Web application Testing using Cyber security tools- Qradar- Nessus Metasploitable

Part 1: Executive Summary

1. Overview

Web application testing is a software testing technique exclusively adopted to test the applications hosted on the web, which will test the application interfaces and other functions.

An organizational security policy is a set of rules or procedures an organization imposes on its operations to protect sensitive data. Identify, protect, detect, respond, and recover; aid organizations in their effort to spot, manage, and counter cyber security events promptly.

IBM Security Qradar Suite is a modernized threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the entire incident lifecycle.

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors. IBM QRadar then performs an accurate time analysis of the log data, and network flows to identify and stop malicious activity quickly, preventing or minimizing damage to the organization.

BM QRadar is used to perform analysis of the log data and the network flows in real time so that malicious activities are identified and stopped as soon as possible.

Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, and more. Nessus works by testing each port on a computer system, identifying which services are running, and then trying each of these services to detect vulnerabilities. Nessus is installed on one computer and then used to test many other computers.

2. List of employees participated

S. No.	Name	Designation	Mobile No.
1	Bakkialakshmi VS	ASSISTANT PROFESSOR	9710933991

3. List of Vulnerable Parameter, Location Discovered

Table:

S.No	Name of the Vulnerability	References - CWE
1.	A01 – Broken Access control	CWE-284: Improper Access Control
2.	A02 – Cryptographic failures	CWE-326: Inadequate Encryption Strength
3.	A03 – Injection	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
4.	A04 – Insecure Design	CWE-657: Violation of Secure Design Principles
5.	A05 – Security misconfiguration	CWE-693: Protection Mechanism Failure
6.	A06 – Vulnerable and outdated components	CWE-1104: Use of Unmaintained Third Party Components
7.	A07 – Identification and Authentication Failures	CWE-288: Authentication Bypass Using an Alternate Path or Channel
8.	A08 – Software and Data Integrity Failures	CWE-829: Inclusion of Functionality from Untrusted Control Sphere
9.	A09 – Security Logging and Monitoring Failures	CWE-778: Insufficient Logging
10.	A010 – Server Slide Request Forgery (SSRF)	CWE-918: Server-Side Request Forgery (SSRF)

1-

1.1. Vulnerability Name : Improper Access Control

CWE	**: CWE -284**
OWASP Category	**: A01 2021 – Broken Access control**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: Improper access control can lead to various security threats, such as: Data breaches: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.**

2-

1.2. Vulnerability Name	**: Inadequate Encryption Strength**
CWE	**: CWE -326**
OWASP Category	**: A02 2021 – Cryptographic failures**
Description	**: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.**
Business Impact	**: If customer data is compromised due to insecure encryption, it can damage the trust and confidence that customers have in an organization, which can have long-term negative impacts on the business..**

3-

1.3. Vulnerability Name	**: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**
CWE	**: CWE -89**
OWASP Category	**: A03 2021 – Injection**
Description	**: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.**
Business Impact	**: For businesses of all sizes, it is vital to understand the seriousness of injection attacks. Legal liabilities, reputational harm, a loss of confidence from clients, and the disruption of vital activities can all have huge financial ramifications. Organizations may proactively set up robust safety measures.**

4-

1.4. Vulnerability Name : Violation of Secure Design Principles

CWE	**: CWE -693**
OWASP Category	**: A04 2021 – Broken Access control**
Description	**: The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.**
Business Impact	**:This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centred around design, it can be resource-intensive to fix design problems. The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation.**

5-

1.5. Vulnerability Name	**: Protection Mechanism Failure**
CWE	**: CWE -284**
OWASP Category	**: A01 2021 – Security misconfiguration**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.**

6-

1.6. Vulnerability Name	**: Vulnerable and outdated components**
CWE	**: CWE -1104**
OWASP Category	**: A01 2021 – Use of Unmaintained Third-Party Components**
Description	**: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.**
Business Impact	**: Failing to fix these vulnerabilities can have serious consequences. Companies can be fined, sued, or even lose their business license if they are found to be using outdated or vulnerable components due to regulatory compliance regulations that mandate that companies have proper patching.**

7-

1.7. Vulnerability Name : Authentication Bypass Using an Alternate Path orChannel

CWE	**: CWE -288**
OWASP Category	**: A07 2021 – Identification and Authentication Failures**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: Improper access control can lead to various security threats, such as: Data breaches: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.**

