Cyber Security Build-a-thon 2023

Team Member: Dr.K.Karunambiga, Professor, Karpagam Institute of Technology

Contact : 9384158988, karunambiga.cse12@gmail.com

Overview:

IBM's Virtual Faculty Build a thon 2023 offered an intensive bootcamp focused on Cyber Security & SEIM, leveraging the power of QRadar. Bringing together a diverse cohort of educators, researchers, and cyber security enthusiasts, the event aimed to foster collaboration, enhance skills, and stimulate innovation in the realm of security information and event management.

Key Sessions of Bootcamp:

Introduction to SEIM and QRadar: Detailed overview of the QRadar platform and its capabilities in the realm of security information and event management.

Hands-on Labs:

1. Guided exercises where participants set up QRadar instances, integrate data sources, and create offense and flow processing.

2. Nessus & Metasploitble tool used to scan the vulnerability in web application

Activation Code: K2DT-YDXH-R8TE-HC83-KNM4

https://localhost:8834/#/

Threat Intelligence with QRadar: Leveraging threat intelligence feeds and integrating them with QRadar for enhanced security analytics.

Advanced Correlation Techniques: Crafting sophisticated correlation rules to detect multi-stage and advanced threats.

Participants were tasked with creating an innovative SEIM solution using QRadar to address a contemporary cyber security challenge. The solutions were judged based on their innovation, technical prowess, scalability, and relevance.

Key Takeaways:

Enhanced Skillset: Participants gained hands-on experience with one of the industry's leading SEIM tools, expanding their cyber security skill set.

Collaboration: The event fostered networking and collaboration among top educators and professionals

in the field.

Innovative Solutions: The Build a thon challenge yielded numerous innovative solutions, showcasing the potential of QRadar in addressing modern cyber security threats.

The event paves the way for future collaborations, research endeavors, and innovations in the realm of cyber security.

List of Vulnerable Parameter, location discovered

1. CWE-285: Improper Authorization

API1:2023 - Broken Object Level Authorization

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.

2. CWE-287: Improper Authentication

API2:2023 - Broken Authentication

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.

3.CWE-639: Authorization Bypass Through User-Controlled Key

API3:2023 - Broken Object Property Level Authorization

This category combines API3:2019 Excessive Data Exposure and API6:2019 - Mass Assignment, focusing on the root cause: the lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties.

4. CWE-400: Uncontrolled Resource Consumption

API4:2023 - Unrestricted Resource Consumption

Satisfying API requests requires resources such as network bandwidth, CPU, memory, and storage. Other resources such as emails/SMS/phone calls or biometrics validation are made available by service providers via API integrations, and paid for per request. Successful attacks can lead to Denial of Service or an increase of operational costs.

5.CWE-284: Improper Access Control

API5:2023 - Broken Function Level Authorization

Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.

6. CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

API6:2023 - Unrestricted Access to Sensitive Business Flows

APIs vulnerable to this risk expose a business flow - such as buying a ticket, or posting a comment - without compensating for how the functionality could harm the business if used excessively in an automated manner. This doesn't necessarily come from implementation bugs.

7. CWE-918: Server-Side Request Forgery

API7:2023 - Server Side Request Forgery

Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.

8.CWE-16 : Configuration

API8:2023 - Security Misconfiguration

APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow security best practices when it comes to configuration, opening the door for different types of attacks.

9.CWE-664: Improper Control of a Resource Through its Lifetime

API9:2023 - Improper Inventory Management

APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions also are important to mitigate issues such as deprecated API versions and exposed debug endpoints.

