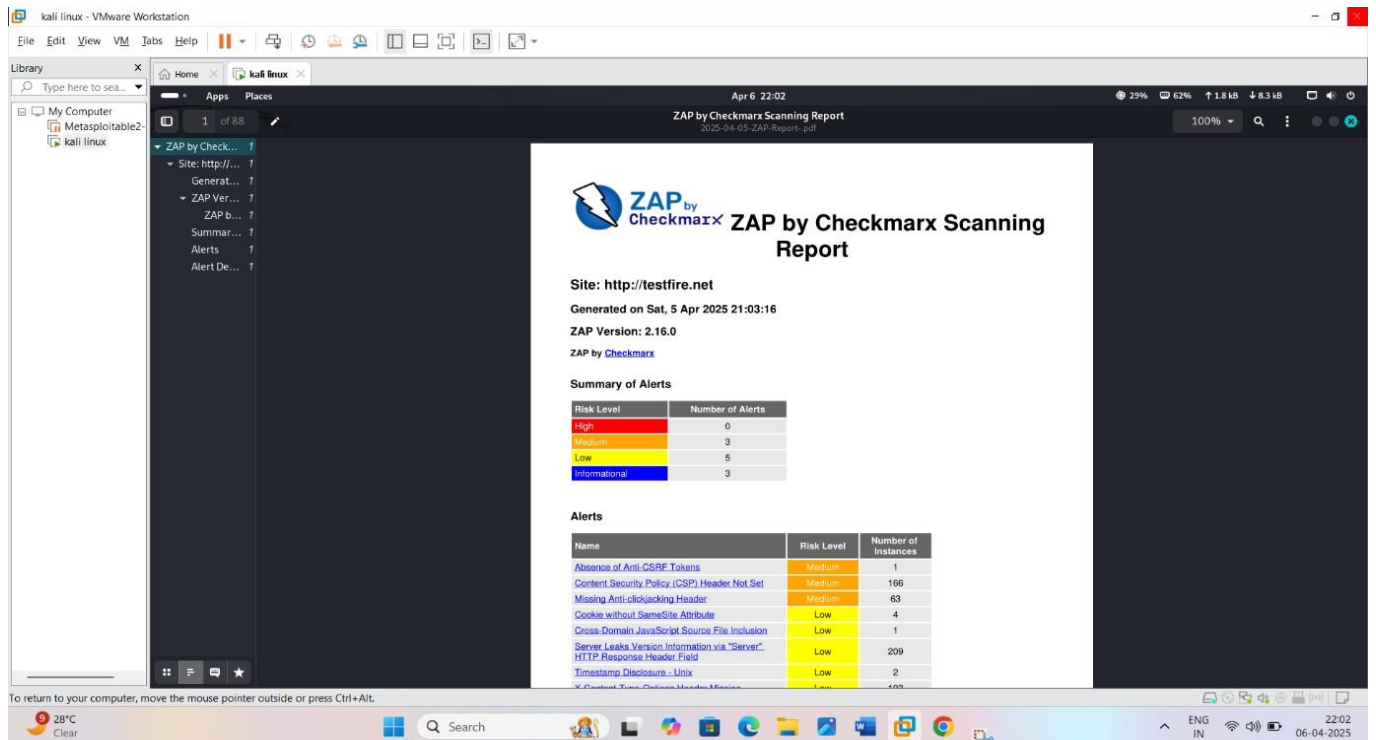
- **Reports and Analysis:**

ZAP can generate reports of its findings, making it easy to document and share vulnerabilities. How ZAP Works:

- **Proxy:** ZAP acts as a proxy between your browser and the web application, intercepting all requests and responses.
- **Scanning:** ZAP can perform both active and passive scans to identify vulnerabilities.
- **Analysis:** ZAP analyzes the traffic and responses to identify potential issues.
- **Reporting:** ZAP can generate reports of its findings, including details about the vulnerabilities it has identified.



●



○ Skipfish :

Skipfish, a web application security reconnaissance tool included in Kali Linux, benefits users by creating interactive sitemaps,

performing dictionary-based probes, and annotating the map with security checks, ultimately aiding in identifying vulnerabilities and improving web application security

```
File Actions Edit View Help
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 2 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 2 total (1.0 req/conn)
  TCP faults : 0 failures, 2 timeouts, 0 purged
External links : 0 skipped
Reqs pending : 0

Database statistics:
File system
  Pivots : 3 total, 3 done (100.00%)
  In progress : 0 pending, 0 init, 0 attacks, 0 dict
Missing nodes : 0 spotted
  Node types : 1 serv, 1 dir, 0 file, 0 pinfo, 1 unkn, 0 par, 0 val
Issues found : 0 info, 2 warn, 0 low, 0 medium, 0 high impact
  Dict size : 5 words (5 new), 0 extensions, 0 candidates
  Signatures : 77 total

[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 3
[+] Looking for duplicate entries: 3
[+] Counting unique nodes: 3
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 3
[+] Generating summary views ...
[+] Report saved to 'skipfishTEST/index.html' [0xea3c8f70].
[+] This was a great day for science!
```

.

Here's a more detailed breakdown of the benefits:

- **Thorough Reconnaissance:**
Skipfish meticulously crawls web applications, mapping their structure and identifying potential vulnerabilities and weaknesses.
- **Interactive Sitemap:**
It generates an interactive sitemap, allowing security professionals to explore the application's structure and identify potential attack vectors.
- **Dictionary-Based Probes:**
Skipfish performs dictionary-based probes to uncover hidden resources and potential vulnerabilities.
- **Security Checks:**
It annotates the sitemap with the output from active (but hopefully nondestructive) security checks, highlighting potential issues.
- **Foundation for Assessments:**
The resulting report serves as a foundation for professional web application security assessments, providing valuable insights for further testing and remediation.
- **Identifying Potential Attack Vectors:**
Skipfish exposes hidden entry points that attackers might exploit, helping security professionals proactively address vulnerabilities.
- **Fuelling Further Testing:**
The data gathered by Skipfish provides valuable ammunition for other penetration testing tools, like SQL injection scanners or web fuzzers.
- **Open Source and Free:**
Skipfish is an open-source, free tool, making it accessible to security professionals and ethical hackers.
- **Easy Installation:**
Skipfish can be installed easily with the command `sudo apt install skipfish`.