8-

1.8. Vulnerability Name : Inclusion of Functionality from Untrusted Control Sphere

CWE	**: CWE-829**
OWASP Category	**: A08 – Software and Data Integrity Failures**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: Inclusion of Functionality from Untrusted Control can lead to various security threats, such as: Data breaches: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.**

9-

1.9. Vulnerability Name : Insufficient Logging

CWE	**: CWE-778**
OWASP Category	**: A09 – Security Logging and Monitoring Failures**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: Insufficient Logging can lead to various security threats, such as: Data breaches: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.**

10-

1.10. Vulnerability Name : Server-Side Request Forgery (SSRF)

CWE	**: CWE-918**
OWASP Category	**: A010 – Server Slide Request Forgery (SSRF)**
Description	**: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.**
Business Impact	**: Server-Side Request Forgery (SSRF) can lead to various security threats, such as: Data breaches: Improper access control can allow attackers to access sensitive data, leading to data breaches, data loss, or unauthorized access to**

confidential information.

Stage : 2 Report NESSUS Vulnerability Report

Overview

Vulnerabilities are instances of a potential security issue found by a plugin. In your scan results,

you canchoose to view all vulnerabilities found by the scan, or vulnerabilities found on a specific host.Nessus identifies exploitable vulnerabilities present in your scan results. The report contains two tableswhich bring focus to the exploitable vulnerabilities.

1. Vulnerability Name

Vulnerabilities are instances of a potential security issue found by a plugin. One can choose to view all vulnerabilities found by the scan, or vulnerabilities found on a specific host.

2. Severity

Vulnerabilities that score in the high range usually have some of the following characteristics: The vulnerability is difficult to exploit. Exploitation could result in elevated privileges. Exploitation could resultin a significant data loss or downtime. Tenable assigns all vulnerabilities a severity (Info, Low, Medium, High, or Critical) based on the vulnerability's static CVSSv2 or CVSSv3 score , depending on your configuration.

3. Plugins

As information about new vulnerabilities is discovered and released into the general public domain, Tenable, Inc. research staff designs programs to enable Tenable Nessus to detect them. These programs are called *plugins*. Tenable writes plugins in the Tenable Nessus proprietary scripting languagecalled *Tenable Nessus Attack Scripting Language* (NASL). Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

4. Port

Default instructs the scanner to scan approximately 4,790 commonly used ports. The list of ports can befound in the nessus-services file on the Nessus scanner. all instructs the scanner to scan all 65,536 ports,including port 0.

5. Solution to port

Users can enter more specific ranges and ports into the scan policy, such as "21-80", "21,22,25,80" or "21-143,1000-2000,60000-60005". Doing so will cause the port scanner to target just those ports during the port scan. If required, 'all' instructs the scanner to scan all 65,536 ports, including port 0.

Target WebSite : Pbel city website

Target IP : 172.67.144.142

S.No	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	HTTP Server Type and Version	High	11219	This plugin attempts to determine the type and the version of the remote web server	N/A	vulnerabilities in Apache HTTP Server Range Header Denial of Service Vulnerability (DoS) is a Medium risk vulnerability that is one of the most frequently found on networks around the world.	80 443 2052 2053 2082 2083 2086 2087 2095 2096 8080 8443
2	Nessus SYN scanner	High	54615	Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).	N/A	Nessus provides a fast, user-friendly way to find and fix vulnerabilities in many kinds of IT assets, including cloud-based and virtualized resources	**2082** **2052** **443** **80**
3	Service Detection	High	22964	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it	N/A	ulnerabilities that could allow unauthorized control or access to sensitive data on a system.	8080, 80, 2096, 2083, 443 , 8880

				receives an HTTP request.			
4	Common Platform Enumeration	Medium	54615	Based on the remote operating system, it is possible to determine whatthe remote system type is (eg: a printer, router, general-purpose computer, etc).	N/A	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.	**2082** **2052** **443** **80**
5	TCP/IP Timestamps Supported	High	25220	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote hostcan sometimes be computed.	N/A	The remote host implements TCP timestamps, as defined by RFC1323.A side effect of this feature is that the uptime of the remote host can sometimes be computed.	0
6	Traceroute Information	High	10287	Makes a traceroute to theremote host.	N/A	The remote host implements TCP timestamps, as defined by RFC1323.A side effect of this feature is that the uptime of the remote host can sometimes be computed.	0 / udp
7	Device Type	High		Based on theremote		A device type is a setof MCI drivers that	N/A

