



AI ENHANCED INTRUSION DETECTION SYSTEM

Team 1.2

Team Members

S.No	Name	College	Contact
1	Sivaraghavi U R	VIT Chennai	sivaraghavi.ur2021@vitstudent.ac.in
2	Sarath Rajan Senthilkumar	VIT Chennai	sarathrajan.senthilkumar2021@vitstudent.ac.in

INDEX

Project Details

Abstract.....5

Background.....5

Objectives:.....5

1. Enhanced Threat Detection: 5

2. Classification and Prioritization: 5

3. Real-Time Response: 5

Methodology:5

Expected Outcomes:.....6

Project Documents 7

Practice Website Vulnerability Table.....8

VULNERABILITY NAME: Cross-Site Scripting (XSS) 9

VULNERABILITY NAME: Cookie Manipulation..... 9

VULNERABILITY NAME: Elevation Of Privilege..... 9

VULNERABILITY NAME: Cross-Site Request Forgery (CSRF) 10

VULNERABILITY NAME: Cross Site Script Inclusion (XSSI)..... 10

VULNERABILITY NAME: Information Disclosure Via Path Traversal 11

VULNERABILITY NAME: DOS - Quit the Server 11

VULNERABILITY NAME: DOS – Overloading the Server..... 12

VULNERABILITY NAME: Unauthorised Access to Server Contents 12

VULNERABILITY NAME: Phishing Via Ajax..... 12

Main Website Vulnerability Table 13

VULNERABILITY NAME: SSH Weak Key Exchange Algorithms Enabled 14

VULNERABILITY NAME: SSH Server CBC Mode Ciphers Enabled 14

VULNERABILITY NAME: HSTS Missing from HTTPS Server..... 15

VULNERABILITY NAME: DNS Server Spoofed Request Amplification 15

VULNERABILITY NAME: DNS Server Recursive Query Cache Poisoning Weakness 16

Brainstorming Map and Empathy Map 17

Overview on Nessus..... 18

What is Nessus?..... 18

Key Features:..... 18

Vulnerability Name: DNS Server Recursive Query Cache Poisoning Weakness 20

Vulnerability Name: DNS Server Cache Snooping Remote Information Disclosure 21

Vulnerability Name: DNS Server Spoofed Request Amplification DDoS 22

Vulnerability Name: SSL Medium Strength Cipher Suites Supported (SWEET32)	23
Vulnerability Name: TLS Version 1.0 Protocol Detection	24
Vulnerability Name: TLS Version 1.1 Protocol Depreciated	25
Ability of IBM QRadar	26
1. Introduction	26
2. Security Operations Center (SOC)	26
3. Security Information and Event Management (SIEM)	27
4. Malware Information Sharing Platform & Threat Sharing (MISP)	27
5. College Network Information	27
6. Deployment of SOC in Your College	27
7. Threat Intelligence	28
8. Incident Response	28
9. IBM Qradar & Understanding About the Tool	28
10. Conclusion	28
Future Scope	29
<i>Stage 1: Future Scope of Web Application Testing</i>	29
<i>Stage 2: Future Scope of Testing Process</i>	30
<i>Stage 3: Future Scope of SOC / SEIM</i>	30
Tools Explored:	31
Knowledge Gained	32
Future Scope of AI Enhanced Intrusion Detection System	33
Conclusion	34

Project Details

Abstract

In our rapidly evolving digital landscape, the protection of organizational networks and sensitive data has become a top priority. This project centres on the creation of an AI-Enhanced Intrusion Detection System, leveraging the power of machine learning to detect, categorize, and respond to network intrusions with unparalleled precision. By uniting cutting-edge machine learning algorithms with deep cybersecurity expertise, this system equips organizations to strengthen their cyber defences and adapt to the ever-changing threat landscape. This project addresses the critical need for advanced cybersecurity measures in an interconnected world, ensuring the integrity and security of vital data.

Background

The increasing reliance on digital infrastructure for business operations and data storage has led to a surge in cyber threats. Traditional intrusion detection systems often struggle to keep pace with the rapidly evolving tactics employed by malicious actors. Hence, there is a pressing need for a system that can adapt in real-time, learning from past incidents and identifying emerging threats with precision.

Objectives:

1. **Enhanced Threat Detection:** The primary objective of this project is to create an intrusion detection system that goes beyond rule-based detection and leverages advanced machine learning algorithms. This system will continuously analyse network traffic, user behaviours, and system anomalies to detect threats, both known and unknown.
2. **Classification and Prioritization:** The project will also focus on the classification and prioritization of threats. By categorizing threats based on their severity and potential impact, the system can guide cybersecurity teams in deploying appropriate responses.
3. **Real-Time Response:** A key goal is to enable real-time response capabilities, automating actions such as isolating compromised systems, blocking malicious traffic, and alerting security personnel.

Methodology:

The development of this AI-Enhanced Intrusion Detection System will involve the integration of machine learning models, anomaly detection algorithms, and threat intelligence feeds. The system will continuously collect and analyse network data, leveraging historical data and patterns to identify deviations and

anomalies. By learning from past incidents, the system becomes more adept at recognizing novel threats.

