Prevention against Vulnerabilities

Project Initialization:

Project objectives: Identify the vulnerabilities exist in the web applications or any existing website.

Analyze the existing system in an organization by creating security assessment.

Key steps for security assessment:

1. Determine the target system: College website(miet.ac.in) and its ip address
2. Vulnerability Scanning and reporting: Scan the vulnerabilities of a website(miet.ac.in) by using Nessus Tool and generate the report for high ,critical, medium and low level vulnerabilities.

Scope: To know about the different types of vulnerabilities or different types of attack done on any application. Identify those vulnerabilities and the different attacks ,so we can minimize the impact of attacks on that application.

Deliverables: Identify the vulnerabilities in the college website or ip addresses using Nessus tools and IBM QRadar.

Part1: Executive Summery

List of vulnerabilities

Vulnerability Number	Name of Vulnerability	Reference CWE
A01	**Broken Access Control**	CWE-284:Improper Access Control
A02	**Cryptographic Failures**	CWE-327: Use of a broken or risk Cryptographic algorithm
A03	**Injection**	CWE-94: Improper Control of Generation of Code ('Code Injection')
A04	**Insecure Design**	CWE-657: Violation of Secure Design Principles
A05	**Security Misconfiguration**	CWE-16: Configuration
A06	**Vulnerable and Outdated Components**	CWE-1395: Dependency on

		Vulnerable Third-Party Component
A07	**Identification and Authentication Failures**	CWE-306: Missing Authentication for Critical Function
A08	**Software and Data Integrity Failures**	*CWE-1214:Date Integrity Issues*
A09	**Security Logging and Monitoring Failures**	CWE-223: Omission of Security-relevant Information
A10	**Server-Side Request Forgery**	CWE-918: Server-Side Request Forgery (SSRF)

Report

1.Vulnerability name: Improper Access Control

CWE:284

OWASP Category:A01 Broken Access Control

Description: It does not restrict or incorrectly restricts access to a website or web application from an unauthorized user.

Business Impact: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

If an attacker is able to gain access to sensitive data, they may be able to use this information for malicious purposes, such as identity theft or fraud. Additionally, **data breaches can damage an organization's reputation and lead to financial losses**.

2.Vulnerability name: Use of a Broken or risk cryptographic algorithm

CWE:CWE-327

OWASP Category:A02 Cryptographic failures

Description: It includes uses a broken or risky cryptographic algorithm.

Business Impact: Insecure cryptography can be exploited to **expose sensitive information, modify data in unexpected ways, spoof identities of other users or devices.**

3.Vulnerability name: Improper Control of Generation of Code ('Code Injection')
CWE:CWE-94

OWASP Category:A03 Injection

Description: It constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Business Impact:

- Compromise of the application or underlying host
- Exposure of sensitive data
- Loss of productivity, reputation, or revenue

4.Vulnerability name: Violation of Secure Design Principles

CWE: CWE-657

OWASP Category:A04 Insecure Design

Description: The product violates well-established principles for secure design.

Business Impact: This can introduce weaknesses in resultant or make it easier for developers to introduce weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

5. Vulnerability name: Configuration

CWE:CWE-16

OWASP Category:A05 Missconfiguration

Description: Weakness is introduced in the system during system configuration.

Business Impact: It can allow attackers to gain unauthorized access to the networks, systems and data which in turn can cause significant monetary and reputational damage to your organization.

6.Vulnerability name: Dependency on Vulnerable Third-Party Component

CWE:CWE-1395

OWASP Category:A06 vulnerable and Outdated Components

Description: The product has a dependency on a third-party component that contains one or more known vulnerabilities.

Business Impact: It can lead to devastating consequences such as data breaches, malware infections, and compromised systems.

7.Vulnerability name: Missing Authentication for Critical Function
CWE: CWE-306

OWASP Category:A07 Identification and Authentication failure

Description: Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks.

Business Impact: Data breaches: Improper authentication can allow unauthorized users to gain access to sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

8.Vulnerability name: Data Integrity Issues
CWE:CWE1214

OWASP Category:A08 Software and Data Integrity Failures

Description: Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations.

Business Impact: Businesses collect and use an enormous amount of customer data, including sensitive or personally identifiable data. Data integrity **ensures that customers are treated correctly, such as receiving proper account crediting and reporting**. Data security must keep that sensitive data safe from loss of theft.

Failing to address data integrity problems can have costly, far-reaching consequences in terms of **lost productivity and revenue, squandered opportunities, and reputation damage**.

9.Vulnerability name: Omission of Security-relevant Information
CWE:CWE-223

OWASP Category:A09 **Security Logging and Monitoring Failures**

Description: The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

Business Impact: Information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

10.Vulnerability name: Server-Side Request Forgery (SSRF)
CWE: CWE-918

OWASP Category:A10 Server side Request Forgery

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: A successful SSRF attack can often result in **unauthorized actions or access to data within the organization**, either in the vulnerable application itself or on other back-end systems that the application can communicate with. Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location. In some situations, the SSRF vulnerability might allow an attacker to perform arbitrary command execution.

Stage 2: Report

NESSUS Vulnerability Report:

Overview: Nessus stands for Numerical Evaluation of Stochastic Structures Under Stress. The tool is a Network and also a vulnerability scanner. The tools are developed and distributed by tenable INC.

Features:

1. Vulnerability Scanning
2. Asset Discovery
3. Network Scanning
4. Vulnerability Assessment
5. Prioritization
6. Policy Management
7. Web Scanning

Vulnerability Scanning with Nessus:

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. For instance, a plugin could be launched and targeted at a host to:
Identify which operating systems and services are running on which ports
Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)

The steps that are followed during scanning are:
Define scan parameters
Create scan
Launch scan
Analyze scan results

Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an attempt to discover which host contains which vulnerabilities.

Ports can be defined in ranges or individually, with valid ports ranging from 1 to 65535.
Nessus gives you the ability to configure your scan based on different scan and policy templates. These templates will determine the settings that will be found within the scan policy settings:
Basic: With this setting, you can specify security-related and organizational aspects of the scan or policy, such as name of the scan, the targets of the scan, whether or not it is scheduled and who has access to it.
Discovery: For defining the ports to be scanned and the methods to be used while conducting this discovery.
Assessment: This setting allows you to determine the type of vulnerability scan to perform and how they are performed.
Report: For determining how scan reports are generated and the information that should be included within them.

Advanced: Here you will define scan efficiency and the operations that the scan should perform.

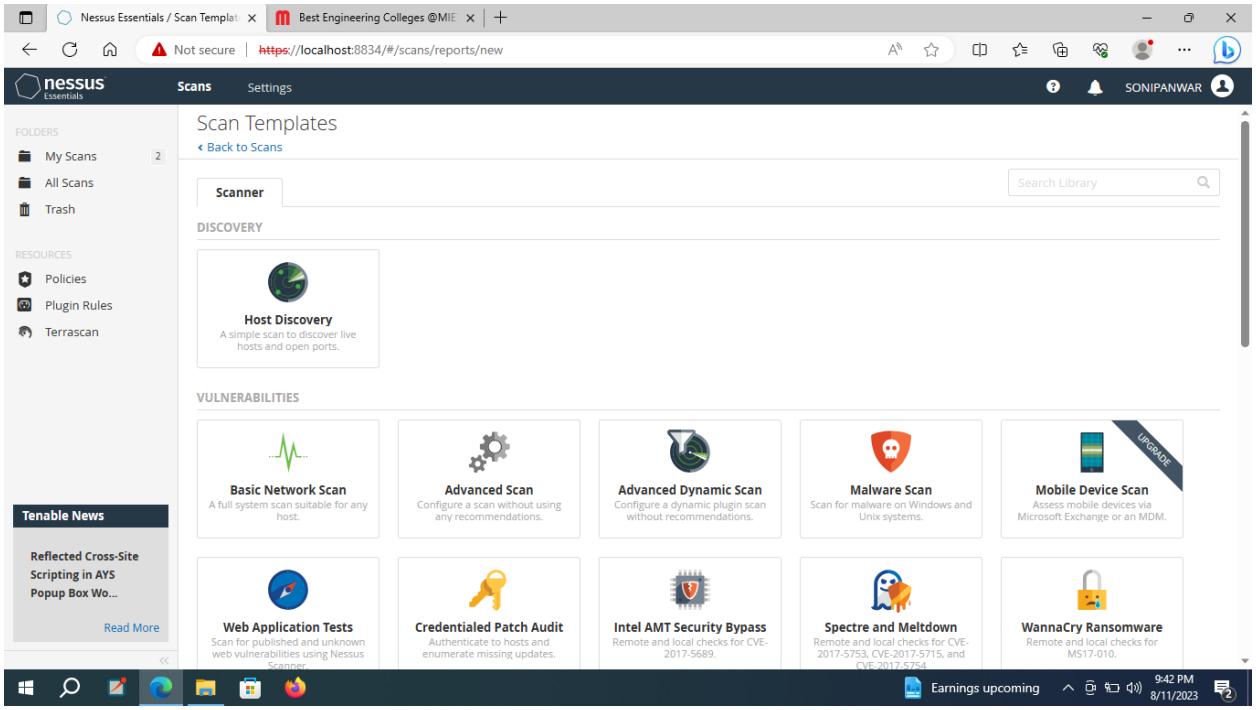
Target Website: Meerut Institute of Engineering College, Meerut (**miet.ac.in**)

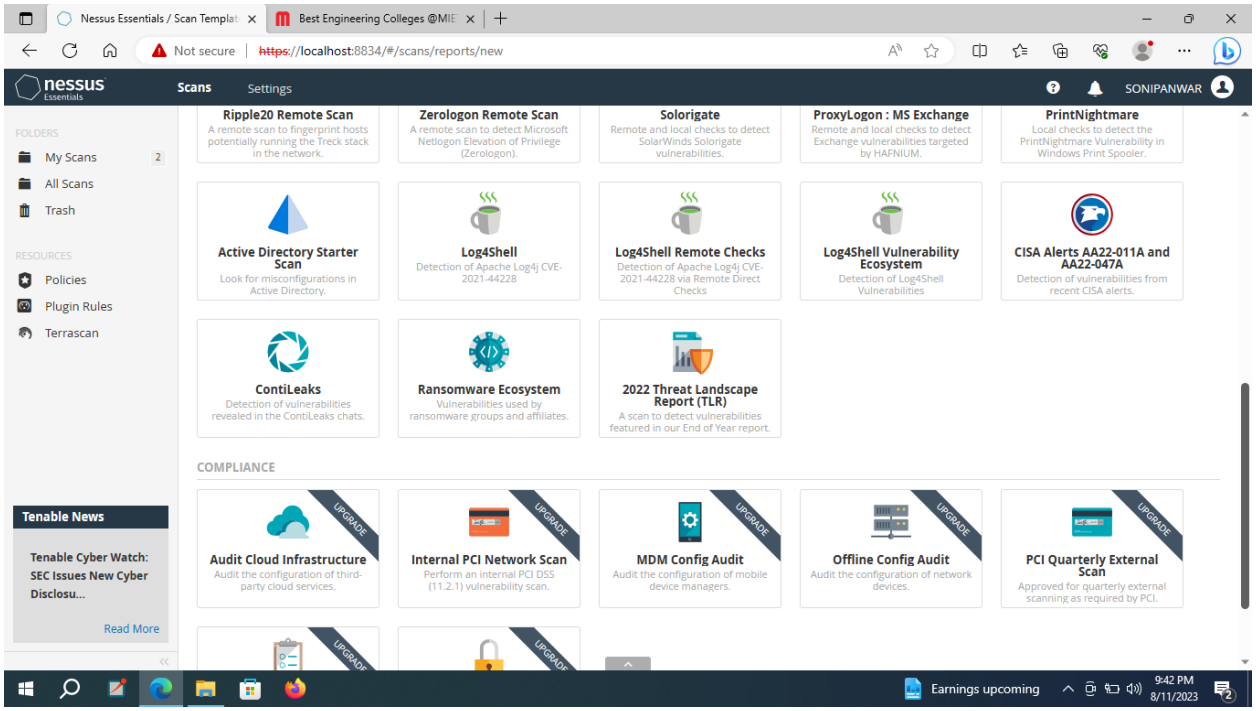
Target IP address:**92.205.6.179**

Step 1:First download the Nessus Essential then install it by using user name and password.

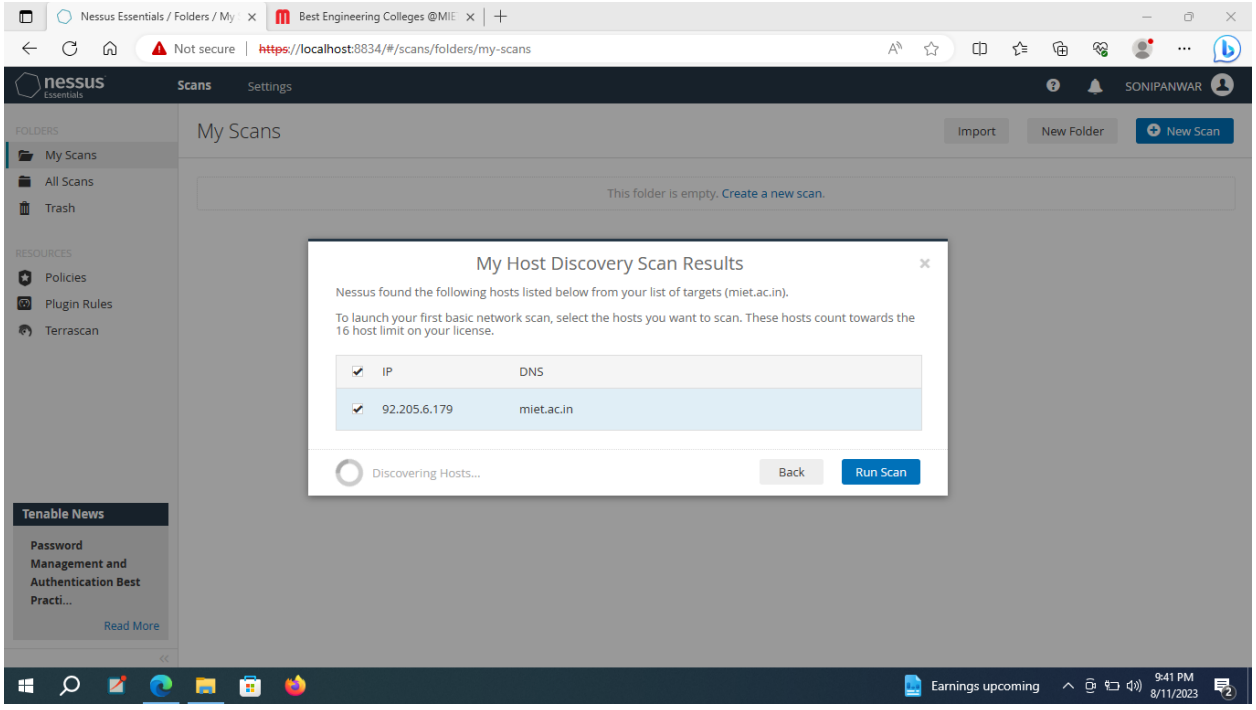
Step 2: After installation login on Nessus Essential and open Scan Template and start the Nessus services.

Step 3: click on My Scans then My Scans Interface will open and click on New San.



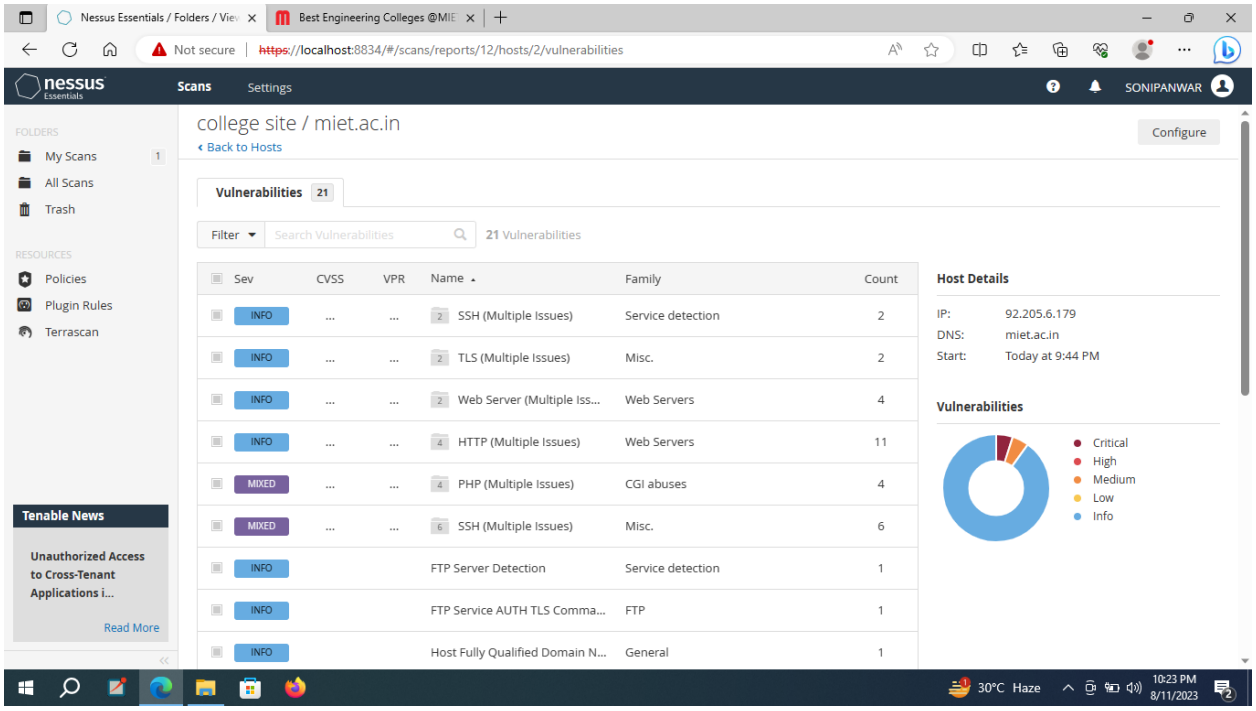


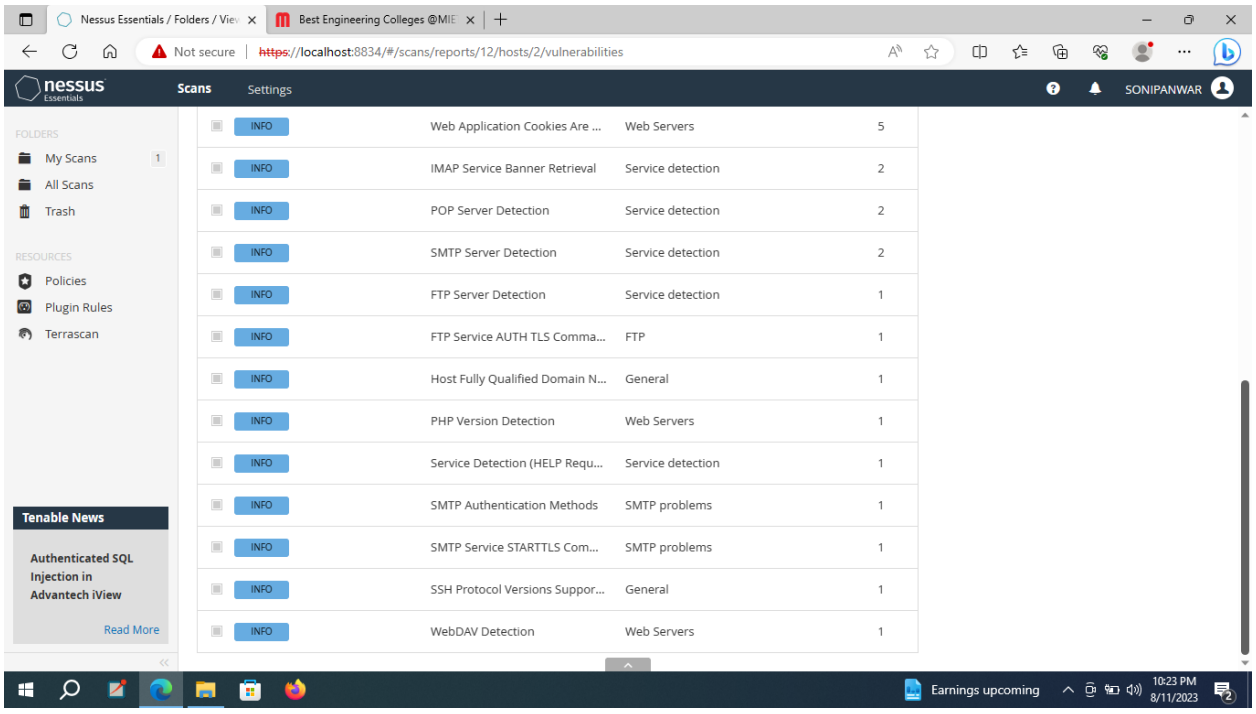
Step 4: enter the name of the website of college or ip address of target website and click on Run Scan then vulnerability scanning will start.