			54615	operating system, it is possible to determine whatthe remote system type is (eg: a printer, router, general-purpose computer, etc).		share a common command set and are used to control similar multimedia devices or data files.Many MCI commands, such as open (MCI_OPEN), require you to specify a device type	
8	OS Identification	High	11936	Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guessthe name of the remote operating systemin use. It is also possible sometimes to guess the versionof the operating system.	N/A	By detecting which operating system a network operates on, hackers have an easier time targetingknown vulnerabilities.	N/A
9	HyperTextTransfer Protocol (HTTP) Information	High	24260	This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipeliningare enabled, etc...		This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,	80, 443, 2052, 2053, 2082, 2083,, 2087,

	Service Detection	High		Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	N/A	It is able to identifythe remote serviceby its banner or by looking at the error message it sends when it receives an HTTP request.	

Stage : 3 Report

Enables deep visibility and improve the security with SOC and SIEM Integration

SOC

SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations to detect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputationin an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT, legal, communications, and executive management, ensuring a cohesive and efficient response to securityincidents.

SOC- Cycle

Step 1: Develop Your StrategyStep 2: Design the Solution
Step 3: Develop Processes, Procedures, and TrainingStep 4: Prepare Your Environment
Step 5: Implement Your Solution Step 6: Deploy End-to-End Use Cases
Step 7: Maintain and Enhance Your Solution

SIEM

Security information and event management, SIEM for short, is a solution that helps organizations detect,analyze, and respond to security threats before they harm business operations.

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzesactivity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more.

SIEM Cycle

The lifecycle of a Security Information and Event Management (SIEM) system involves several interconnected stages that ensure the effectiveimplementation, operation, and maintenance of the SIEM solution. The**SIEM life cycle typically includes the following phases:**

Planning and Assessment:

Define the objectives and scope of the SIEM implementation, considering the organization's securityrequirements and compliance goals. Conduct a thorough assessment of the existing security infrastructure, data sources, and log management practices to identify gaps and necessary improvements.

Design and Architecture:

Design the SIEM architecture based on the organization's requirements and data sources, consideringfactors like scalability, redundancy, and performance.

Data Collection and Integration:

Implement data collectors and agents to gather logs and events from various sources, such as firewalls,network devices, servers, applications, and endpoints. Normalize and enrich the collected data to facilitate efficient analysis and correlation.

MISP

The MISP Threat Sharing project consists of multiple initiatives, from software to facilitate threat analysisand sharing to freely usable structured Cyber Threat Information and Taxonomies. MISP Threat Sharing is an open source threat intelligence platform. The project develops utilities anddocumentation for more effective threat intelligence, by sharing indicators of compromise. There areseveral organizations who run MISP instances, who are listed on the website

Your college network information Name : SRM University, Kattankulathur Ip address : 13.235.158.125

Threat intelligence

Threat intelligence allows organizations to be proactive instead of reactive when it comes to cyber attacks. Without understanding security vulnerabilities, threat indicators, and how threats are carried out,it is impossible to defend against cyber attacks effectively.

Incident response

Incident response is a term used to describe the process by which an organization handles a data breach or cyber attack, including the way the organization attempts to manage the consequences of the attack orbreach. Although the dynamic management of risk is continuous throughout the incident, the focus of operational activity will change as the incident evolves. It is, therefore, useful to consider the process during three separate stages of an incident. These are; The Initial Stage , The Development Stage ,The Closing Stage.

Qradar & understanding about tool

Successful enterprises make security core to their business transformation agenda. IBM Security Servicesis a trusted partner — delivering advisory, integration and managed security services, to offensive and defensive capabilities, we combine a global team of experts with proprietary and partner technology to co-create tailored security programs that transform security into a business enabler.

IBM Security Qradar Suite is a modernized threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle. The portfolio is embedded with enterprise-grade AI and automation to dramatically increase analyst productivity, helpingresource-strained security teams work more effectively across core technologies. It offers integrated products for endpoint security (EDR, XDR, MDR), log management, SIEM and SOAR—all with a common user interface, shared insights and connected workflows.

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

BM QRadar Security Intelligence Platform advantages

- Provides real-time visibility to the entire IT infrastructure for threat detection and prioritization.
- Reduces and prioritizes alerts to focus security analyst investigations on an actionable list of suspected,high probability incidents.
- IBM helps transform cybersecurity to propel our business

Capabilities of Qradar in cyber security

X-Force Red Offensive Security Services.
Global team of hackers hired to hack anything to secure everything.

