**EASTERN INTERNATIONAL UNIVERSITY**

**SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY**

**DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS**

**PROJECT 2**

**MANAGE AND EXPLOIT**

**NETWORK-CONNECTED DEVICES**

**Student**

Nguyen Thanh Dong – 2131220022

Ha Quang Minh - 1931220012

**Supervisor**

Ph.D. Huynh Tan Phuoc

**Binh Duong, Nov, 2024**

**EASTERN INTERNATIONAL UNIVERSITY**

**SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY**

**DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS**

**PROJECT 2**

**MANAGE AND EXPLOIT**

**NETWORK-CONNECTED DEVICES**

**Student**

Nguyen Thanh Dong – 2131220022

Ha Quang Minh - 1931220012

**Supervisor**

Ph.D. Huynh Tan Phuoc

**Binh Duong, Nov, 2024**

**Abstract**

We successfully deployed OpenVAS, Nessus, Zabbix, and Grafana to perform vulnerability scanning and monitoring on test environments. OpenVAS, being free and open-source, suits technical users and small setups with its flexibility for exploit testing via tools like Metasploit, though its complex interface and slower performance on large networks, along with fewer updates compared to Nessus, are notable drawbacks. Nessus offers a user-friendly interface, fast scanning, and detailed reports, making it ideal for enterprises, but its free version is limited, and paid options are costly, lacking direct exploitation features. Zabbix excels in real-time system monitoring and network tracking, integrating well with Grafana, yet it focuses solely on monitoring, not vulnerability scanning, and requires manual configuration. Grafana provides powerful, easy-to-understand data visualization through charts and dashboards, integrating with Zabbix, Nessus, and OpenVAS, but it relies on external data and demands skill to optimize dashboards. We applied RESTful API to automate scanning and data extraction from OpenVAS, Nessus, and Zabbix, saving time and effort. Logs from these tools were processed using Regex and Data Parsing, then visualized in Grafana with team support, enabling real-time tracking of vulnerabilities and system performance. Based on the results, we suggest updating end-of-life systems like Windows 7 to Windows 10/11, patching critical vulnerabilities like SMBv1 (MS17-010), disabling unnecessary services (RPC, TCP/ICMP timestamps), tightening firewall settings, using Zabbix for ongoing monitoring, and optimizing Grafana for real-time alerts to enhance system safety.

**KeyWord:**.

### Acknowledgement

We would like to express our deepest gratitude to PhD. Huynh Tan Phuoc, whose expertise, guidance, and continuous support have been instrumental in the successful completion of this project. We are also grateful to the publishers of the Ubuntu, Kali Linux, VMware, Zabbix, Grafana, OpenVAS, and Nessus software for providing the resources and environment necessary for carrying out this research. Finally, we extend our appreciation to our peers and family for their encouragement throughout this journey.

TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF ABBREVIATION

# Chapter 1. Introduction

## Reason for Choosing the Topic

Effective IT monitoring, visualization, and security assessment are essential for system stability and optimization. Zabbix, Grafana, OpenVAS, and Nessus are widely used tools that provide comprehensive solutions in these areas.

Zabbix is an open-source monitoring solution offering scalable and flexible monitoring for networks, servers, and applications. It provides proactive alerts, multiple data collection methods, and cost-effective enterprise-level features. Grafana enhances monitoring with customizable dashboards, real-time data analysis, and seamless integration with various databases, improving visualization and decision-making.

For security, OpenVAS and Nessus are powerful vulnerability scanners. OpenVAS, an open-source tool, detects weaknesses in servers and networks, offering regular database updates for enhanced security. Nessus, a commercial alternative, provides extensive vulnerability coverage, risk assessments, and compliance auditing, ensuring security policy adherence.

By integrating these tools, organizations achieve a complete monitoring and security solution. Zabbix collects data, Grafana visualizes it, and OpenVAS/Nessus identify vulnerabilities, helping administrators enhance performance, detect threats, and maintain cybersecurity. Their robust features, strong community support, and cost-effectiveness make them ideal choices for IT infrastructure management.

## Research Content

Analyze network monitoring and security assessment processes using Zabbix, Grafana, OpenVAS, and Nessus. Research methods for system monitoring, log analysis, and performance optimization. Study approaches for vulnerability scanning, risk assessment, and penetration testing. Explore the implementation of virtual environments (VMware) for testing network security through supporting tools such as OpenVAS, Nessus, Nmap, and other security frameworks.

## Scientific and Practical Significance

* **Proactive network and system monitoring:** Zabbix provides real-time network and system health tracking, helping administrators detect and resolve performance issues before they escalate.
* **Enhanced data visualization:** Grafana enables in-depth data analysis and dashboard customization, improving decision-making through clear and interactive visual representations.
* **Comprehensive vulnerability scanning:** OpenVAS and Nessus help identify security weaknesses in network infrastructures, ensuring that vulnerabilities are promptly detected and mitigated.
* **Compliance with security standards:** The use of OpenVAS and Nessus assists organizations in meeting security compliance requirements, such as PCI DSS, GDPR, HIPAA, and ISO 27001.
* **Efficient incident response and mitigation:** By integrating these tools, organizations can streamline their security operations, quickly respond to potential threats, and strengthen overall system resilience.
* **Optimization of IT infrastructure:** Continuous monitoring and vulnerability assessment improve system performance, reduce downtime, and enhance overall network security.

# Chapter 2: Theoretical Basis and Tools Utilized

## Overview of computer network information security theory

Computer Network Information Security Theory encompasses the principles, models, and practices designed to protect data, resources, and communication over networks. Below is an overview:

### Key Concepts

* **Confidentiality:** Ensuring that data is accessible only to those authorized to view it.
* **Integrity:** Ensuring that data remains unchanged and unaltered unless done by authorized processes.
* **Availability:** Ensuring that data and resources are available to users when needed.
* **Authentication:** Verifying the identity of a user or system before granting access.
* **Authorization:** Controlling access to resources based on user identity or role
* **Non-repudiation:** Guaranteeing that actions or transactions cannot be denied after the fact.

### Threats in Network Security

* **Eavesdropping**: Unauthorized interception of data during transmission. Man-in-the-Middle (MITM) Attacks: Attacker intercepts and potentially alters communications between two parties.
* **Phishing and Social Engineering**: Deceptive methods to gain confidential information.
* **Malware**: Viruses, worms, ransomware, and spyware that harm or exploit systems.
* **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**: Overwhelming a system to make it unavailable to users.
* **SQL Injection and Cross-Site Scripting (XSS):** Exploits targeting web applications.
* **Zero-Day Exploits**: Exploiting vulnerabilities before they are known or patched.

### Security Measures and Techniques

* **Network and System Monitoring:** Zabbix provides real-time tracking of system performance, ensuring early detection of anomalies and potential security threats.
* **Data Visualization for Security Insights:** Grafana helps analyze logs and monitoring data, offering clear dashboards that highlight security incidents and trends.
* **Vulnerability Scanning and Risk Assessment:** OpenVAS and Nessus scan for security flaws in servers, networks, and applications, enabling proactive mitigation.
* **Automated Security Alerts and Incident Response:** Zabbix and OpenVAS integrate to provide automated notifications, allowing security teams to respond quickly.
* **Compliance and Security Auditing:** Nessus assists organizations in meeting compliance standards by identifying misconfigurations and weaknesses in security policies.
* **Penetration Testing for System Hardening:** Using OpenVAS alongside other tools like Nmap allows security teams to simulate attacks, test defenses, and improve resilience.

### Network Security Architectures

* + - * Defense in Depth with Multi-Layer Monitoring**:** Zabbix continuously monitors system health, network traffic, and security events at multiple layers to provide comprehensive protection.
      * Zero Trust with Continuous Verification: Nessus and OpenVAS regularly scan for vulnerabilities, ensuring that no device or service is implicitly trusted.
      * Endpoint Security via Real-Time Alerts: Zabbix and Grafana integrate to track endpoint performance and detect suspicious activity, helping secure connected devices.
      * Secure Remote Access through VPN & Encryption: Implementing VPN solutions ensures safe remote access, while TLS/SSL encryption secures data transmission.
      * Automated Threat Detection and Response: Combining Zabbix, OpenVAS, and Nessus allows for automated security auditing, real-time alerts, and proactive incident response.

### Standards and Frameworks

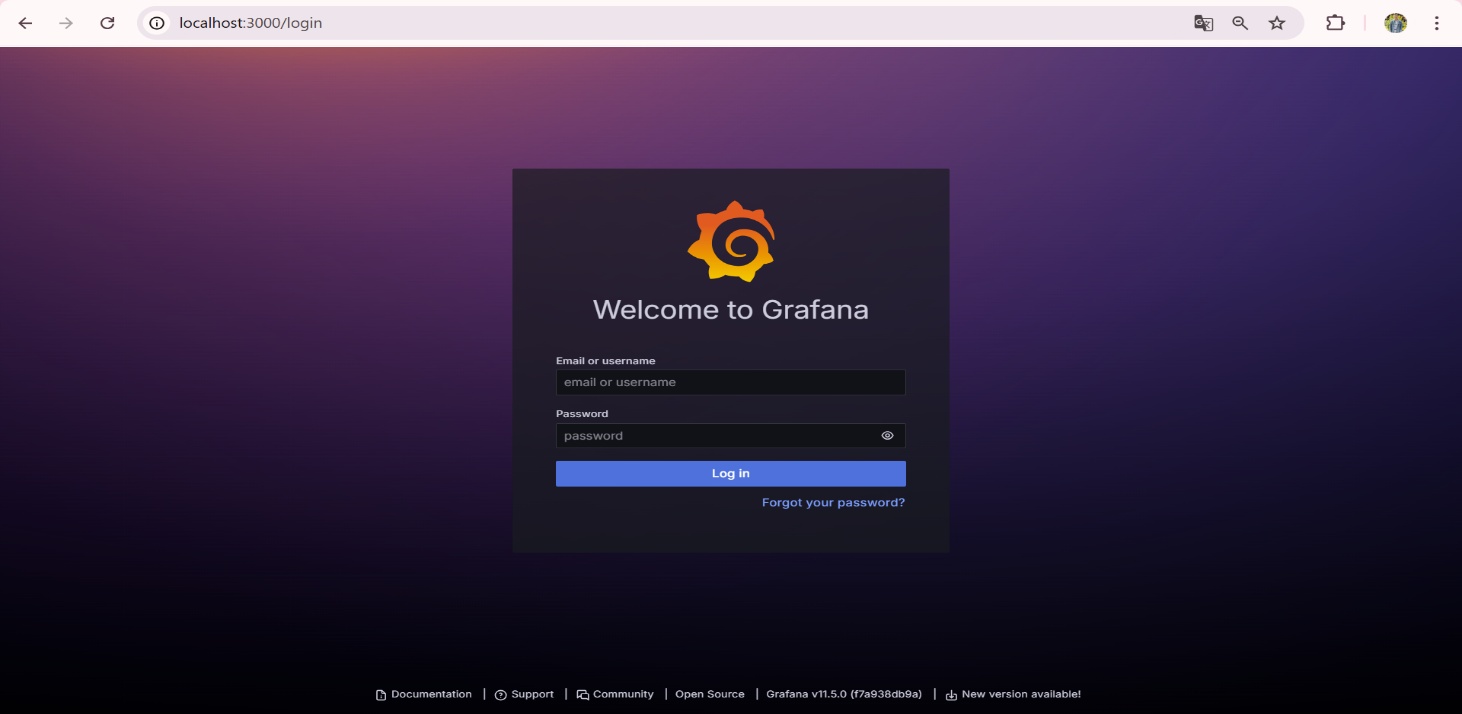
* + - * **ISO/IEC 27001 Compliance through Continuous Monitoring:** Zabbix helps organizations maintain ISO/IEC 27001 compliance by providing real-time monitoring, log analysis, and anomaly detection.
      * **NIST Cybersecurity Framework Implementation:** OpenVAS and Nessus support risk assessment, vulnerability scanning, and security control validation as recommended by NIST guidelines.
      * **Regulatory Compliance with GDPR & HIPAA:** Security auditing tools like Nessus ensure compliance with GDPR and HIPAA by identifying misconfigurations, enforcing data encryption, and monitoring access controls.
      * **Automated Security Reporting and Auditing:** Grafana and Zabbix generate detailed reports on security incidents, helping organizations track compliance with industry standards.

