

## **Title of the project :**

### **Intelligent Threat Detection and Response: AI Integration in Cybersecurity Frameworks:-**

#### **Stage 1: SANS 20 - AI Based Threat**

Understanding SANS 20: Research and comprehend the SANS 20 framework and its AI-based threat components..

**Review Documentation:** Gather and study official SANS 20 documentation, whitepapers, and guidelines. Understand its structure, objectives, and the overall framework architecture.

**Identify Core Principles:** Analyze the fundamental principles of SANS 20, such as prioritization of cybersecurity controls, risk management, and their integration with AI-based threat mitigation.

**Explore Case Studies:** Investigate case studies or reports highlighting successful implementations of SANS 20, especially focusing on how AI contributes to threat identification and management within this framework.

#### **AI-Based Threat Identification Within SANS 20**

AI in Threat Mitigation: Research the specific role of AI and machine learning within the SANS 20 framework. Understand how AI is utilized to identify, analyze, and respond to cybersecurity threats.

Examine AI Algorithms: Explore various AI algorithms and techniques employed in threat identification, such as anomaly detection, behavior analysis, and predictive analytics, as per SANS 20's guidelines.

Study Integration Practices: Investigate best practices and recommended methodologies for integrating AI-driven threat identification into the SANS 20 framework.

#### **Stage 2: Nessus Plugins & Threat Detections And Response**

Understanding Nessus Plugins: Deep dive into the functionality and capabilities of Nessus plugins for threat detection.

#### **Plugin Catalog Exploration**

Plugin Database Review: Dive into the Nessus plugin database/catalog. Explore the range of plugins available, categorized based on vulnerability assessments, compliance checks, malware detection, etc.

Plugin Classification: Understand how plugins are categorized and organized within Nessus, focusing on their functionalities and intended uses for threat detection.

### Stage 3: Threat Detection Strategies

#### 1. Customizing Dashboards

Qradar allows to create customized dashboards that provide real-time visibility into crucial security metrics and events. Tailor these dashboards according to specific requirements, ensuring that we have a clear overview of organization's security posture and any emerging threats.

#### 2. Setting Up Alerts and Notifications

To prevent potential security incidents from going unnoticed, configure alerts and notifications within Qradar system. Determine the thresholds and conditions for generating alerts and ensure that we have appropriate escalation procedures in place to address any identified threats.

#### 3. SOC Dashboard Management

Manage the SOC dashboard effectively by regularly reviewing and fine-tuning it. This includes ensuring that the right metrics and key performance indicators (KPIs) are being tracked, and that the dashboard provides actionable insights to SOC analysts. Regularly update and optimize the dashboard based on the evolving security landscape organizational requirements.

#### 4. Continuous Monitoring and Analysis

Maintain a proactive approach to security by continuously monitoring and analyzing the data collected by Qradar. This allows us to quickly detect any anomalies or suspicious activities and respond promptly to mitigate potential risks. Use the insights gained from monitoring and analysis to improve security operations and strengthen organization's defenses.

By following these steps, we can enhance the security operations and effectively manage the SIEM Qradar and SOC dashboard.

List of teammates– S.No	Name	Collage	Contact
1	M.Malathi	National Engineering College	9500468498

### List of Vulnerability Table:

S.no	Vulnerability Name	CWE - No
1	172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	CVE CVE-2023-25690 CVE CVE-2023-27522 XREF IAVA:2023-A-0124
2	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	IAVA: 2023-A-0047-S CVE: CVE-2006-20001, CVE-2022-36760, CVE- 2022-37436
3	cpe:/a:apache:http_server	EDB-ID: 21002 OWASP: OWASP-CM-004 BID: 3009 CVE: CVE-2001-0731

### REPORT:-

#### 1. Vulnerability Name:-

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

#### CWE :

CWE-444 - Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

#### OWASP Category:

Security Misconfiguration

#### Description:-

Just like misconfigured access controls, more general security configuration errors are huge risks that give attackers quick, easy access to sensitive data and site areas.

#### 2. Vulnerability Name:

Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

#### CWE :

moderate: mod\_dav out of bounds read, or write of zero byte (CVE-2006-20001)A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

This issue affects Apache HTTP Server 2.4.54 and earlier.

#### OWASP Category:

Insufficient Logging and Monitoring

**Description:-**

Failing to log errors or attacks and poor monitoring practices can introduce a human element to security risks. Threat actors count on a lack of monitoring and slower remediation times so that they can carry out their attacks before you have time to notice or react

**3. Vulnerability Name:-**

cpe:/a:apache:http\_server

**CWE :**

CVE-2001-0731

**OWASP Category:**

Using Components with Known Vulnerabilities

**Description:-**

No matter how secure your own code is, attackers can exploit APIs, dependencies and other third-party components if they are not themselves secure.