Cyber Simulation Services
Build effective preparation and incident response capabilities with a security command center cyber rangeexperience.

Cybersecurity services
AI-powered threat defense, 24x7 across endpoints, networks, systems and applications.

Threat Management Services
A smarter security framework to manage the full threat lifecycle.

Managed Security Services
Explore the latest managed security services for today's hybrid cloud world.

Cloud Security Services
Retain visibility, control and security as you move to hybrid cloud environments.

Identity and Access Management Services
Get your workforce and consumer identity and access management program on the road to success.

Data Security Services
Comprehensive data protection for the most critical enterprise data.

Zero Trust Acceleration Services
Accelerate adoption of a zero trust strategy.

According to IBM, the QRadar Security Information and Event Management is an essential tool that wouldaid the security teams in prioritizing the threats across the enterprise and detecting them accurately. The tool offers the necessary intelligent insights that would help the teams to respond as quickly as possible and reduce the impact of the incidents. Network flow data and log events from thousands of endpoints, devices, and applications over the network are consolidated.

QRadar then correlates all the different information and these related events are compiled to produce single alerts so that remediation and incident analysis can be accelerated. QRadar and SIEM are available in on-premises and cloud environments.

The following is the significance of IBM QRadar - why it has stood out, despite all the different services offered across the world.

- **Comprehensive visibility** - The product helps to gain a centralized insight into the data flows,events, and logs on the SaaS (software-as-a-service) and IaaS (infrastructure-as-a-service) environments and on-premises.
- **Elimination of manual tasks** - All the events in a certain threat can be centrally seen in one placeand the expensive manual tracking can be eliminated. Analysts can focus on investigating the matter (security threat), followed by a proper response.
- **Easily cater to the compliance protocols** - It becomes easier to comply with the international policies and the external regulations that are achieved by leveraging the pre-built reports and templates.

- **Real-time threat detection** - Out-of-the-box analysis is leveraged that analyzes the network flowsand logs automatically and generates proper alerts and the attacks are then directed via the proper kill chain.

The IBM QRadar offers the necessary compliance support and situational awareness. A combination of security event correlation, flow-based network knowledge, and assessment-based vulnerability assessment is used by QRadar SIEM.

Conclusion

Stage 1 :- what you understand from Web application testing .

Web testing, or web application testing, is a software practice that ensures quality by testing that the functionality of a given web application is working as intended or as per the requirements. Web application testing allows you to find bugs at any given time, prior to a release, or on a day-to-day basis.

Web application testing is the process of evaluating and assessing all aspects of a web application's functionality, like detecting bugs with usability, compatibility, security, and performance. This testingpractice ensures the quality of the web application and its working as per the end-user requirements.

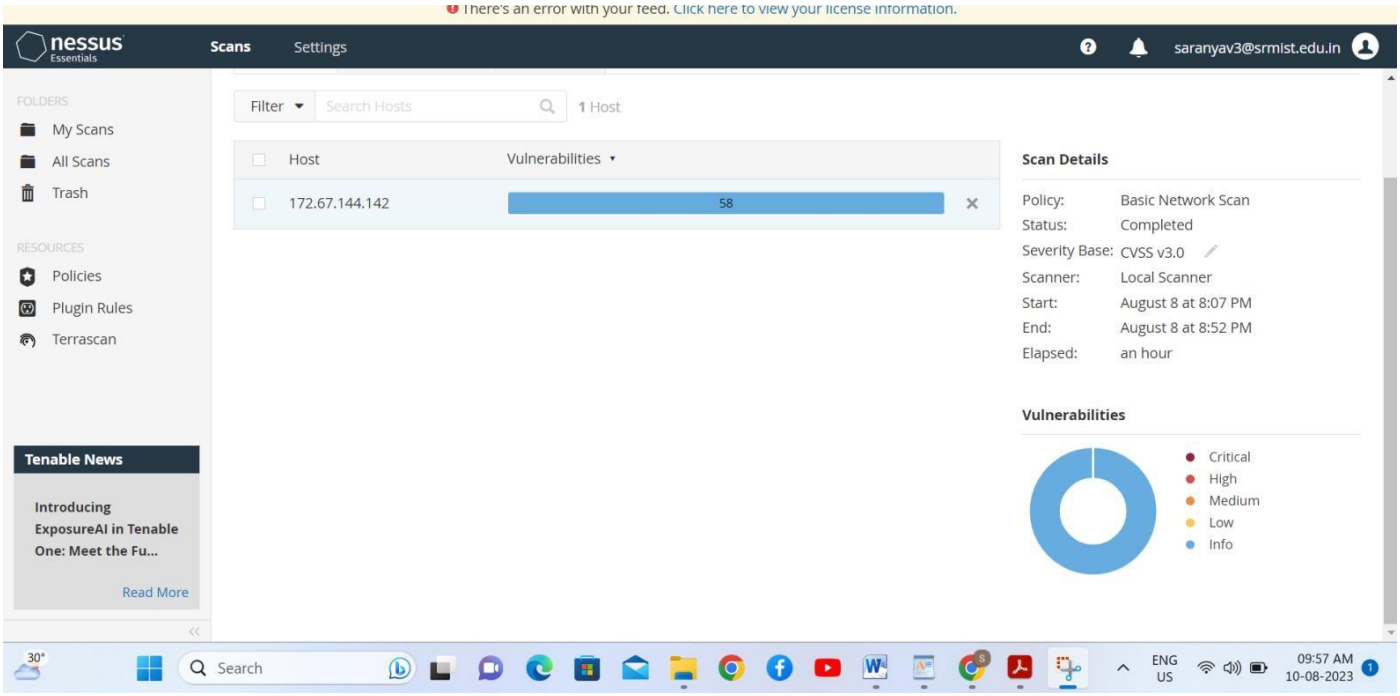
It helps in minimizing bugs and errors in the application. It helps in making the website more user- friendly. It helps in improving search engine rankings. It helps in gaining users' trust and bringing morevisitors.