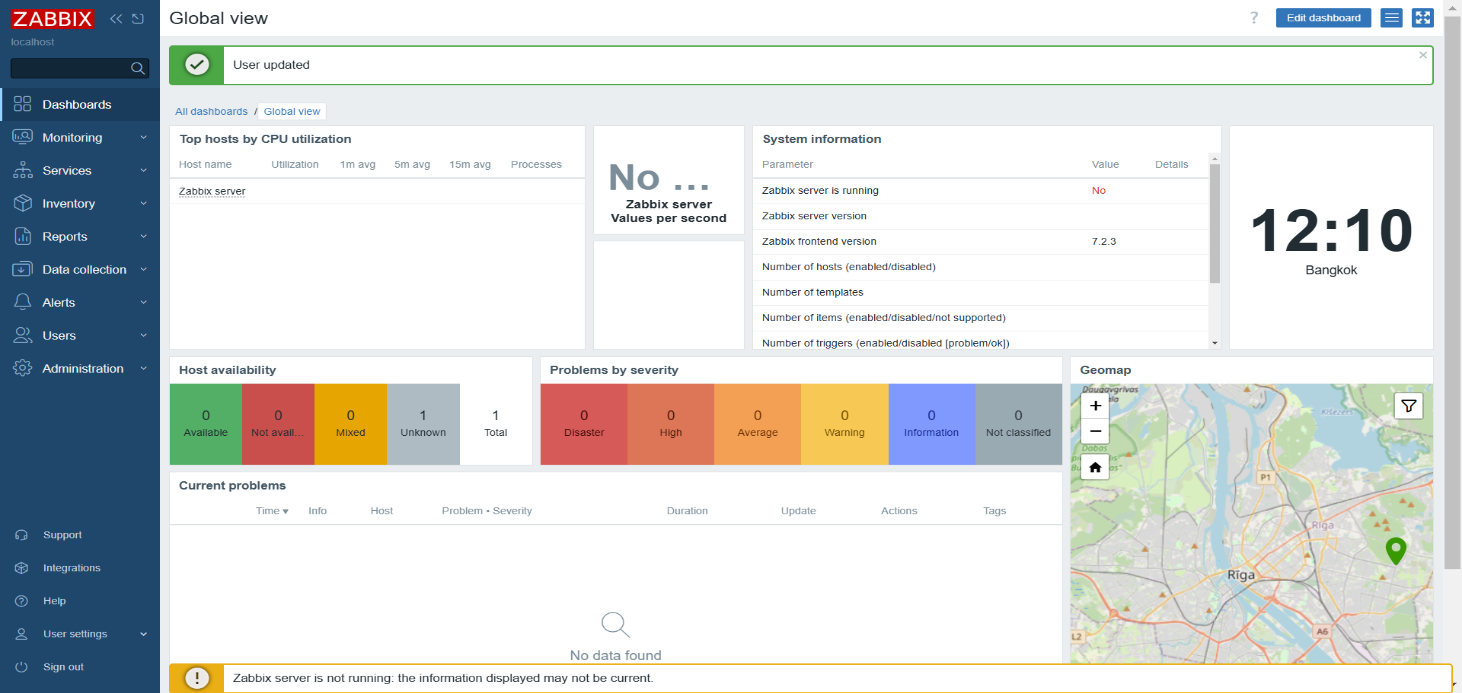
### Emerging Trends

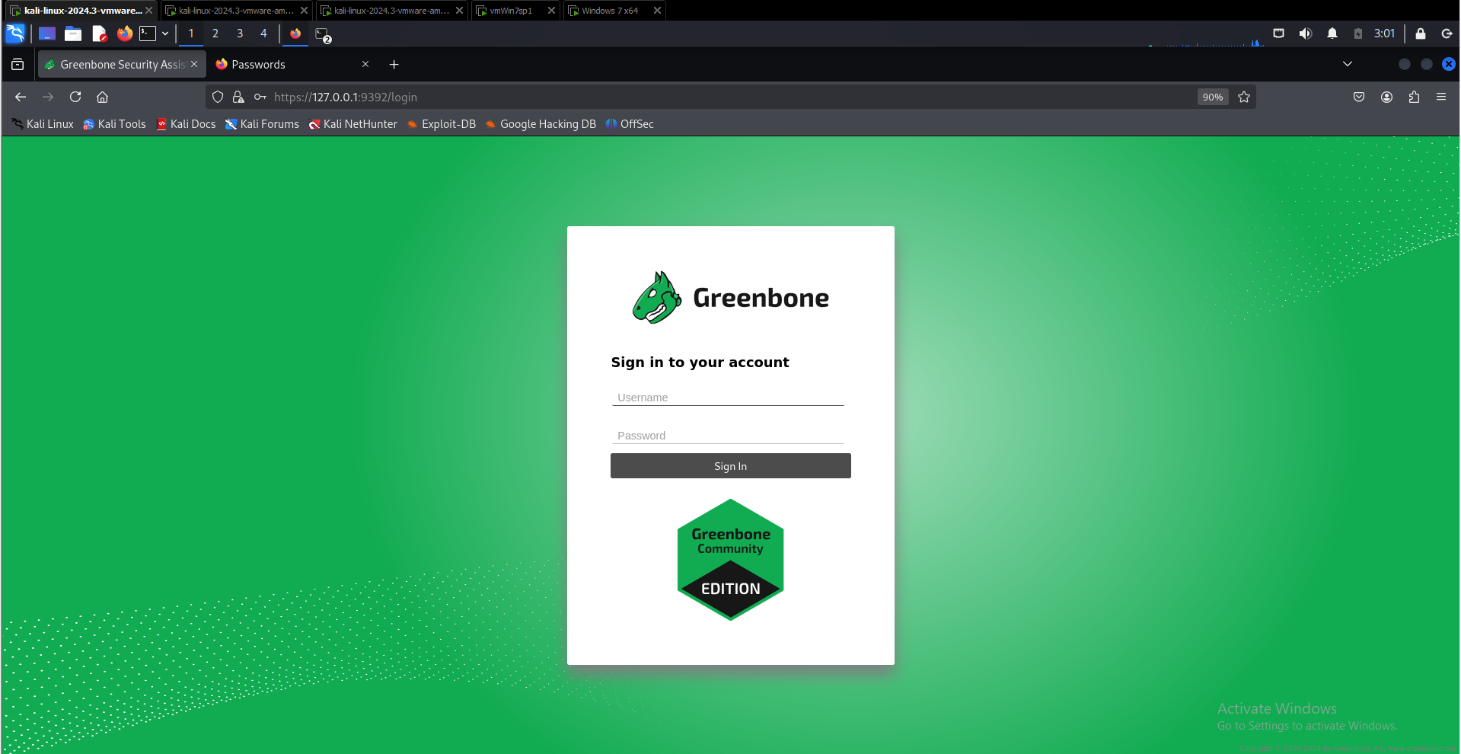
* + - * **AI-Driven Anomaly Detection:** Zabbix and OpenVAS are increasingly integrating AI and machine learning to detect unusual network behavior and predict potential security threats.
      * **Quantum-Safe Cryptography:** Future-proofing security measures by researching post-quantum cryptographic algorithms to secure sensitive network communications.
      * **IoT Security Challenges:** Monitoring IoT devices with Zabbix to detect vulnerabilities, ensuring real-time visibility and proactive threat mitigation.
      * **Cloud-Native Security Monitoring:** Using Grafana to analyze security logs from cloud environments, ensuring compliance with security policies and protecting against data breaches.
      * **Automated Threat Intelligence:** Enhancing Nessus and OpenVAS with automated security updates and real-time threat intelligence to identify zero-day vulnerabilities.

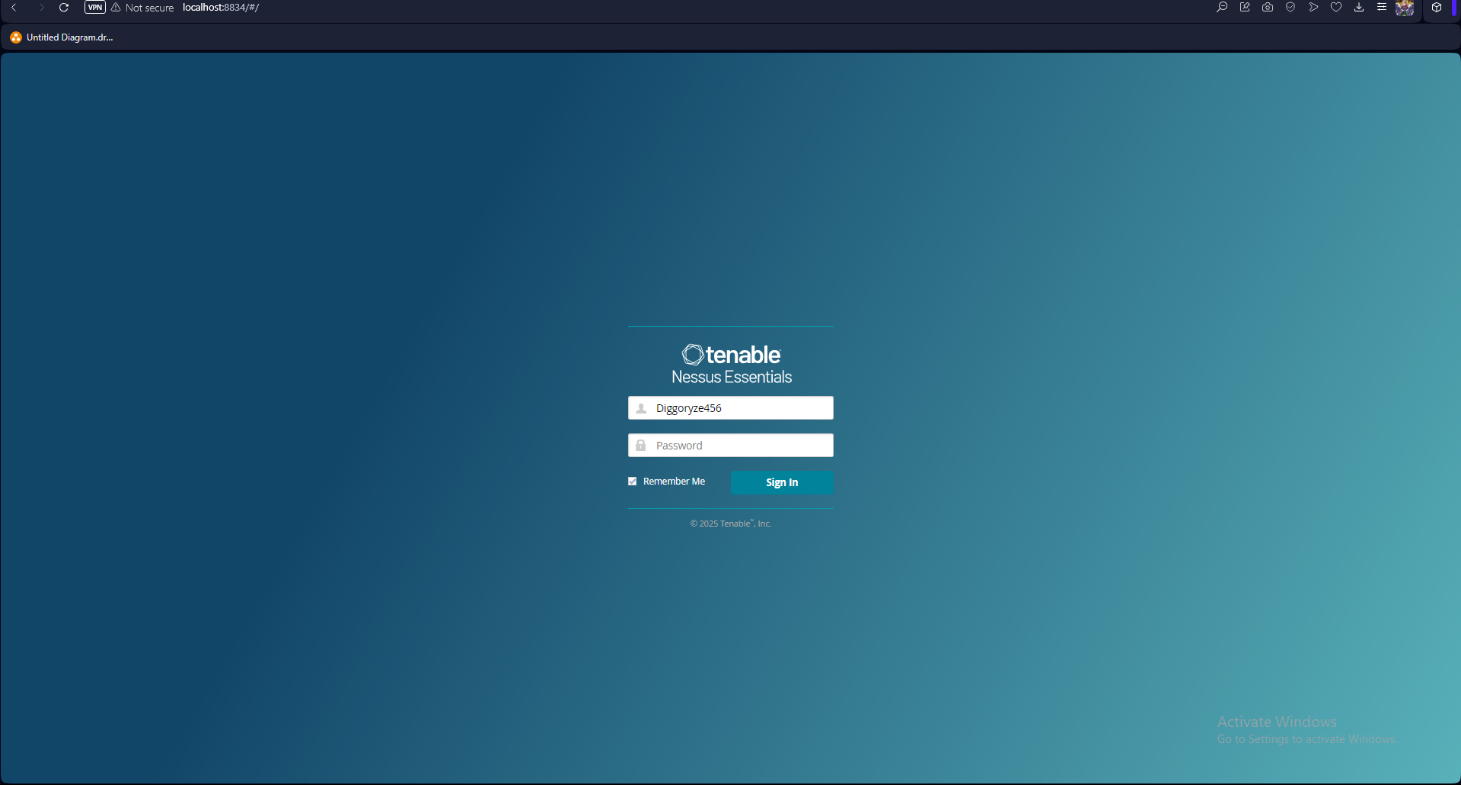
## Tools Utilized

### Virtual environment design of Zabbix, Grafana, Nessus and OpenVas.

In this project, **Ubuntu, Kali Linux and Browser** are used as the primary operating system for deploying and testing network monitoring and security tools. By utilizing virtualization tools, we can establish a simulated network system, allowing us to assess monitoring performance and security vulnerabilities safely without impacting real systems. We will get used to software interfaces such as Figure 1, 2, 3 and 4. Each interface is in charge of different software: Grafana, Zabbix, Openvas and Nessus, respectively.