Expected Outcomes:

The successful implementation of this project will result in an Intrusion Detection System that:

- Reduces false positives, minimizing unnecessary alerts.
- Provides real-time, context-aware threat detection and response.
- Enhances the overall cybersecurity posture of organizations by adapting to emerging threats.
- Offers significant cost savings by automating response actions.

Example:

Consider a scenario where an organization's network experiences a sudden surge in unusual traffic patterns. Traditional intrusion detection systems might trigger numerous false alarms, overwhelming security personnel. In contrast, the AI-Enhanced Intrusion Detection System, based on its learning from past incidents and real-time analysis of network traffic, can accurately identify and classify this anomalous activity as a potential DDoS attack. It can then automatically respond by isolating the affected systems and alerting security teams, ensuring a timely and appropriate reaction.

In conclusion, the AI-Enhanced Intrusion Detection System addresses the critical need for advanced cybersecurity measures in an interconnected world. By harnessing the power of artificial intelligence and machine learning, it empowers organizations to fortify their cyber defences, adapt to the ever-changing threat landscape, and safeguard their vital data in an era of evolving cyber threats.

Project Documents

Practice Website Vulnerability Table

Website: <https://google-gruyere.appspot.com/595415950294913840432014314475390761256/>

S.No	Vulnerability Name	CWE Number
1	CROSS-SITE SCRIPTING (XSS)	CWE-79
2	COOKIE MANIPULATION	CWE-565
3	ELEVATION OF PRIVILEGE	CWE-269
4	CROSS-SITE REQUEST FORGERY (CSRF)	CWE-352
5	CROSS SITE SCRIPT INCLUSION (XSSI)	CWE-829
6	INFORMATION DISCLOSURE VIA PATH TRAVERSAL	CWE-22
7	DOS - QUIT THE SERVER	CWE-602
8	DOS – OVERLOADING THE SERVER	CWE-400
9	UNAUTHORISED ACCESS TO SERVER CONTENTS	CWE-200
10	PHISHING VIA AJAX	CWE-79

VULNERABILITY NAME: Cross-Site Scripting (XSS)

CWE: CWE-79

OWASP Category: A03:2021-Cross-Site Scripting (XSS)

Description: Cross-Site Scripting is a vulnerability that allows an attacker to inject malicious scripts into web pages viewed by other users. These scripts can steal sensitive information, manipulate content, or perform actions on behalf of the victim user. XSS vulnerabilities often occur when user input is not properly validated and escaped.

Business Impact: XSS can lead to unauthorized access to sensitive data, data manipulation, and compromised user accounts. The business impact includes reputational damage, intellectual property theft, and financial losses. It can also result in operational disruption and legal consequences if sensitive customer data is exposed.

VULNERABILITY NAME: Cookie Manipulation

CWE: CWE-565

OWASP Category: A05:2021-Security Misconfiguration

Description: Cookie Manipulation is a security vulnerability that allows an attacker to manipulate cookies to gain unauthorised access or privileges within a web application.

Business Impact: This vulnerability can lead to unauthorized actions, impersonation of other users, and exploitation of the application's logic, potentially causing reputational damage, financial losses, and operational disruption.

VULNERABILITY NAME: Elevation Of Privilege

CWE: CWE-269

OWASP category: A05:2021-Security Misconfiguration

Description: Unauthorised Elevation of Privilege can allow an attacker to gain unauthorised privileges by allowing them to elevate their level of access.

Business Impact: This vulnerability can lead to unauthorized actions, and exploitation of the application's logic, potentially causing reputational damage, financial losses, and operational disruption.

VULNERABILITY NAME: Cross-Site Request Forgery (CSRF)

CWE: CWE-352

OWASP Category: A08:2021-Cross-Site Request Forgery (CSRF)

Description: Cross-Site Request Forgery is a security vulnerability where an attacker tricks a user into unknowingly performing actions on a different website without their consent. This typically happens when a user is authenticated on a site and visits another site that maliciously triggers actions on the first site.

Business Impact: CSRF can lead to unauthorized actions being performed on behalf of the victim user. The business impact includes compromised user accounts, reputational damage, and financial losses due to unauthorized transactions or actions.

VULNERABILITY NAME: Cross Site Script Inclusion (XSSI)

CWE: CWE-829

OWASP Category: A05:2021-Security Misconfiguration

Description: Cross Site Script Inclusion (XSSI) is a vulnerability that allows an attacker to include an external script or content into a web page viewed by other users. Attackers can exploit this vulnerability to execute malicious scripts in the context of a trusted website, potentially stealing user data, session cookies, or performing actions on behalf of the victim user.

Business Impact: XSSI can lead to unauthorized access to sensitive data, user sessions, and potentially compromising user accounts. The business impact includes reputational damage, data breaches, intellectual property theft, and financial losses. XSSI attacks can also result in operational disruption and legal consequences.

VULNERABILITY NAME: Information Disclosure Via Path Traversal

CWE: CWE-22

OWASP Category: A05:2021-Security Misconfiguration

Description: Information disclosure via path traversal is a security vulnerability where an attacker exploits the improper handling of file paths to gain unauthorized access to sensitive information.