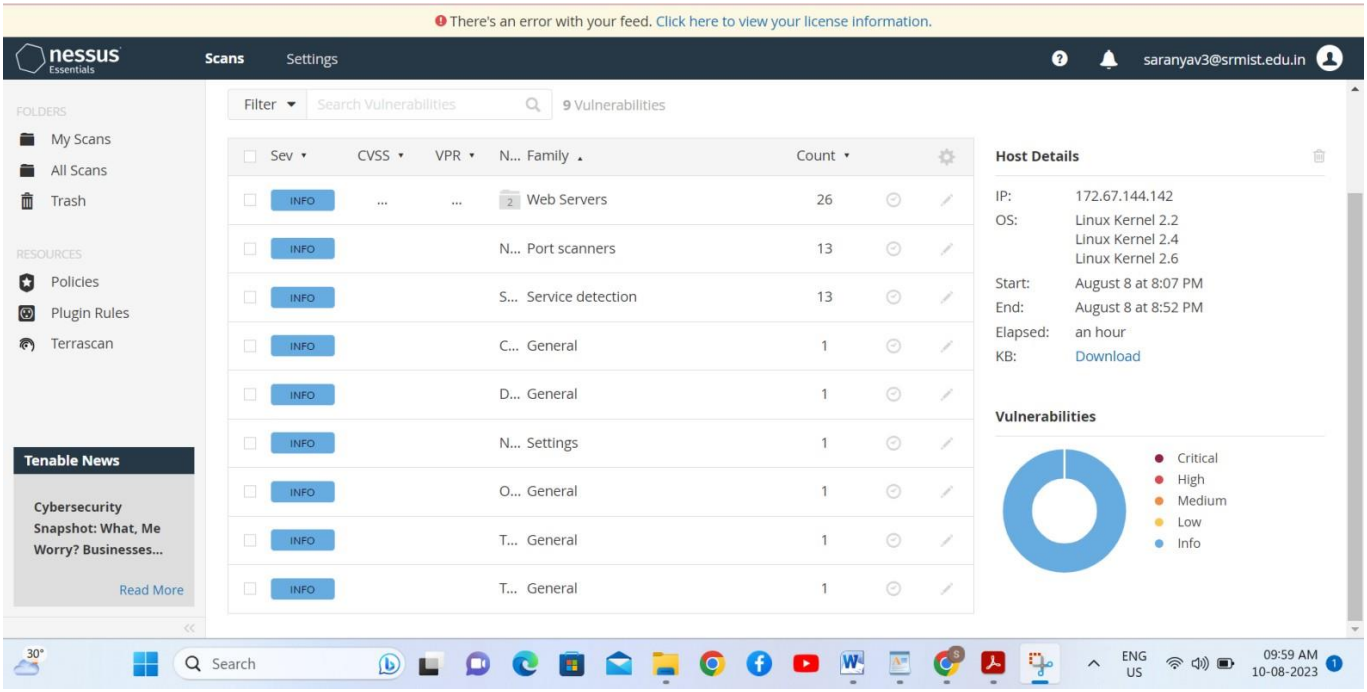
Software testing is the process of evaluating and verifying that a software product or application does what it is supposed to do. The benefits of testing include preventing bugs, reducing development costsand improving performance.