*Figure 1: The interface Grafana  
Figure 2: The interface Zabbix*

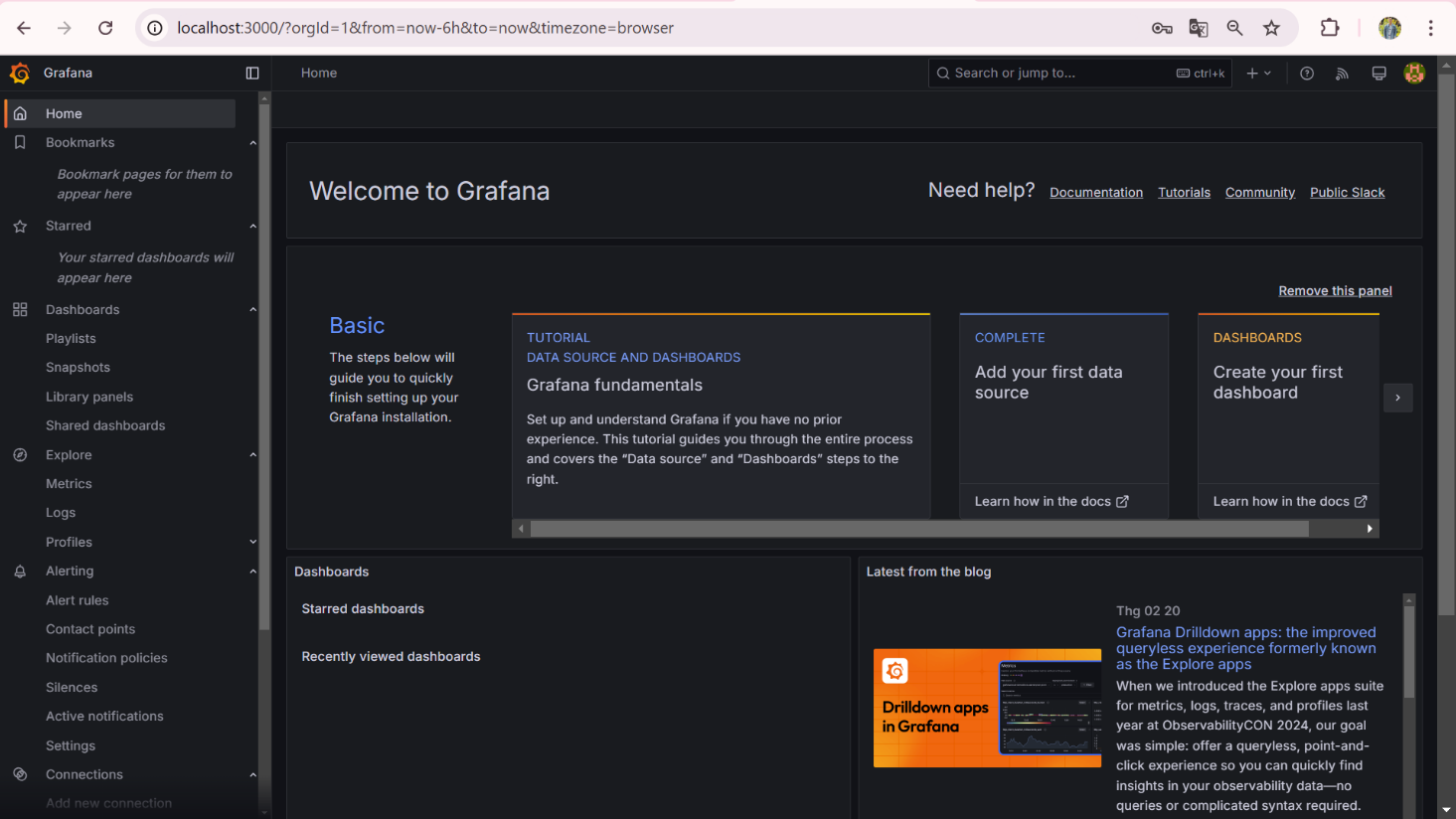
*Figure 3: The interface* *OpenVas*



*Figure 4: The interface Nessus*

### Introduction of Grafana.

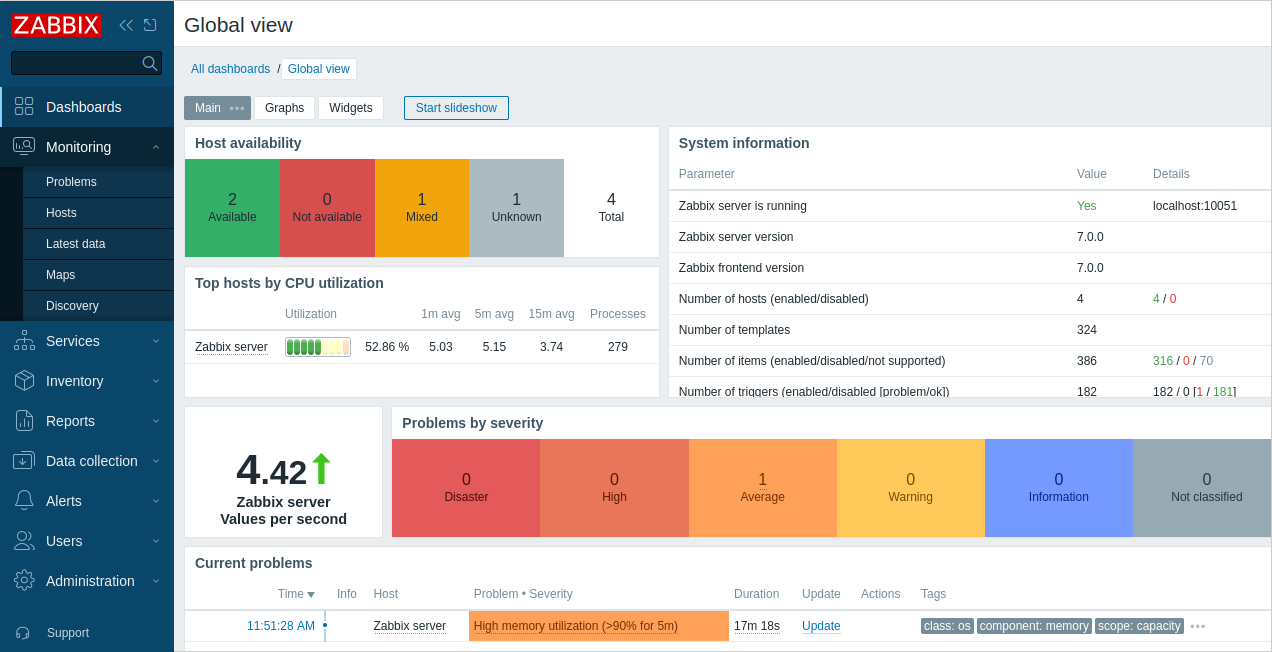
Grafana is an open-source platform for monitoring and observability that allows users to visualize, analyze, and understand their data through interactive dashboards. It supports various data sources, including Prometheus, InfluxDB, MySQL, PostgreSQL, and Zabbix. Grafana provides a user-friendly interface, powerful query editors, and customizable visualizations, making it an essential tool for infrastructure monitoring, application analytics, and operational intelligence. As Figure 5 is Grafana's main menu.



*Figure 5: The main menu of Grafana*

### Introduction of Zabbix

Zabbix is an open-source software for monitoring the performance and status of IT infrastructure such as networks, servers, virtual machines, and cloud services. Launched in 2001, it offers real-time data collection, analysis, and visualization, supporting both agent-based and agentless monitoring (SNMP, IPMI, JMX). Zabbix features alerting, customizable dashboards, detailed reporting, and automation, making it suitable for both small and large enterprises. It is free under the GPL license, with commercial support available. As Figure 6 is Zabbix's main menu



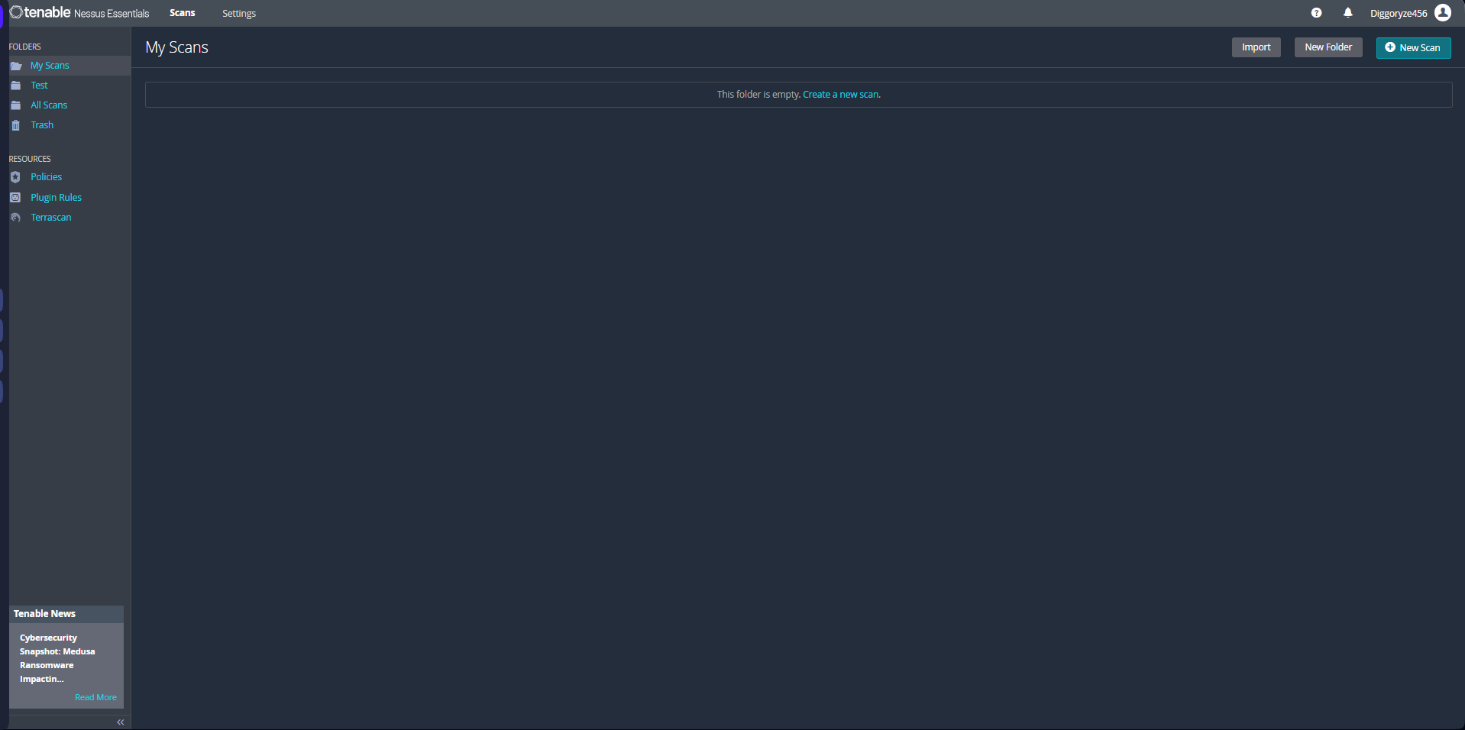
*Figure 6: The main menu of Zabbix*

### Introduction of Nessus

Nessus is a widely used vulnerability scanner developed by Tenable, Inc., designed to identify security flaws in networks, systems, and applications. Originally launched in 1998 by Renaud Deraison as a free, open-source tool, it transitioned to a proprietary model in 2005 with the release of Nessus 3. Today, it’s a leading solution in cybersecurity, trusted by organizations to detect vulnerabilities like software bugs, missing patches, and misconfigurations.