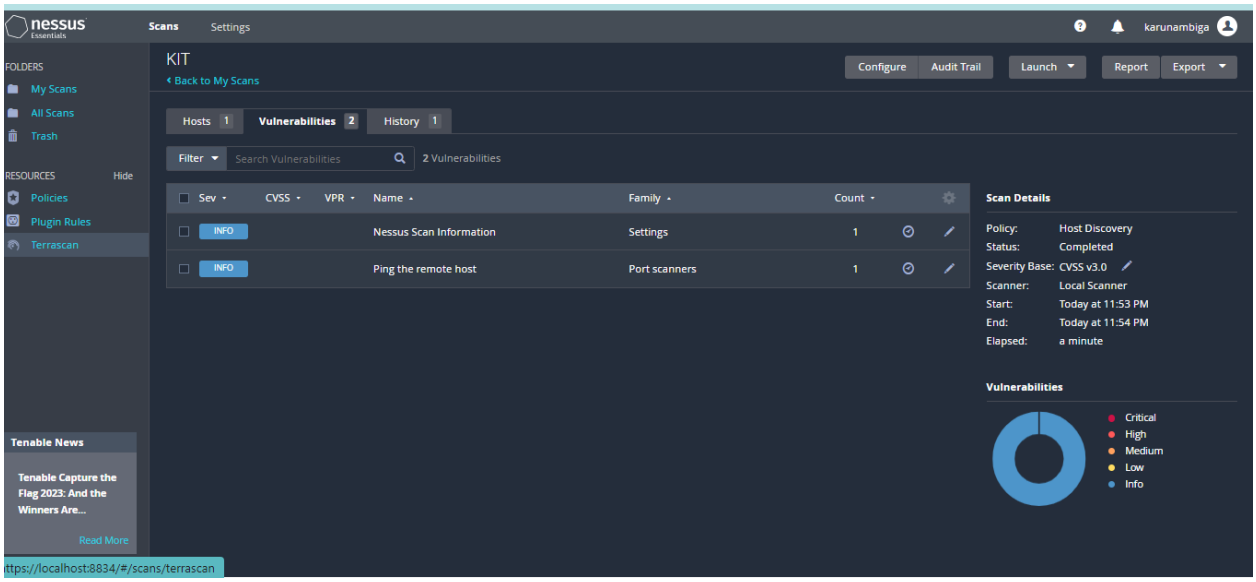
10. CWE-648: Incorrect Use of Privileged APIs

API10:2023 - Unsafe Consumption of APIs

Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. In order to compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly.

NESSUS Vulnerability Report

Nessus is one of the most widely used vulnerability scanning tools. When Nessus performs a scan on a system or network, it checks against a database of known vulnerabilities and produces a report detailing any vulnerabilities that were found. This tool is used to scan our college website https://kargamtech.ac.in. The report of the Nessus tool is given below.



Report: Installation of QRadar Community Edition using Oracle VirtualBox and MobaXterm

Introduction:

The objective of this report is to detail the process of installing the IBM QRadar Community Edition (CE) on a virtual machine using Oracle VirtualBox and remotely managing it with MobaXterm.

Environment Setup:

Host Machine OS: Windows 10 Pro

Virtualization Software: Oracle VirtualBox v6.1

Remote Management Tool: MobaXterm v21.0

Target Software: QRadar Community Edition

Steps Undertaken:

1. Virtual Machine Creation in Oracle VirtualBox:

VirtualBox Configuration:

Launched Oracle VirtualBox and initiated a new virtual machine.

Named the VM as "QRadarCE" and selected "Linux" and "Red Hat (64-bit)" as the OS type and version,

respectively.

Allocated 8GB RAM and created a 200GB virtual hard disk.

Network Setup:

Configured the VM's network adapter to "Bridged Adapter" to ensure it could acquire an IP address from the main network.

2. QRadar CE Installation:

a. Boot and Install:

Started the VM, initiating the QRadar CE installation.

Followed on-screen prompts, set network configurations, and other system parameters.

b. Completion:

After installation, the system rebooted into QRadar, displaying the IP address assigned to the system.

3. Remote Access with MobaXterm:

a. SSH Configuration:

Launched MobaXterm on the host machine.

Initiated an SSH session with the IP address displayed on the QRadar VM.

Utilized default QRadar credentials (admin and the predefined password) to access the system.

b. Management:

Successfully SSH'd into the QRadar instance and managed configurations and viewed logs using MobaXterm's terminal.

4. Web UI Access:

Accessed QRadar's web interface from a browser using the provided IP address.

