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 that are hosted on web in which the application interfaces and other functionalities are tested.

An organizational security policy is a set of rules or procedures that is imposed by an organization on its operations to protect its 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 full incident lifecycle.

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. IBM QRadar then performs real-time analysis of the log data and network flows to identify malicious activity so it can be stopped 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 can be 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 testing each of these services to detect vulnerabilities. Nessus can be installed on one computer and then can be used to test many other computers.

2. List of employees participated

S. No.	Name	Designation	Mobile No.
1	SARANYA VS	ASSISTANT PROFESSOR	9080584021

3. List of Vulnerable Parameter, Location discovered

S. No.	Name of The Vulnerability	References-CWE
1	**Broken Access control**	CWE- 284 - Improper access control
2	**Cryptographic Failures**	CWE-310 cryptographic issues
3	**Injection**	CWE-94 improper control of generation of code

4	**Insecure design**	VE -209 Generation of Error message containing sensitive information
5	**Secure misconfiguration**	CWE-16: configuration
6	**Vulnerable and outdated components**	WE-1104: Use of unmaintained Third party components
7.	**Identification and authentication failures**	VE-434: Unrestricted Upload of File with Dangerous Type
8	**Software and Data Integrity Failures**	WE-829 Inclusion of functionality from untrusted control sphere
9	**Security Logging and Monitoring Failures***	Cwe-117 improper output Neutralization for logs
10	**Server – Side Request Forgery**	ve- 1286 incorrect validation of intended decimal based ip

	(SSRF)*	address format

1. Vulnerability Name: **Broken Access control**

CWE : CWE-284

OWASP Category: A01:2021 – **injection**

Description: an application that allows any user to view or edit sensitive data without authenticating first.

Business Impact: Access control ensures that people can only gain access to things they're supposed to have access to. When access control is broken, an attacker can obtain unauthorized access to information or systems that can put an organization at risk of a data breach or system compromise. In addition to viewing unauthorized content, an attacker might be able to change or delete content, perform unauthorized functions, or even take over site administration.

2 .Vulnerability Name: Cryptographic Failures

CWE : CWE-310

OWASP Category: A02 :2021

Description: An a security failure that occurs when a third-party entity (apps, web pages, different websites) exposes sensitive data.

Business Impact: Modern web applications process data at rest and in transit, which require **stringent security controls** for comprehensive threat mitigation. Some deployments employ weak cryptographic techniques that can be cracked within a reasonable time frame. Even with the perfect implementation of cryptographic techniques, users may avoid embracing data protection best practices, subsequently making sensitive information susceptible to sensitive data theft.

3 . Vulnerability Name: Injection

CWE : CWE-94

OWASP Category:A03: 2021- Improper control of generation of code

Description: vulnerability in that applications allow an attacker to relay malicious code through an application to another system.

Business Impact: Attacks using SQL injection can have devastating impacts on enterprises. One of the oldest and most dangerous web-based application vulnerabilities is SQL injection. SQL injection is ranked #6 in the CWE Top 25 for 2021 and is identified as CWE-89: Improper Neutralisation of Special Elements Used in a SQL Command.

4 . Vulnerability Name: Insecure design

CWE : CWE-209

OWASP Category: A04:2021-Injections

Description: a broad category related to critical design and architectural flaws in web applications that hackers can exploit.

Business Impact: One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

5 . Vulnerability Name: Secure misconfiguration

CWE : CWE-16

OWASP Category: A51:2021 – Secure misconfiguration

Description: when security options are not defined in a way that maximizes security, or when services are deployed with insecure default settings

Business Impact: security misconfigurations is This vulnerability can occur at any level of an application stack, including network services, platform, web server, application server, database, frameworks, custom code, pre-installed virtual machines, containers, and storage. Security misconfiguration can stem from the failure to implement all of the security controls for a server or web application, or from implementing security controls in a way that introduces errors. It can also occur when defaults are used for security settings.

6 . Vulnerability Name: Vulnerable and outdated components

CWE : CWE-1104

OWASP Category: A06 :2021- Vulnerable and outdated components

Description: A vulnerable and outdated component is a software component that is no longer being supported by the developer, making it susceptible to security vulnerabilities.