Nessus operates by scanning devices and networks using a vast, regularly updated database of known vulnerabilities, employing plugins to check for specific issues. It supports both agentless scanning (remotely testing systems without installation) and agent-based options for deeper visibility. Key features include detailed reporting, remediation suggestions, and customizable scans, making it ideal for security professionals, IT admins, and developers. Available in free (Nessus Essentials) and paid versions (Nessus Professional, Nessus Expert), it caters to diverse needs, from small-scale assessments to enterprise-level security management.

As Figure 7 is Nessus's main menu:



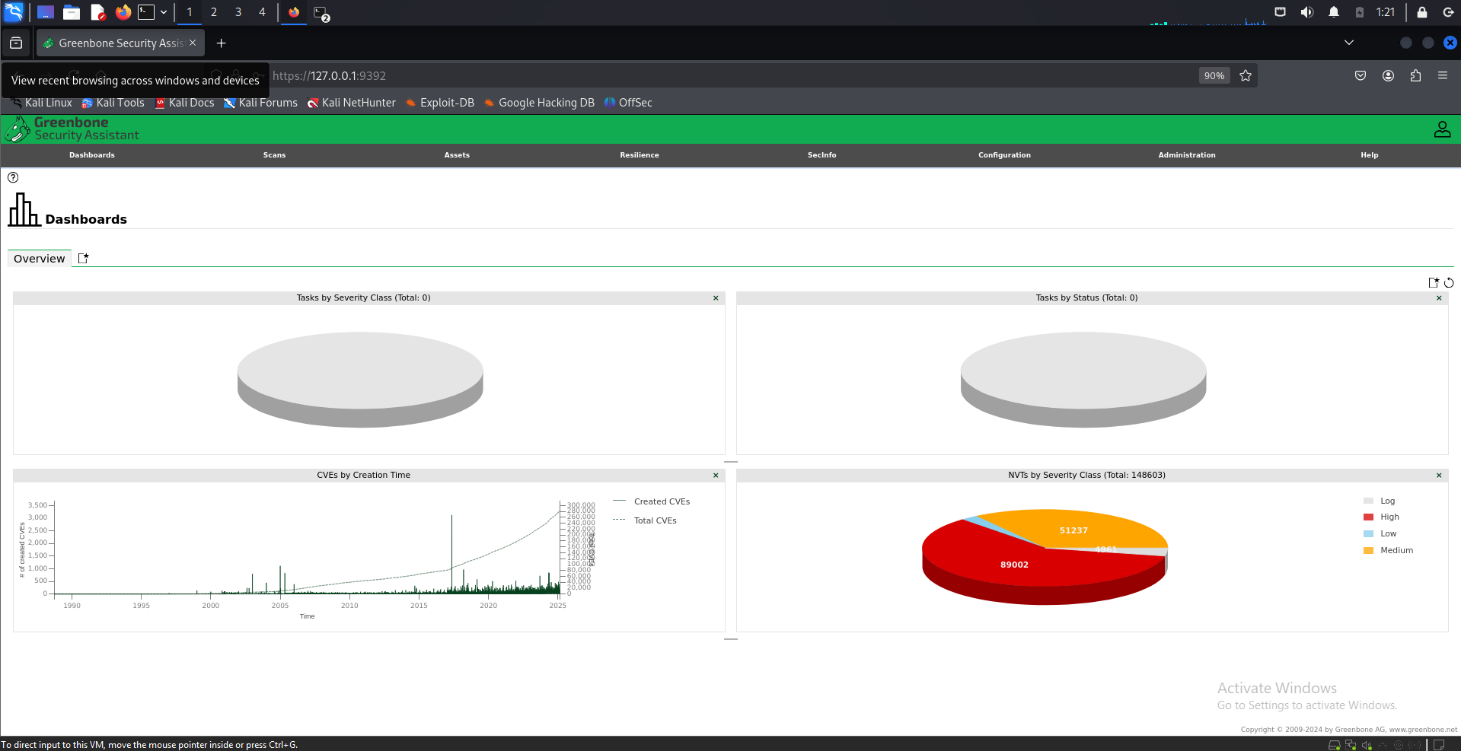
*Figure 7: The main menu of Nessus*

### Introduction of OpenVas

OpenVAS, or Open Vulnerability Assessment System, is an open-source vulnerability scanner designed to identify security weaknesses in networks, systems, and applications. It originated as a fork of Nessus in 2005 when Nessus became proprietary, and it’s now maintained by Greenbone Networks under the GNU General Public License (GPL). OpenVAS is a free, community-driven alternative for organizations seeking robust vulnerability management without licensing costs.

Built on a client-server architecture, OpenVAS uses a comprehensive, frequently updated vulnerability database (the Greenbone Community Feed) to scan for issues like unpatched software, misconfigurations, and exposed services. It performs agentless scanning via protocols like SSH, SNMP, and WMI, and offers features such as detailed reports, risk prioritization, and customizable scan profiles. While it lacks some of the polish and advanced integrations of commercial tools, its flexibility and cost-effectiveness make it popular among small businesses, security enthusiasts, and open-source advocates.

As Figure 8 is OpenVas's main menu:



*Figure 8: The main menu of OpenVas*

# Chapter 3: The Architectural Design

## Survey of Current State and Requirement

## Survey of Current State

The current landscape of IT infrastructure monitoring and security management relies heavily on a combination of tools to ensure system performance and protect against vulnerabilities. In this project, four key tools are evaluated: OpenVAS, Grafana, Zabbix, and Nessus. OpenVAS serves as an open-source vulnerability scanner, widely adopted for its cost-effectiveness and flexibility, though it lacks the advanced user interface and support of commercial alternatives [1]. Nessus, a proprietary vulnerability scanner, dominates the market with its extensive plugin ecosystem and detailed reporting, catering to both small and enterprise-level needs [2]. Zabbix provides real-time monitoring of system performance metrics (e.g., CPU, memory, network) across diverse environments, offering scalability and automation capabilities [3]. Grafana, a visualization platform, is currently used to create intuitive dashboards, integrating data from multiple sources for comprehensive analysis [4]. However, the lack of native integration among these tools often results in fragmented workflows, manual data aggregation, and delayed responses to threats or performance issues.

## Requirements

The architectural design must meet the following requirements to create an effective, integrated monitoring and vulnerability management system:

* **Vulnerability Detection**: Leverage OpenVAS and Nessus to perform comprehensive vulnerability scans, ensuring coverage of both open-source and proprietary scanning capabilities. The system should support scheduled and on-demand scans with minimal overlap in functionality.[1][2]
* **Performance Monitoring**: Utilize Zabbix to monitor real-time system health metrics (e.g., CPU usage, disk space, network traffic) across servers, virtual machines, and network devices, with automated alerts for anomalies.[3]
* **Data Visualization**: Integrate Grafana as the central visualization layer, pulling data from OpenVAS, Nessus, and Zabbix to provide unified dashboards for system performance and security status.[4]
* **Interoperability**: Ensure seamless data exchange between tools, such as feeding vulnerability data from OpenVAS and Nessus into Grafana for visualization and correlating it with Zabbix performance metrics.
* **Scalability**: Design the system to handle increasing numbers of devices and scan targets, supporting both small-scale and enterprise environments.[3]
* **Automation**: Enable automated workflows, such as triggering scans in response to performance degradation detected by Zabbix or generating remediation reports from vulnerability findings.[2]
* **Security and Accessibility**: Implement secure data handling (e.g., encrypted communication between components) and role-based access control for users interacting with the system.[1]
* **Cost Efficiency**: Maximize the use of OpenVAS’s open-source nature while integrating Nessus’s advanced features selectively for critical systems.

## Network System Analysis

The network system analysis examines the roles of Grafana, Zabbix, Nessus, and OpenVAS in monitoring and securing network infrastructure. Zabbix monitors network performance (e.g., bandwidth, latency) using SNMP and ICMP, but its data collection can strain bandwidth in large setups [3]. Nessus and OpenVAS scan for vulnerabilities, with Nessus offering faster, detailed scans via plugins and OpenVAS providing a cost-effective alternative, though both require careful scheduling to avoid network congestion [1][2]. Grafana integrates data from all tools to visualize network health and security through dashboards, with minimal bandwidth impact [4]. The architecture demands a centralized server, secure communication (e.g., TLS/SSL), network segmentation, and scalability planning to handle growing data volumes while ensuring performance and security.

# Chapter4:Project Performance and Evaluation

## Programs and Results

### Zabbix

#### A screenshot of a computer Description automatically generatedPrograms:

*Figure 9: Zabbix interface*

After spending time handling minor external tasks, I will go inside Zabbix to manage

A screenshot of a computer

Description automatically generatedmonitoring configurations and analyze system performance.

*Figure 10: Main menu of Zabbix interface*

#### A screenshot of a computer Description automatically generated

*Figure 11: Dashboard of Zabbix interface*

**Dashboard:** This is an interface that displays visual dashboards for administrators to view directly. Administrators can create multiple different dashboards, but only one dashboard can be viewed on a tab screen at a time.

From the Dashboard, users can quickly link to components such as Graphs, Screens, and Maps by adding desired elements to the **Favourite Graphs**, **Favourite Screens**, and **Favourite Maps** sections.

#### A screenshot of a computer Description automatically generated

*Figure 12: Dashboard of Zabbix interface*

#### A screenshot of a computer Description automatically generated

*Figure 13: Status of zabbix*

#### Results:

#### **System Status:** Displays the alert levels of hosts within each group.

#### A screenshot of a graph Description automatically generated

*Figure 14:System status of zabbix*

#### **Problems:** Displays all issues occurring with hosts in the groups, categorized by time.

#### A screenshot of a recovery program Description automatically generated

*Figure 15: Problems*

#### **Predefined Tables:** Used to display available **Graphs, Screens, and Maps**.

#### A screenshot of a computer Description automatically generated

*Figure 16: Graphs, Screens and Maps*

### Grafana

#### Programs:

First, when we access the Grafana login interface on the browser (as shown in Figure 9) via http://localhost:3000/ you need to log in to access the dashboard and monitoring features (as shown in Figure 2). Next, we will navigate through the menu to configure data sources, create dashboards, and set up visualizations for monitoring system performance (as shown in Figure 10).

*A screenshot of a computer

Description automatically generatedFigure 17: Login Grafana interface*

*A screenshot of a computer

Description automatically generatedFigure 18 : Main menu of Grafana*

After getting used to the Grafana interface, we will have various options available in the main menu. These include Dashboards – where we can visualize data, Explore – for querying and inspecting logs, and Alerting ( shown in Figure 11 ).