**Detecting vulnerability is the stage 1 where we understand web application testing using Qradar.**

**Stage-2****Stage 2****Overview of Nessus:**

Nessus is a widely used vulnerability assessment tool developed by Tenable Network Security. It is designed to identify and assess vulnerabilities in computer systems, networks, and applications. Nessus helps organizations identify potential security weaknesses in their IT infrastructure by conducting comprehensive scans and providing detailed reports on identified vulnerabilities.

Key features of Nessus include:

1. **Vulnerability Scanning:** Nessus scans networks, systems, and applications for known vulnerabilities. It uses a vast database of vulnerability checks and plugins to identify security issues.
2. **Remote and Local Scanning:** Nessus can perform both remote and local vulnerability scans. Remote scans are conducted over the network, while local scans are executed on the target system itself.
3. **Compliance Checking:** The tool can assess systems against various compliance standards and policies, helping organizations meet regulatory requirements.
4. **Customizable Scans:** Users can configure scans based on their specific needs, such as targeting certain IP ranges, ports, or specific vulnerabilities.
5. **Reporting:** Nessus generates detailed reports after each scan, outlining discovered vulnerabilities, their severity levels, and recommendations for mitigation.
6. **Risk Assessment:** It assigns severity levels (such as high, medium, or low) to vulnerabilities based on their potential impact and likelihood.
7. **Continuous Monitoring:** Nessus supports continuous monitoring by allowing regular scans to ensure that new vulnerabilities are promptly identified and addressed.
8. **Integration:** Nessus can integrate with other security tools and platforms, enabling seamless collaboration and remediation.

**Target website :**

www.nec.edu.in (National Engineering College, Kovilpatti, Tamilnadu)

**Target ip address:**

103.84.178.40

List of Vulnerability:

S. No.	SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
1	Critical	9.8	9.4	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
2	Critical	9.0	6.5	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
3	Medium	6.5	-	51192	SSL Certificate Cannot Be Trusted
4	Medium	5.3	2.2	10704	Apache Multiviews Arbitrary Directory Listing

## REPORT:-

**1. Vulnerability Name:** Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

**Severity:** Critical

**Plugin:** 172186

**Port:** 443 / tcp / www

### Description:

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory. - HTTP request splitting with mod\_rewrite and mod\_proxy: Some mod\_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod\_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.\*) http://example.com:8080/elsewhere?\$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690) - Apache HTTP Server: mod\_proxy\_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod\_proxy\_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client. Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

### solution:

Upgrade to Apache version 2.4.56 or later.

**Business Impact:** 1. Website Outages: Exploiting vulnerabilities in the web server could lead to crashes, outages, or denial-of-service attacks, causing the organization's website to become unavailable. This can result in lost revenue, damage to reputation, and customer frustration.

2. Data Breaches: Depending on the nature of the vulnerabilities, attackers might be able to gain unauthorized access to sensitive data or server configurations. This could result in data breaches, compromising customer information, proprietary data, or sensitive business data.

## **2. Vulnerability Name:** Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

**Severity:** Critical

**Plugin:** 170113

**Port:** 443 / tcp / www

### **Description:**

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory. - A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001) - Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod\_proxy\_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. (CVE-2022-36760) - Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

### **solution:**

Upgrade to Apache version 2.4.56 or later.

**Business Impact:** 1. Website Outages: Exploiting vulnerabilities in the web server could lead to crashes, outages, or denial-of-service attacks, causing the organization's website to become unavailable. This can result in lost revenue, damage to reputation, and customer frustration.

2. Malware Distribution: If attackers gain control over a compromised web server, they might use it to distribute malware or launch attacks on visitors. This can lead to infections on users' computers, which could have legal, financial, and reputational implications.

## **3. Vulnerability Name:** SSL Certificate Cannot Be Trusted

**Severity:** Medium

**Plugin:** 51192

**Port:**

4444 / tcp /

www

4443 / tcp /

**Competitive Impact:** A publicized security incident could cause customers to lose confidence in the organization's ability to secure their data. This loss of trust might drive customers to competitors who are perceived to have stronger security practices.

**Reputation Damage:** Publicly known vulnerabilities and breaches can damage an organization's reputation, eroding trust and confidence among customers, partners, and stakeholders.

## **4. Vulnerability Name:** Apache Multiviews Arbitrary Directory Listing

**Severity:** Medium

**Plugin:** 10704

**Port:** 80 / tcp / www

### **Description:**

The Apache web server running on the remote host is affected by an information disclosure vulnerability. An unauthenticated, remote attacker can exploit this, by sending a crafted request, to display a listing of a remote directory, even if a valid index file exists in the directory. For Apache web server later than 1.3.22, review listing directory configuration to avoid disclosing sensitive information

### **solution:**

Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews.