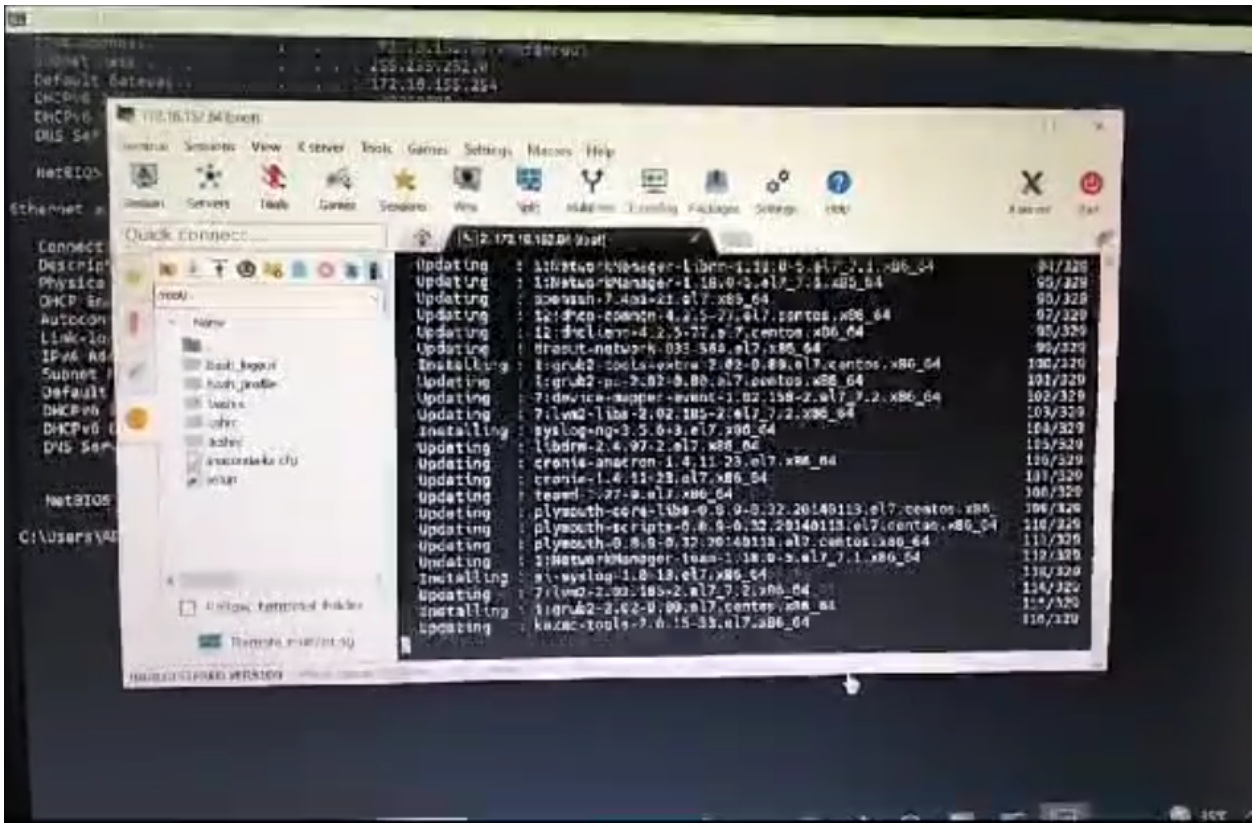
Logged in and interacted with the UI to set up log sources, rules, and view offenses.

Observations:

Performance: The performance of QRadar CE in a virtualized environment was satisfactory for learning and experimental purposes. However, for production or heavy usage, dedicated resources would be recommended.

MobaXterm Utility: Using MobaXterm streamlined the remote management process, offering a range of tools and functionalities beyond just SSH.

Network Configuration: Using Bridged Adapter mode facilitated easier access to the VM both for SSH and web UI.



Conclusion:

The installation of QRadar Community Edition on Oracle VirtualBox was successful, and the use of MobaXterm facilitated efficient remote management. The setup serves as a valuable environment for learning, experimentation, and preliminary SIEM activities.