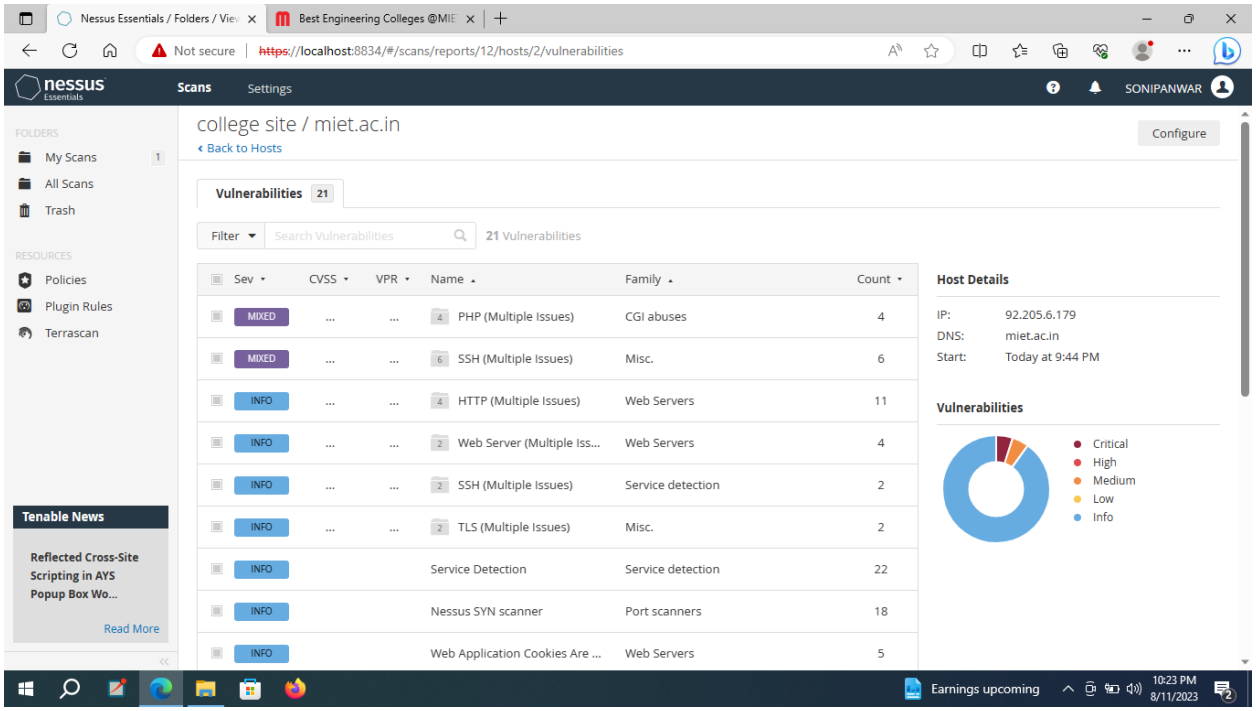


These all are the vulnerabilities exit in the college website miet.ac.in .

There are 21 vulnerabilties exist in the target website.







Stage 3:Report on Qradar

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

SIEM (Security Information and Event Management):

It is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

By incorporating threat intelligence feeds, vulnerability management tools, and endpoint security platforms, QRadar SIEM creates a robust integration ecosystem, offering a highly tailored security experience for analysts to detect and remediate threats faster.

It combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which can use for threat detection and prioritization.

The core components of QRadar are SIEM, User Behavior Analytics, Network Insights, Vulnerability Manager, and Incident Forensics.

Features:

- AI/Machine Learning.
- Behavioral Analytics.
- Compliance Management.
- Endpoint Management.
- Endpoint Protection.
- Incident Management.
- Network Monitoring.
- Prioritization.

Security Information and Event Management (SIEM) systems aggregate security data from across the enterprise; help security teams detect and respond to security incidents; and create compliance and regulatory reports about security-related events.

It is used for logging and monitoring network security, security analysis, and monitoring for network-related attacks.

A Security Operations Center (SOC) and a Security Incident and Event Management (SIEM) platform are different strategies for monitoring a network environment, and they work together to help corporations prevent data breaches and alert them to potential ongoing cyber-events.

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors.

SOC is a team of security experts who are dedicated to the use of SIEM tools to monitor the IT infrastructure of a business, search for potential threats, and respond in case of attacks.

Planning: Analyze the existing infrastructure, systems, and security controls.:

Analyze the existing system in an organization by creating security assessment.

Key steps for security assessment:

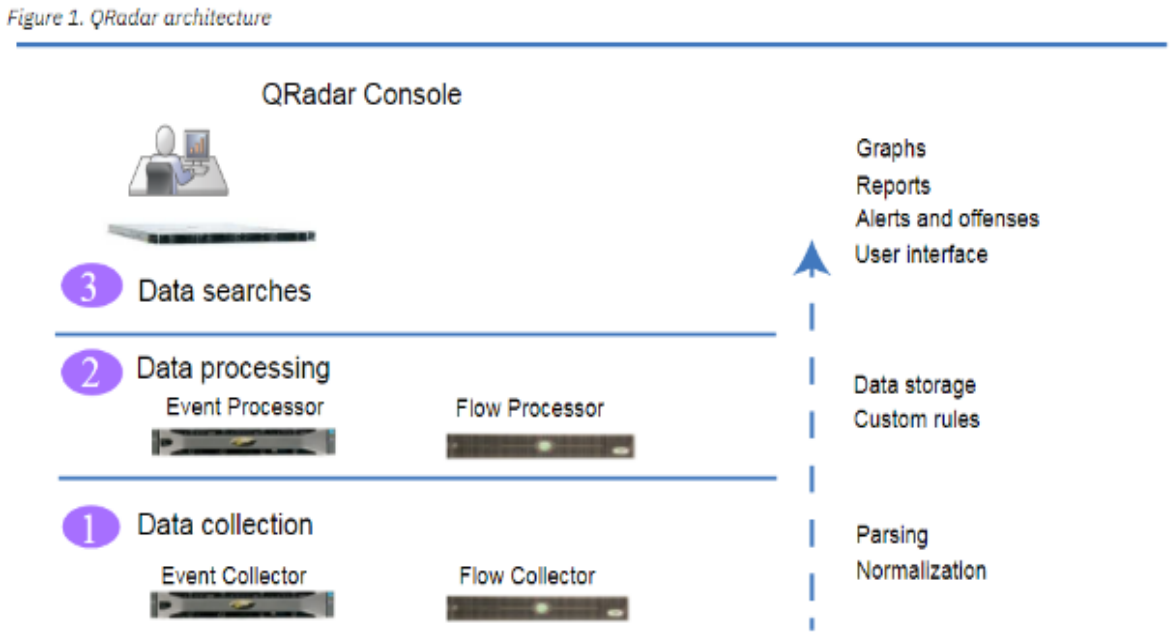
1.Determine the target system: College website(miet.ac.in) and its ip address

2.Vulnerability Scanning and reporting: Scan the vulnerabilities of a website(miet.ac.in) by using Nessus Tool and generate the report for high ,critical, medium and low level vulnerabilities.

Architecture and deployment strategy for QRadar SOC/SIEM:

IBM QRadar collects, processes, aggregates, and stores network data in real time. QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.

IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale QRadar to meet your log and flow collection, and analysis needs. You can add integrated modules to your QRadar platform, such as QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics.
The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up the QRadar architecture.
Figure 1. QRadar architecture



The following diagram shows the layers that make up the QRadar architecture.

Data collection

It is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.
The core functionality of QRadar SIEM is focued on event data collection, and flow collection.

Data processing

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.
Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Data searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console.
In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.
Develop use cases, rules, and correlation logic based on security requirements:

Build the USE case:

Detection of possible brute force attack:(Attempts to) compromise user credentials
Detection of insider threat: Unwanted escalation of privilege
Misuse of an account
Unusual behavior on privileged accounts
Application Defense Check: Protection against data loss
Suspicious behavior of log source
Detection of anomalous ports, services and unpatch hosts/network devices
Secure cloud based applications
Threat hunting
Instances of Denial of Service
Detection of malware
Phishing efforts.

Build the rules for your use case: 1:No of attempts is fixed otherwise lock the account.
2:According to the authority provide the privileges don't give unnecessary privilege.
3.Continuosly monitor the logs if there is any suspicious activity block the user.
4. Use of antimalware and on the firewall protection.
Test and tune: Test
Monitor performance. Acceptable Use Monitoring (AUP)

QRadar SOC/SIEM Rule Development And Optimization

Rule Development
Creating custom rules in QRadar to detect specific security events or policy violations based on the organization's use cases.

Before create a new rule, user must have the **Offenses** > **Maintain Custom Rules** permission.

Step 1:
From the **Offenses**, **Log Activity**, or **Network Activity** tabs, click **Rules**.
Step 2:
From the **Display** list, select **Rules** to create a new rule.
Optional: From the **Display** list, select **Building Blocks** to create a new rule by using building blocks.

Step 3:
From the **Actions** list, select a rule type.
Each rule type tests against incoming data from different sources in real time. For example, event rules test incoming log source data and offense rules test the parameters of an offense to trigger more responses.

Step 4:
In the Rule Wizard window, select the **Skip this page when running this rules wizard** checkbox and click **Next**.
If you select the **Skip this page when running this rules wizard** checkbox, the Welcome page does not appear each time that you start.
On the Rule Test Stack Editor page, in the Rule pane, type a unique name that you want to assign to this rule in the **Apply** text box.

Step 5:
From the list box, select **Local** or **Global**.
If you select **Local**, all rules are processed on the Event Processor on which they were received and offenses are created only for the events that are processed locally.

- If you select **Global**, all matching events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth and processing resources.

Step 6:
From the **Test Group** list, select one or more tests that you want to add to this rule. The CRE evaluates rule tests line-by-line in order. The first test is evaluated and when true, the next line is evaluated until the final test is reached.

Step 7:
Step 7:

Step 7:
If you want to select the **when the event matches this AQL filter query** test for a new event rule, click the add **(+)** icon. In the Rule pane, click **This** and enter an AQL WHERE clause query in the **Enter an AQL filter query** text box.

Step 8:

To export the configured rule as a building block to use with other rules, click **Export as Building Block**.

Step 9:

On the Rule Responses page, configure the responses that you want this rule to generate.

Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.

Anomaly detection rules perform tests on the results of saved flow or event searches to detect when unusual traffic patterns occur in your network.

1. Log in to the QRadar UI.
2. Click Log Activity tab.
3. Use the following AQL Query in Advanced Search: ...
4. Click Search and View the Results.
5. Click Save Criteria.
6. Use the Name "Test Threshold" for 5-minute interval, Include in my Quick Searches, Share with Everyone.
7. Click OK.
8. Click Rules > Add Threshold Rule.

QRadar analyzes the following information:

- Incoming events and flows
- Asset information
- Known vulnerabilities

System Deployment And Configuration:

Installing and configuring the QRadar SOC/SIEM system according to the organization's requirements and architecture.

Setting up the necessary hardware prerequisites:

Download the virtual box with version 6 according to the existing operating system(windows/mac) and its configuration(32/64).
Hardware requirements: 8 GB RAM
4 Processor

and network connectivity: through the Bridged adapter network to support the QRadar components or port with providing the local and manual ipv4 address on NAT with port number.

QRadar Community Edition:

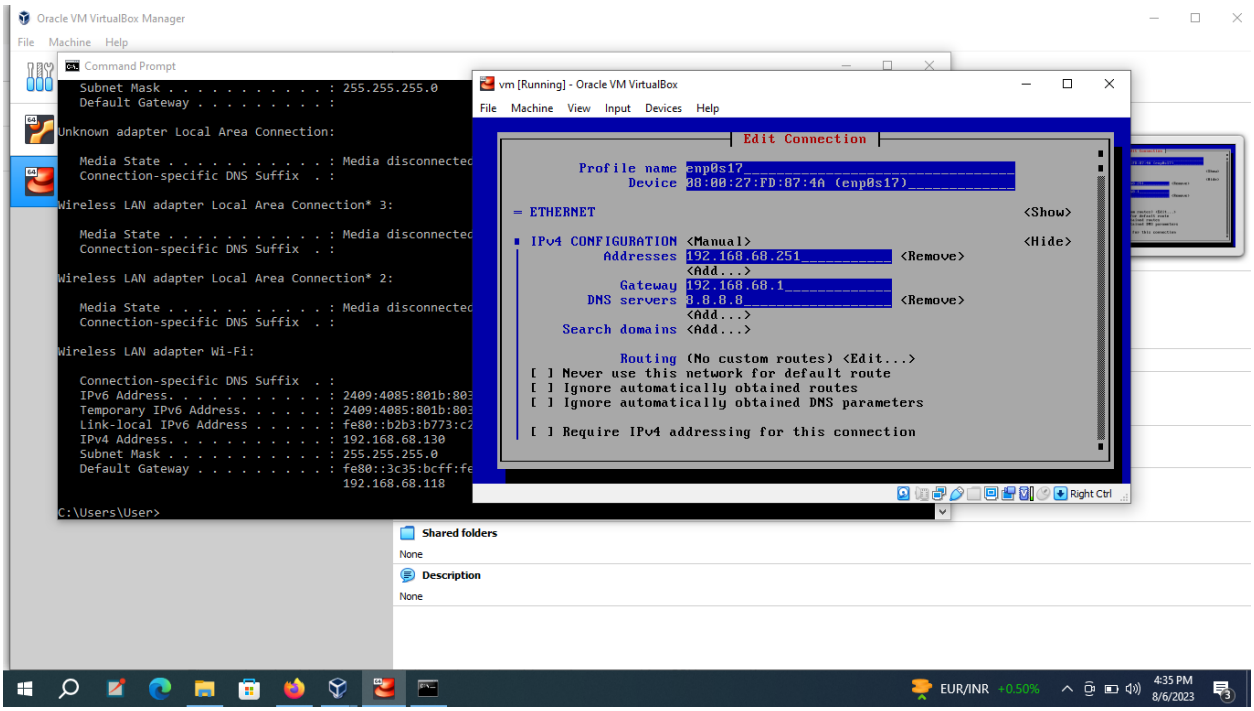
Install the QRadar :
Step 1:Download the QRadar

Step 2:Download the virtual box according the operating system. Unzip the virtual box and install the virtual box.

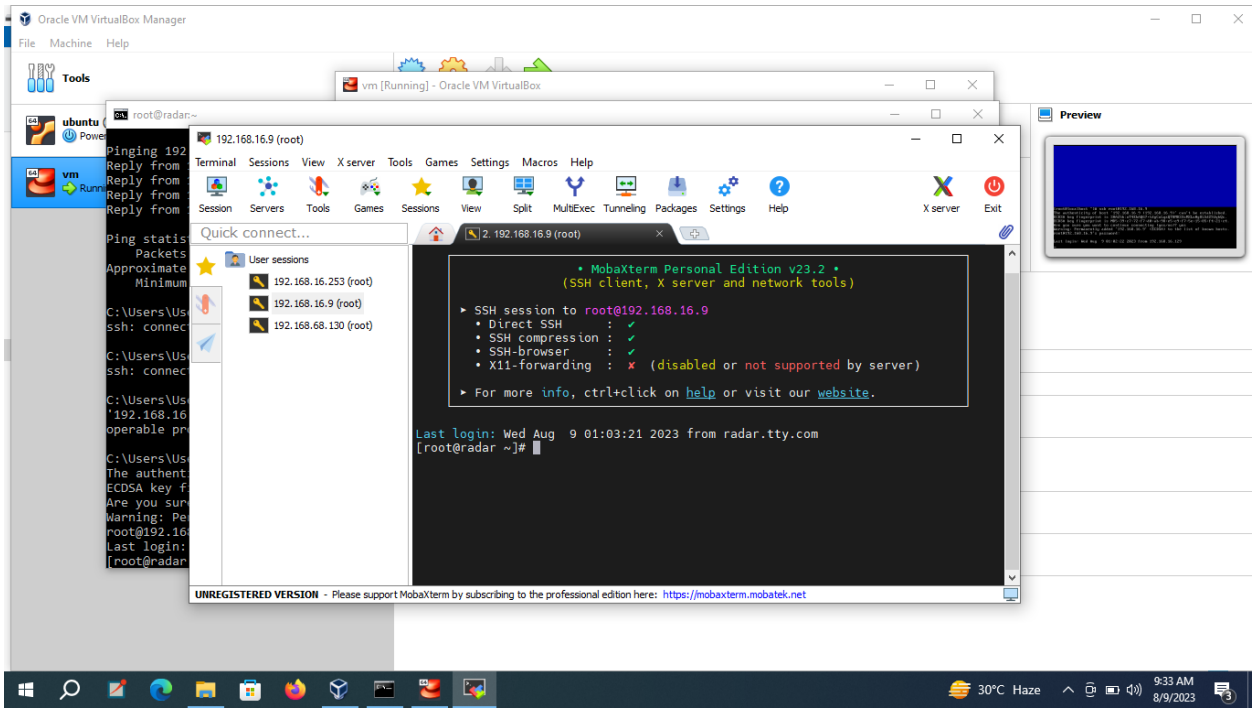
Step 3: Open the virtual box and import the QRadar with minimum 6 GB RAM and 2 processor but for properly working RAM must 6.5 GB and 4 processor or Click on the QRadar and it will open in virtual box and apply the setting ,it will install in virtual box.