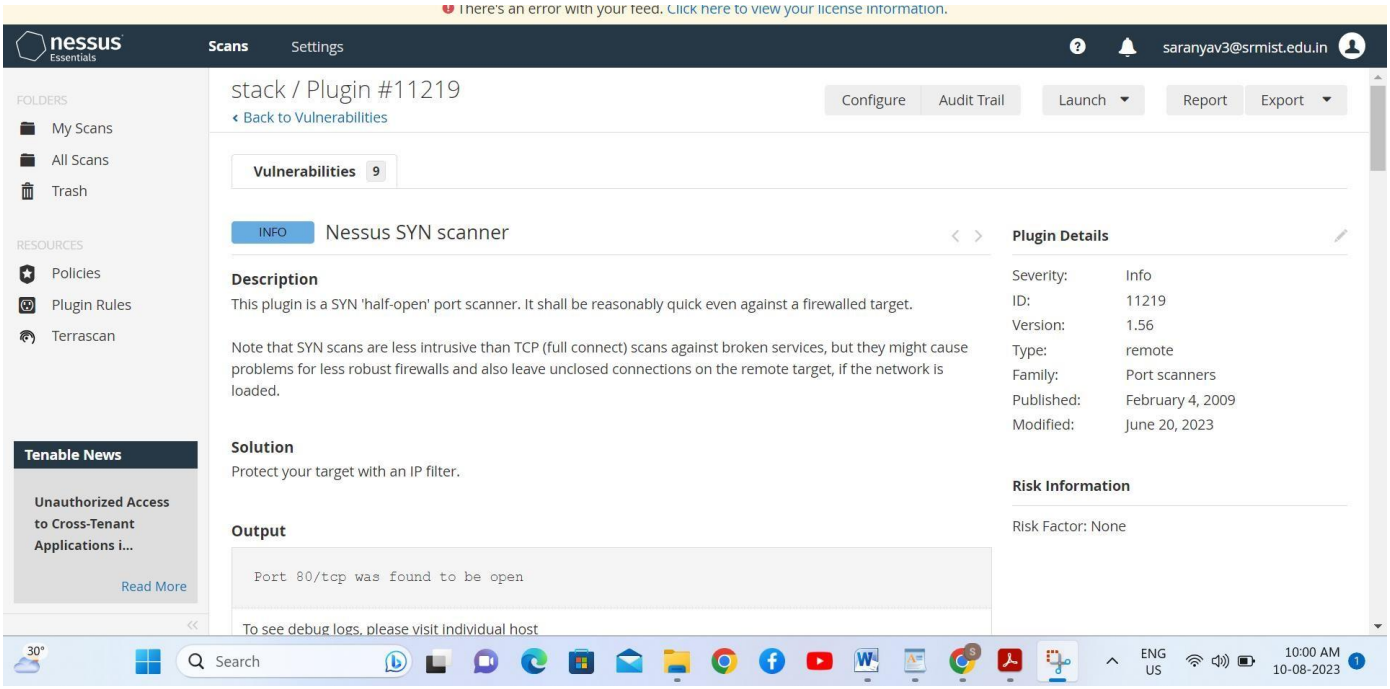
Stage 2 :- what you understand from the nessus report .