A screenshot of a computer

Description automatically generated

*Figure 19: Choices of Grafana*

#### Result:

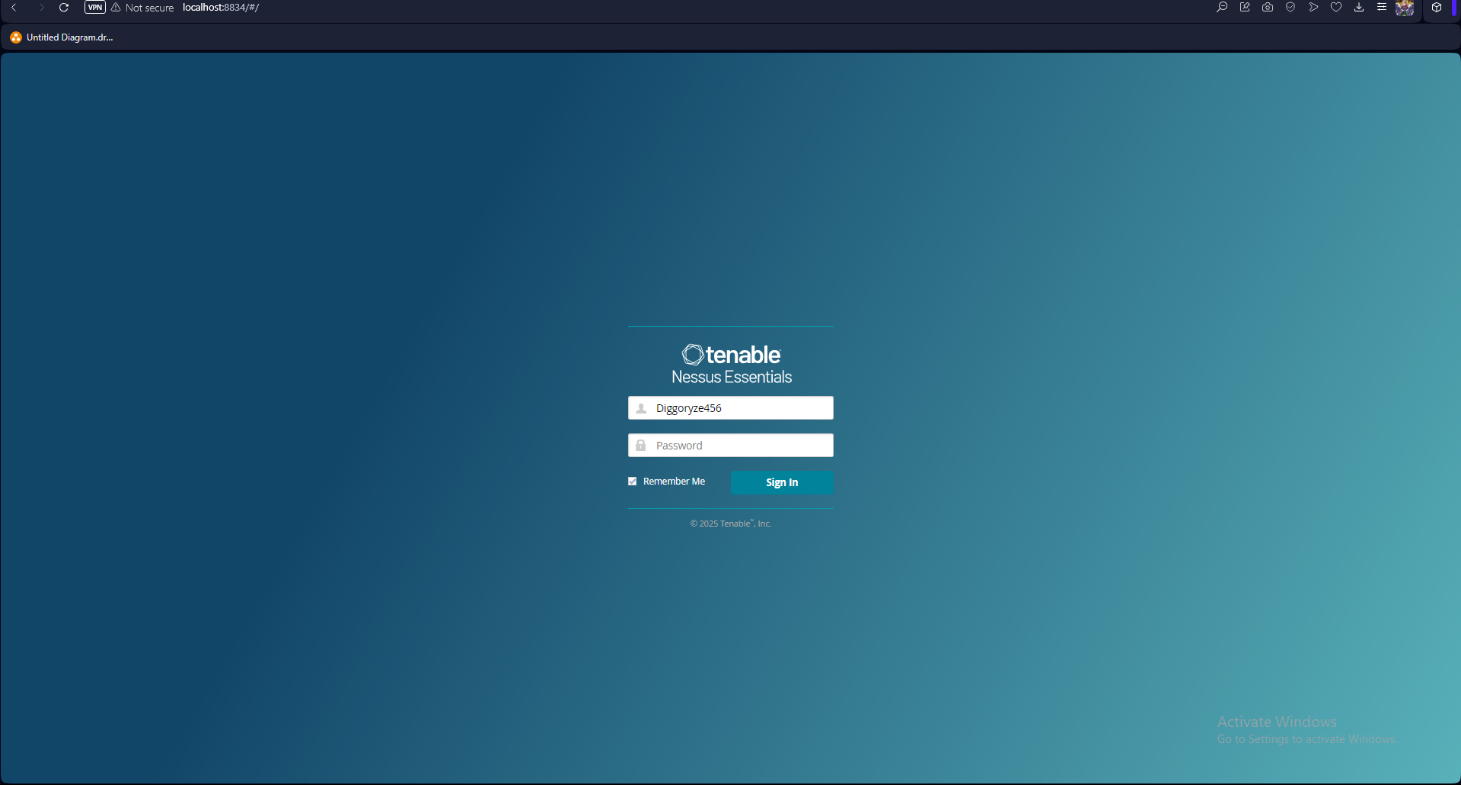
Here's a report on creating a Grafana Dashboard for MySQL monitoring ( Figure 12) below

*A screenshot of a computer

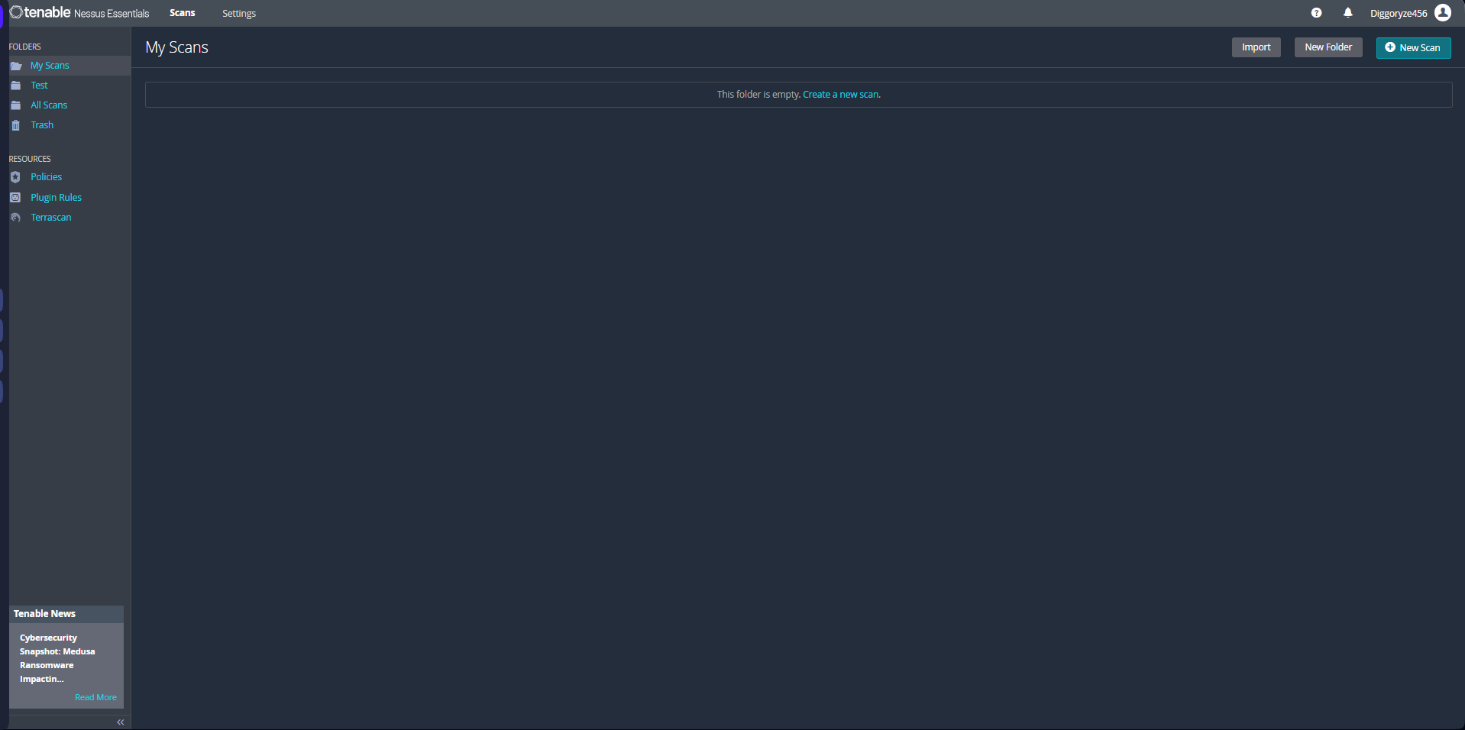
Description automatically generatedFigure 20: Edit panel of Grafana*

### Nessus

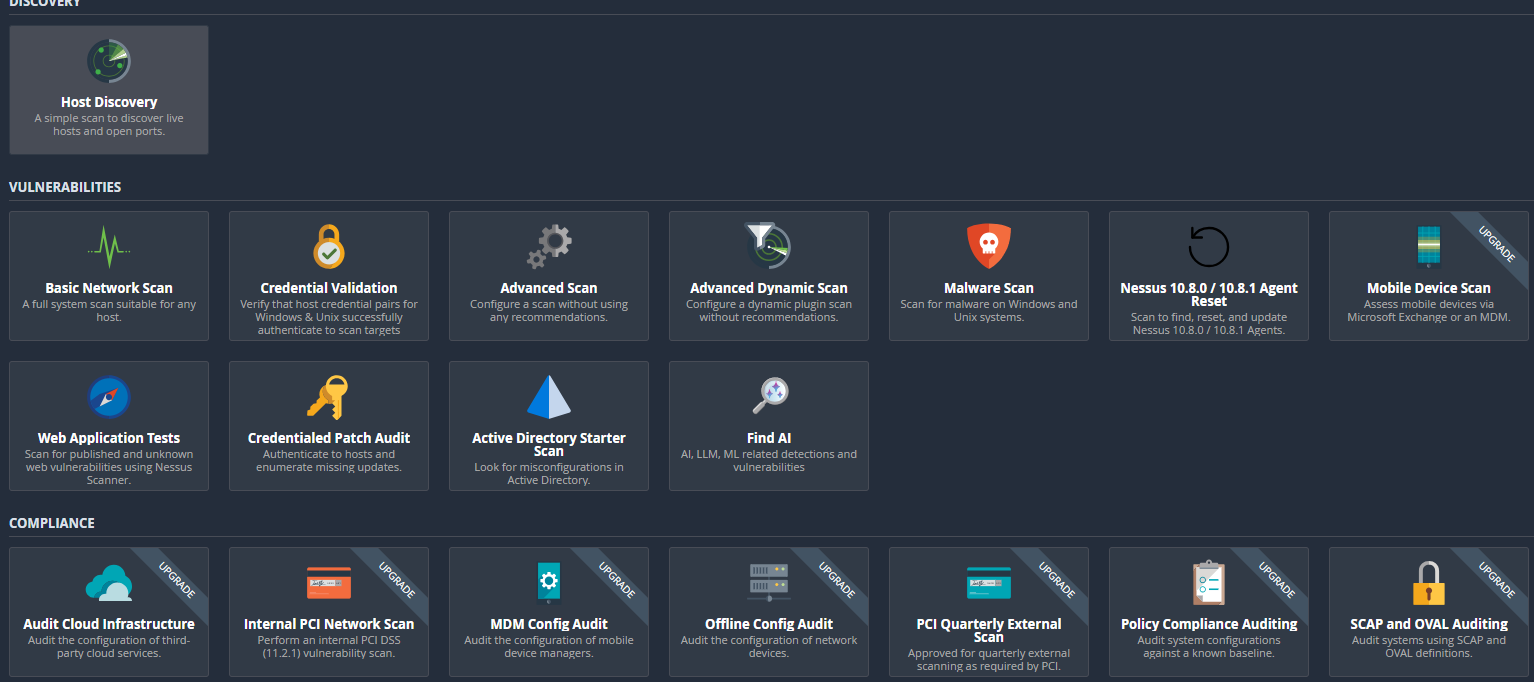
#### Program:

First, when we access the Nessus login interface on the Browser (as shown in Figure 15) via <https://localhost:8834/#/> or https: // <ip-server>: 8834 (if installed on the server), you need to log in to be able to manipulate on the menu of Nessus (as shown in Figure 16). Next we will manipulate scanning through the menu, And it will give us a lot of choices to scan in our network that is using (as shown in Figure 17).