**Business Impact:**

**Business Disruption:** Exploiting vulnerabilities could disrupt the organization's online services, impacting operations and customer interactions. This can lead to lost productivity, missed business opportunities, and unhappy customers.

**Legal and Regulatory Consequences:** Depending on the nature of the vulnerabilities and the data involved, organizations might face legal consequences for not adequately protecting customer data or for not complying with data protection regulations

### **Stage 3**

#### **Report**

#### **Title :- Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management**

#### **Soc**

**Security Operations Center (SoC):** In the context of cybersecurity, a Security Operations Center (SoC) is a centralized unit within an organization responsible for monitoring, detecting, responding to, and mitigating security incidents and threats. A SoC typically uses a combination of technology, processes, and skilled security analysts to monitor network traffic, system logs, and other data sources for signs of unauthorized access, malicious activity, and potential vulnerabilities. When a potential security threat is detected, the SoC takes appropriate actions to investigate, contain, and remediate the threat. The goal of a SoC is to enhance an organization's overall security posture by ensuring a rapid and effective response to security incidents.

#### **SOC Cycle**

The SoC cycle is iterative and adaptive. As new threats emerge and technologies evolve, the SoC continually refines its processes and technologies to effectively detect, respond to, and mitigate evolving cybersecurity risks. Effective communication, collaboration among teams, and staying up-to-date with the latest threat landscape are key factors for the success of a Security Operations Center.

- ☐ Preparation, planning and prevention
- ☐ Monitoring, detection and response
- ☐ Recovery, refinement and compliance

#### **Siem**

**SIEM** stands for Security Information and Event Management. It's a comprehensive approach to cybersecurity management that combines security information management (SIM) and security event management (SEM) into a single solution. SIEM systems provide a centralized platform for collecting, analyzing, correlating, and responding to security-related data from various sources across an organization's IT environment.

Here's an overview of the key components and functions of a SIEM system:

1. **Data Collection:** SIEM systems gather data from a wide range of sources, including network devices, servers, applications, security appliances, and more. This data includes logs, events, and other security-related information.
2. **Event Correlation:** SIEM tools analyze and correlate the collected data to identify patterns, anomalies, and potential security incidents. By connecting seemingly unrelated events, SIEM can detect complex threats that might go unnoticed by individual security tools.
3. **Alert Generation:** When the SIEM identifies suspicious or malicious activities based on predefined rules or behavioral analysis, it generates alerts for security analysts to investigate further.
4. **Incident Response:** SIEM systems facilitate incident response by providing tools for security analysts to investigate alerts, conduct forensic analysis, and take appropriate actions to mitigate threats. This might include isolating compromised systems, blocking malicious IP addresses, and more.
5. **Real-time Monitoring:** SIEM solutions offer real-time monitoring of security events, enabling organizations to respond quickly to ongoing threats and attacks.

6. Reporting and Dashboards: SIEM generates detailed reports and visual dashboards that provide insights into the organization's security posture, trends, and potential vulnerabilities. This information is useful for compliance, audits, and management decisions.
7. Compliance and Regulatory Requirements: SIEM systems help organizations meet compliance requirements by collecting and storing the necessary data to demonstrate adherence to security policies and regulations.
8. Threat Detection and Hunting: SIEM platforms support proactive threat hunting by allowing security analysts to search for suspicious patterns and behaviors that might not trigger predefined alerts.
9. Data Correlation: SIEM tools correlate data from different sources, such as user activity logs, network traffic, and system logs, to provide a holistic view of security incidents.
10. Log Management: SIEM includes log management capabilities, ensuring that logs from various sources are securely stored, archived, and easily accessible for analysis and compliance purposes.
11. Integration: SIEM systems can integrate with other security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, and more, to enhance overall threat detection and response capabilities.

SIEM solutions play a crucial role in modern cybersecurity strategies by providing organizations with the ability to monitor, detect, and respond to security threats in a more centralized and efficient manner. They help organizations achieve better visibility into their IT environment and improve their overall security posture.

### **My college network information**

**(Through Nessus)**

IP:192.168.56.1

DNS:ITUG-II26.dc.cds

Start:Today at 2:16 PM

End:Today at 2:17 PM

Elapsed:a few seconds

## **Threat intelligence**

Threat intelligence refers to the collection, analysis, and dissemination of information about potential or existing cybersecurity threats. It involves gathering data about various types of cyber threats, including malware, vulnerabilities, attack techniques, threat actors, and indicators of compromise (IoCs), and then converting this data into actionable insights that help organizations protect their systems and data.