Business Impact: Applications often become vulnerable to attacks because they use outdated software components with known security vulnerabilities. Hackers can exploit these vulnerabilities to gain access to the application's data or to take control of the application entirely.

7. Vulnerability Name: Identification and authentication failures

CWE : CWE-434

OWASP Category: A07:2021 – Injections

Description: occur when the application fails to correctly implement functions associated with the user's identity, authenti- city, and session management.

Business Impact: Such failures often lead to persistent system-level threats exploited by malicious actors to assume a user's identity, data theft, or an entire system compromise. This post discusses identification and authentication failures, their types, inherent vulnerabilities that cause such failures, and prevention measures.

8 . Vulnerability Name: Software and data Integrity failures

CWE : CWE-352

OWASP Category:A05:2021 – Security Misconfiguration

Description: when the code implementation and the underlying infrastructure lack the ability to protect the code against all 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.

9 . Vulnerability Name: Security Logging and monitoring failures

CWE : 117

OWASP Category: A09:2021 – Security Logging and monitoring failures

Description: The absence of telemetry that could help network defenders detect and respond to hostile attempts to compromise a system.

Business Impact: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to attack systems further, maintain persistence, pivot to more systems, and tamper, extract or destroy data.

10. Vulnerability Name: Server – Side Request Forgery

CWE : CWE-1286

OWASP Category: A10:2021 – **Server – Side Request Forgery**

Description: A Server-Side Request Forgery (SSRF) attack involves an attacker abusing server functionality to access or modify resources.

Business Impact: Simply identifying a blind SSRF vulnerability that can trigger out-of-band HTTP requests doesn't in itself provide a route to exploitability. Since you cannot view the response from the back-end request, the behavior can't be used to explore content on systems that the application server can reach.

Stage : 2 Report
NESSUS Vulnerability Report

Overview

Vulnerabilities are instances of a potential security issue found by a plugin. In your scan results, you can choose 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 tables which 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 result in 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 language called *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 be found 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 : SiS queens town 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 what the 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 host can 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 the remote 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 the remote		A device type is a set of MCI drivers that	N/A

			54615	operating system, it is possible to determine what the 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 guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.	N/A	By detecting which operating system a network operates on, hackers have an easier time targeting known vulnerabilities.	N/A
9	HyperText Transfer Protocol (HTTP) Information	High	24260	This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are 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,

10	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 receives an HTTP request.	N/A	It is able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	8880, 2083, 443 , 2096, 80, 8080, 2095, 2086, 8443

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 reputation in 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 security incidents.

SOC- Cycle

Step 1: Develop Your Strategy
Step 2: Design the Solution
Step 3: Develop Processes, Procedures, and Training
Step 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 analyzes activity 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 effective implementation, 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 security requirements 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, considering factors 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 analysis and sharing to freely usable structured Cyber Threat Information and Taxonomies.
MISP Threat Sharing is an open source threat intelligence platform. The project develops utilities and documentation for more effective threat intelligence, by sharing indicators of compromise. There are several 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 or breach. 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 Services is 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, helping resource-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 log data 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 range experience.

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 would aid 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 place and 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 flows and 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 testing practice ensures the quality of the web application and its working as per the end-user requirements.