Step 4: A Qradar console screen will open and ask for username and password.
User name : root
Pasword: Userchoice
Confirm Password: Userchoice
It will set for Qradar login for terminal.
→check the address using ip addr command on terminal.
→set the network setting using network manager using nmtui command, network manager will pop up. Set the wired connection name enp07s with ipv4 address(manual) that's fetch in previous step.Add the default gateway 8.8.8.8 .Ignore the ipv6 address and then click ok.
→set the host name in proper domain such as qradar.tty.com and then click ok.

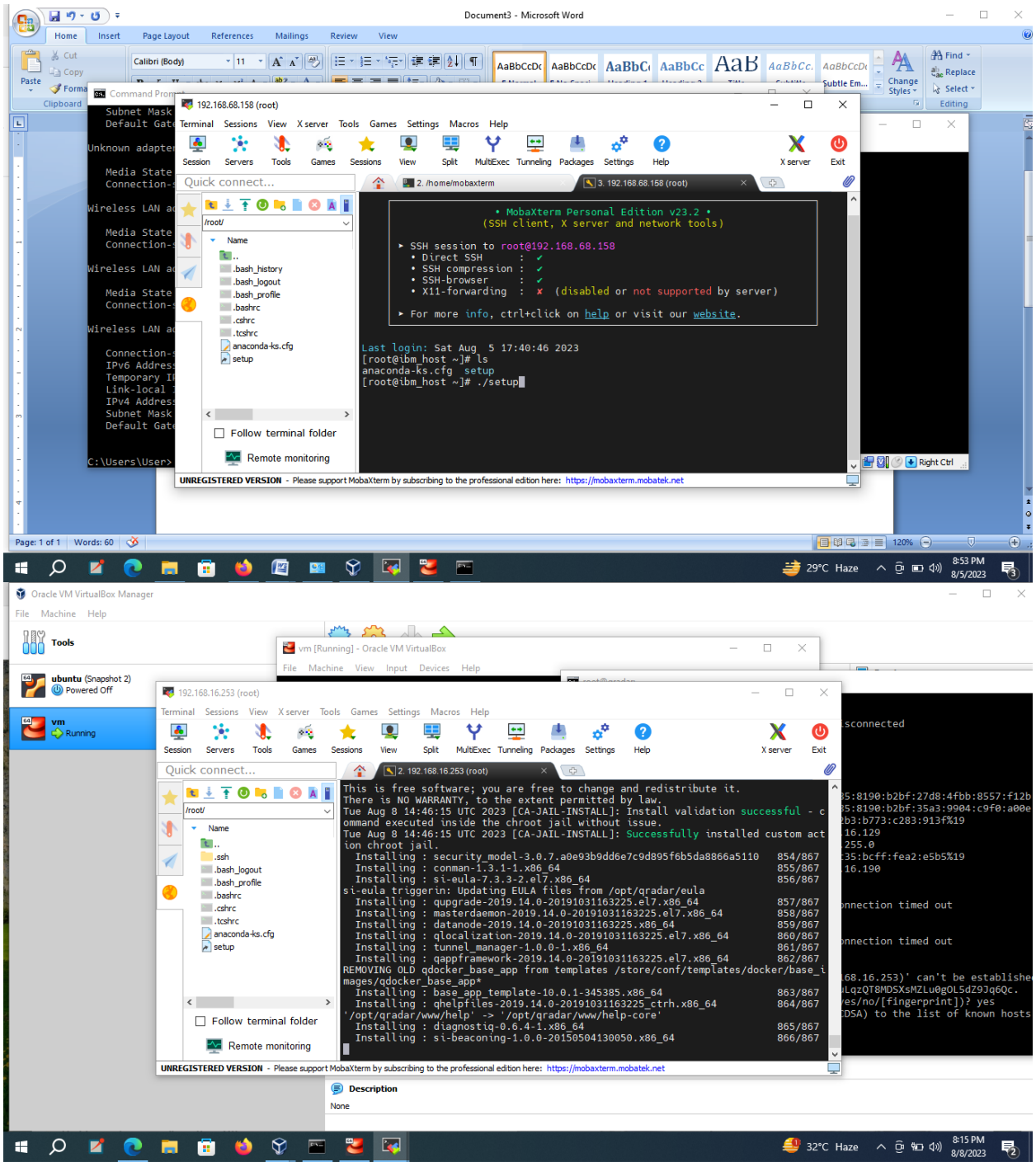
- ➔ Activate the connection and then click ok.



Step 5: Install mobexterm. Open it and open the SSH terminal enter the ip address and the selct root and click ok connection will build and then type the command ssh root@ipaddr command it will ask for password. After successful connection it will remotely login the Qradar terminal.



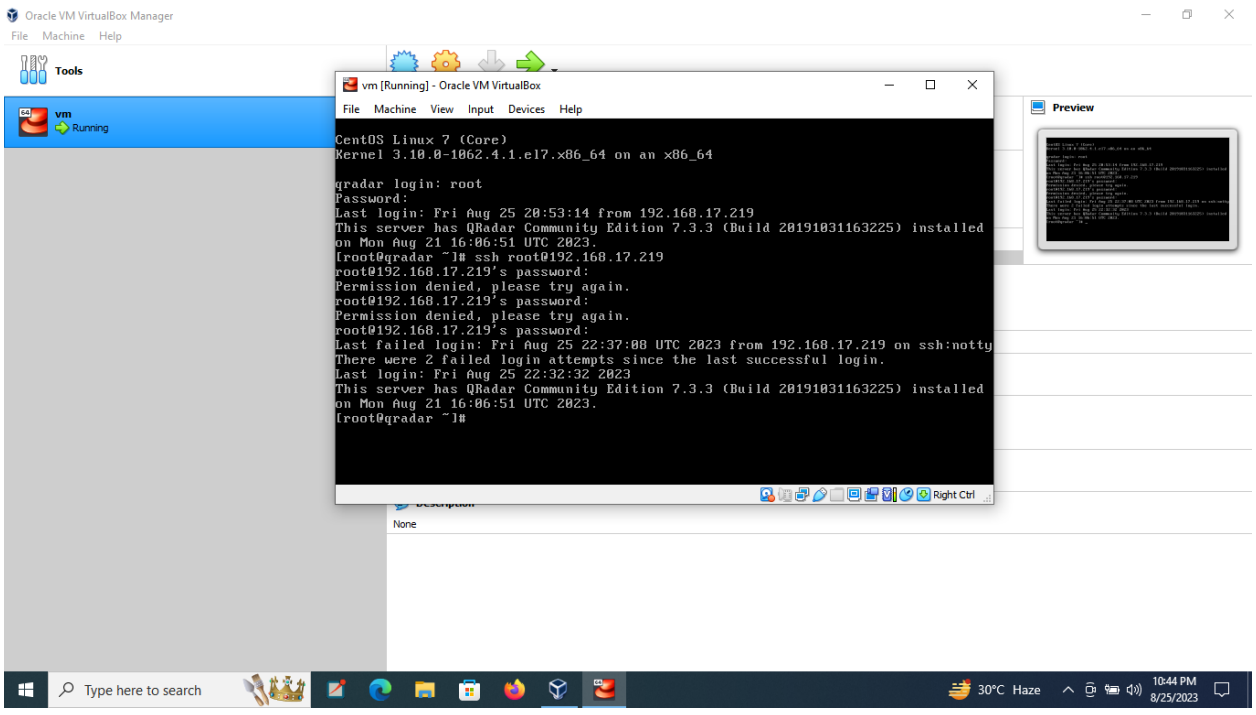
→type ls then enter
→type ./setup then enter it will start the installation process of QRadar and install all the packages and files of QRadar ,it will take time.

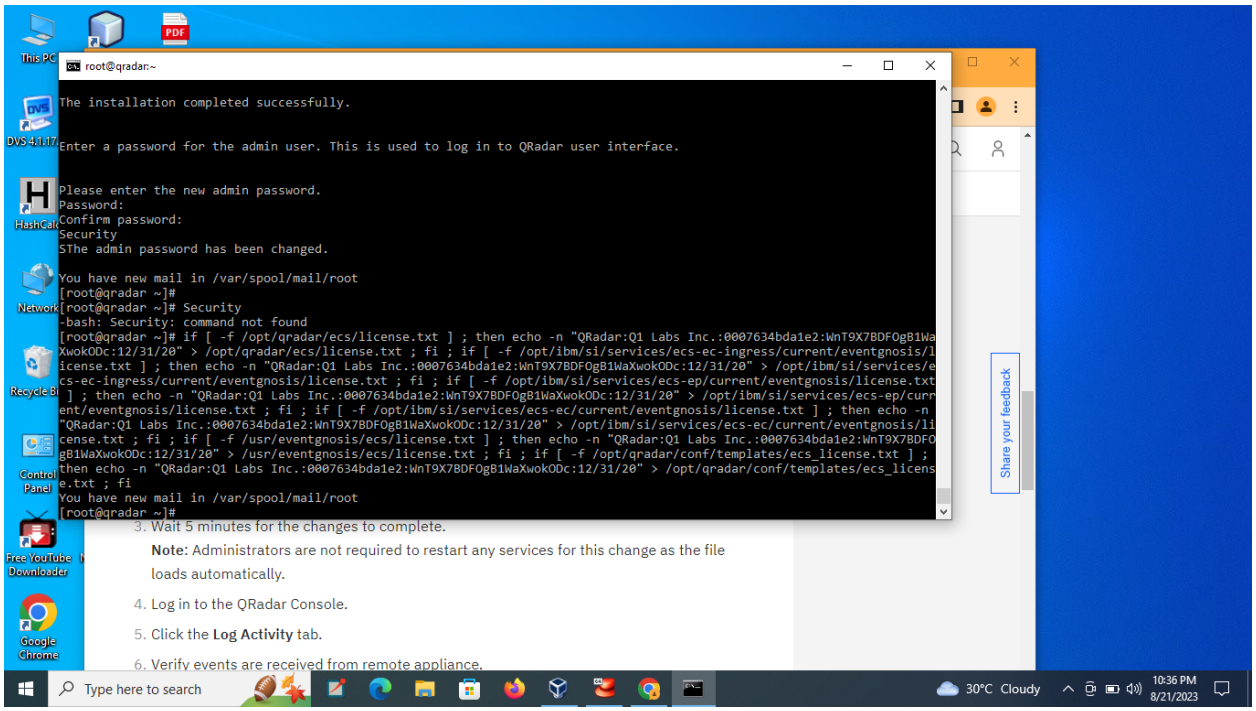


After successful installation type enter and it will ask for
username: admin and
password: ********
confirm password:*******
Installation will be complete and paste the statement of community edition from QRADAR community edition then press enter.

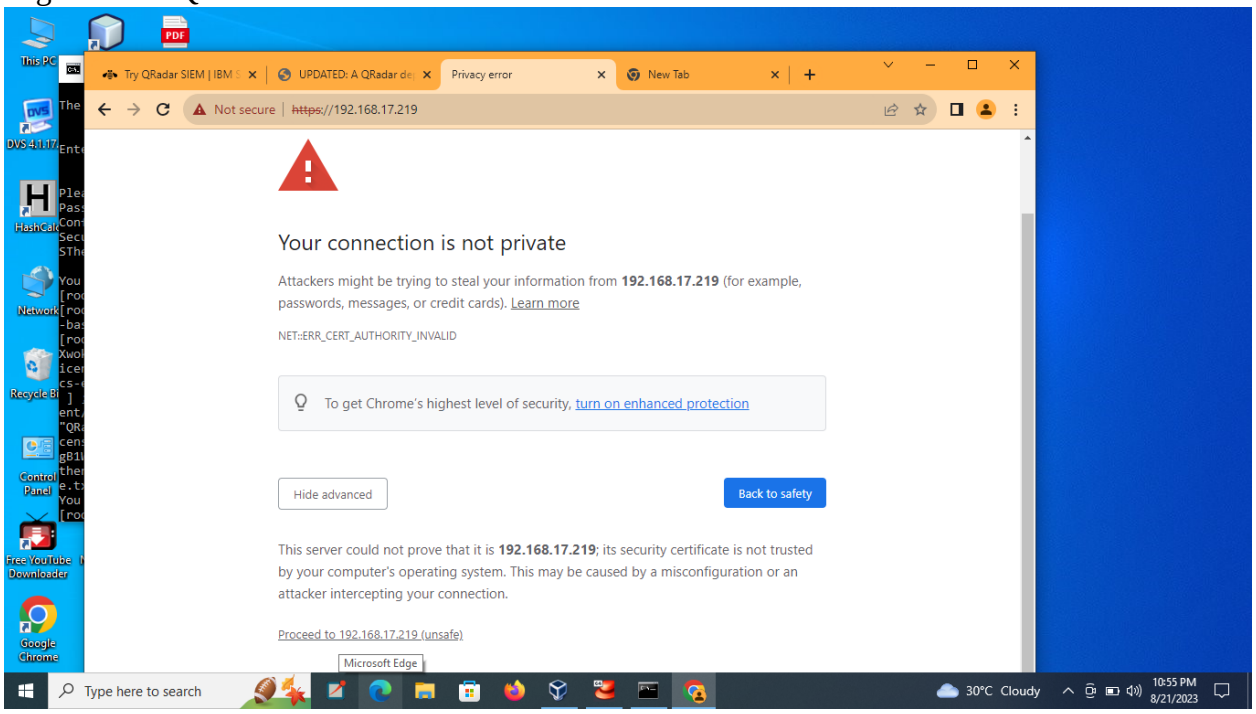
1. To update the license file, select the following command

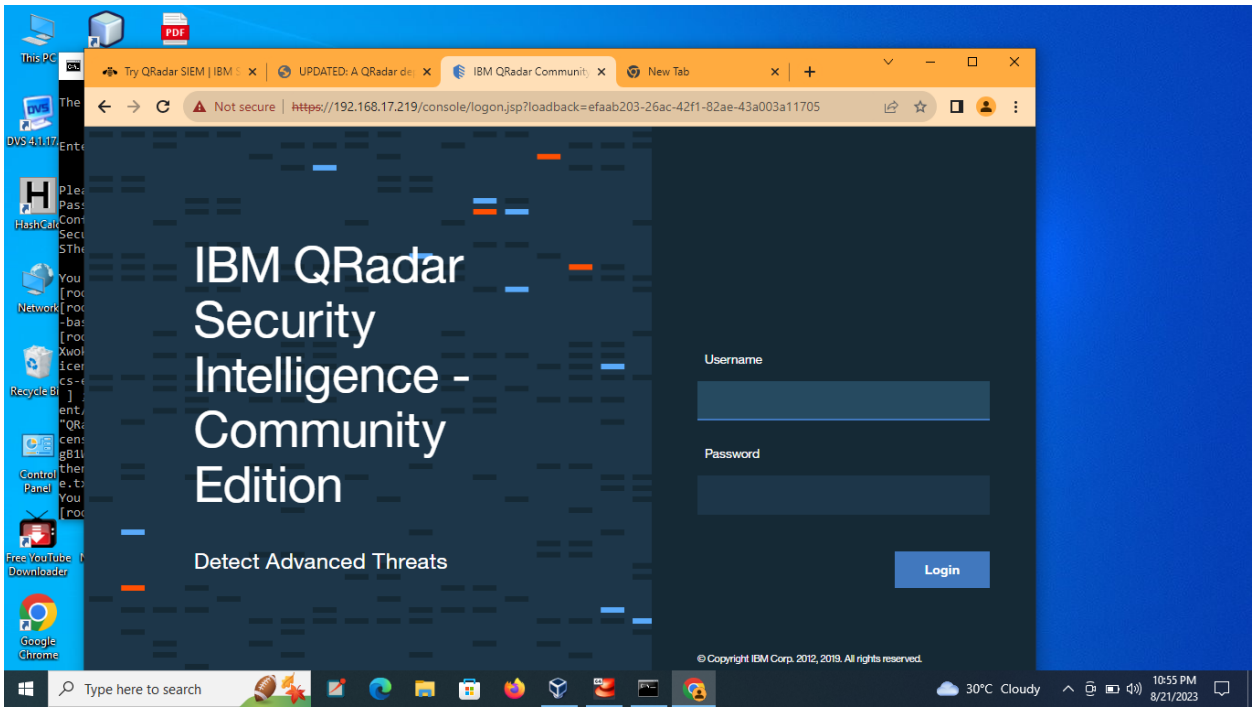
For QRadar Community Edition:if [-f /opt/qradar/ecs/license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/qradar/ecs/license.txt ; fi ; if [-f /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ; fi ; if [-f /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ; fi ; if [-f /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt ; fi ; if [-f /usr/eventgnosis/ecs/license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /usr/eventgnosis/ecs/license.txt ; fi ; if [-f /opt/qradar/conf/templates/ecs_license.txt] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/qradar/conf/templates/ecs_license.txt ; fi
Wait 5 minutes for the changes to complete.