Threat intelligence helps organizations stay ahead of cyber threats by providing valuable context and information to inform decision-making and enhance their overall cybersecurity posture. Here are some key aspects of threat intelligence:

**Data Collection:** Threat intelligence involves collecting data from a wide range of sources, including security research reports, security vendors, open-source intelligence, government agencies, industry groups, and proprietary sources.

**Analysis:** The collected data is analyzed to identify patterns, trends, and emerging threats.

Analysts work to understand the tactics, techniques, and procedures (TTPs) employed by threat actors.

**Classification:** Threat intelligence is often categorized into different levels based on the level of specificity and relevance. This can include strategic intelligence (high-level trends), operational intelligence (specific threats), and tactical intelligence (technical details).

**Indicators of Compromise (IoCs):** IoCs are specific artifacts associated with a threat, such as IP addresses, domain names, file hashes, and URLs. Threat intelligence provides IoCs that organizations can use to detect and block threats in their environments.

**Threat Actor Profiles:** Threat intelligence provides information about the motivations, capabilities, and characteristics of threat actors and hacking groups. This helps organizations understand potential adversaries.

**Vulnerability Intelligence:** Threat intelligence includes information about newly discovered vulnerabilities in software and systems, helping organizations prioritize patching efforts.

**Sharing and Collaboration:** Organizations can share threat intelligence within their industry or



sector to collectively defend against common threats. Sharing threat intelligence helps the broader community respond faster to emerging threats. Incident Response: Threat intelligence supports incident response by providing information that helps organizations identify the extent of a breach, mitigate its impact, and prevent future attacks. Proactive Defense: Threat intelligence allows organizations to proactively identify and address vulnerabilities and threats before they are exploited. Security Automation: Threat intelligence feeds can be integrated into security tools and platforms to automate threat detection and response processes. Risk Management: Threat intelligence assists in understanding the potential risks associated with specific threats, helping organizations allocate resources more effectively. Situational Awareness: Threat intelligence provides a clearer picture of the threat landscape, enabling organizations to make informed decisions about their security strategies. Cybersecurity Strategy: Organizations can use threat intelligence to shape their overall cybersecurity strategies, adapt to evolving threats, and allocate resources appropriately. Threat intelligence is a dynamic field that requires continuous monitoring of the threat landscape. It's an essential component of modern cybersecurity, helping organizations proactively defend against increasingly sophisticated cyber threats.

### **Incident response**

Incident response is a structured approach that organizations follow to effectively manage and mitigate the impact of cybersecurity incidents. An incident can include any unauthorized or unexpected event that poses a risk to an organization's IT systems, data, operations, or overall security posture. Incident response aims to minimize damage, restore normal operations, and prevent similar incidents in the future.

Create a detailed plan that outlines roles, responsibilities, communication procedures, escalation paths, and specific actions to be taken during different types of incidents.

Identify individuals from various departments (IT, security, legal, PR) who will be responsible for different aspects of incident handling.

Define priorities: Classify incidents based on their severity and potential impact to prioritize responses.

Detect incidents: Monitor logs, alerts, and security tools to identify unusual activities or signs of a potential incident.

### **QRadar & understanding about tool**

IBM QRadar is a security information and event management (SIEM) solution designed to help organizations detect and respond to security threats and incidents in real-time. It offers advanced capabilities for collecting, analyzing, and correlating security data from various sources to provide insights into potential threats and vulnerabilities. QRadar is widely used by enterprises and organizations to enhance their cybersecurity posture.

- QRadar collects data from various sources, including network devices, servers, applications, firewalls, and endpoints.
- It supports log and event collection using various protocols, such as syslog, SNMP, and more.
- QRadar uses advanced correlation techniques to analyze collected data and identify patterns, anomalies, and potential security incidents.
- It correlates events in real-time to provide a comprehensive view of the organization's security posture.
- QRadar employs predefined rules and custom rules to detect suspicious activities and potential threats.
- When a rule is triggered, QRadar generates alerts with details about the detected incident.
- QRadar uses behavioral analytics to identify deviations from normal behavior, helping to detect unknown threats and insider threats.
- The solution provides tools for security analysts to investigate alerts and incidents in-depth.
- Analysts can use visualizations, search capabilities, and context-rich data to understand the scope and impact of incidents.

- QRadar supports forensic analysis by providing historical data for incidents, allowing analysts to backtrack and understand the sequence of events.
- QRadar offers customizable dashboards and reports that provide insights into security events, trends, and risks.
- Reports can be used for compliance audits, management reporting, and sharing insights with stakeholders.

QRadar integrates with threat intelligence feeds to enhance threat detection and provide context about known threats.