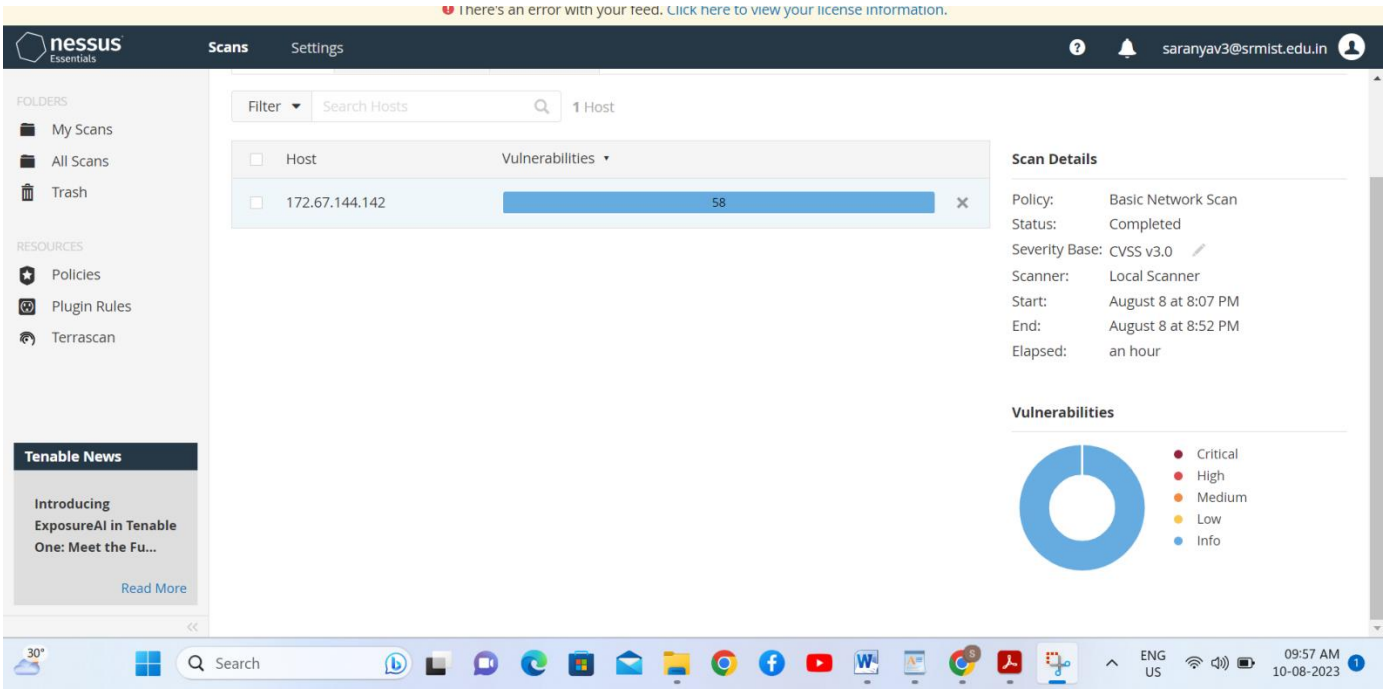
It helps in minimizing bugs and errors in the application. It helps in making the website more user-friendly. It helps in improving search engine rankings. It helps in gaining users' trust and bringing more visitors.

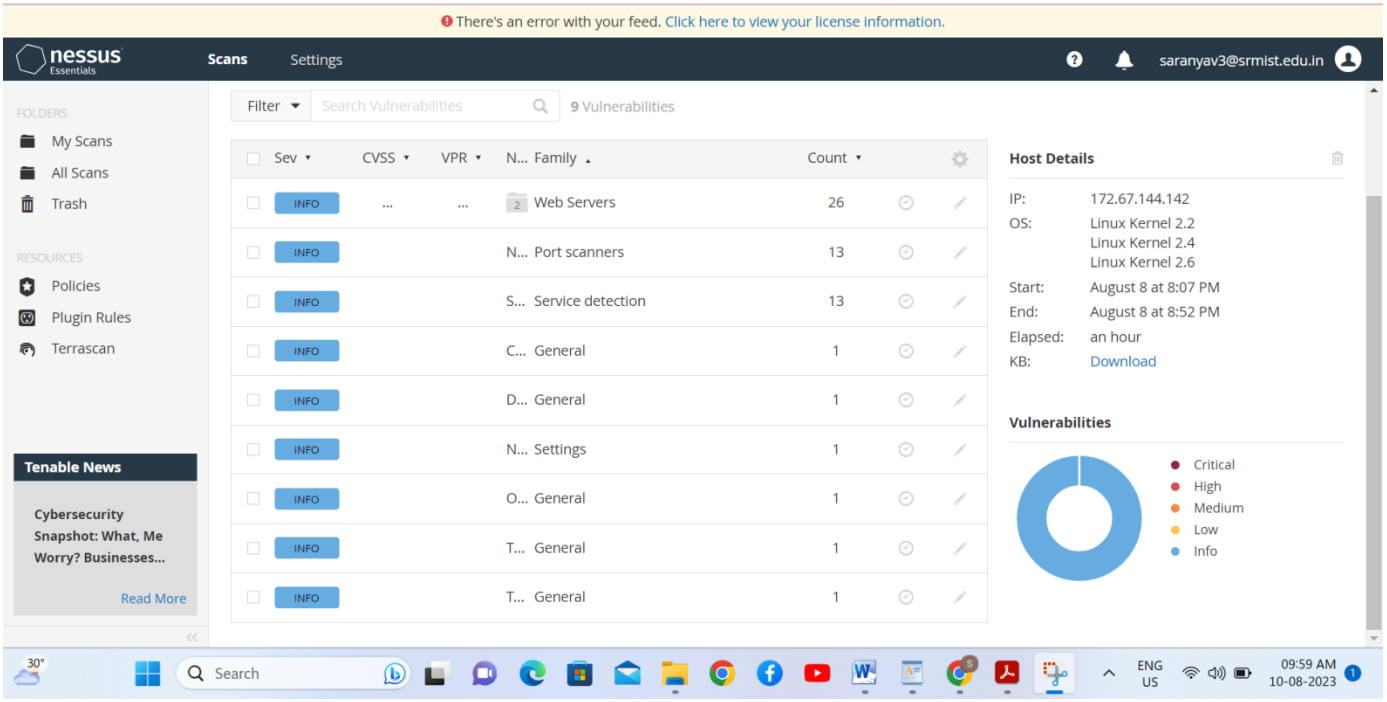
Software testing is the process of evaluating and verifying that a software product or application does what it is supposed to do. The benefits of testing include preventing bugs, reducing development costs and improving performance.