Business Impact: Information disclosure via path traversal can lead to unauthorized access to sensitive data, compromising confidentiality and potentially violating regulatory compliance. The business impact includes reputational damage, intellectual property theft, financial losses, and operational disruption.

VULNERABILITY NAME: DOS - Quit the Server

CWE: CWE-602

OWASP: A01:2021-Broken Access Control

Description: DoS – Quit the Server is a security vulnerability where an attacker can command a server to shut down.

Business Impact: Denial of Service (DoS) attacks aiming to force a server to quit can have severe business impacts. This disruption results in prolonged downtime, rendering services inaccessible to users. The financial toll includes potential revenue loss, damage to reputation, and the costs associated with implementing robust security measures to prevent future occurrences.

VULNERABILITY NAME: DOS – Overloading the Server

CWE: CWE-400

OWASP Category: A04:2021-Insecure Design

Description: DoS – Overloading the Server is a Design Vulnerability which leads to overloading of server resources when processing a request.

Business Impact: DoS - Quit the Server attacks have severe business impacts, causing downtime, financial losses, and reputational damage. The disruption disrupts services, leading to frustrated users, potential customer churn, and increased operational costs for implementing security measures.

VULNERABILITY NAME: Unauthorised Access to Server Contents

CWE: CWE-200

OWASP Category: A01:2021-Broken Access Control

Description: Unauthorised access to server contents can lead to security vulnerability in which unauthorised user can gain access to server contents such as passwords.

Business Impact: Unauthorized access to server contents poses serious business risks, including data breaches, financial losses, and reputational damage. The potential theft of sensitive information and intellectual property can lead to legal consequences and impact customer trust.

VULNERABILITY NAME: Phishing Via Ajax

CWE: CWE-79

OWASP Category: A04:2021-Insecure Design

Description: Phishing via AJAX involves attackers manipulating asynchronous JavaScript requests to deceive users into interacting with malicious content. By exploiting the dynamic nature of AJAX, phishing attempts can dynamically alter page content in real-time, tricking users into divulging sensitive information or interacting with seemingly legitimate but fraudulent forms or pop-ups.

Business Impact: Phishing with AJAX can lead to severe business consequences, including compromised user credentials, data breaches, and reputational damage as attackers exploit the dynamic nature of asynchronous JavaScript requests to trick users into revealing sensitive information.

Main Website Vulnerability Table

Website: <https://www.havmor.com/>

S.No	Vulnerability Name	CWE Number
1	SSH Weak Key Exchange Algorithms Enabled	CWE-326
2	SSH Server CBC Mode Ciphers Enabled	CWE-327
3	HSTS Missing from HTTPS Server	CWE-523
4	DNS Server Spoofed Request Amplification DDoS	CWE406
5	DNS Server Recursive Query Cache Poisoning Weakness	CWE-682

VULNERABILITY NAME: SSH Weak Key Exchange Algorithms Enabled
CWE: CWE-326

OWASP Category: A02:2021-Cryptographic Failures.

Description: The vulnerability "SSH Weak Key Exchange Algorithms Enabled" signifies a security concern where the Secure Shell protocol is configured to allow the use of outdated and potentially exploitable cryptographic algorithms during key exchange. This weakness could expose systems to the risk of unauthorized access or data compromise.

Business Impact: The business impact of "SSH Weak Key Exchange Algorithms Enabled" can be severe, leading to unauthorized access, data breaches, and potential compromise of sensitive information. Such vulnerabilities could result in financial losses, damage to reputation, and legal consequences.

VULNERABILITY NAME: SSH Server CBC Mode Ciphers Enabled
CWE: CWE-327

OWASP Category: A02:2021-Cryptographic Failures.

Description: The vulnerability "SSH Server CBC Mode Ciphers Enabled" indicates that the Cipher Block Chaining (CBC) mode ciphers are active in the configuration of the Secure Shell (SSH) server. CBC is a block cipher mode widely used in cryptographic protocols, but it is known to have certain vulnerabilities, particularly related to information leakage and padding oracle attacks. When CBC mode ciphers are enabled in the SSH server, it poses a potential risk of exploitation by attackers.

Business Impact: Enabling "SSH Server CBC Mode Ciphers" poses a significant business impact by exposing organizations to data confidentiality risks and potential unauthorized access. This vulnerability may lead to regulatory compliance concerns, attracting legal consequences and fines for failing to meet industry standards. Additionally, the exploitation of insecure SSH configurations could damage the organization's reputation and result in operational disruptions, emphasizing the critical need for prompt mitigation measures.

VULNERABILITY NAME: HSTS Missing from HTTPS Server

CWE: CWE-523

OWASP Category: A05:2021-Security Misconfiguration

Description: The absence of HTTP Strict Transport Security (HSTS) from an HTTPS server represents a security vulnerability where the server fails to enforce a policy instructing web browsers to communicate exclusively over secure HTTPS connections. HSTS is a critical security mechanism designed to mitigate the risk of man-in-the-middle attacks and enhance the overall security posture of web applications.

Business Impact: The business impact of HSTS missing from an HTTPS server includes heightened security risks, increasing the vulnerability to man-in-the-middle attacks and potential unauthorized access to sensitive data. This absence may lead to data breaches, erode user trust, and result in regulatory non-compliance, impacting the organization's reputation and exposing it to legal consequences. Without HSTS, there is a risk of session hijacking, potentially causing financial losses and putting the business at a competitive disadvantage in a security-conscious market.