- QRadar can be integrated with other security tools, such as vulnerability scanners, endpoint protection, and identity and access management solutions.
- QRadar supports automation of response actions to quickly mitigate threats.
- It can be integrated with incident response playbooks to streamline response procedures.
- QRadar can analyze user behavior to detect unusual or risky activities.
- QRadar can monitor and secure cloud environments, on-premises systems, and hybrid infrastructures.
- QRadar provides features to assist organizations in meeting compliance requirements.
- IBM QRadar is a comprehensive SIEM solution that helps organizations detect, respond to, and mitigate cybersecurity threats effectively. Its advanced features, integration capabilities, and user-friendly interface make it a popular choice for organizations seeking to enhance their security operations.

## **Conclusion :-**

### **Stage 1:**

Maintain a proactive approach to security by continuously monitoring and analyzing the data collected by QRadar. This allows us to quickly detect any anomalies or suspicious activities and respond promptly to mitigate potential risks. Use the insights gained from monitoring and analysis to improve overall security operations and strengthen our organization's defenses.

### **Stage 2 :**

Nessus is a widely used vulnerability assessment tool developed by Tenable Network Security. It is designed to identify and assess vulnerabilities in computer systems, networks, and applications. Nessus helps organizations identify potential security weaknesses in their IT infrastructure by conducting comprehensive scans and providing detailed reports on identified vulnerabilities.

### **Stage 3 :**

A SoC typically uses a combination of technology, processes, and skilled security analysts to monitor network traffic, system logs, and other data sources for signs of unauthorized access, malicious activity, and potential vulnerabilities. When a potential security threat is detected, the SoC takes appropriate actions to investigate, contain, and remediate the threat. SIEM is a comprehensive approach to cybersecurity management that combines security information management (SIM) and security event management (SEM) into a single solution. SIEM systems provide a centralized platform for collecting, analyzing, correlating, and responding to security-related data from various sources across an organization's IT environment.