*Figure 15: Login interface*

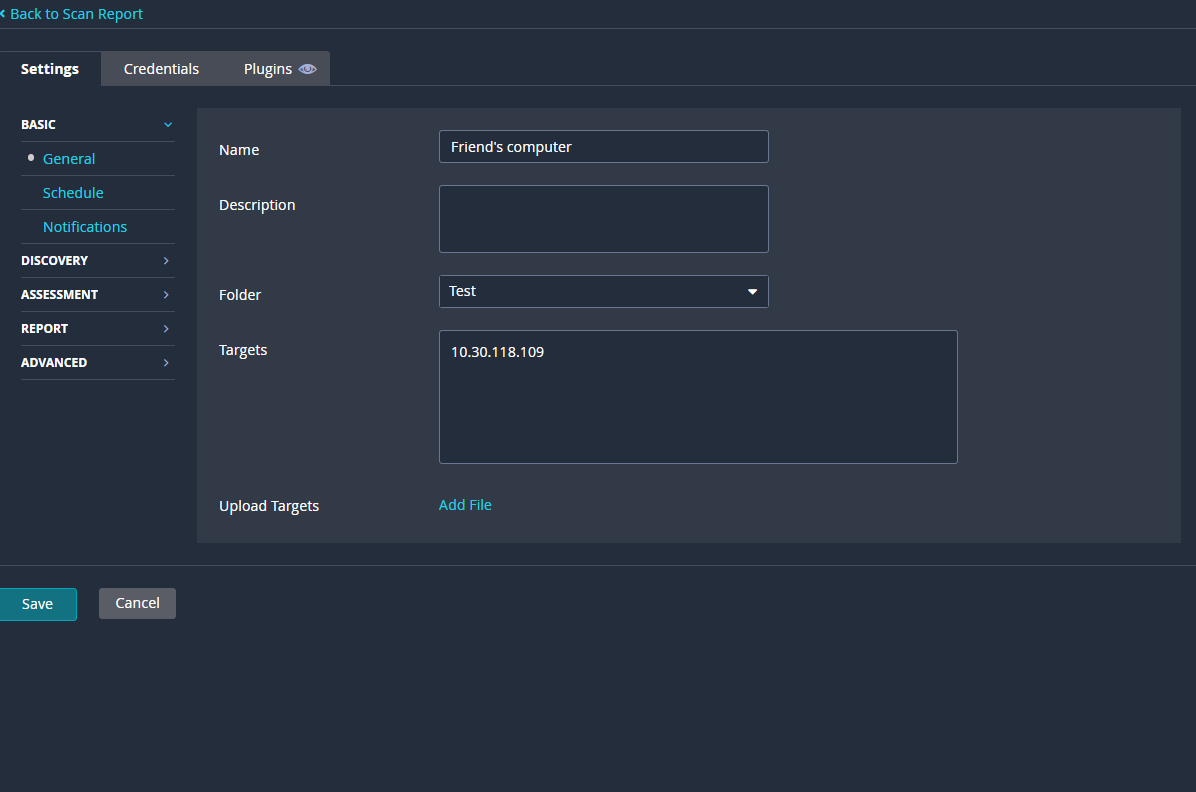
**

*Figure 16: Main Menu Of Nessus*

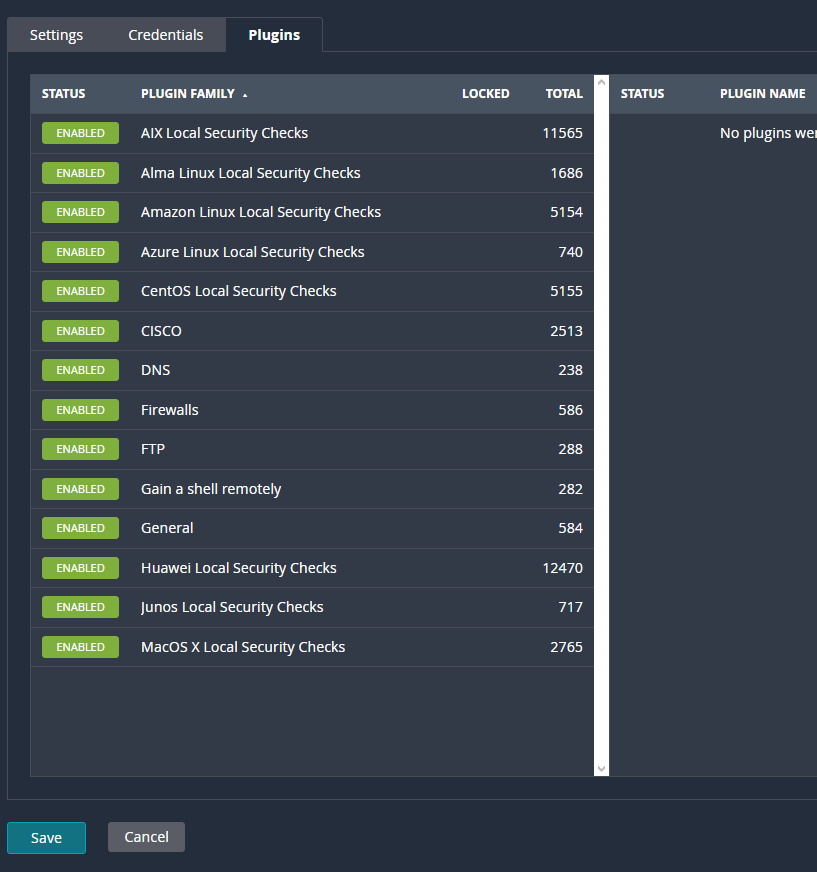


*Figure 17: Scanning function*

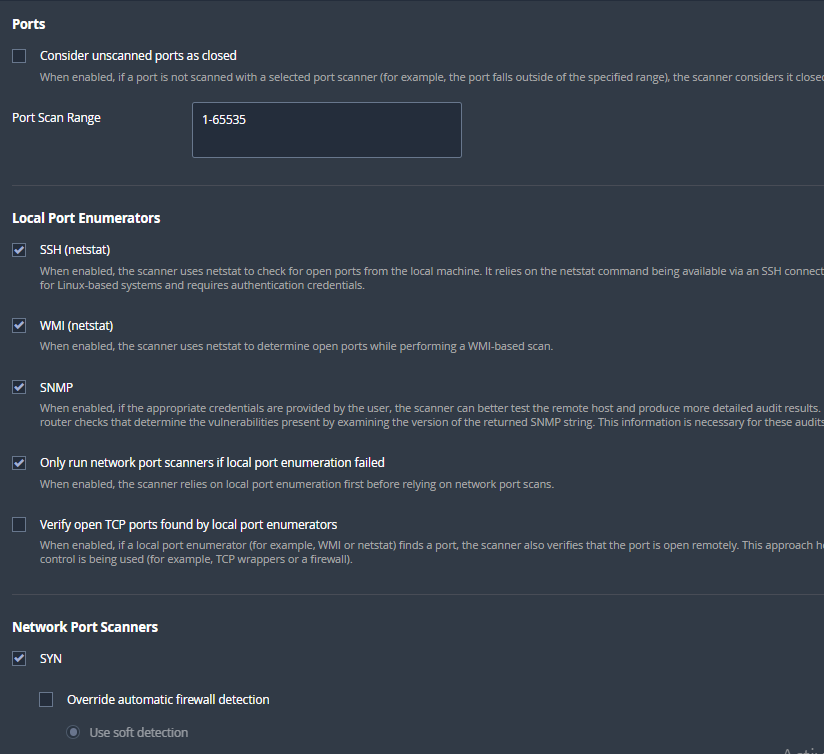
After getting used to scanning interfaces, we will have options for scanning as follows: Basic Network Scan - System overview (as shown in Figure 17). It can be seen that I was actively sweeping my friend's device with IP 10.30.118.109 (as shown in Figure 18).

*Figure 18: Setup for Basic Scanning*

And Nessus also supports other types of scanning, including Advanced Scanning. This mode performs a deeper analysis of vulnerabilities, identifying each one (e.g., EthGeneral, NeSettings...) to determine which service they belong to or using Nessus for detailed inspection. If necessary, the scan can be rerun with a more powerful configuration. Figure 19,20 and 21 show the setup process for this mode.

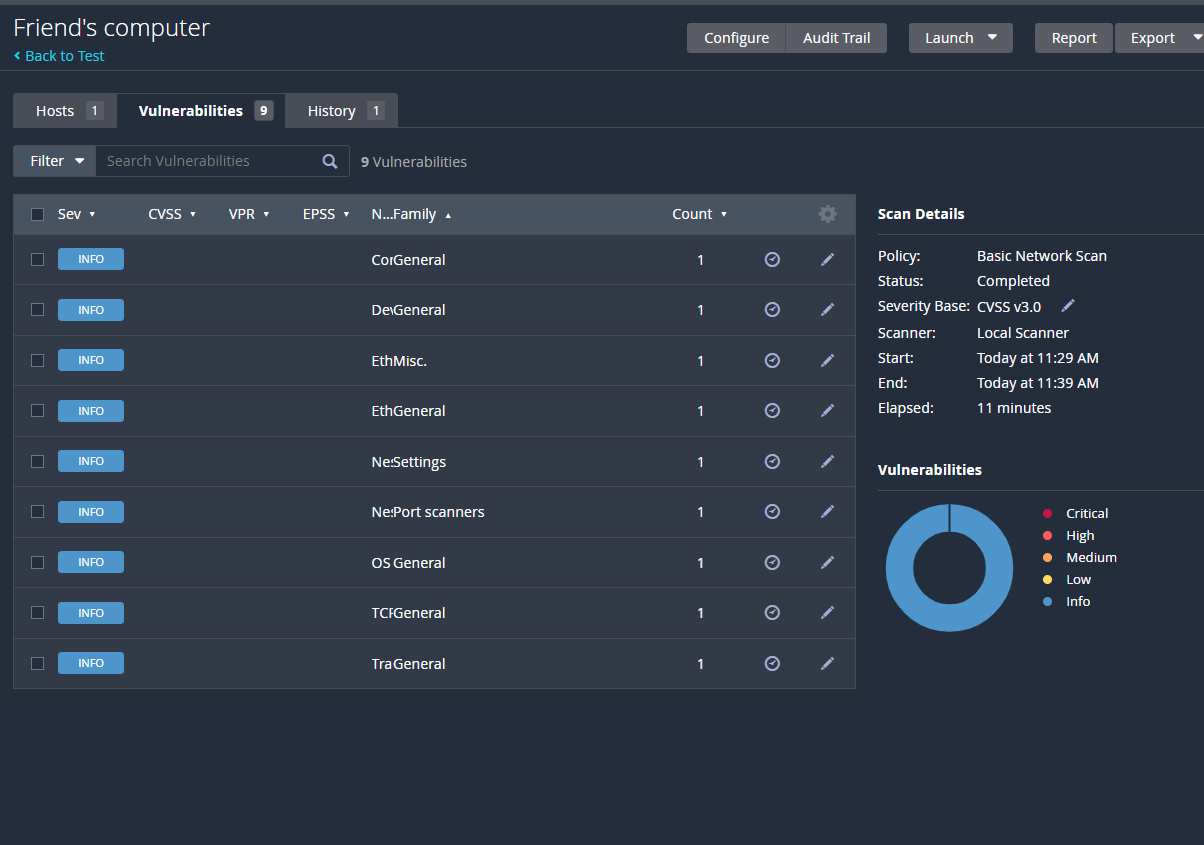
*Figure 19: Setup for Advanced Scanning* 

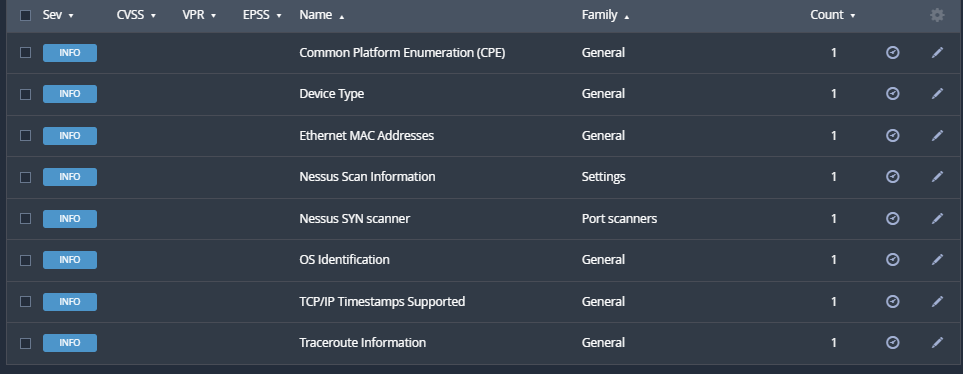
*Figure 20: Select plugins*

*Figure 21: Select more options*

#### Result:

After running the scanning, we obtain results: Figure 22 illustrates the results for Basic Scanning, while Figure 23 describes those for Advanced Scanning.