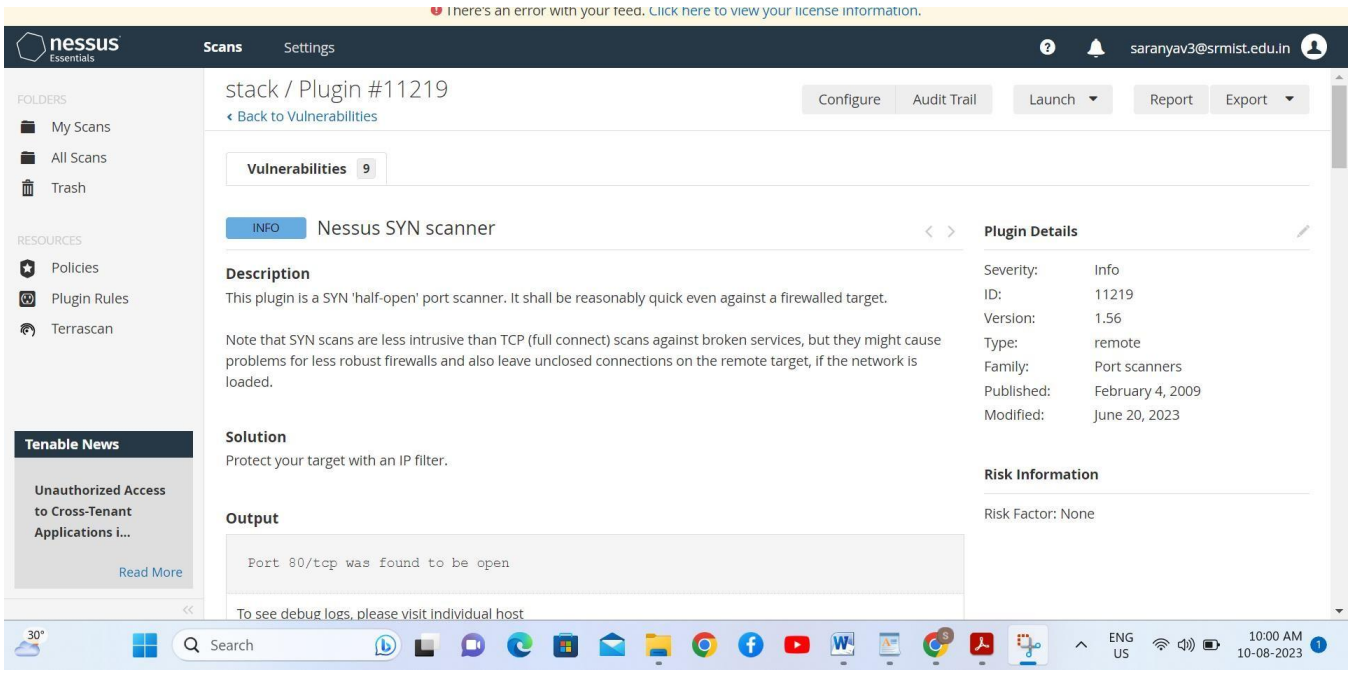
Nessus is a vulnerability scanning tool used to identify and report securityissues in computer systems and networks.

The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels areusually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
saranyav3@srmist.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Introducing ExposureAI in Tenable One: Meet the Fu...
Read More
Filter
Search Hosts
1 Host
Host
Vulnerabilities
172.67.144.142
58
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: August 8 at 8:07 PM
End: August 8 at 8:52 PM
Elapsed: an hour
Vulnerabilities
Critical
High
Medium
Low
Info
Search
ENG US
09:57 AM 10-08-2023


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
saranyav3@srmist.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: What, Me Worry? Businesses...
Read More
Filter
Search Vulnerabilities
9 Vulnerabilities
Sev
CVSS
VPR
N... Family
Count
INFO ... ... Web Servers 26
INFO N... Port scanners 13
INFO S... Service detection 13
INFO C... General 1
INFO D... General 1
INFO N... Settings 1
INFO O... General 1
INFO T... General 1
INFO T... General 1
Host Details
IP: 172.67.144.142
OS: Linux Kernel 2.2
Linux Kernel 2.4
Linux Kernel 2.6
Start: August 8 at 8:07 PM
End: August 8 at 8:52 PM
Elapsed: an hour
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Search
ENG US
09:59 AM 10-08-2023


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
saranyav3@srmist.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Unauthorized Access to Cross-Tenant Applications i...
Read More
stack / Plugin #11219
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 9
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 80/tcp was found to be open
To see debug logs, please visit individual host
Plugin Details
Severity: Info
ID: 11219
Version: 1.56
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: June 20, 2023
Risk Information
Risk Factor: None
Search
ENG US
10:00 AM 10-08-2023


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
saranyav3@srmist.edu.in
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Unauthorized Access to Cross-Tenant Applications i...
Read More
stack / Plugin #11219
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 9
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 80/tcp was found to be open
To see debug logs, please visit individual host
Plugin Details
Severity: Info
ID: 11219
Version: 1.56
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: June 20, 2023
Risk Information
Risk Factor: None
Search
ENG US
10:00 AM 10-08-2023

Stage 3 :- what you understand from SOC / SEIM / Qradar DashboardSOC

(Security Operations Center):

The function of the security operations center (SOC) is to monitor, prevent, detect, investigate, and
respond to cyber threats around the clock.