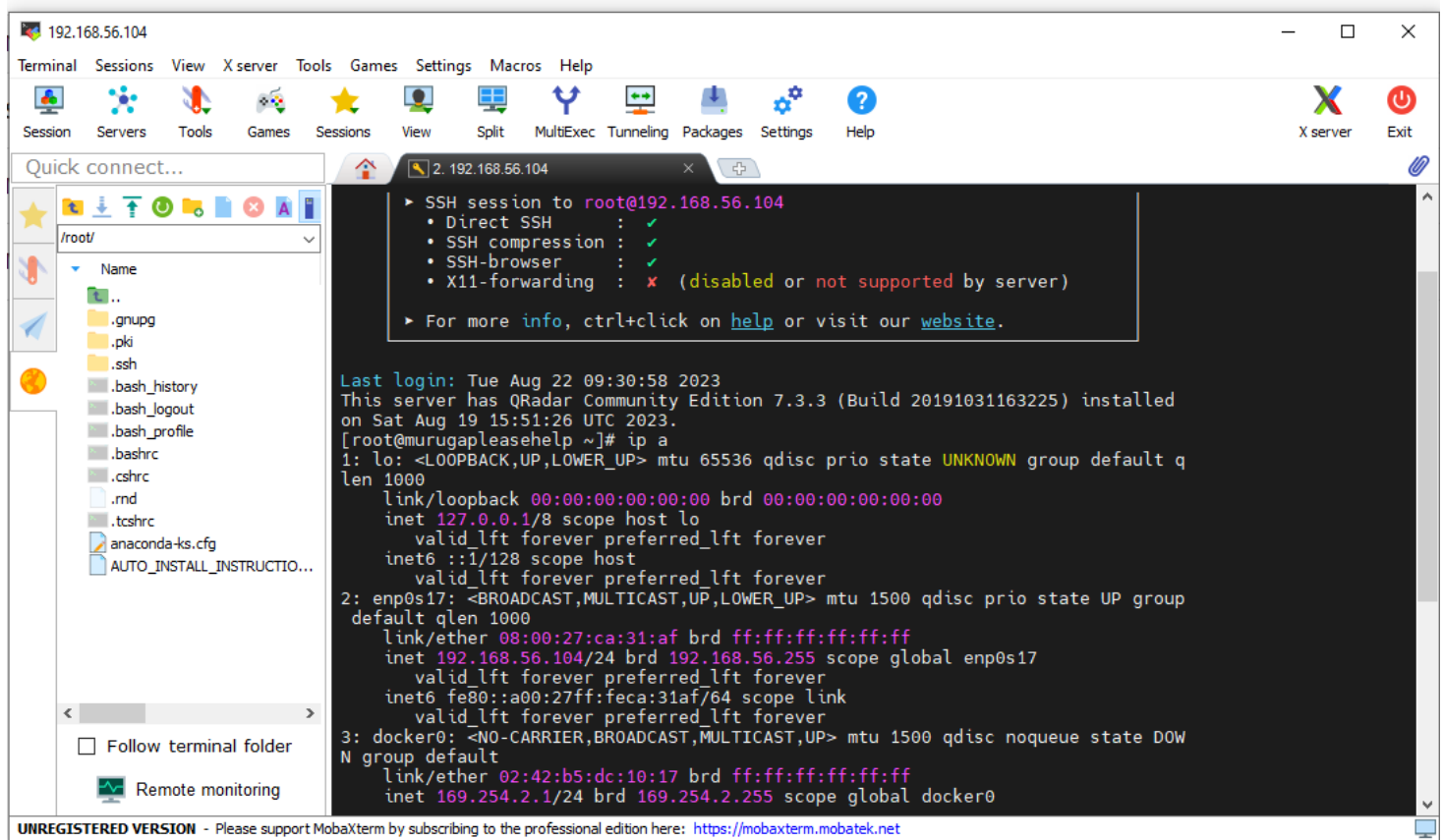
## **Topics explored :**

- ☐ Qradar
- ☐ SIEM
- ☐ SOC
- ☐ Vulnerability detection
- ☐ Cyber security
- ☐ OWASP