*Figure 22:* *Result For Basic Scanning*

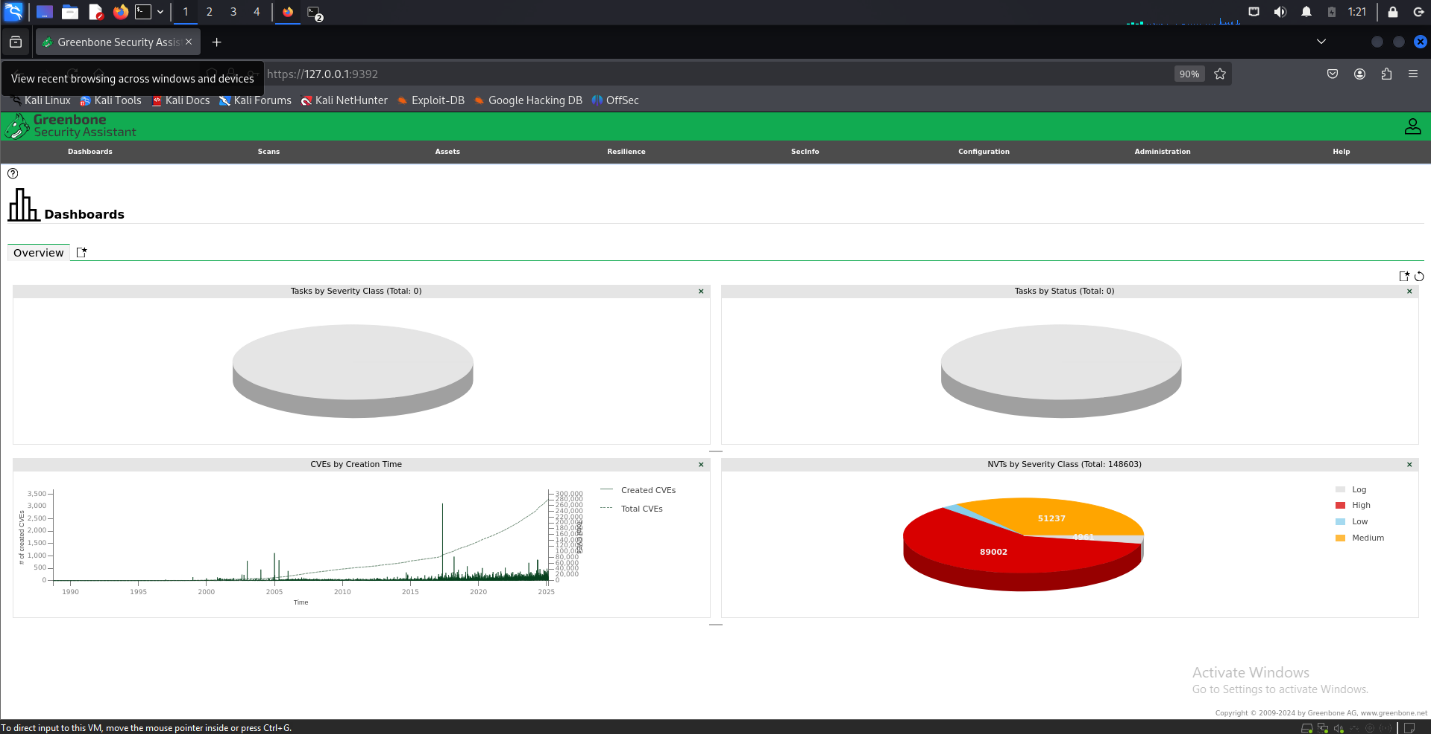
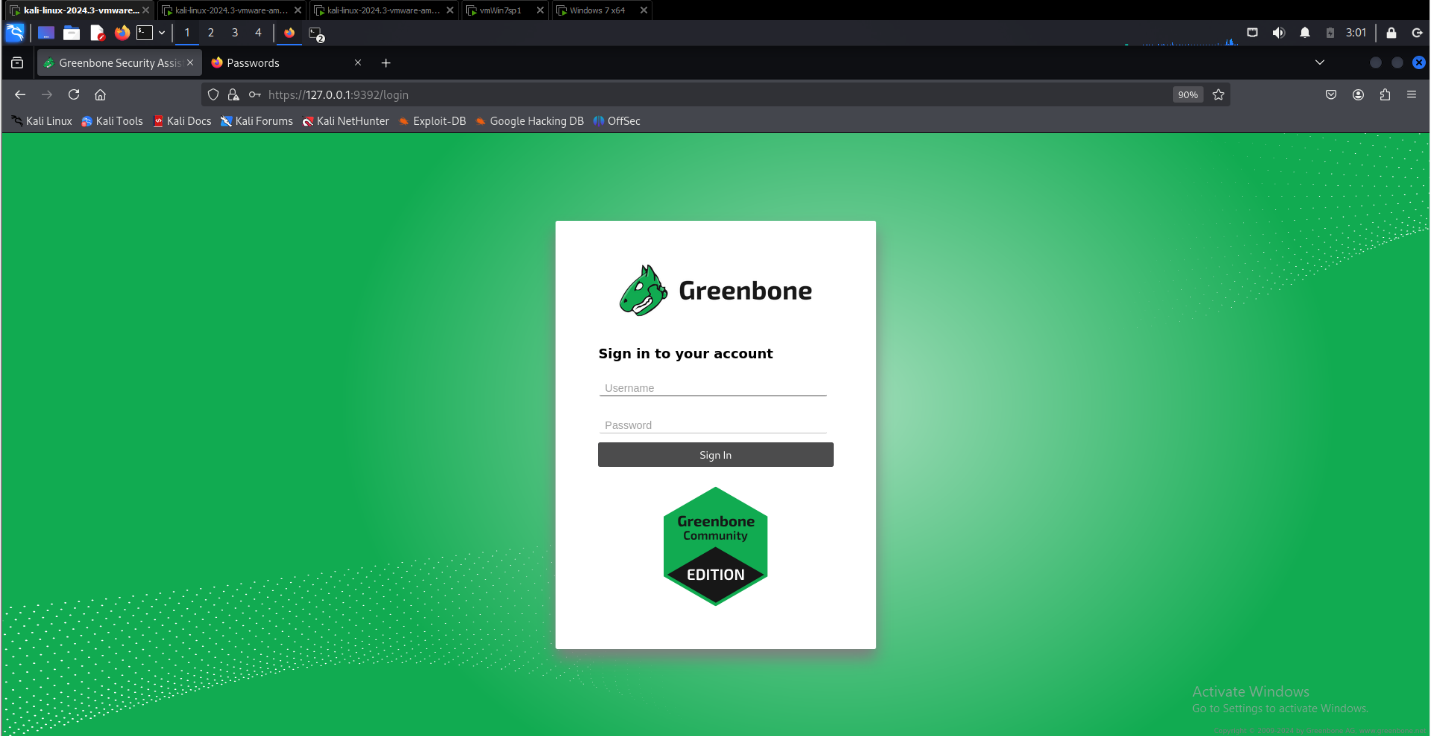


*Figure 23: Result for Advanced Scanning*

### OpenVas

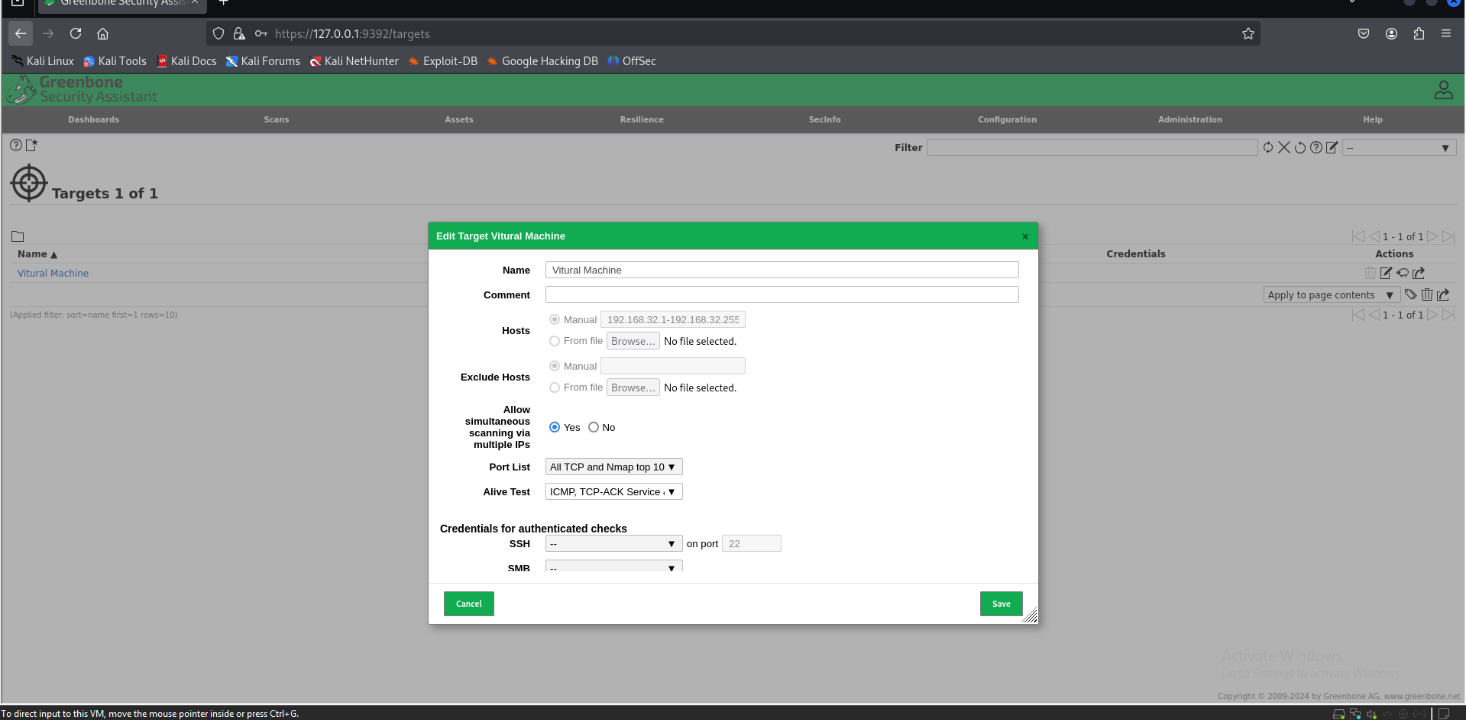
#### Program:

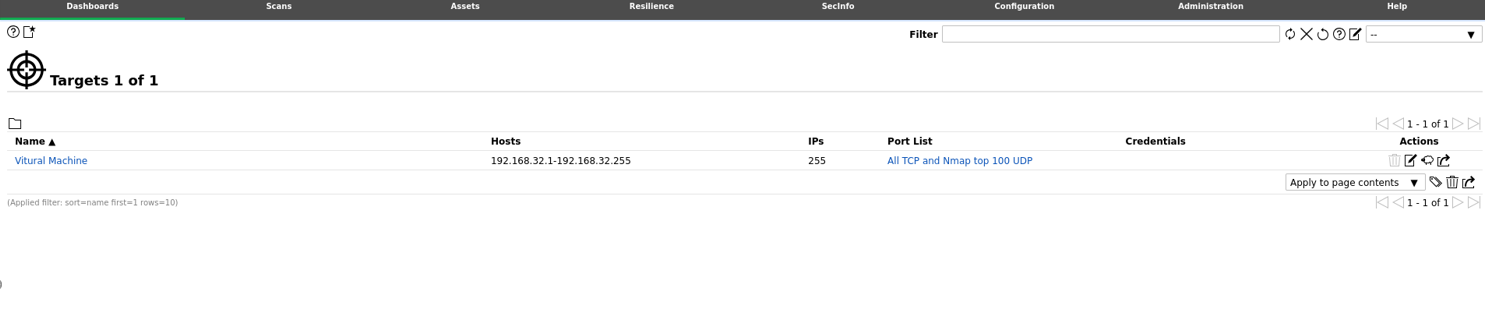
First, when we access the Nessus login interface on the Browser in the Kali Linux (as shown in Figure 24) via https://127.0.0.1:9392 or https://<IP-của-Kali>:9392 (if installed on the server), you need to log in to be able to manipulate on the menu of OpenVas (as shown in Figure 25).