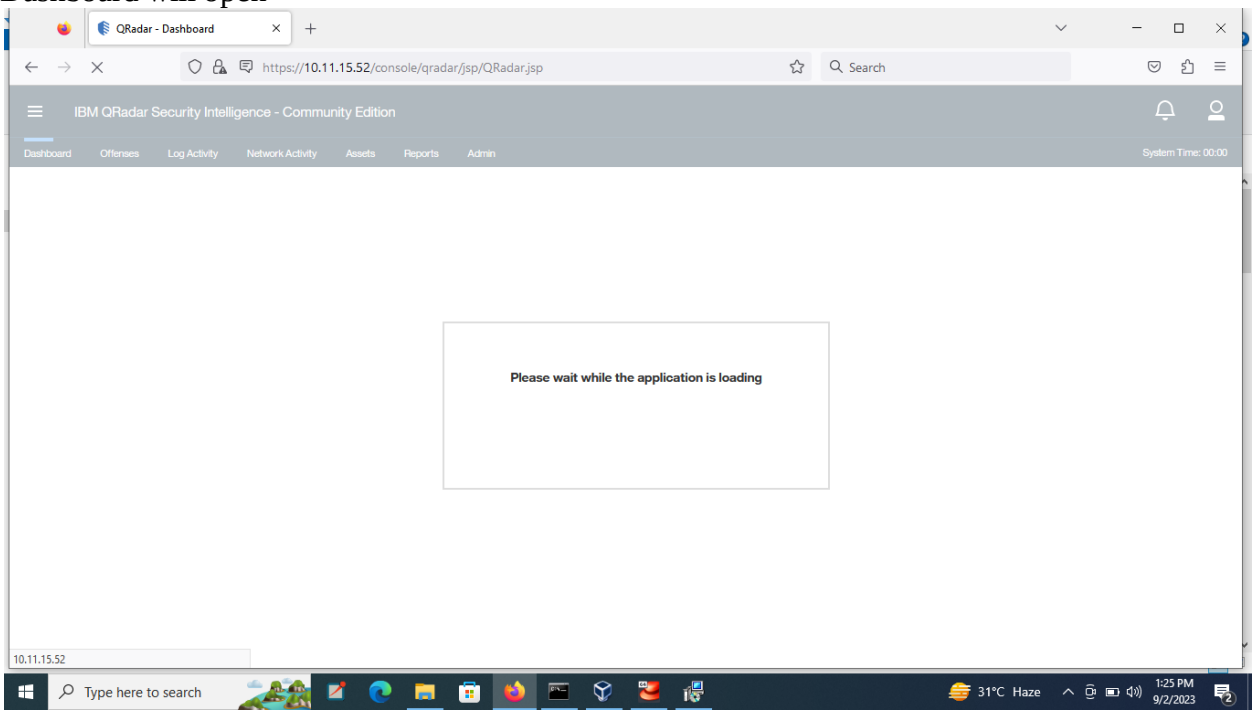


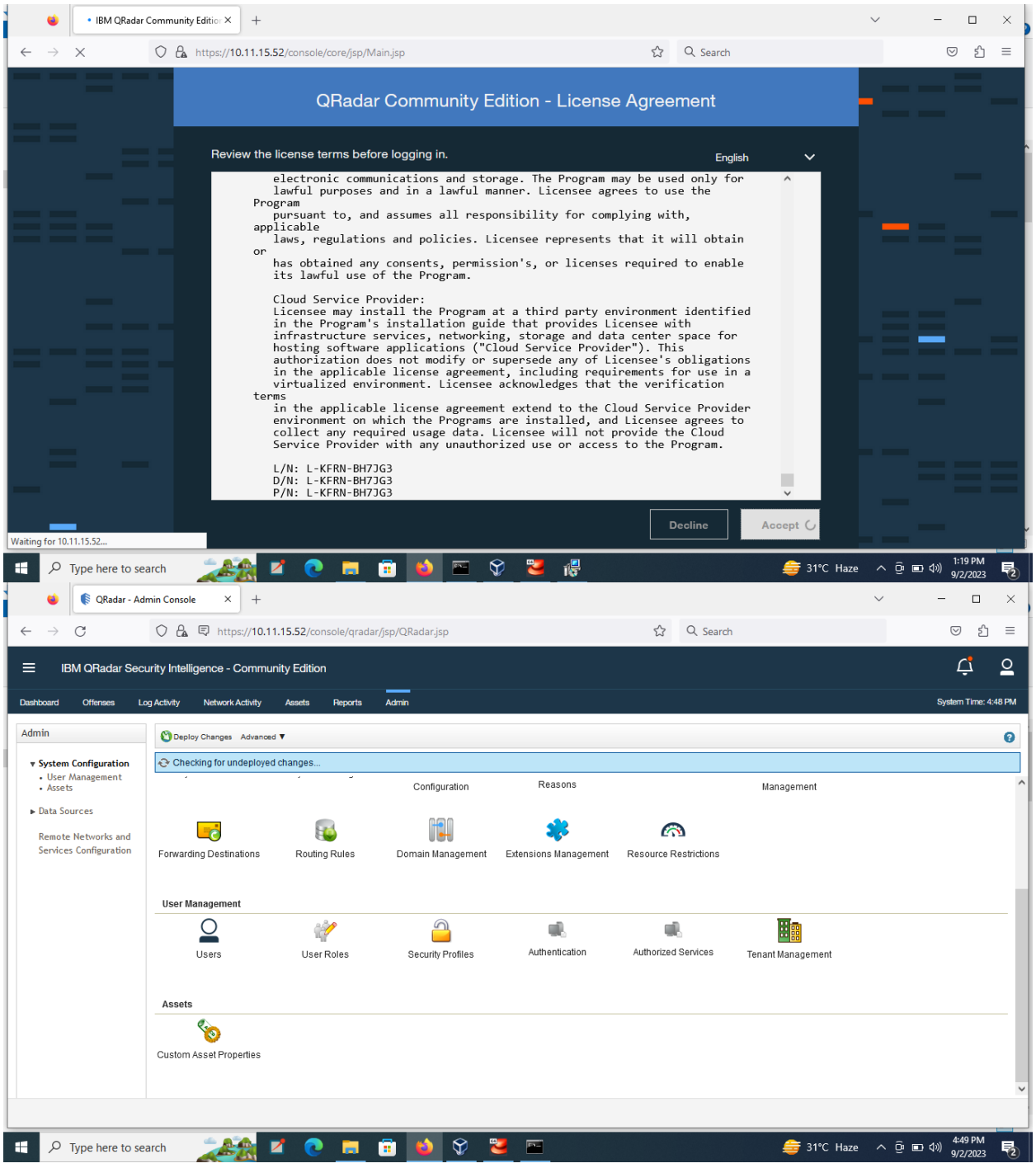
Step 6:open the GUI interface by writing the url :https://ipaddr/console then press enter.
Log in to the QRadar Console.

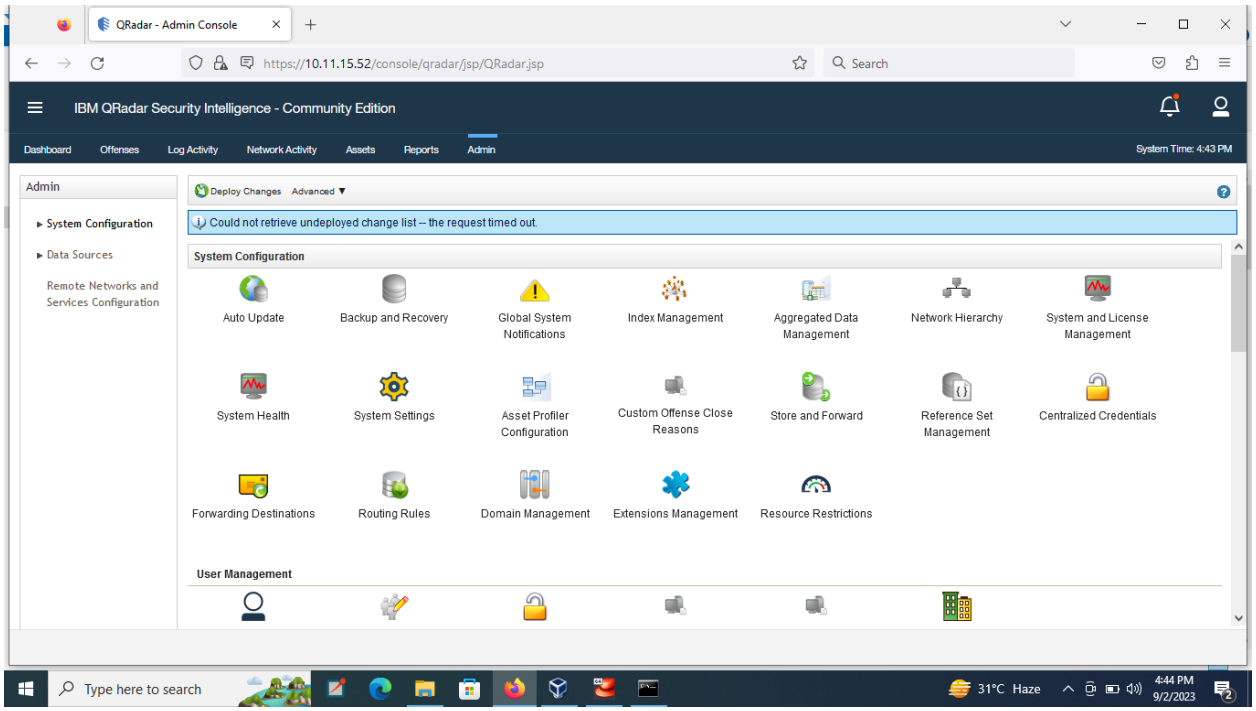




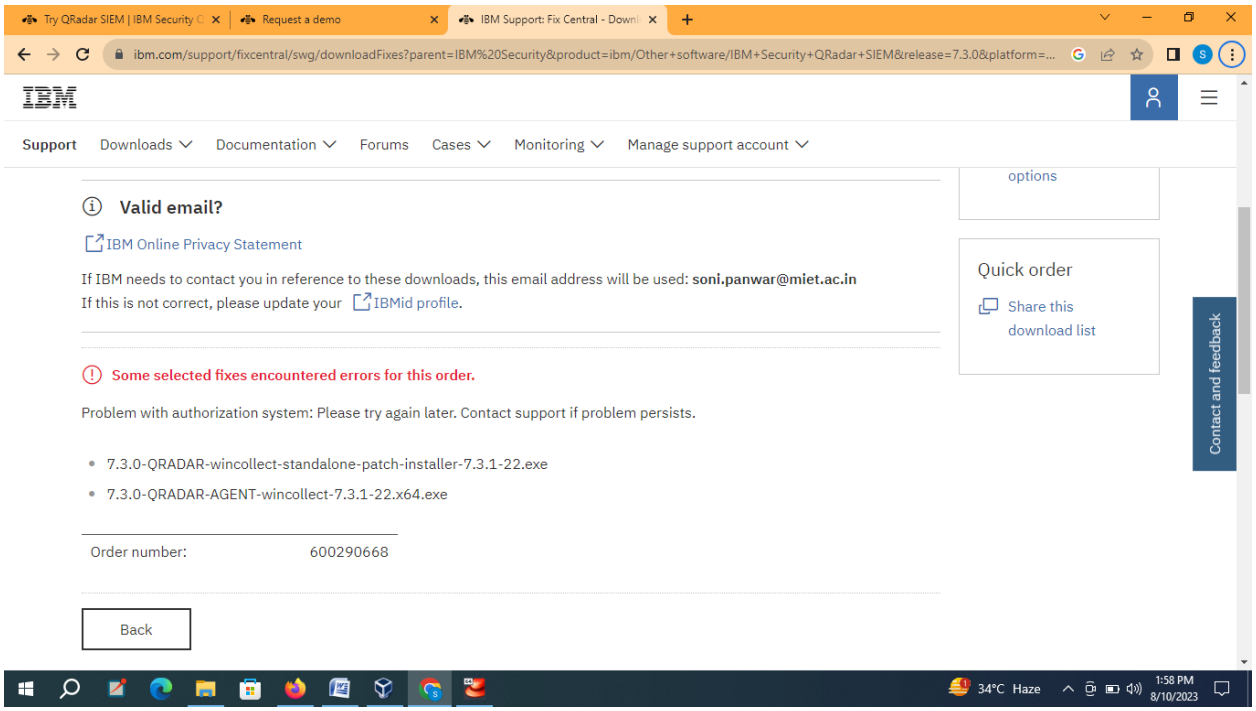
Dashboard will open




IBM QRadar Community Edition
https://10.11.15.52/console/core/jsp/Main.jsp
Search
QRadar Community Edition - License Agreement
Review the license terms before logging in.
English
electronic communications and storage. The Program may be used only for lawful purposes and in a lawful manner. Licensee agrees to use the Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permission's, or licenses required to enable its lawful use of the Program.
Cloud Service Provider:
Licensee may install the Program at a third party environment identified in the Program's installation guide that provides Licensee with infrastructure services, networking, storage and data center space for hosting software applications ("Cloud Service Provider"). This authorization does not modify or supersede any of Licensee's obligations in the applicable license agreement, including requirements for use in a virtualized environment. Licensee acknowledges that the verification terms in the applicable license agreement extend to the Cloud Service Provider environment on which the Programs are installed, and Licensee agrees to collect any required usage data. Licensee will not provide the Cloud Service Provider with any unauthorized use or access to the Program.
L/N: L-KFRN-BH7JG3
D/N: L-KFRN-BH7JG3
P/N: L-KFRN-BH7JG3
Decline
Accept
Waiting for 10.11.15.52...
Type here to search
31°C Haze
1:19 PM
9/2/2023
QRadar - Admin Console
https://10.11.15.52/console/qradar/jsp/QRadar.jsp
Search
IBM QRadar Security Intelligence - Community Edition
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
System Time: 4:48 PM
Admin
System Configuration
User Management
Assets
Data Sources
Remote Networks and Services Configuration
Deploy Changes
Advanced
Checking for undeployed changes...
Configuration
Reasons
Management
Forwarding Destinations
Routing Rules
Domain Management
Extensions Management
Resource Restrictions
User Management
Users
User Roles
Security Profiles
Authentication
Authorized Services
Tenant Management
Assets
Custom Asset Properties
Type here to search
31°C Haze
4:49 PM
9/2/2023



Step 7: To see the log file first download the wincollect software for windows and install it using filezilla. Then log file will open in GUI interface .
Click the **Log Activity** tab.
Verify events are received from remote appliance.



Configuring system settings, log sources, and integration with external systems based on the gathered information and use cases.

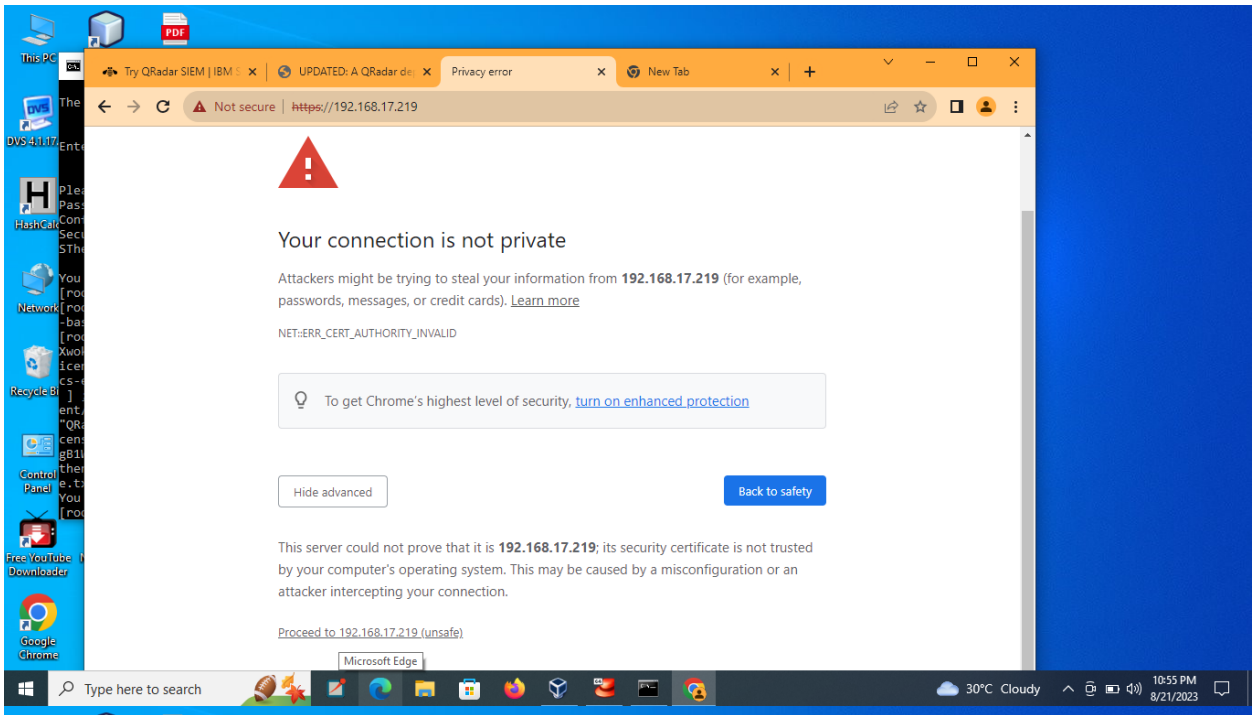
Downloading the virtual machine:

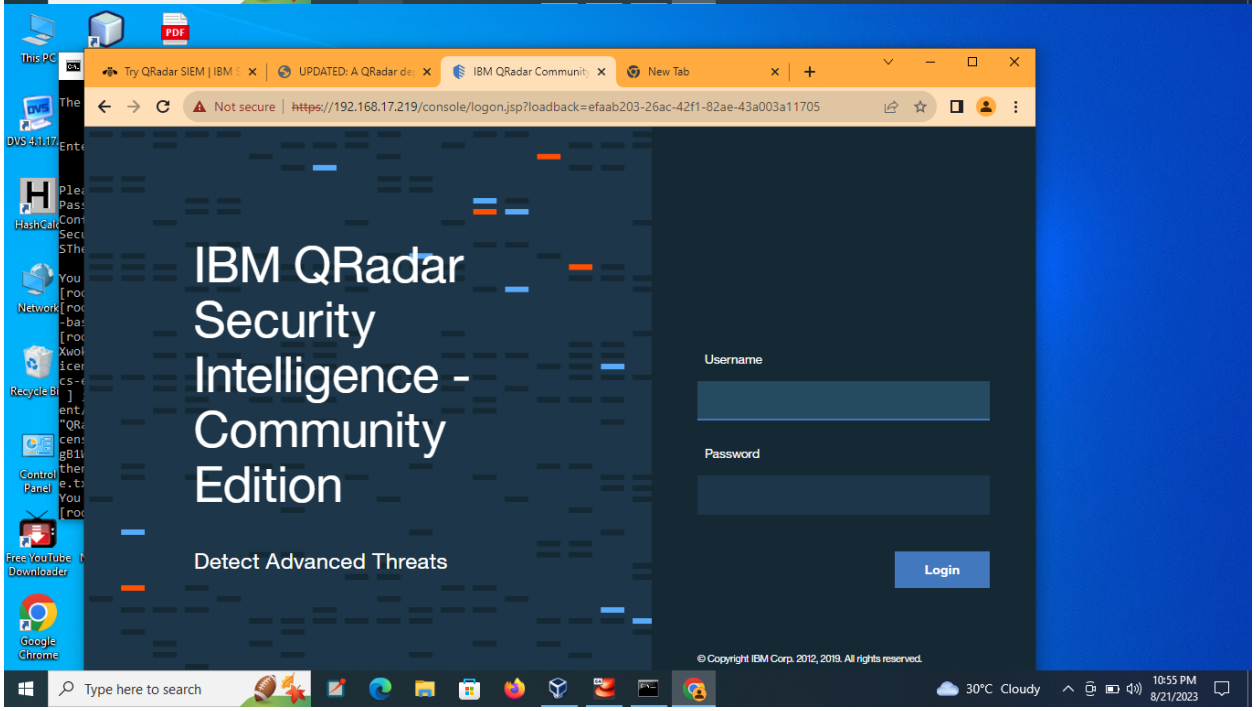
Download the virtual box according the requirement of operating system.