The basic responsibilities of a SOC team include the following:

- **Asset discovery and management** involves obtaining a high awareness of all tools, software, hardware and technologies used within the organization. These also focus on ensuring all assets areworking properly and regularly patched and updated.
- **Continuous behavioral monitoring** incudes examining all systems 24/7 year-round. This enables SOCsto place equal weight on reactive and proactive measures as any irregularity in activity is instantly detected. Behavioral models train data collection systems on what activities are suspicious and can beused to adjust information that might register as false positives.
- **Keeping activity logs** enables SOC team members to backtrack or pinpoint previous actions that may have resulted in a breach. All communications and activity across an organization should be logged bythe SOC.
- **Alert severity ranking** helps teams ensure the most severe or pressing alerts are handled first. Teamsmust regularly rank cybersecurity threats in terms of potential damage.
- **Defense development and evolution** is important to help SOC teams stay up to date. Teams
should create an incident response plan (IRP) to defend systems against new and old attacks. Teamsmust also adjust the plan as necessary when new information is obtained.
- **Incident recovery** enables an organization to recover compromised data. This includes reconfiguring,updating or backing up systems.
- **Compliance maintenance** is key to ensuring SOC team members and the company follow regulatoryand organizational standards when carrying out business plans.

SIEM (Security Information and Event Management):
SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they havea chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

SIEM ingests event data from a wide range of sources across an organization's entire IT infrastructure, including on-premises and cloud environments. Event log data from users, endpoints, applications, data sources, cloud workloads, and networks—as well data from securityhardware and software such as firewalls or antivirus software—is collected, correlated and analyzed in real-time.

Future Scope

Stage 1 :- Future scope of web application testing

With the wide diffusion of the service-oriented software paradigm, the more recent Web based applications are being developed as Web services, as well as many 'legacy' Web applications andlegacy systems are being migrated towards Web services. Web services introduce new peculiarities in the context of Web applications, raising new interesting testing issues and questions, such as those regarding testing models and strategies.

The very large number of users characterizing Web applications and the strategic value of the services they offer, make the verification of both non-functional and functional requirements of aWeb application a critical issue.

Stage 2 :- Future scope of testing process you understood .

User Experience Testing will be a bigger and bigger part of Testing field in the future. Most of thetime, real users take part in this kind of testing, which helps test different parts of the user experience. This helps determine the best way for a product and its audience to work together.

The future scope of the testing process will see increased automation, integration with emergingtechnologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing

Stage 3 :- Future scope of SOC / SEIM

Commonly externalized SOC services include Deeper malware analysis , Threat intelligenceSIEM, EDR, and other tool management and tuning .SOC tool tuning and use case analysis,Managed threat hunting.

The key learning of many SOC leaders and operators of today is that every SOC ends up being a hybrid model, with one or more of the tasks being handled by the third party. In the ideal state, and with an effective workforce strategy in place, those taskings address the problem of capacity,rather than capability. Rethinking the organization of the modern SOC towards skills rather than tiers, coupled with a heightened focus on automation, can significantly mitigate today's widespread people and skills shortage in cybersecurity.

Future scope of SEIM

Security teams using legacy security information and event management (SIEM) fill their days by either creating new searches to identify bad behavior or responding to a breach. They operate with low confidence that investigations spanning several months back will ever ultimately providethe answers to the questions they have as practitioners.

Every SIEM provider likes to position themselves as the next generation in security information and event management, but are they? Many SIEM providers have their roots in SIM logging toolsand have struggled to adopt modern technologies, especially as they relate to cloud services.

Topics explored :-

In this Faculty Build-A-Thon conducted by SmartInternz and Sponsored by IBM course,

- OSI layers its functions and different types of attacks in cyber world were discussed. Cyber security based terminologies are also discussed.
- Important attacks like Phishing attack, Dumpster diving , spying , foot printing attacks and socialengineering attacks are also discussed.
- How to identify and quantify the attack vulnerability, Common Weakness Enumeration (CWS) ,vulnerability management life cycle are discussed.

- White hackers, black hackers ,Assessment tools, scanning tools to detect the cyber-attacks is alsodiscussed.

The courses that are available to explore our self with cyber world is also conveyed effectively by theinstructor. Different types of stacks its functions web based services, protocols of the stacks were discussed.

Tools explored :-

Qradar, Nessus, metasploitable, QRadar for SOC dashboard presentation, Kali linux