VULNERABILITY NAME: DNS Server Spoofed Request Amplification DDoS

CWE: CWE-406

OWASP Category: A04:2021-Insecure Design.

Description: The "DNS Server Spoofed Request Amplification DDoS" vulnerability allows attackers to exploit weaknesses in DNS servers by sending malicious requests with spoofed source IPs. By leveraging the DNS protocol's amplification characteristics, the attackers generate large responses to small requests, overwhelming the target with a flood of traffic and causing a Distributed Denial of Service (DDoS) scenario.

Business Impact: A "DNS Server Spoofed Request Amplification DDoS" attack can inflict severe business impact, causing service disruptions, financial losses, and reputational damage. Downtime and unavailability may lead to dissatisfied customers, legal consequences, and increased operational costs for mitigating and recovering from the attack. Businesses may also face a competitive disadvantage as resilient competitors gain market share during disruptive periods, emphasizing the critical need for robust DDoS mitigation strategies.

VULNERABILITY NAME: DNS Server Recursive Query Cache Poisoning
Weakness

CWE: CWE-682

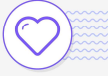
OWASP Category: A05:2021-Security Misconfiguration

Description: DNS Server Recursive Query Cache Poisoning is a security weakness where an attacker exploits vulnerabilities in a DNS (Domain Name System) server's handling of recursive queries. In this scenario, an adversary can manipulate the responses to these queries, injecting fraudulent DNS records into the server's cache.

Business Impact: DNS Server Recursive Query Cache Poisoning can disrupt services, compromise sensitive data, and erode customer trust by redirecting legitimate traffic to malicious destinations. The financial consequences include operational costs for remediation, potential legal repercussions, and a competitive disadvantage in the market. This vulnerability necessitates urgent mitigation to prevent business impacts such as downtime, data breaches, and damage to reputation and customer relationships.


Brainstorming Map and Empathy Map

Template



Empathy map canvas

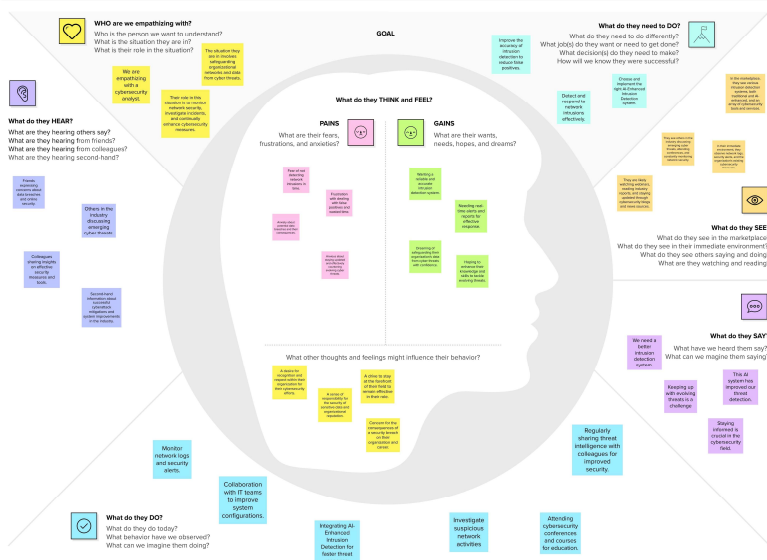
Use this framework to empathize with a customer, user, or any person who is affected by a team's work. Document and discuss your observations and note your assumptions to gain more empathy for the people you serve.


Originally created by Dave Gray at 

[Share template feedback](#)




AI-Enhanced Intrusion Detection System


The user persona for the AI-Enhanced Intrusion Detection System is a cybersecurity analyst. They prioritize reliability, real-time alerts, and staying informed about evolving threats. Their concerns include false positives, data breaches, and the need to continually enhance their skills.





Need some inspiration?
Get a random selection of this template to kickstart your work.
[Open example](#)





Brainstorm & Idea prioritization

Use this template to plan, plan, and prioritize your ideas and projects. It's a great way to get your team's input and to make sure you're focusing on the most important tasks.

1. Brainstorming
2. Prioritization
3. Planning

Define your problem statement

What problem are you trying to solve? What are the goals of your project? What are the constraints?

1. Define the problem
2. Define the goals
3. Define the constraints

Brainstorm

What ideas do you have? What are your thoughts? What are your feelings? What are your hopes? What are your dreams?

1. Brainstorming
2. Prioritization
3. Planning

Plan

What are your next steps? What are your goals? What are your constraints? What are your risks? What are your opportunities?

1. Plan
2. Prioritize
3. Execute

Execute

What are your next steps? What are your goals? What are your constraints? What are your risks? What are your opportunities?

1. Execute
2. Monitor
3. Evaluate

Monitor & Evaluate













What are your next steps? What are your goals? What are your constraints? What are your risks? What are your opportunities?

1. Monitor
2. Evaluate
3. Report

Report

What are your next steps? What are your goals? What are your constraints? What are your risks? What are your opportunities?