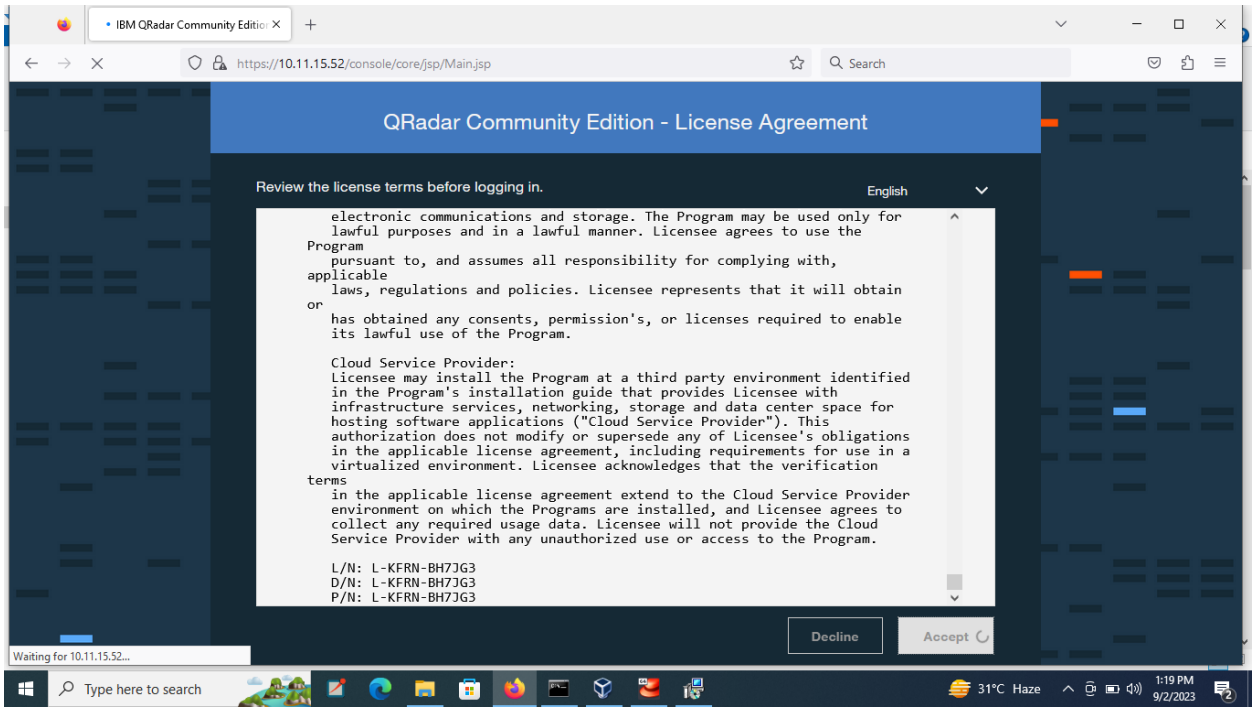
Such as download virtual box for windows *64 with the requirement of 8 GB RAM and 4 processor.

Login the console with username and password

On your host system, in a Web browser, go to this URL, replacing the IP address with the IP address of your QRadar VM.
https://172.16.1.226/console/
Approve the self-signed certificate.
Log in with these credentials, as shown below.
Username: admin
Password: P@ssw0rd

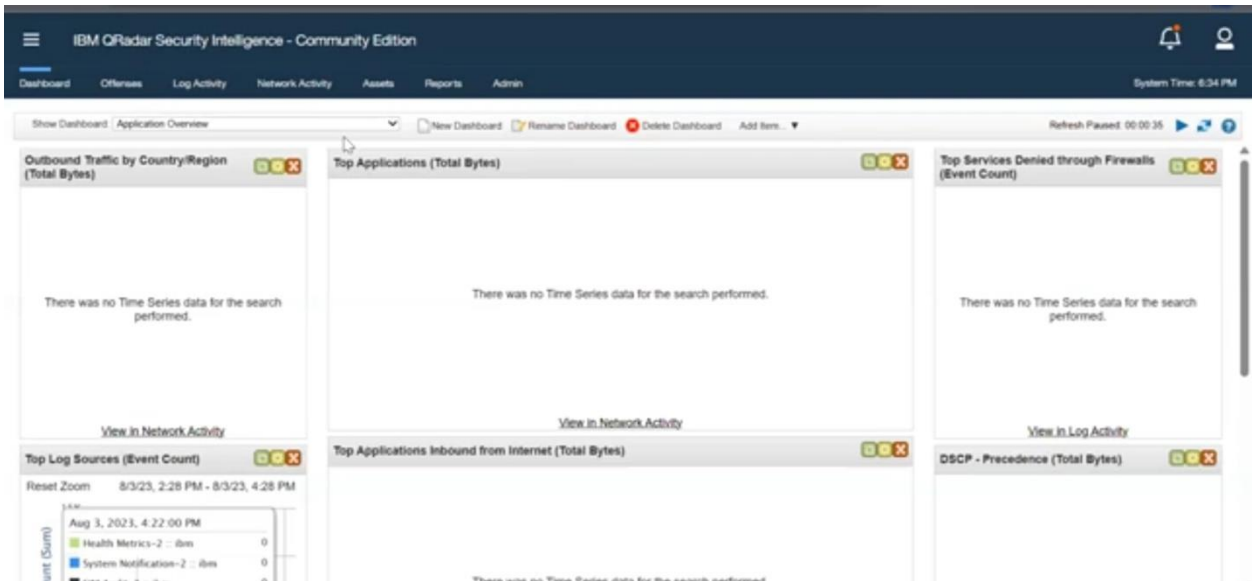

Try QRadar SIEM | IBM
UPDATED: A QRadar de
Privacy error
New Tab
Not secure | https://192.168.17.219
Your connection is not private
Attackers might be trying to steal your information from 192.168.17.219 (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
To get Chrome's highest level of security, turn on enhanced protection
Hide advanced
Back to safety
This server could not prove that it is 192.168.17.219; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to 192.168.17.219 (unsafe)
Microsoft Edge
Type here to search
30°C Cloudy
10:55 PM
8/21/2023

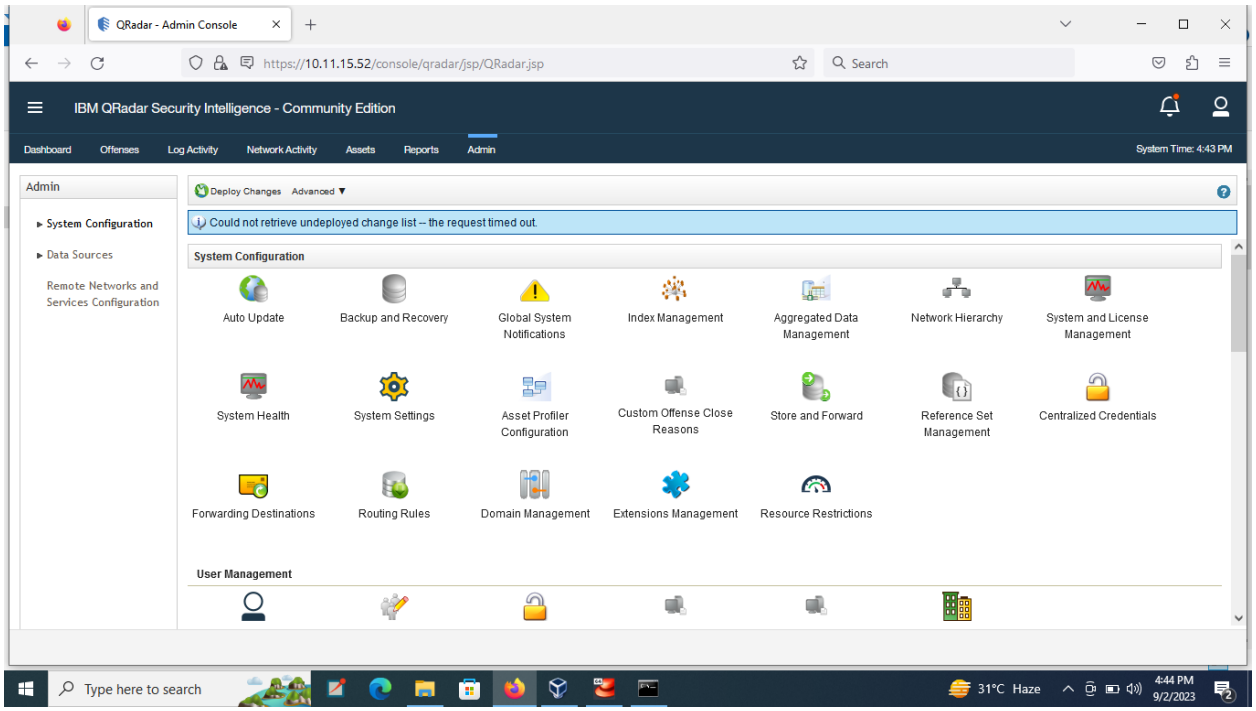

Try QRadar SIEM | IBM
UPDATED: A QRadar de
IBM QRadar Communit
New Tab
Not secure | https://192.168.17.219/console/logon.jsp?loadback=efaab203-26ac-42f1-82ae-43a003a11705
IBM QRadar Security Intelligence - Community Edition
Detect Advanced Threats
Username
Password
Login
© Copyright IBM Corp. 2012, 2019. All rights reserved.
Type here to search
30°C Cloudy
10:55 PM
8/21/2023

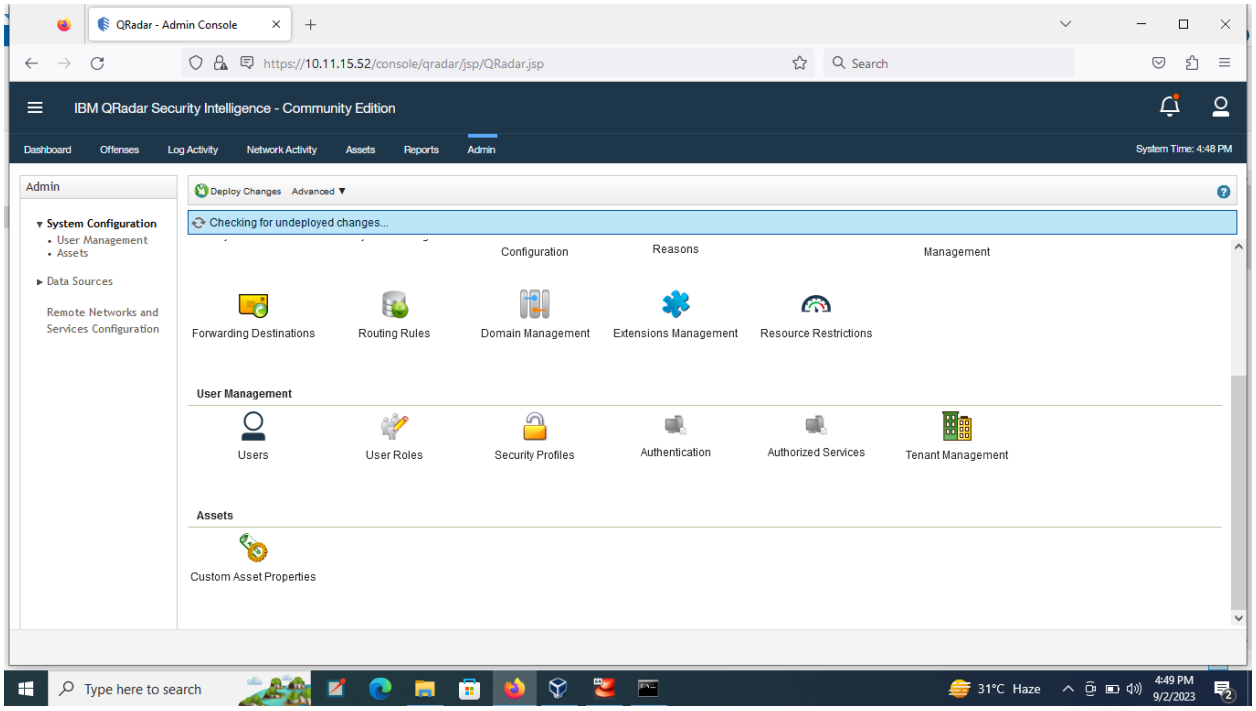


Viewing Log Sources

In the QRader administration page, at the top center, click the Admin tab.
Scroll down to the "Data Sources" section and click "Log Sources", as shown below.
A box pops up, as shown below.
In the top center, click the Add button.



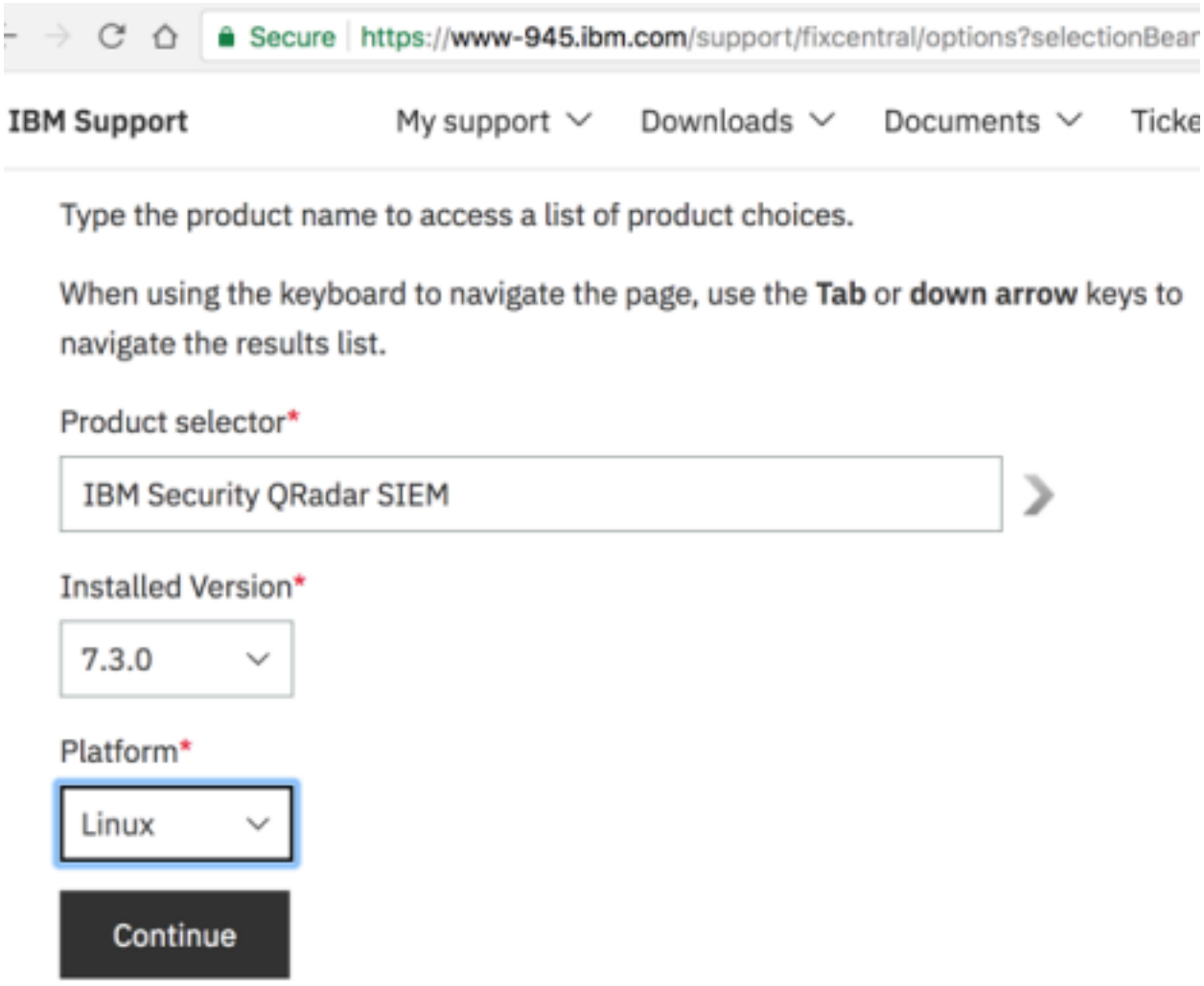




An "Add a log source" window appears. In the "Log Source Type" list box, scroll down to see "Microsoft Windows Security Event Log", as shown below.
You don't need to select it at this time; just to verify that it's there. It's not included in the default QRadar Community Edition installation, but I added it to the VM you downloaded already.
Close the "Add a log source" window.

Downloading WinCollect

The WinCollect agent is free software from IBM to send Windows event logs to Qradar.
In a Web browser, go to
https://www-945.ibm.com/support/fixcentral
Make these selections:
? Product selector: IBM Security QRadar SIEM
? Installed Version: 7.3.0
? Platform: Linux'
As shown below .
Click Continue.