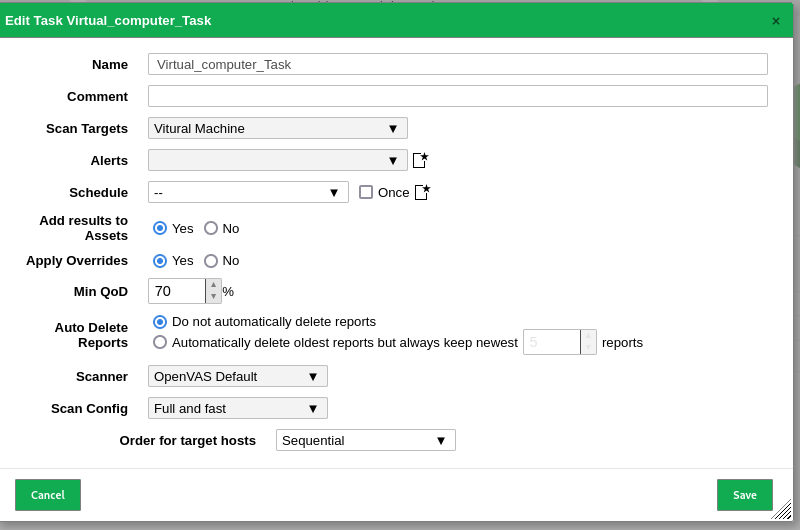
*Figure 24: Login interface* 

*Figure 25: Main Menu of OpenVas*

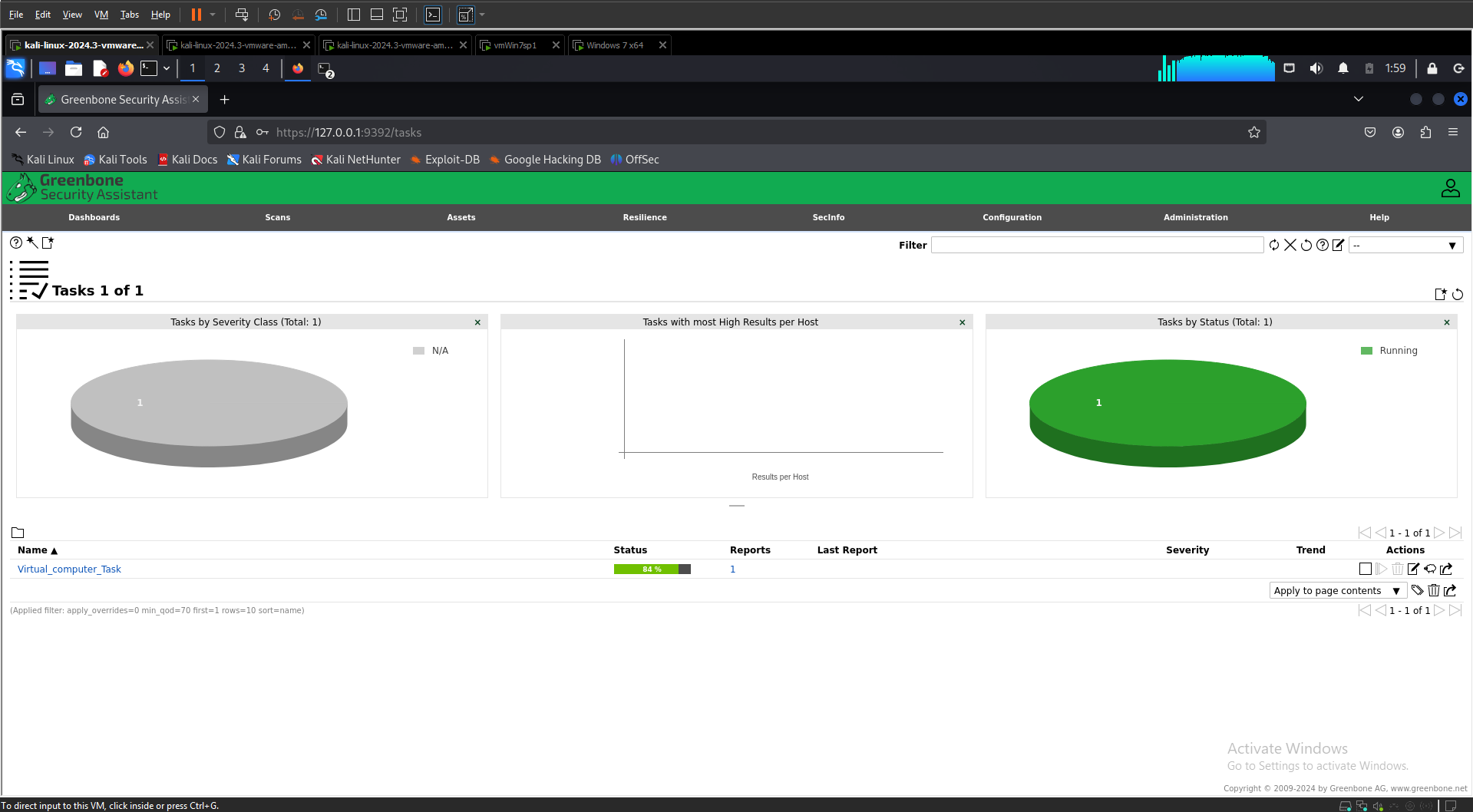
Creating a scan similar to Nessus through a web interface, as shown in Figure 26, involves setting up a specific scan object. Once created, this object can be monitored, as illustrated in Figure 27.

*Figure 26: Setup Targets*

*Figure 27: Getting Targets*

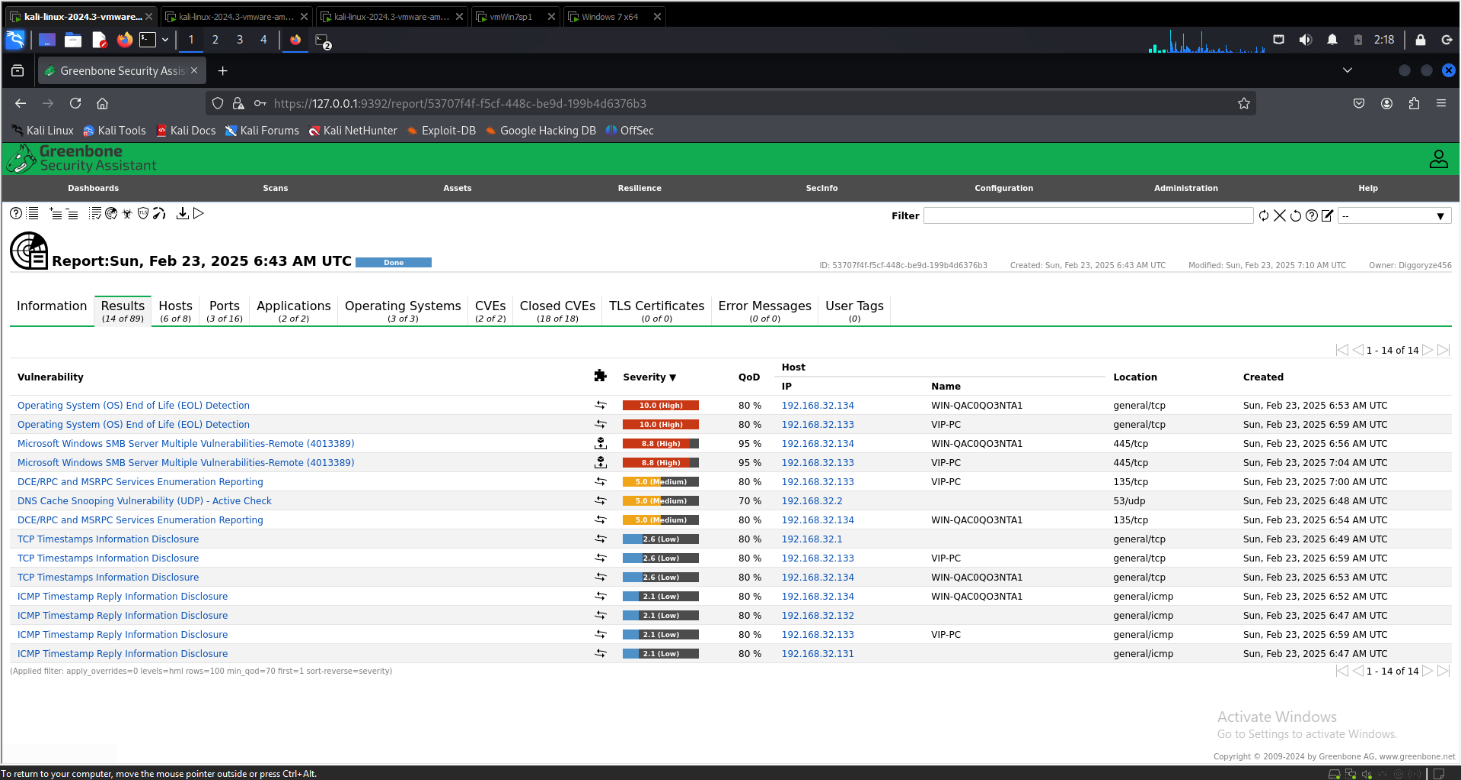
Next, a Task must be set up for the object to initiate the scanning process, as described in Figure 28. Finally, the system will enter a waiting state for the scanning to complete, as shown in Figure 29.

*Figure 28: Getting Targets*

*Figure 29: Watting for Scanning*

#### Result:

*Figure 30: Result for OpenVas*

*Figure 31: Details of Result*

The results reveal vulnerabilities ranging from critical to low severity. Critical vulnerabilities may include issues such as **Operating System (OS) End of Life (EOL) Detection** (10.0 - High) or **Microsoft Windows SMB Server Multiple Vulnerabilities (4013389 / MS17-010 - EternalBlue)** (8.8 - High). These critical vulnerabilities can lead to **loss of system control, remote attacks, and malware infections**.

Additionally, the scan also identifies **medium-severity vulnerabilities** (e.g., **DCE/RPC and MSRPC Services Enumeration** (5.0 - Medium)) and **low-severity issues** (e.g., **TCP & ICMP Timestamp Information Disclosure**).

## Solution for Mitigation

To enhance security and mitigate potential threats, we utilize four key tools: **Grafana, OpenVAS, Nessus, and Zabbix**. Each plays a crucial role in identifying vulnerabilities, monitoring system health, and ensuring proactive threat mitigation.

* **Grafana** – Used for real-time monitoring and visualization of security-related metrics. It helps track system performance, detect anomalies, and generate alerts based on predefined security thresholds.
* **OpenVAS** – Conducts vulnerability assessments by scanning systems for known security flaws. It helps identify weaknesses in the infrastructure and provides recommendations for mitigation.
* **Nessus** – Performs in-depth vulnerability scanning and compliance checks. By regularly scanning the network, it ensures that security gaps are identified and addressed before exploitation.
* **Zabbix** – Monitors network activity, server health, and application performance. It provides automated alerts and logs to detect suspicious behavior, allowing quick incident response.

## Future Development Direction

In the future, we aim to enhance security by integrating **Grafana, OpenVAS, Nessus, and Zabbix** into a centralized monitoring system. We plan to implement **automated incident response**, improve **scalability**, and extend **cloud security monitoring**. Additionally, we will integrate **threat intelligence feeds** to enhance vulnerability detection and develop **training programs** to strengthen security awareness. These improvements will ensure a **proactive and adaptive** security framework.

# Chapter 6: Conclusion

# Summary

This report explores the use of **Grafana, OpenVAS, Nessus, and Zabbix** for security monitoring and vulnerability management. Each tool plays a crucial role in identifying threats, analyzing system performance, and ensuring proactive mitigation. We discussed their integration, effectiveness in detecting vulnerabilities, and strategies to enhance security. Additionally, future developments focus on automation, scalability, cloud security, and improved threat intelligence integration.

# Conclusion

By leveraging **Grafana, OpenVAS, Nessus, and Zabbix**, we establish a **comprehensive security monitoring framework** that enhances threat detection and mitigation. Continuous improvement through **automation, cloud expansion, and training** will further strengthen our cybersecurity posture. These efforts will ensure a **resilient, proactive, and adaptive** security system against evolving threats.

# Reference

[1]. Greenbone Networks. (2023). OpenVAS: Vulnerability scanning for everyone, from <https://www.openvas.org/>

[2]. Tenable. (2024). Nessus: The world’s most widely deployed vulnerability scanner, from <https://www.tenable.com/products/nessus>

[3]. Zabbix SIA. (2023). Zabbix: Enterprise-class monitoring solution, from <https://www.zabbix.com/>

[4]. Grafana Labs. (2024). Grafana: The open observability platform, from <https://grafana.com/>