1. Report
2. Review
3. Reflect



Overview on Nessus

What is Nessus?

Nessus is a widely-used vulnerability assessment and penetration testing tool developed by Tenable, Inc. It is designed to identify and assess vulnerabilities, misconfigurations, and security issues within computer systems, networks, and applications.

Key Features:

1. *Vulnerability Scanning:*

Nessus conducts comprehensive vulnerability scans to identify weaknesses in systems and applications. It covers a wide range of vulnerabilities, including known and emerging threats.

2. *Policy Compliance Checks:*

Nessus assesses systems against security policies and compliance standards to ensure adherence to regulatory requirements.

3. *Plugin Architecture:*

The tool utilizes a modular plugin architecture, allowing users to customize scans based on specific needs. Constant updates ensure coverage for the latest vulnerabilities and threats.

4. *Multiple Platform Support:*

Nessus supports various operating systems, making it versatile for scanning diverse environments, including Windows, Linux, and macOS.

5. *Scalability:*

Suitable for both small businesses and large enterprises, Nessus scales to meet the needs of different network sizes.

6. *Report Generation:*

Nessus generates detailed reports with actionable insights, aiding security professionals in prioritizing and addressing identified vulnerabilities.

Target Website: <https://google-gruyere.appspot.com/595415950294913840432014314475390761256/>

Target IP Address: 142.250.97.153

S.No	Vulnerability Name	Severity	Plugins
1	DNS Server Recursive Query Cache Poisoning Weakness	Medium	10539
2	DNS Server Cache Snooping Remote Information Disclosure	Medium	12217
3	DNS Server Spoofed Request Amplification DDoS	High	35450
4	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	42873
5	TLS Version 1.0 Protocol Detection	Medium	104743
6	TLS Version 1.1 Protocol Deprecated	Medium	157288

Vulnerability Name: DNS Server Recursive Query Cache Poisoning Weakness

Severity: Medium

Plugin: 10539

Port: 53

Description: It is possible to query the remote name server for third-party names. If this is your internal nameserver, then the attack vector maybe limited to employees or guest access if allowed. If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org). This allows attackers to perform cache poisoning attacks against this nameserver. If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

Solution:

1. Restrict recursive queries to the hosts that should use this nameserver, such as those of the LAN connected to it.
2. If you are using bind 8, you can achieve this by using the 'allow-recursion' instruction in the 'options' section of your named.conf.
3. If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command. Then, within the 'options' block, explicitly state: 'allow-recursion { hosts_defined_in_acl }'.
4. If you are using another name server, consult its documentation.

Business Impact:

The DNS Server Recursive Query Cache Poisoning weakness poses significant business risks. This vulnerability can result in service disruption, potentially impacting the availability of network resources and online services. Moreover, the compromise of cached information opens the door to unauthorized access and potential data exposure, posing a serious threat to sensitive information. Beyond the immediate technical consequences, successful exploitation of this weakness may lead to reputational damage, eroding trust in the affected organization's online services and potentially affecting customer or user confidence.

Vulnerability Name: DNS Server Cache Snooping Remote Information Disclosure

Severity: Medium

Plugin: 12217

Port: 53

Description: The remote DNS server exhibits a security concern by responding to queries for third-party domains without the recursion bit set. This vulnerability opens the door for a potential remote attacker to discern recently resolved domains via this name server. Consequently, the attacker could determine which hosts have been visited recently. For example, an attacker might leverage this vulnerability to construct a statistical model regarding a company's usage of online services from a specific financial institution. Beyond financial institutions, this attack methodology can be employed to uncover B2B partners, analyse web-surfing patterns, identify external mail servers, and reveal various other sensitive information. This highlights the critical need for addressing and remedying this vulnerability to fortify the security posture of the DNS server.

Solution:

1. Contact the vendor of the DNS software for a fix.

Business Impact: The DNS Server Cache Snooping vulnerability poses a substantial business risk, potentially leading to remote information disclosure. This flaw allows an unauthorized attacker to clandestinely inspect the cached information on the DNS server, potentially exposing sensitive data. Such information disclosure could be leveraged to gain insights into an organization's internal network structure, identify critical servers, and gather intelligence on the company's digital infrastructure. The consequences extend to the potential compromise of confidential business information, intellectual property, and sensitive client data.

Vulnerability Name: DNS Server Spoofed Request Amplification DDoS

Severity: High

Plugin: 35450

Port: 53

Description: The identified vulnerability in the remote DNS server is significant as it responds to any request, enabling potential exploitation through a technique known as amplification. Specifically, an attacker can query the name servers (NS) of the root zone ('.') and receive an answer larger than the original request. By spoofing the source IP address, the attacker can leverage this amplification effect to launch a denial-of-service (DoS) attack against a third-party host using the vulnerable DNS server. This susceptibility emphasizes the need for proactive measures to secure DNS servers, preventing them from being unwittingly used as tools for malicious activities, thereby ensuring the integrity and availability of online services.