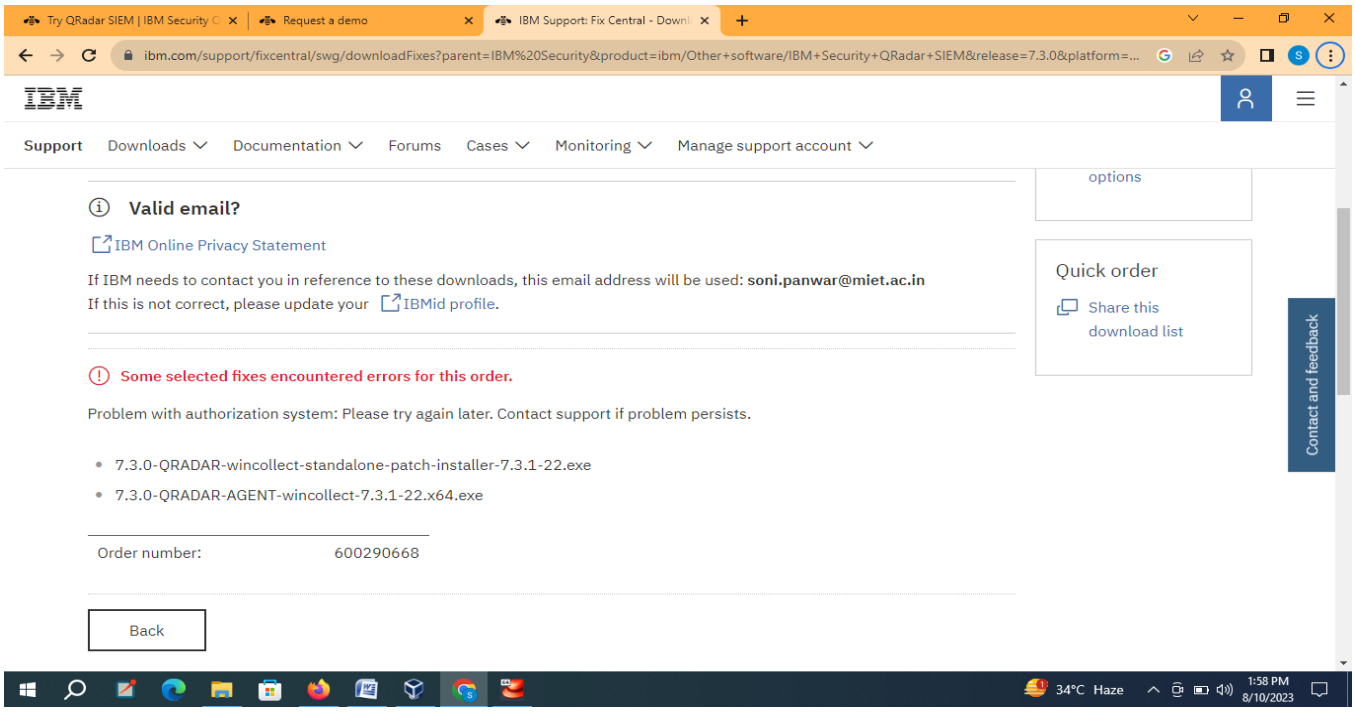


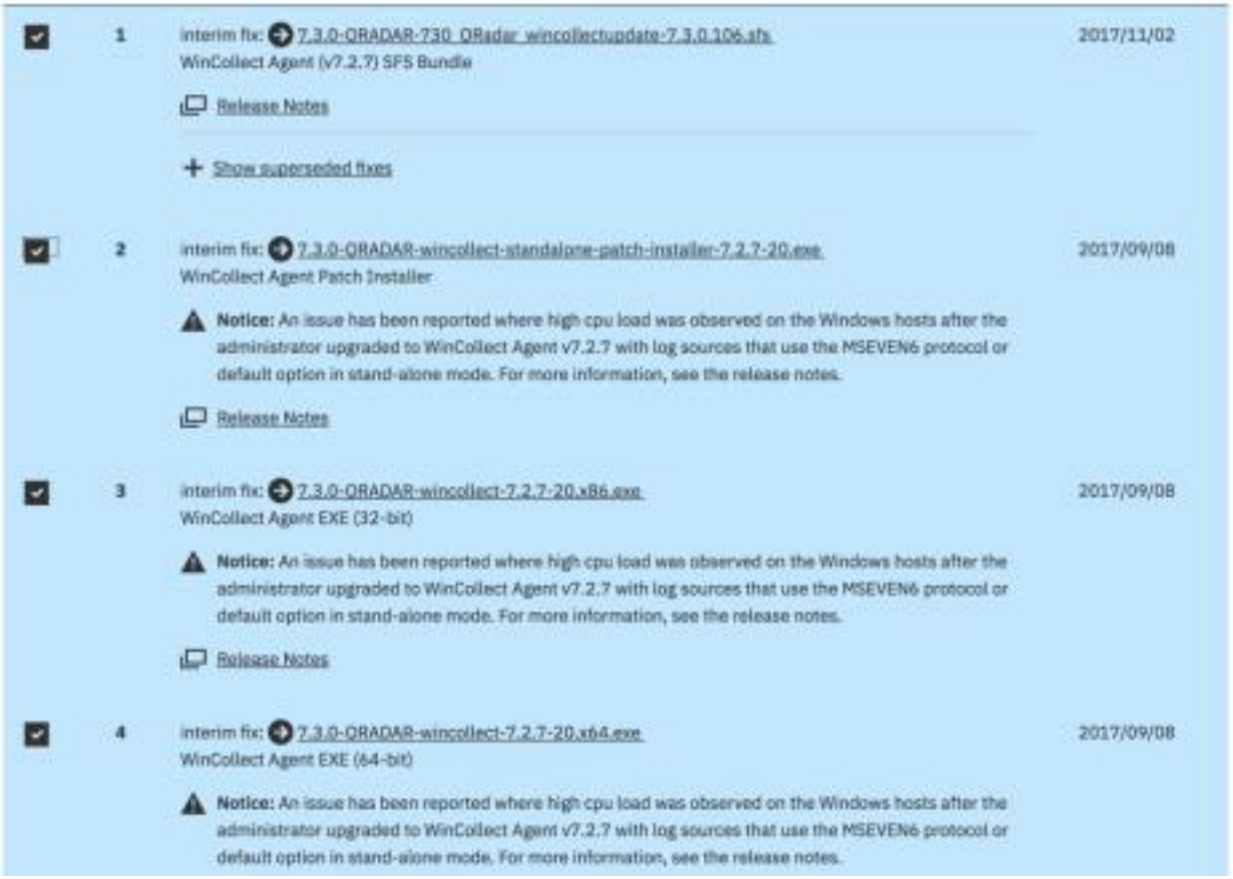
At the bottom of the next page, click the Text button and type in Windows as shown below.
Click Continue.

In the results, scroll down to the WINCOLLECT section, as shown below.

There are several items here, including the main engine for 32-bit and 64-bit windows, and various "interim fix" patches.

We only need the first 4 files. Check them, as shown below.

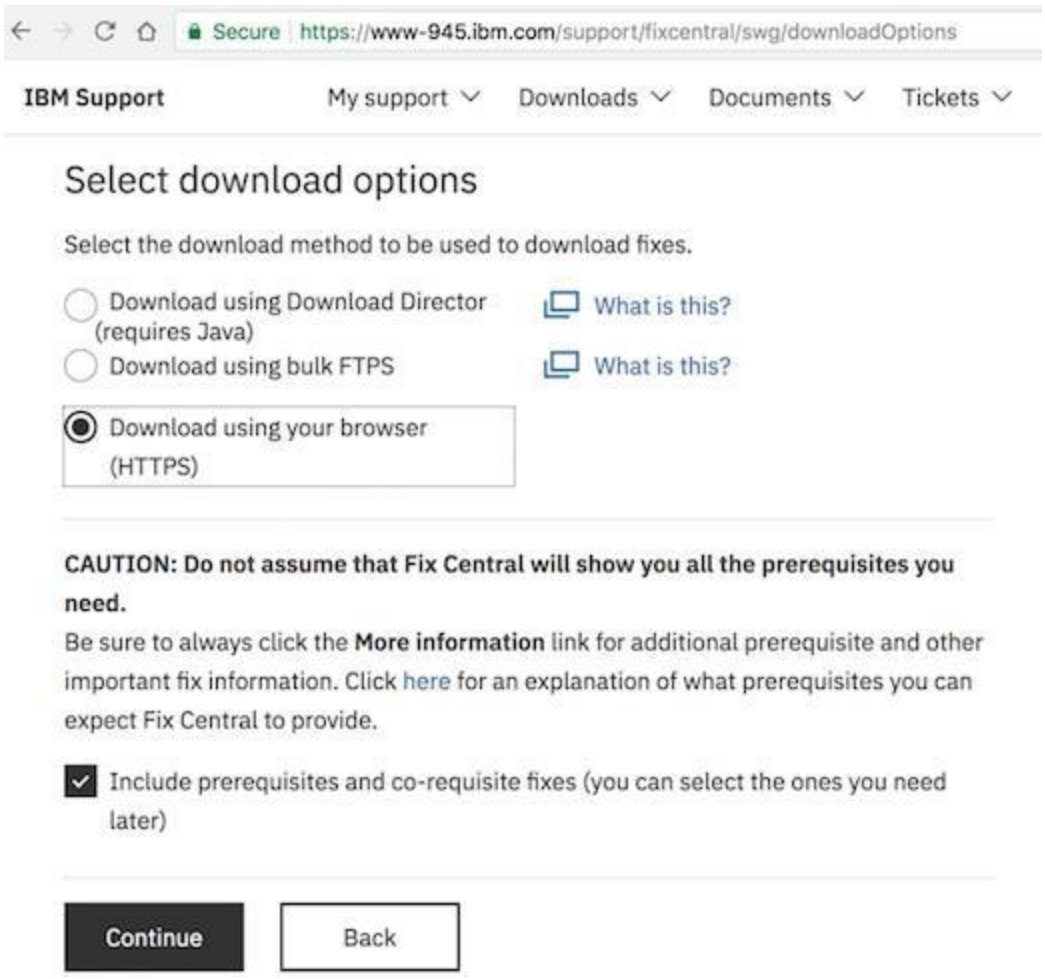




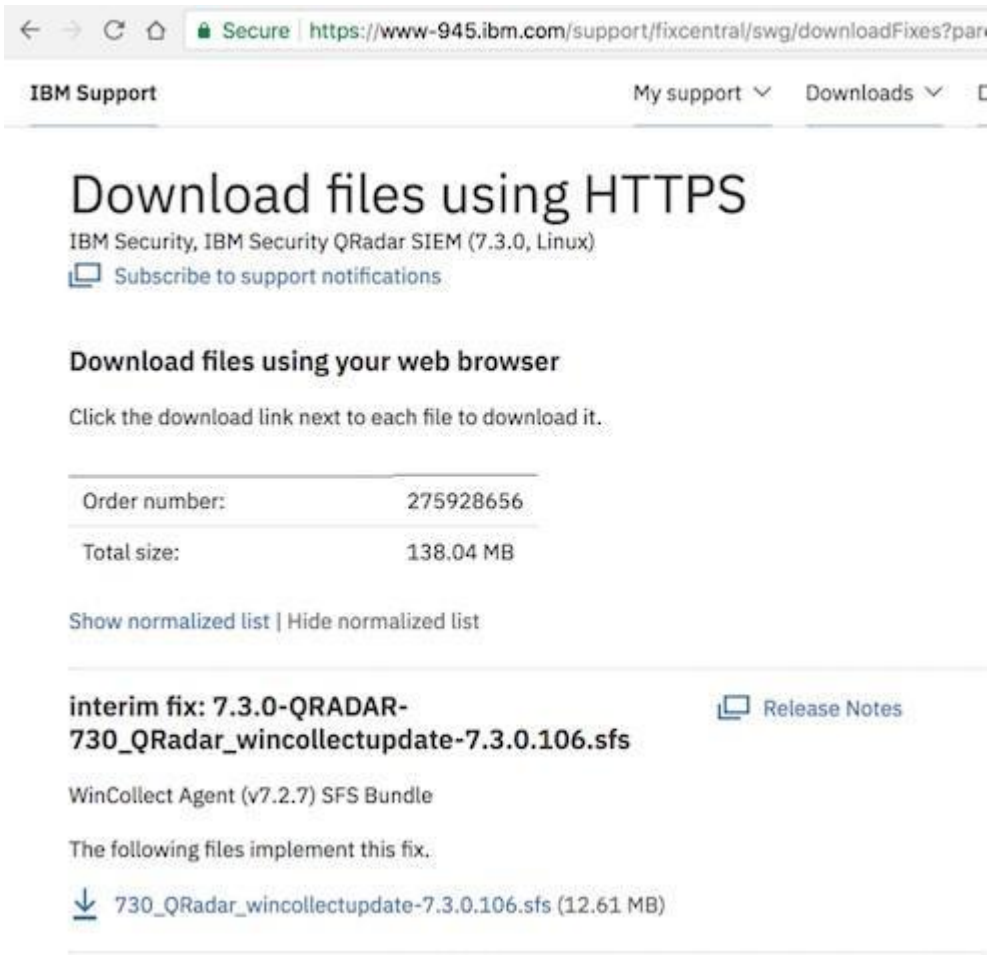
At the bottom, click the Continue button.

If you are prompted to, sign in to your IBM account.

On the next page, click the "Download using your browser" button, as shown below, and click Continue".



On the next page, click the blue downward-pointing arrow next to each product you want, one by one, as shown below,



Overview Of WinCollect Installation

To collect windows logs, we'll need to do these steps:

On the QRadar VM

7.3.0-QRADAR-730_QRadar_wincollectupdate-7.3.0.106.sfs

On 64-Bit Windows Systems

Install these files, in this order:

- wincollect-7.2.7-20.x64.exe
- wincollect-standalone-patch-installer-7.2.7-20.exe

Installing FileZilla

We need to update software on the QRadar VM. We'll need FileZilla to do that.

In a Web browser, go to

https://filezilla-project.org/download.php?platform=osx Install

FileZilla with the default options.

Run FileZilla. At the top, enter these values, as shown below:

- Host: Enter the IP address of your QRadar VM
- Username: root
- Password: P@ssw0rd
- Port: 22

At the top right, click the Quickconnect button.

A box pops up asking whether to remember passwords. For this project, there's no need to worry about unauthorized use of your QRadar VM, so click "Save passwords" and click OK.

An "Unknown host key" box pops up. Click OK. FileZilla

connects, as shown below.

The left pane shows your host system, and the right pane shows your QRadar VM.

Installing Software On The QRadar VM

In the right pane of FileZilla, click the top yellow folder icon for /

In the folder list, click /tmp

In the left pane of FileZilla, navigate to your Downloads folder.

Drag the
7.3.0-QRADAR-730_QRadar_wincollectupdate-7.3.0.106.sfs file from the left pane to the right pane, as shown below.

n your QRadar VM console, execute these commands, as shown below.

mkdir -p /media/updates cd /tmp

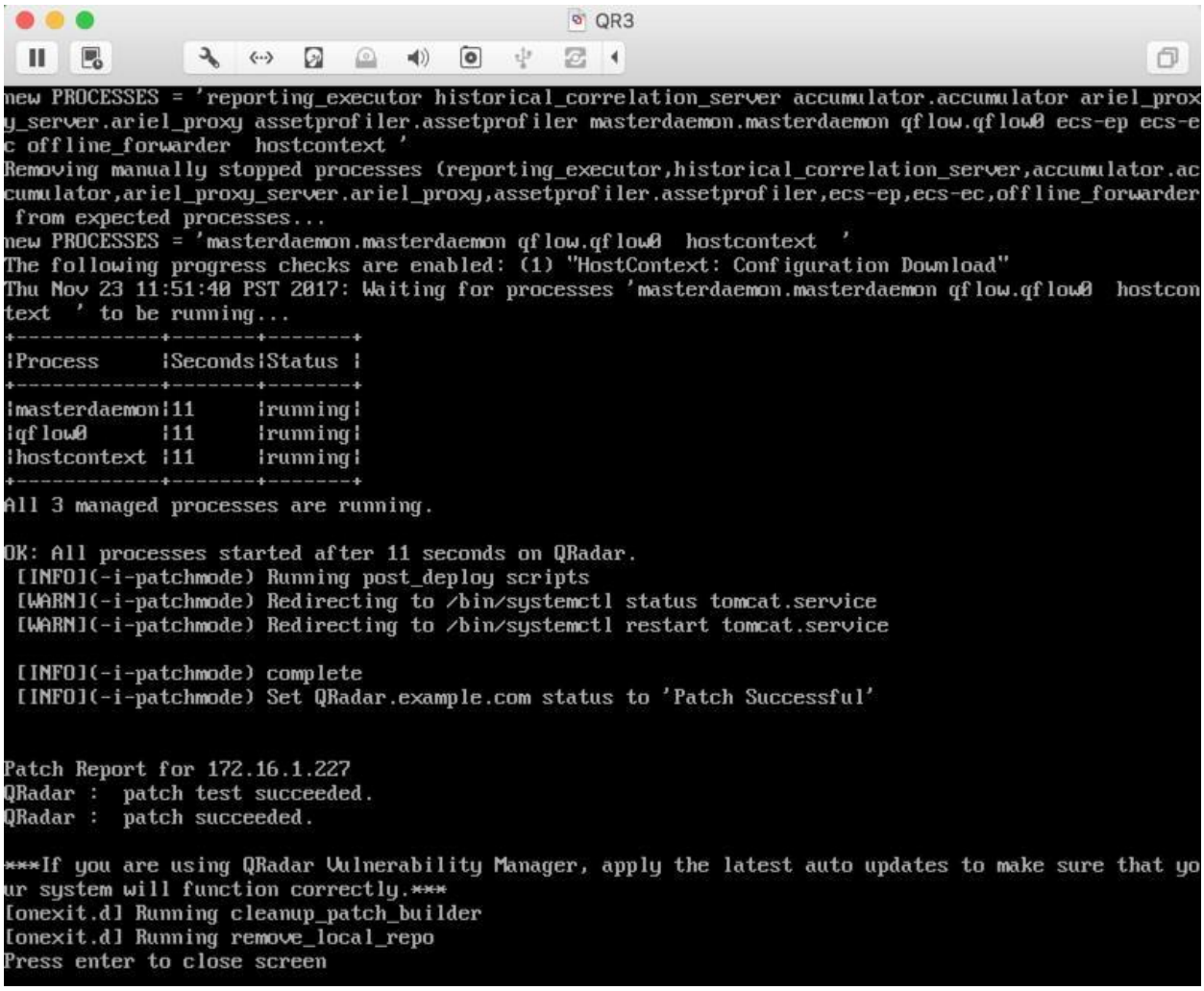
mount -o loop -t squashfs 730_QRadar_wincollectupdate-7.3.0.106.sfs /media/updates

/media/updates/installer

A message asks "Do you wish to continue?". Enter Y.

he installation takes about 5 minutes, and a lot of messages scroll by. Tomcat restarts, which is slow as always.