#### Tools explored :

- ☐ Qradar
- ☐ VirtualBox
- ☐ Nessus

#### Screenshot:



**Fig.1.Qradar**

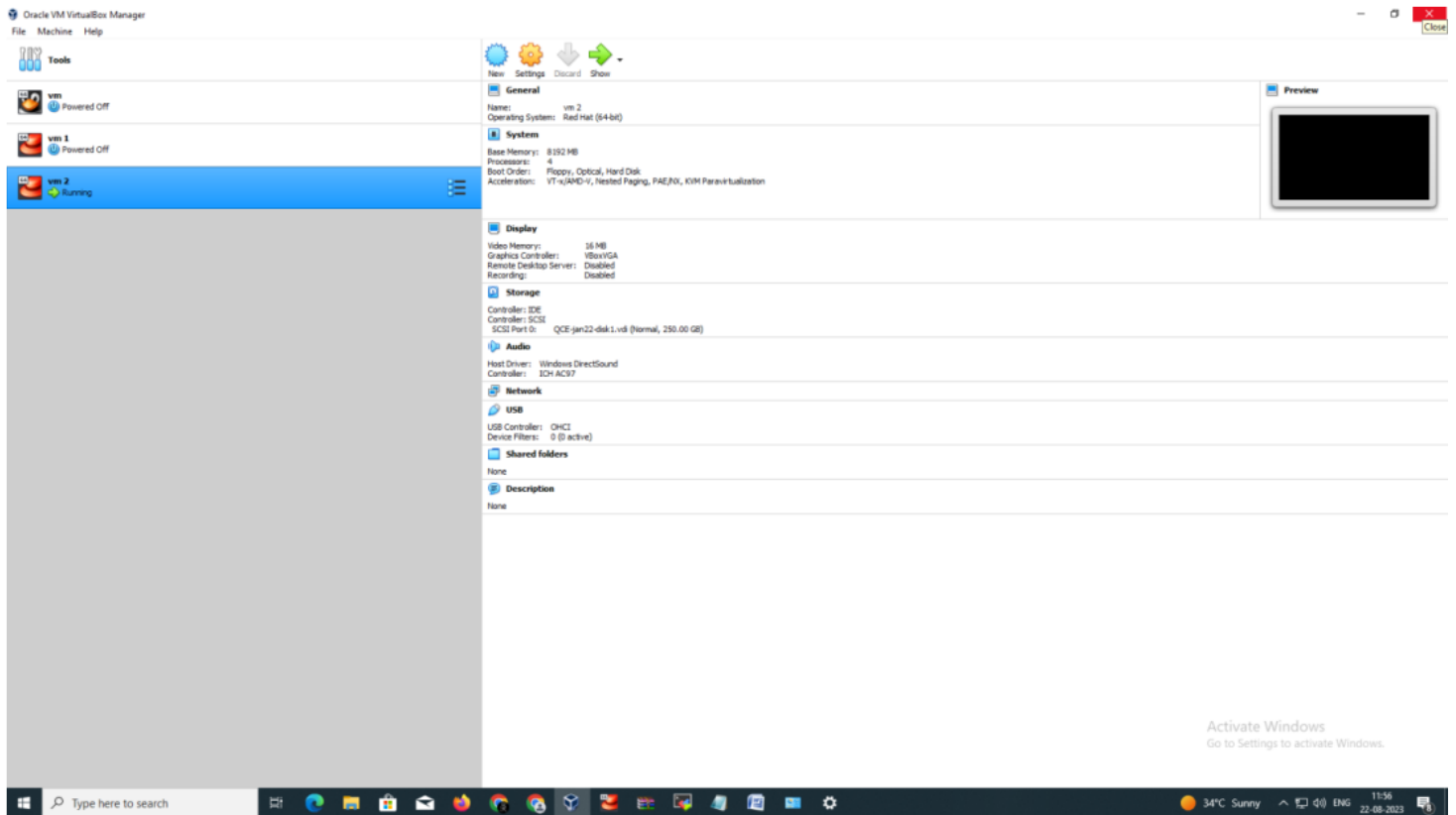


fig2: Virtual Box

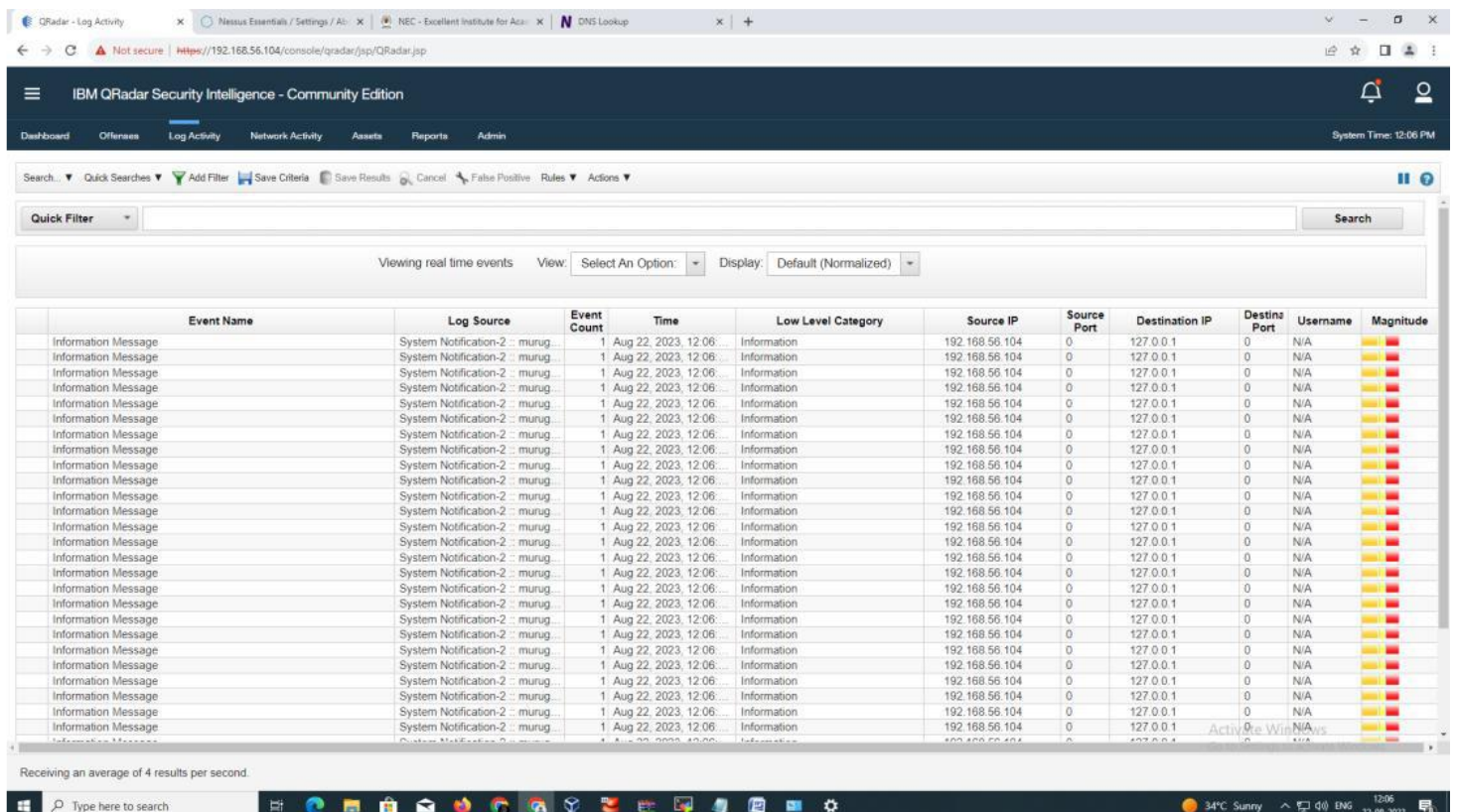


fig 3: Thread intelligence

**My Basic Network Scan / 192.168.56.1**

Configure Audit Trail Launch Report Export

Vulnerabilities 14

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	CVSS	VPR	Name	Plugin ID: 57608	Family	Count
MEDIUM	5.3		SMB Signing not required		Misc.	1
INFO			SMB (Multiple Issues)		Windows	6
INFO			Microsoft Windows (Multiple Issues)		Windows	2
INFO			DCE Services Enumeration		Windows	10
INFO			Asset Attribute: Fully Qualified Domain Na...		General	1
INFO			Authenticated Check: OS Name and Insta...		Settings	1
INFO			Common Platform Enumeration (CPE)		General	1
INFO			Device Type		General	1
INFO			Host Fully Qualified Domain Name (FQDN...		General	1
INFO			Nessus Scan Information		Settings	1
INFO			OS Identification		General	1