Solution:

1. Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Business Impact: The DNS Server Spoofed Request Amplification vulnerability introduces a substantial business impact by exposing the infrastructure to potential Distributed Denial of Service (DDoS) attacks. This weakness allows malicious actors to manipulate the DNS server by sending spoofed requests that trigger an amplification effect, generating larger responses than the original queries. Through this technique, attackers can orchestrate DDoS attacks, overwhelming the targeted systems with an influx of traffic. The consequences of such attacks are severe, encompassing service disruptions, degraded user experiences, and potential financial losses.

Vulnerability Name: SSL Medium Strength Cipher Suites Supported (SWEET32)

Severity: High

Plugin: 42873

Port: 443

Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Solution:

1. Reconfigure the affected application, if possible, to avoid use of medium strength ciphers.

Business Impact: The presence of SSL Medium Strength Cipher Suites, specifically vulnerable to the SWEET32 attack, poses a significant business risk. These cipher suites, which operate with weaker encryption algorithms, can be exploited by adversaries to launch attacks that compromise the confidentiality of transmitted data. The SWEET32 vulnerability allows attackers to exploit the inherent weaknesses in these cipher suites and potentially decrypt sensitive information exchanged between clients and servers. The business impact extends to the potential exposure of confidential customer data, intellectual property, and other sensitive information.

Vulnerability Name: TLS Version 1.0 Protocol Detection

Severity: Medium

Plugin: 104743

Port: 443

Description: The remote service currently accepts encrypted connections using TLS 1.0, a protocol known to have cryptographic design flaws. While modern implementations of TLS 1.0 attempt to address these issues, it is recommended to prioritize the use of newer TLS versions such as 1.2 and 1.3, as they are specifically designed to counteract these flaws. Notably, starting from March 31, 2020, endpoints not enabled for TLS 1.2 and higher may experience functionality issues with major web browsers and vendors.

In alignment with security standards, PCI DSS v3.2 mandates the complete disabling of TLS 1.0 by June 30, 2018, except for Point of Sale (POS), Point of Interaction (POI) terminals and the associated SSL/TLS termination points. The latter must be verifiably secure against known exploits. Adhering to these guidelines is imperative for maintaining the security of encrypted connections, ensuring compatibility with contemporary web technologies, and meeting regulatory requirements within the specified timelines.

Solution:

1. Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Business Impact: The detection of TLS Version 1.0 protocol on a system poses a notable business impact due to its inherent security vulnerabilities. TLS 1.0 has known cryptographic design flaws, and while modern implementations aim to mitigate these issues, the protocol itself is considered outdated. The continued use of TLS 1.0 exposes the organization to heightened cybersecurity risks, potentially leading to unauthorized access, data breaches, and compromised confidentiality. Moreover, compliance requirements, such as PCI DSS v3.2, mandate the cessation of TLS 1.0 usage to enhance overall security.

Vulnerability Name: TLS Version 1.1 Protocol Deprecated

Severity: Medium

Plugin: 157288

Port: 443

Description: The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution:

1. Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Business Impact: The deprecation of TLS Version 1.1 carries a significant business impact as it renders systems using this protocol susceptible to security vulnerabilities. TLS 1.1 is considered outdated, and its continued use poses increased risks of unauthorized access, data breaches, and compromised confidentiality. With the deprecation, organizations may face challenges in meeting evolving compliance standards and industry regulations, potentially leading to legal and reputational consequences.

Ability of IBM QRadar

1. Introduction

In the modern landscape of cybersecurity, it is crucial for organizations to implement advanced security measures. This report delves into the concept of an AI Enhanced Intrusion Detection System, exploring various components, methodologies, and considerations that contribute to a more robust security posture. The report covers Security Operations Center (SOC), Security Information and Event Management (SIEM), Malware Information Sharing Platform & Threat Sharing (MISP), deployment strategies, threat intelligence, incident response, and IBM QRadar.

Example: In recent years, the frequency and sophistication of cyberattacks have increased significantly. Organizations, including educational institutions like colleges, face a growing need to bolster their cybersecurity measures. An AI Enhanced Intrusion Detection System is a critical element in fortifying defenses against these evolving threats.

2. Security Operations Center (SOC)

2.1 SOC Overview

A Security Operations Center (SOC) is the central hub for monitoring, detecting, and responding to security threats within an organization. It acts as the first line of defense against cyberattacks, continuously monitoring network traffic, systems, and applications.

Example: When a SOC detects an unusual pattern in network traffic, such as multiple failed login attempts from different locations, it can raise an alert, allowing security analysts to investigate and respond promptly.

2.2 SOC Cycle

The SOC operates in a cyclical manner, involving phases such as monitoring, detection, analysis, and response. This cyclical process ensures that security incidents are identified and mitigated promptly, maintaining a high level of security.

Example: Consider a real-world scenario where a SOC identifies a suspicious data exfiltration attempt. The cycle involves monitoring network traffic, detecting the anomaly, analyzing the potential breach, and responding by isolating the affected systems to prevent data loss.

3. Security Information and Event Management (SIEM)

3.1 SIEM Overview

Security Information and Event Management (SIEM) is a critical technology that aids in collecting, analyzing, and correlating security event data. It provides organizations with real-time insights into their security posture and enables early threat detection.

Example: A SIEM system can correlate seemingly unrelated security events, such as a failed login attempt, followed by unauthorized access to a critical system. This correlation can trigger an alert, potentially preventing a security breach.