When it finishes, you'll see "patch succeeded", as shown below.



In your Web browser, log in to the QRadar GUI again with the credentials admin and P@ssw0rd

Installing Wincollect on the Windows System

Copy the appropriate version of Wincollect from your host machine's Downloads folder to your Windows machine.

- For 32-bit Windows: wincollect-7.2.7-20.x86.exe
- For 64-bit Windows: wincollect-7.2.7-20.x64.exe

Start the installer. Accept the default selections until you see the "Setup Type" box.

Click "Stand Alone, as shown below, and then click Next.

In the "Log Source Auto-creation Parameters" box, make these selections, as shown below.

- Check the "Create Log Source" box
- Enter a Log Source Identifier of Win-YOURNAME (using your own name, not the literal text "YOURNAME"
- Clear the System check

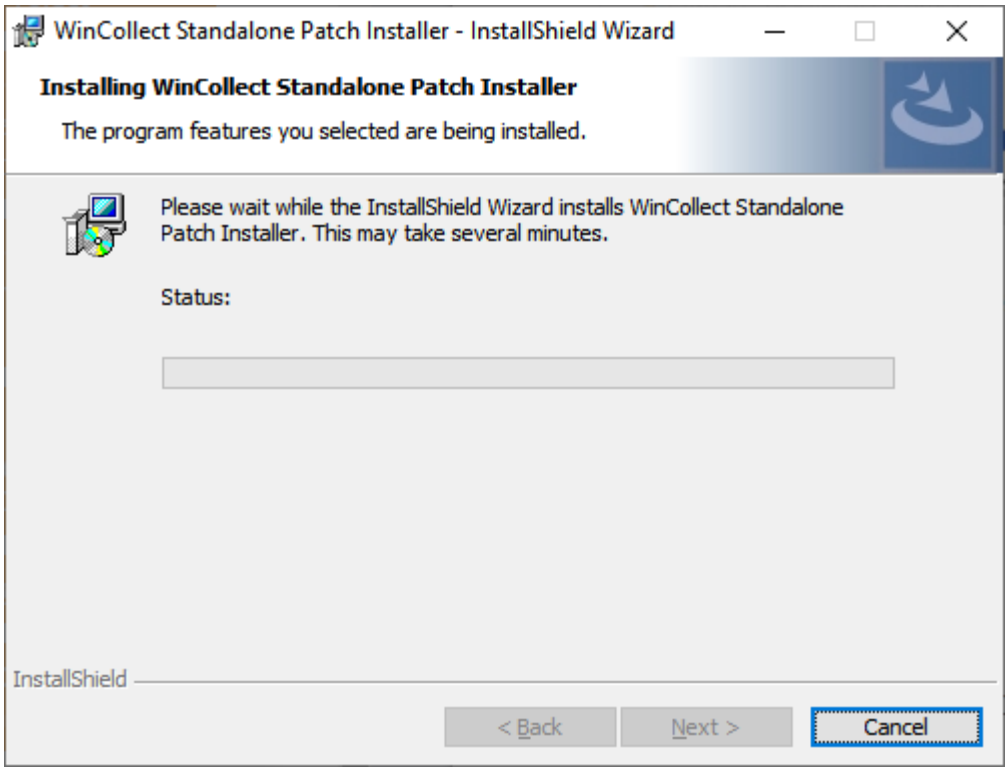
  box Click Next.

In the next box, make these selections, as shown below.

Replace the IP address with the correct IP address of your QRadar VM.

- Destination Name: QRadar
- Hostname / IP:

Click Next.



In the next box, accept the default Machine poll interval and click Next.

In the "Heartbeat Parameters" box, accept the default options and click **Next.**

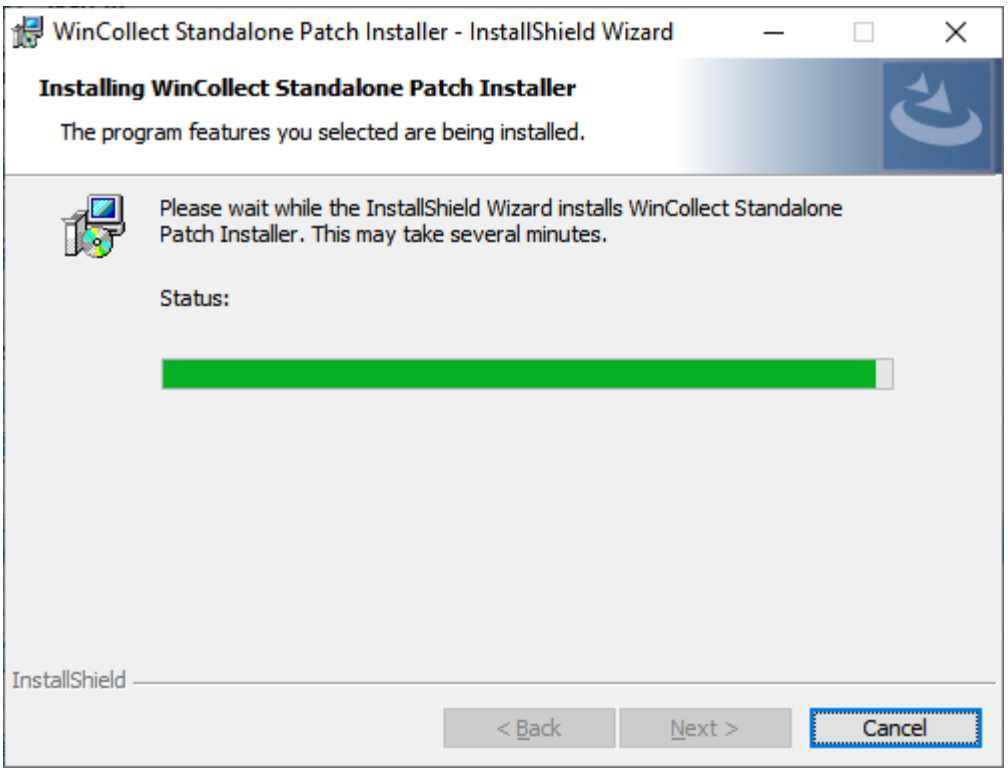
In the "Installation Parameters Summary" box, click Next. Click Install.

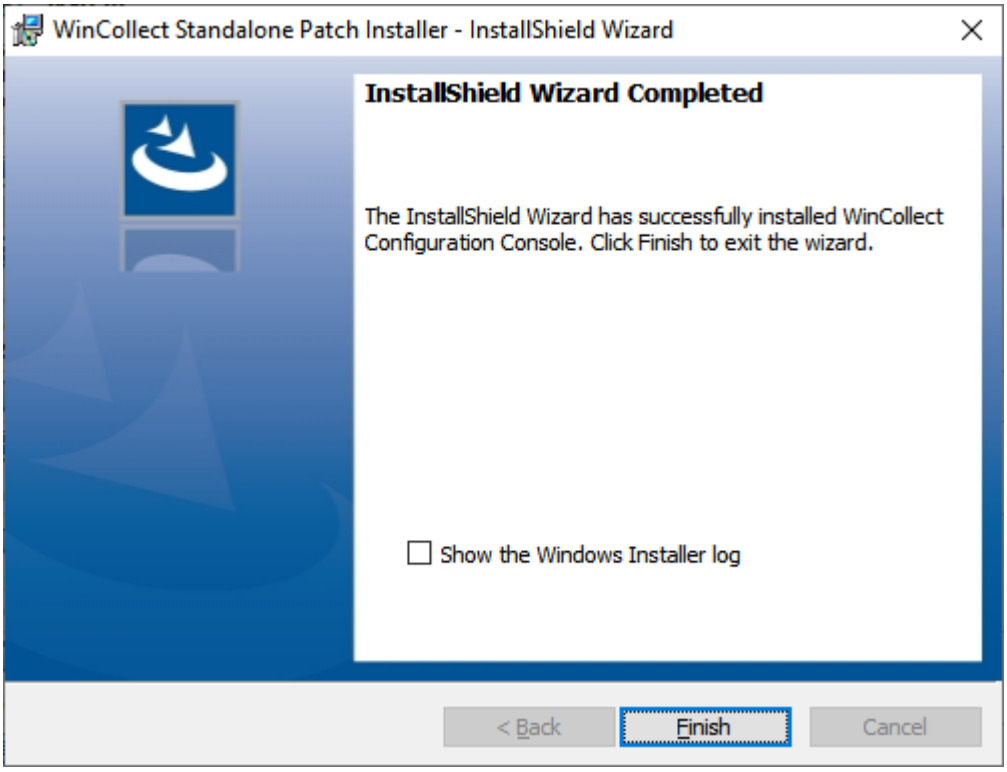
Click Finish.

Installing the Patch

Drag the wincollect-standalone-patch-installer-7.2.7-20.exe file into your Windows VM and double-click it.

Install it with the default options. If it wants to install .NET, allow it to do that.

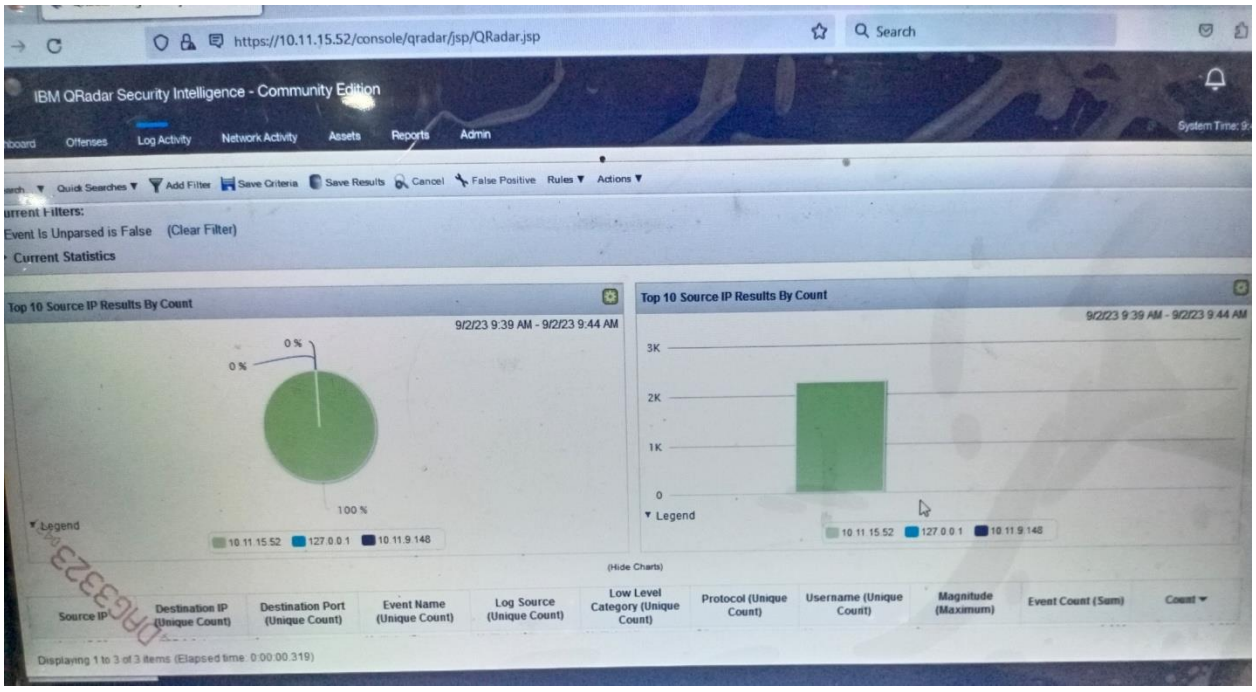


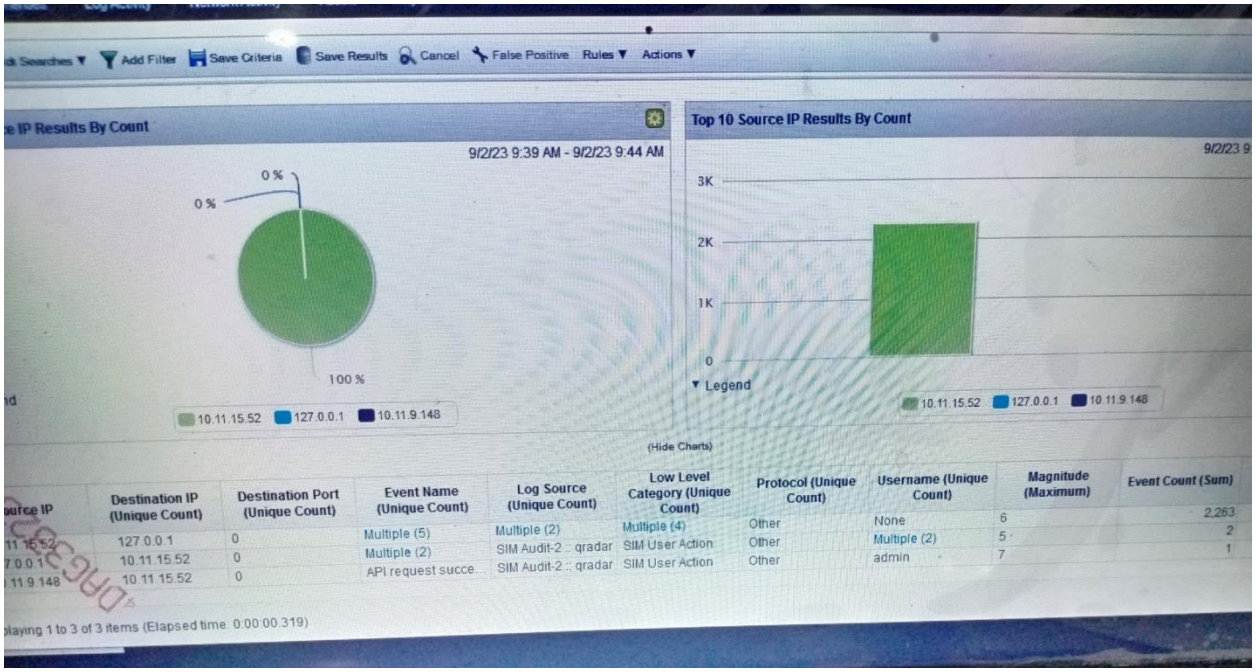


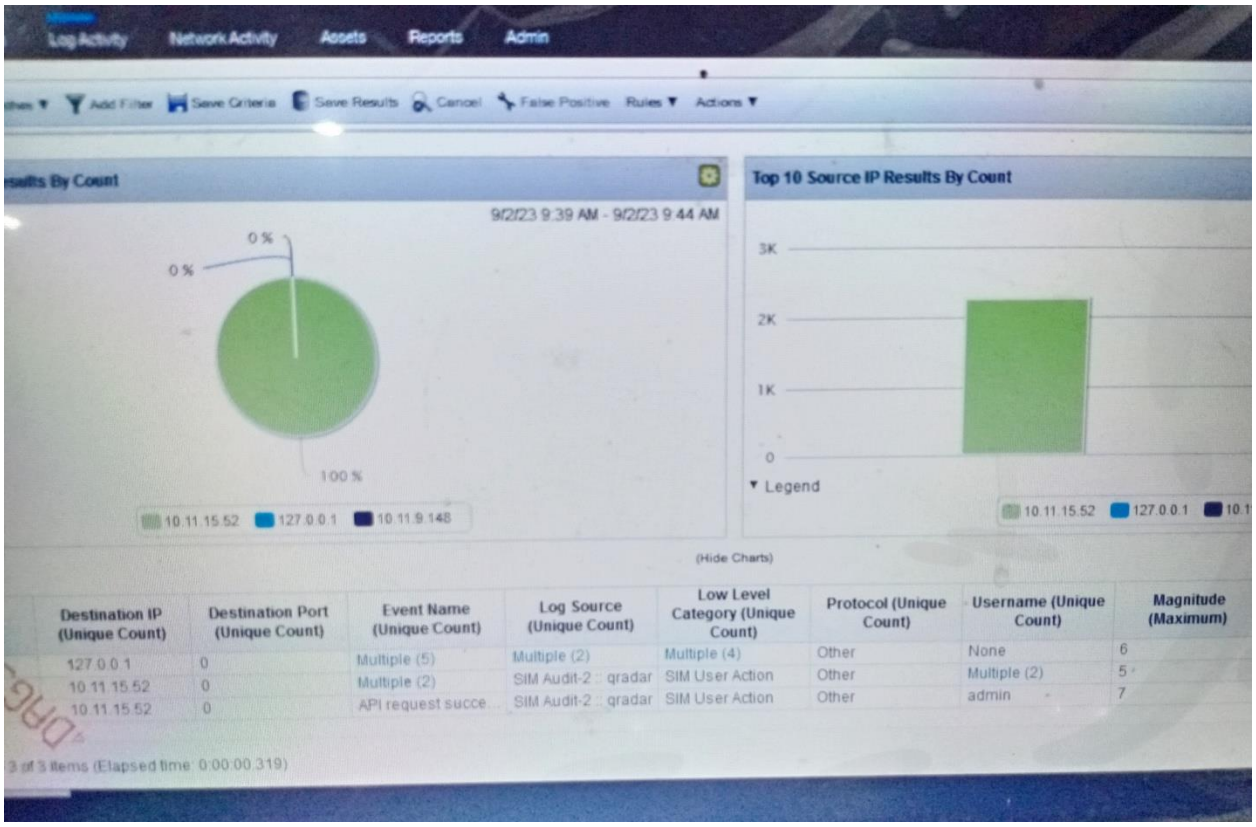
Viewing Log Sources

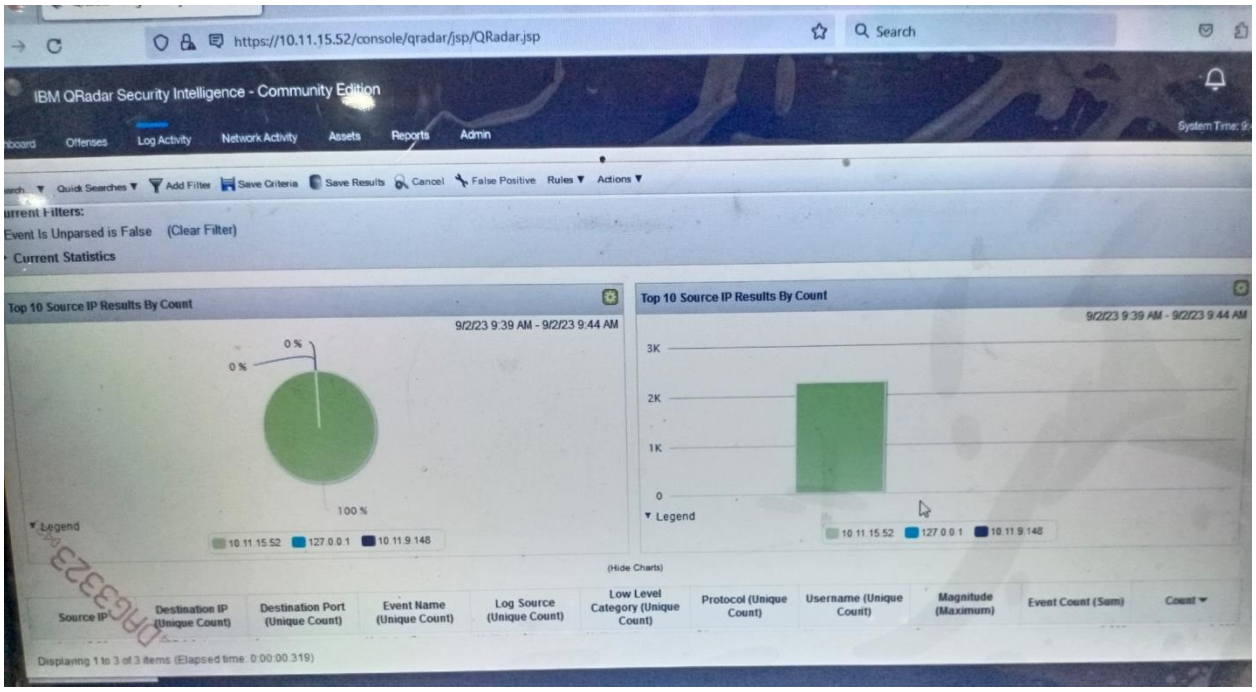
In the QRader administration page, at the top center, click the Admin tab.
Scroll down to the "Data Sources" section and click "Log Sources", as shown below.
A box pops up, as shown below.
In the top center, click the Add button.