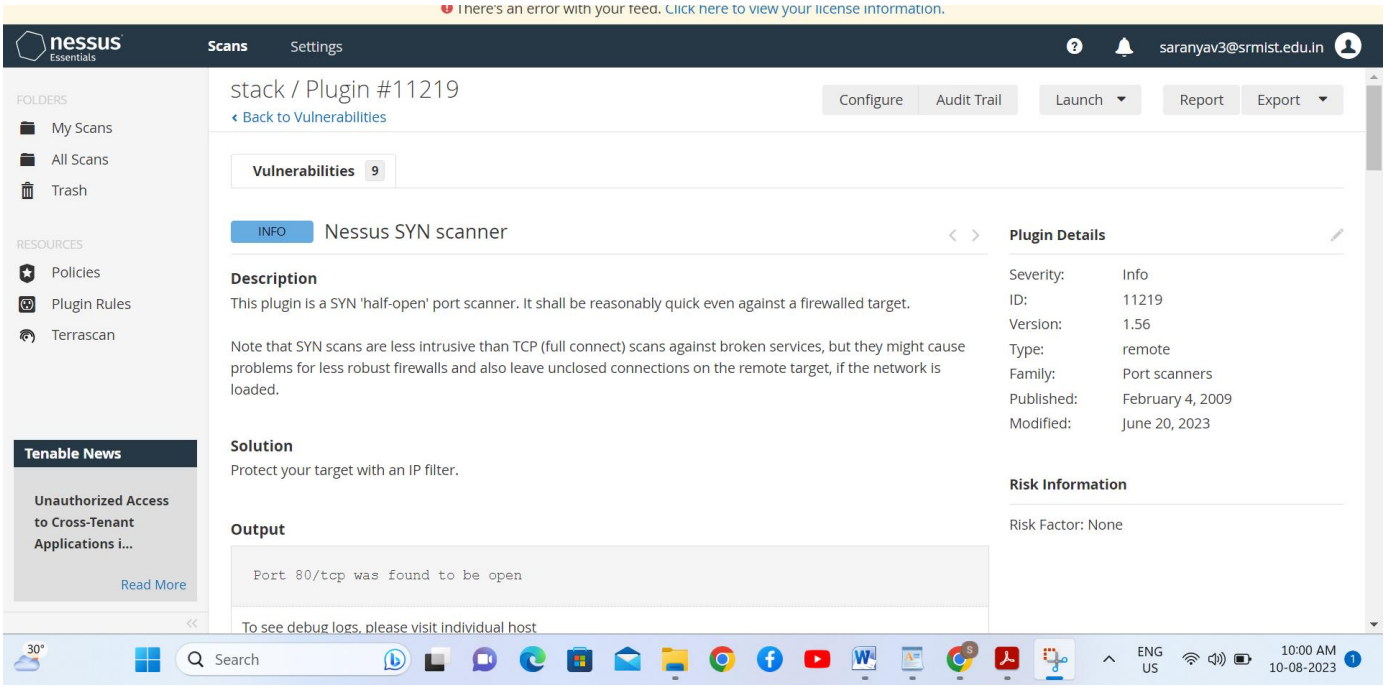
Stage 2 :- what you understand from the nessus report .