3.2 SIEM Cycle

The SIEM deployment cycle involves data collection, event correlation, alerting, and reporting. This iterative process enhances an organization's ability to respond to evolving threats and vulnerabilities.

Example: After collecting data from various sources, including firewalls, intrusion detection systems, and endpoint protection, a SIEM system can correlate these data points to identify a potential security incident, alert security analysts, and generate reports for further analysis and compliance reporting.

4. Malware Information Sharing Platform & Threat Sharing (MISP)

Example: Let's imagine a scenario where a college's SOC identifies a new strain of malware that attempted to infiltrate the network. The college can use MISP to share information about this malware, such as its signature, with other educational institutions. This proactive sharing helps other organizations strengthen their defenses against the same threat.

5. College Network Information

Example: In your college network, which comprises multiple departments and hundreds of users, various devices are connected. These include computers, servers, IoT devices, and network equipment, making it a diverse and complex environment. With such diversity, the potential attack surface is broad, necessitating a robust intrusion detection system.

6. Deployment of SOC in Your College

Example: To illustrate the deployment strategy, let's consider a scenario where your college decides to establish a SOC with limited budget and resources. In this case, you might opt for a cloud-based SIEM solution, allowing for scalability and cost-effectiveness while ensuring comprehensive threat detection.

7. Threat Intelligence

Example: A practical example of threat intelligence is the utilization of feeds that provide information about recent cyber threats, including indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by threat actors. This information can help your college's SOC stay updated and well-prepared against emerging threats.

8. Incident Response

Example: In a real-world incident response scenario, a breach is detected where unauthorized access has compromised sensitive student data. The incident response team follows a predefined plan, isolates the affected systems, investigates the extent of the breach, and takes steps to prevent data leakage. Lessons learned during the incident response process inform future security improvements.

9. IBM Qradar & Understanding About the Tool

Example: Your college chooses IBM Qradar as its SIEM solution. This tool provides real-time monitoring and advanced threat detection capabilities. For instance, it can identify unusual patterns in network traffic that may indicate a Distributed Denial of Service (DDoS) attack, enabling the SOC to respond promptly.

10. Conclusion

In this report, we have delved into several critical aspects of cybersecurity, web application testing, Nessus reports, and the role of a SOC/SEIM/Qradar dashboard. Each of these stages provides a unique perspective on enhancing the security posture of an organization, including your college network. Let's summarize the key takeaways from each of these stages:

Stage 1: Web Application Testing

Web application testing is a fundamental practice in ensuring the security and reliability of web-based services. It involves a comprehensive assessment of web applications to identify vulnerabilities, assess their potential impact, and mitigate them effectively. Through techniques such as vulnerability scanning, penetration testing, and code review, we can uncover and remediate issues like SQL injection, cross-site scripting, and other potential threats. By incorporating web application testing into your college's security strategy, you not only protect sensitive data but also uphold the integrity of online services provided to students and staff.

Stage 2: Nessus Report

The Nessus report plays a pivotal role in identifying vulnerabilities within an organization's network and systems. This tool provides detailed insights into potential security weaknesses, helping security professionals prioritize their efforts and remediation actions. The Nessus report includes crucial information such as vulnerability severity, affected assets, and remediation recommendations. It serves as a valuable guide in addressing vulnerabilities and maintaining a secure network environment. By regularly utilizing Nessus reports, your college can stay proactive in addressing emerging security risks.

Stage 3: SOC / SIEM / Qradar Dashboard

The Security Operations Center (SOC), Security Information and Event Management (SIEM), and the Qradar dashboard are essential components of a proactive cybersecurity strategy. The SOC serves as the central hub for monitoring, detecting, and responding to security threats. SIEM solutions like Qradar collect, correlate, and analyze security event data from various sources, providing real-time insights into an organization's security posture. The Qradar dashboard visually represents this data, making it accessible and actionable for security analysts. By adopting these technologies, your college can strengthen its defense against cyber threats, swiftly respond to incidents, and ensure the continuity of secure educational services.

Future Scope

As technology continues to evolve, the future of cybersecurity and intrusion detection is an ever-expanding field. Let's explore the potential future developments and trends in each of the topics and tools discussed in this report:

Stage 1: Future Scope of Web Application Testing

The future scope of web application testing holds several promising developments:

1. AI and Machine Learning Integration: Web application testing is expected to incorporate AI and machine learning to enhance automation, speed, and accuracy in vulnerability detection and exploitation. AI-driven testing tools will adapt to emerging threats and sophisticated attack techniques.

2. Enhanced IoT Security Testing: With the proliferation of Internet of Things (IoT) devices, future web application testing will include comprehensive security assessment of IoT applications and their integration into web services.

3.Container and Serverless Security: As containerization and serverless computing gain popularity, web application testing will focus on assessing the security of these technologies, ensuring that applications and data remain protected in dynamic environments.

4.DevSecOps Integration: Future web application testing will be seamlessly integrated into DevSecOps pipelines, allowing for continuous security testing and rapid vulnerability remediation.