**Host Details**

IP: 192.168.56.1  
 DNS: ITUG-IT26.dc.cds  
 OS: Windows  
 Start: Today at 10:20 AM  
 End: Today at 10:33 AM  
 Elapsed: 13 minutes  
 KB: Download

**Vulnerabilities**

Activate Windows  
Go to Settings to activate Windows.

Fig 4: Nessus – My basic network scan

**My Basic Network Scan / Plugin #57608**

Configure Audit Trail Launch Report Export

Vulnerabilities 14

**MEDIUM** SMB Signing not required

**Description**  
 Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
 Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u7df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u774b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u7a3cac4ea>

**Output**  
 No output recorded.  
 To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.56.1

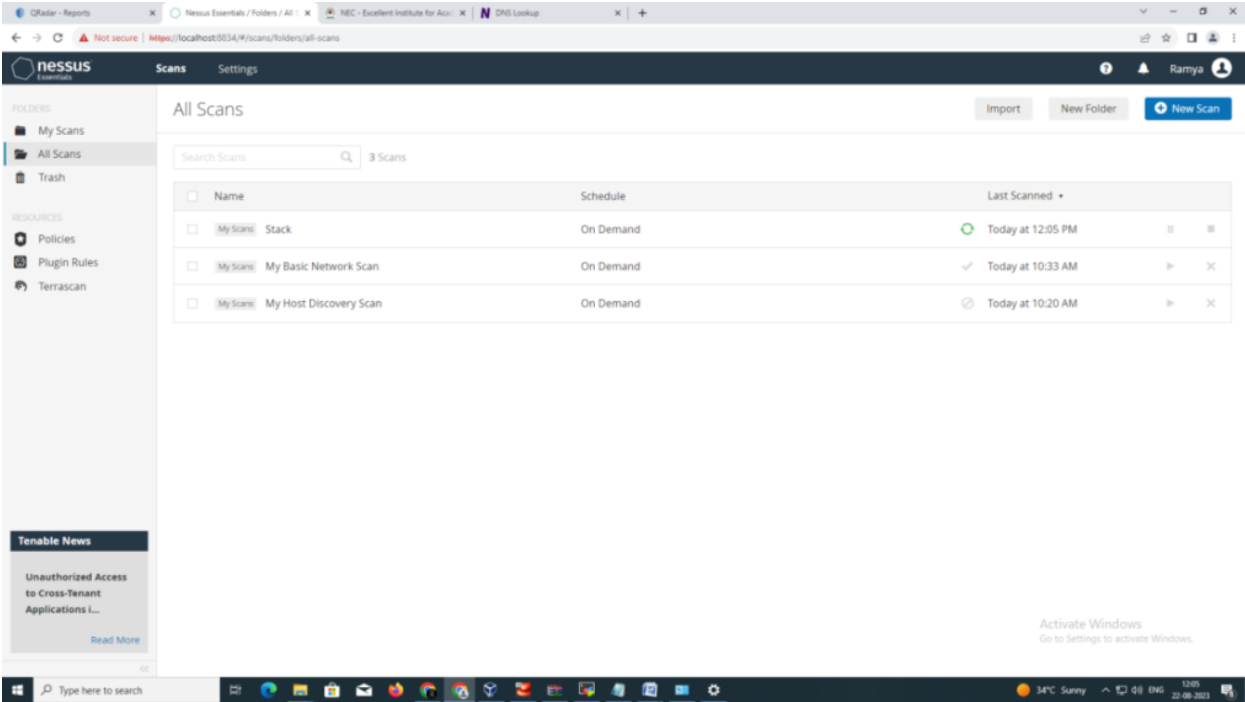
**Plugin Details**

Severity: Medium  
 ID: 57608  
 Version: 1.20  
 Type: remote  
 Family: Misc.  
 Published: January 19, 2012  
 Modified: October 5, 2022

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score 5.3**  
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N  
 CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C  
 CVSS v3.0 Temporal Score: 4.6  
 CVSS v2.0 Base Score: 5.0  
 CVSS v2.0 Temporal Score: 3.7  
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:L/P:A:N  
 CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

**Fig:5** My basic network scan



**Fig :ALL scans**