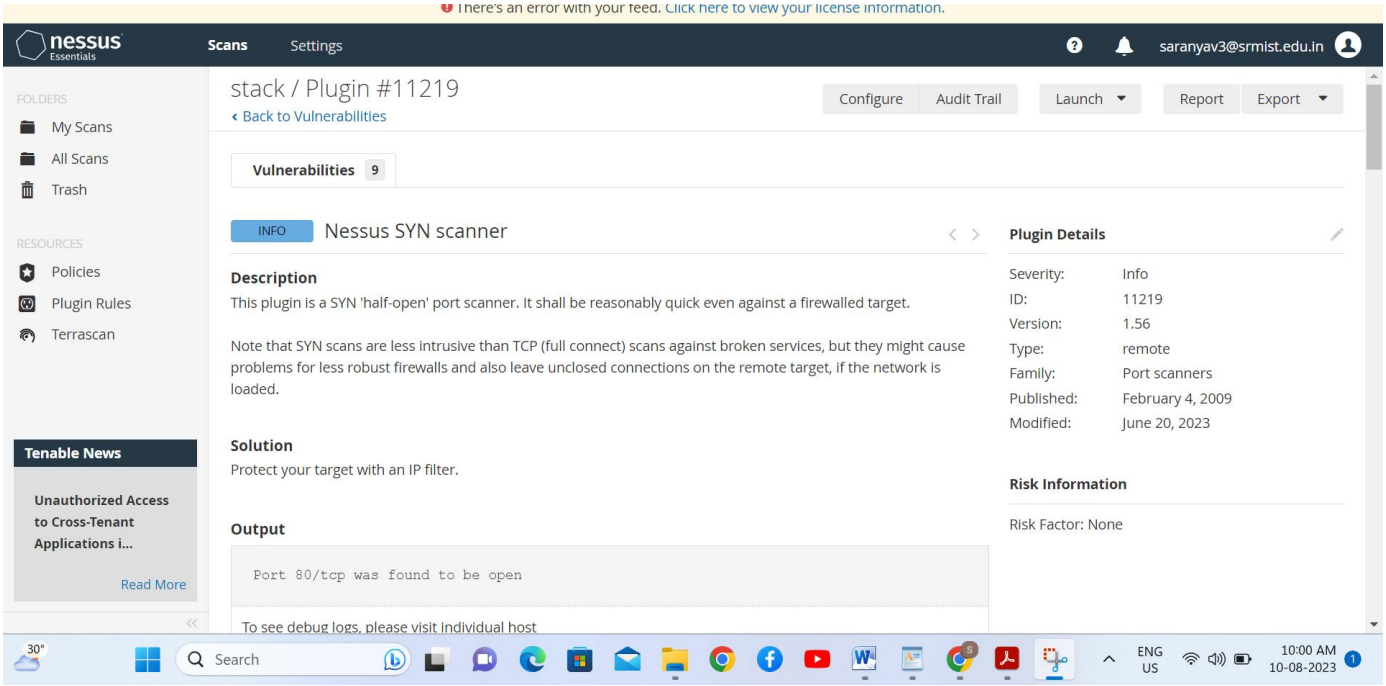
Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks.

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 are usually 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 Dashboard

SOC (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 are working properly and regularly patched and updated.
- **Continuous behavioral monitoring** incudes examining all systems 24/7 year-round. This enables SOCs to 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 be used 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 by the SOC.
- **Alert severity ranking** helps teams ensure the most severe or pressing alerts are handled first. Teams must 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. Teams must 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 regulatory and 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 have a 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 security hardware 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 and legacy 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 a Web 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 the time, 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 emerging technologies, 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 intelligence SIEM, 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 provide the 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 tools and 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 social engineering 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 also discussed.

The courses that are available to explore our self with cyber world is also conveyed effectively by the instructor. 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