An "Add a log source" window appears. In the "Log Source Type" list box, scroll down to see "Microsoft Windows Security Event Log", as shown below.
You don't need to select it at this time; just to verify that it's there. It's not included in the default QRadar Community Edition installation, but I added it to the VM you downloaded already.
Close the "Add a log source" window.


https://10.11.15.52/console/qradar/jsp/QRadar.jsp
Search
IBM QRadar Security Intelligence - Community Edition
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Event Is Unparsed is False
(Clear Filter)
Current Statistics
Top 10 Source IP Results By Count
9/2/23 9:39 AM - 9/2/23 9:44 AM
0 %
0 %
100 %
Legend
10.11.15.52
127.0.0.1
10.11.9.148
3K
2K
1K
0
(Hide Charts)
Source IP
Destination IP (Unique Count)
Destination Port (Unique Count)
Event Name (Unique Count)
Log Source (Unique Count)
Low Level Category (Unique Count)
Protocol (Unique Count)
Username (Unique Count)
Magnitude (Maximum)
Event Count (Sum)
Count
Displaying 1 to 3 of 3 items (Elapsed time: 0:00:00.319)


Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Top 10 Source IP Results By Count
9/2/23 9:39 AM - 9/2/23 9:44 AM
0 %
0 %
100 %
10.11.15.52
127.0.0.1
10.11.9.148
3K
2K
1K
0
Legend
(Hide Charts)
Destination IP (Unique Count)
Destination Port (Unique Count)
Event Name (Unique Count)
Log Source (Unique Count)
Low Level Category (Unique Count)
Protocol (Unique Count)
Username (Unique Count)
Magnitude (Maximum)
Event Count (Sum)
127.0.0.1
10.11.15.52
10.11.9.148
Multiple (5)
Multiple (2)
API request succe...
Multiple (2)
SIM Audit-2 :: qradar
SIM Audit-2 :: qradar
Multiple (4)
SIM User Action
SIM User Action
Other
Other
Other
None
Multiple (2)
admin
6
5
7
2,263
2
1


Log Activity
Network Activity
Assets
Reports
Admin
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Top 10 Source IP Results By Count
9/2/23 9:39 AM - 9/2/23 9:44 AM
0 %
0 %
100 %
10.11.15.52
127.0.0.1
10.11.9.148
3K
2K
1K
0
Legend
(Hide Charts)
Destination IP (Unique Count)
Destination Port (Unique Count)
Event Name (Unique Count)
Log Source (Unique Count)
Low Level Category (Unique Count)
Protocol (Unique Count)
Username (Unique Count)
Magnitude (Maximum)
127.0.0.1 0 Multiple (5) Multiple (2) Multiple (4) Other None 6
10.11.15.52 0 Multiple (2) SIM Audit-2 :: qradar SIM User Action Other Multiple (2) 5
10.11.15.52 0 API request succe... SIM Audit-2 :: qradar SIM User Action Other admin 7
3 of 3 items (Elapsed time: 0:00:00.319)

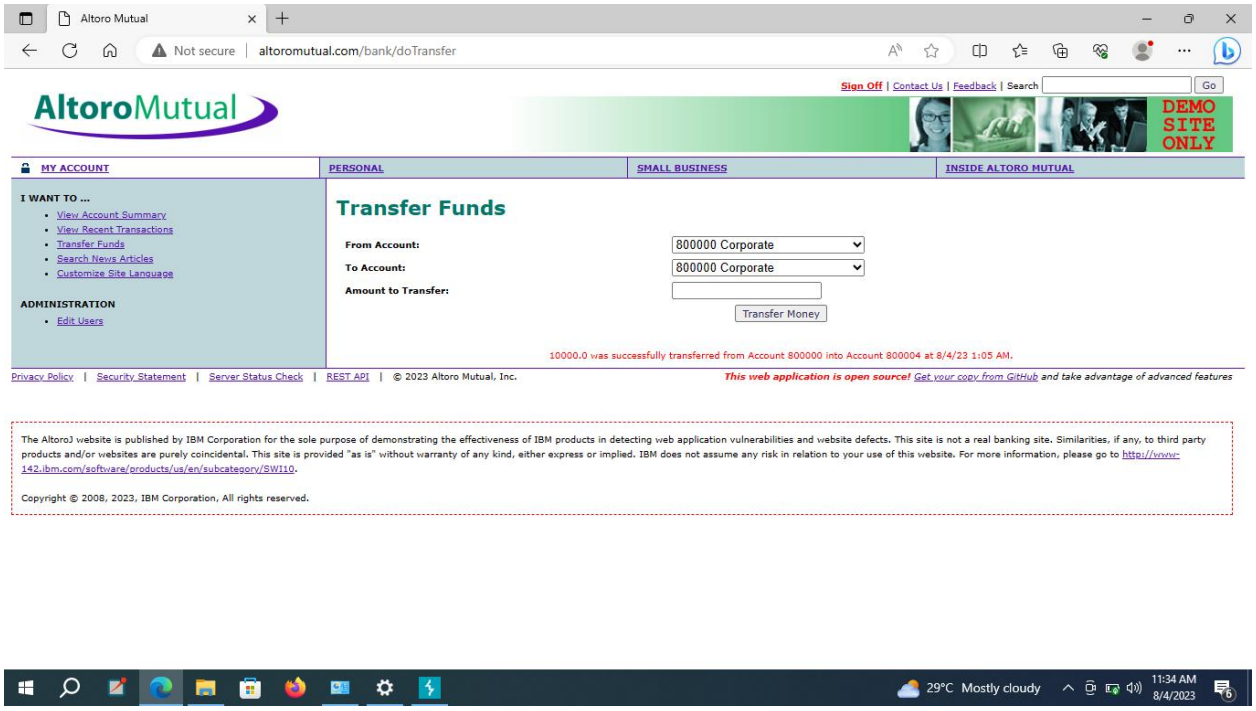

https://10.11.15.52/console/qradar/jsp/QRadar.jsp
Search
IBM QRadar Security Intelligence - Community Edition
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Event Is Unparsed is False (Clear Filter)
Current Statistics
Top 10 Source IP Results By Count
9/2/23 9:39 AM - 9/2/23 9:44 AM
0 %
0 %
100 %
Legend
10.11.15.52
127.0.0.1
10.11.9.148
3K
2K
1K
0
(Hide Charts)
Source IP
Destination IP (Unique Count)
Destination Port (Unique Count)
Event Name (Unique Count)
Log Source (Unique Count)
Low Level Category (Unique Count)
Protocol (Unique Count)
Username (Unique Count)
Magnitude (Maximum)
Event Count (Sum)
Count
Displaying 1 to 3 of 3 items (Elapsed time: 0:00:00.319)

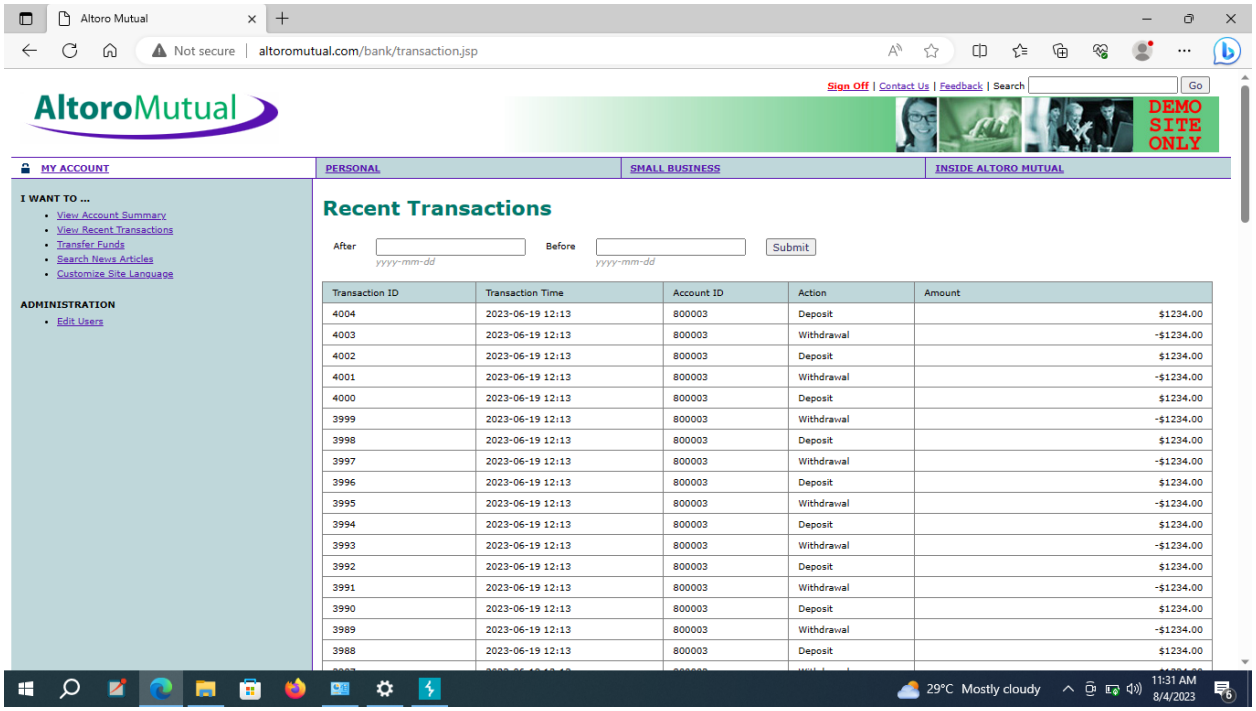
Conclusion:

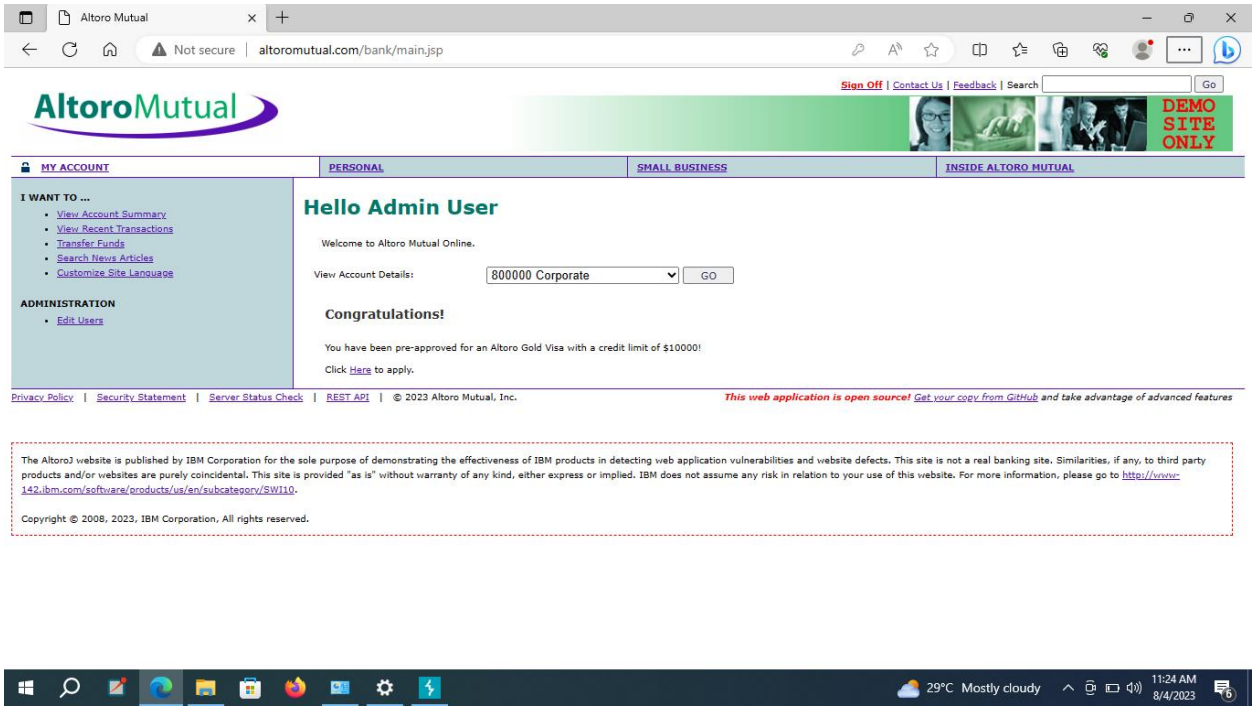
During this I learnt the work on different tools to analyze the vulnerabilities esist in the network or system and we can minimize the vulnerabilities so we can reduce the attacks.

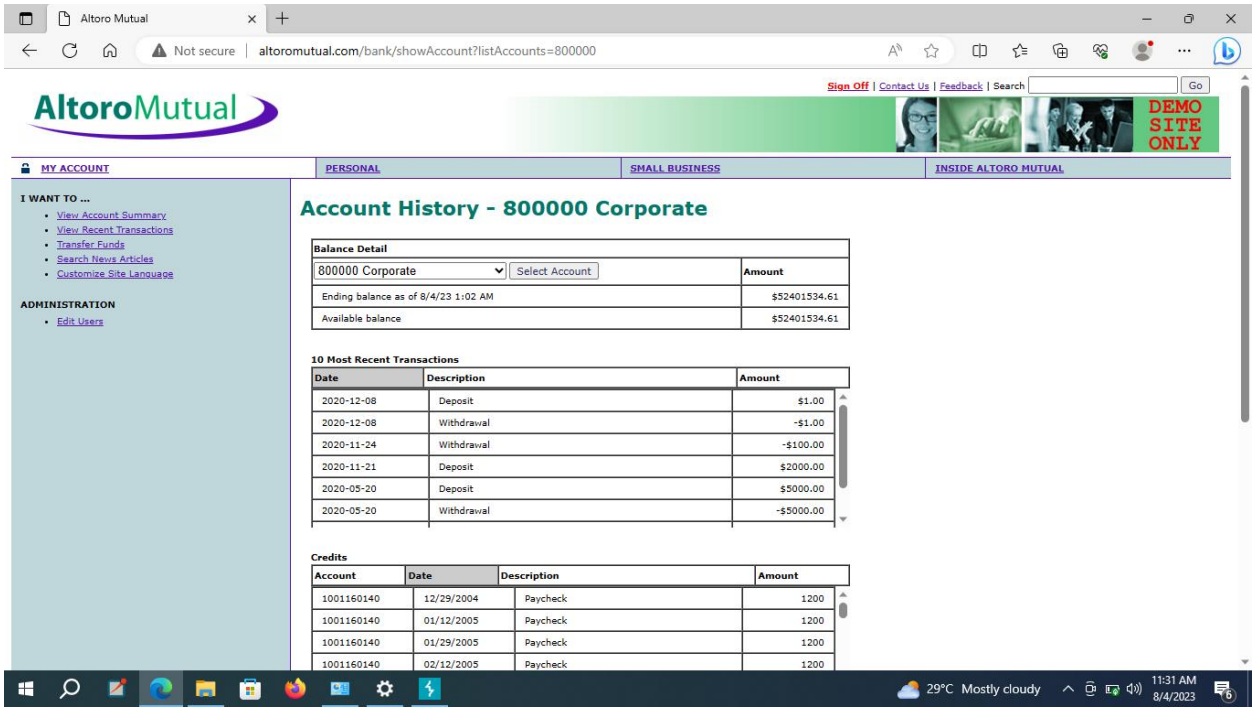
I learn how different attacks performed such as SQL Attacks , cross site scripting etc.

Identify the vulnerabilities using nessus tools, burpsuite, kali linux and metasploit etc.




Altoro Mutual
Not secure
altoromutual.com/bank/transaction.jsp
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Recent Transactions
After
yyyy-mm-dd
Before
yyyy-mm-dd
Submit
Transaction ID | Transaction Time | Account ID | Action | Amount
4004 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
4003 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
4002 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
4001 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
4000 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3999 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3998 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3997 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3996 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3995 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3994 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3993 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3992 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3991 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3990 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
3989 | 2023-06-19 12:13 | 800003 | Withdrawal | -$1234.00
3988 | 2023-06-19 12:13 | 800003 | Deposit | $1234.00
29°C Mostly cloudy
11:31 AM
8/4/2023


Altoro Mutual
Not secure
altoromutual.com/bank/main.jsp
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details:
800000 Corporate
GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.
29°C Mostly cloudy
11:24 AM
8/4/2023



After identifying the vulnerabilities remove them from the system.

Monitor the network and system using IBM QRadar Community edition it work using SIEM and SOC capabilities.