Stage 2: Future Scope of Testing Process

The testing process will continue to evolve in the following ways:

1.Shift-Left Testing: The future of testing emphasizes "shift-left," where testing activities are introduced earlier in the software development lifecycle. This ensures that security and quality are integral to the development process, reducing vulnerabilities and costs associated with late-stage defect detection.

2.Automation and AI-Driven Testing: Testing processes will be increasingly automated, with AI-driven testing tools becoming the norm. Test cases will be generated automatically, and AI will assist in test scenario selection.

3.Security Testing as Code: Security testing will be treated as code, with security tests defined in scripts and configurations that can be version-controlled, allowing for continuous security testing.

4.Continuous Testing: Testing will become a continuous and ongoing process, rather than a discrete phase, ensuring that software remains secure and high-quality throughout its lifecycle.

Stage 3: Future Scope of SOC / SEIM

The future of SOC/SEIM includes the following advancements:

1.Threat Intelligence Integration: SOC/SEIM solutions will incorporate advanced threat intelligence feeds and predictive analytics to anticipate and prepare for emerging threats, allowing for proactive threat mitigation.

2.Cloud and Hybrid Environments: As organizations transition to cloud and hybrid infrastructures, SOC/SEIM solutions will adapt to monitor and secure these environments effectively.

3. User and Entity Behavior Analytics (UEBA): UEBA will play a more significant role in detecting insider threats and abnormal user behavior, enhancing the ability to prevent data breaches.

4. Integration with Endpoint Detection and Response (EDR): The integration of SEIM with EDR solutions will offer comprehensive threat detection and response capabilities, ensuring that security incidents are addressed swiftly and comprehensively.

Tools Explored:

- Nessus:

Nessus is poised for continued innovation, with advancements such as:

1. Cloud Security Assessments: Nessus will evolve to assess cloud environments and infrastructure, providing organizations with a comprehensive view of their security in the cloud.

2. IoT Vulnerability Scanning: As IoT devices become more prevalent, Nessus will incorporate specialized scanning for vulnerabilities in IoT devices and their associated networks.

- IBM Qradar:

IBM Qradar will continue to adapt to changing security landscapes:

1. AI-Driven Threat Detection: Qradar will employ AI and machine learning for more accurate and real-time threat detection, reducing false positives and enhancing threat response.

2. Container Security: Qradar will expand its capabilities to monitor and secure containerized environments, catering to modern microservices architectures.

In conclusion, the future of cybersecurity, web application testing, testing processes, SOC/SEIM, and the tools explored in this report is promising. As the digital landscape evolves, these areas will continue to adapt and innovate to meet the ever-increasing challenges posed by cyber threats. Staying informed about these future developments and trends is crucial for maintaining a strong security posture and effectively defending against emerging threats.

Knowledge Gained

1. Basics of Cybersecurity.
2. SIEM/SOC tools.
3. Real world uses of IBM QRadar.
4. How to utilize IBM QRadar.
5. Purpose of Intrusion Detection System.
6. How does AI work.
7. How to use AI in Cybersecurity.
8. How to embed AI and IDS together.

Future Scope of AI Enhanced Intrusion Detection System

The future scope of AI-enhanced Intrusion Detection Systems (IDS) is promising and holds the potential for significant advancements in cybersecurity. Some key areas of development include:

1. Advanced Machine Learning Algorithms: AI-driven IDS will continue to evolve with more sophisticated machine learning algorithms. These algorithms will enable better anomaly detection, reducing false positives and enhancing the accuracy of threat identification.

2. Behavioral Analysis: Future IDS systems will focus on comprehensive behavioural analysis, allowing them to detect subtle deviations from normal behaviour, which are indicative of advanced threats and insider attacks.

3. Integration with Threat Intelligence: The integration of AI-IDS with threat intelligence feeds will become more seamless. This will provide real-time access to the latest threat information, enhancing the system's ability to detect and respond to emerging threats.

4. Automated Response: AI-IDS will increasingly incorporate automated response capabilities, enabling real-time threat mitigation. These systems will not only detect threats but also take immediate action to isolate affected systems or block malicious activity.

5. IoT and Cloud Security: With the expansion of IoT devices and cloud infrastructures, AI-IDS will extend its coverage to include these areas. Protecting IoT devices and cloud resources from cyber threats will be a critical focus.

Conclusion

The deployment of an AI-enhanced Intrusion Detection System is crucial in the ever-evolving landscape of cybersecurity. This report has explored the various components and methodologies that contribute to a more robust security posture. By integrating advanced machine learning, behavioural analysis, threat intelligence, and automated response capabilities, AI-IDS provides a proactive defence against a wide range of cyber threats.

As the digital landscape continues to change and threats become more sophisticated, AI-IDS will play an increasingly vital role in safeguarding critical assets and data. It not only detects known threats but also identifies emerging and novel attack patterns. The future scope of AI-IDS promises to further enhance its capabilities, making it an indispensable tool for organizations seeking to protect their networks and data.

In conclusion, the implementation of an AI-enhanced Intrusion Detection System is an investment in proactive security, and it underscores a commitment to data protection and the continuous availability of secure services. As the realm of cybersecurity evolves, AI-IDS will stand as a stalwart guardian, fortifying defences against emerging threats and ensuring the ongoing integrity of network and system security.