Automated Security Penetration & Assessment System for Web and Local Network

BY
Sajibe Kanti Sarkar
ID : 191-15-12174

Md. Abdullah
ID : 191-15-12599

This Report Presented in Partial Fulfillment of the Requirements for the

Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Touhid Bhuiyan
Professor & Head

Department of CSE

Daffodil International University

Co-Supervised By

Most. Hasna Hena

Assistant Professor
Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH
DECEMBER 2021

APPROVAL

This Project titled **"Automated Security Penetration & Assessment System for Web and Local Network"**, submitted by Sajibe Kanti Sarkar and Md. Abdullah to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 20/12/2021.

BOARD OF EXAMINERS

______________________ **Chairman**

Dr. Touhid Bhuiyan (DTB)

Professor and Head

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

____

Md. Riazur Rahman (RR)

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

____

Md. Ohidujjaman Tuhin (MOT)

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Imran

External Examiner

____

Shah Md. Imran

Industry Promotion Expert

LICT Project, ICT Division, Bangladesh

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Touhid Bhuiyan, Professor & Head, Department of CSE Daffodil International University**. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Touhid Bhuiyan (DTB)

Professor and Head

Department of CSE

Daffodil International University

Co-Supervised by:

Most. Hasna Hena

Assistant Professor

Department of CSE

Daffodil International University

Submitted by:

Sajibe

Sajibe Kanti Sarkar

ID: -191-15-12174

Department of CSE

Daffodil International University

Abdullah

____

Md.Abdullah
ID: -191-15-12599

Department of CSE

Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Touhid Bhuiyan, Professor & Head, Department of CSE Daffodil International University, Dhaka,** Deep Knowledge &amp; keen interest of our supervisor in the field of Cyber Security to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Touhid Bhuiyan, Most. Hasna Hena and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The goal of this project is to ensure the security of any business or institution. A major problem in the twenty-first century is cyber security and data breaches. The covid-19 situations drive every end user and institution to go online to accomplish their job, and lack of security can put billions of users at risk. Security threats and data breaches are increasing. The most prevalent reason for this problem is an old and unpatched vulnerability, as well as human error and an unawareness. Vulnerability scanning, network scanning, and reporting are all major methods used in this project. Following a successful scan, we discovered the network's overall structure, which hosts are vulnerable, which are critical, which are moderate, detailed about the vulnerability, port distribution, and other key information. We discovered a small performance drop while utilizing a low-spec computer because of the CPU load. This can be rectified by using a high-performance system or a good VPS. This can be used in a range of situation ns. System admins and network engineers can use this to increase the security of their digital assets, from small to midsize businesses to educational institutions.

Table of Contents

CONTENTS **PAGE**

BOARD OF EXAMINERS **Error! Bookmark not defined.**

DECLARATION iv

ACKNOWLEDGEMENT v

ABSTRACT vi

Chapter 1: Introduction 11

1.1 Introduction 11

1.2 Motivation 11

1.3 Objectives 12

1.4 Expected Outcomes 13

1.5 Project Management and Finance 13

Chapter 2: Background 14

2.1 Preliminaries/Terminologies 14

2.2 Related Works 14

2.3 Comparative Analysis 15

2.4 Scope of the Problem 15

2.5 Challenges 15

Chapter 3: Requirement Specification 17

3.1 Business Process Modeling 17

3.2 Requirement Collection and Analysis 17

3.3 Use Case Modeling and Description 18

3.4 Logical Data Model 19

Chapter 4: Design Specification 21

4.1 Front-end Design 21

4.1.1 Front-end Program 21

4.2 Back-end Design 22

4.2.1 Languages for the back end 26

4.2.2 Frameworks for the back end 26

4.3 Interaction Design and User Experience (UX) 26

4.4 Implementation Requirements 27

Chapter 5: Implementation and Testing 28

5.1 Implementation of Database 28

5.2 Implementation of Front-end Design 28

5.3 Testing Implementation 28

5.3.1 Prerequisites 28

5.3.2 Deployment Recommendation 29

5.3.3 Deployment using Docker 29

5.3.4 Deployment in VPS / Server 30

5.3.5 Multi Node Installation 31

5.4 Test Results and Reports 31

Chapter 6: Impact on Society, Environment and Sustainability 34

6.1 Impact on Society 34

6.2 Impact on Environment 34

6.3 Ethical Aspects 34

6.4 Sustainability Plan 35

Chapter 7: Conclusion and Future Scope 36

7.1 Discussion and Conclusions 36

7.2 Future work and Further Development 36

REFERENCES 37

LIST OF FIGURES

Figure 3.1: Gantt chart 17

Figure 3.3: system diagram 19

Figure 3.4: Logical Data Model 20

Figure 4.1.1: Login Page 22

Figure 4.2.1: Dashboard 23

Figure 4.2.2: Quick Start 23

Figure 4.2.3: Dashboard with Scan Result Details 24

Figure 4.2.5: Assessment 25

Figure 4.2.6: Network Topology of targeted IP 25

Figure 4.2.7: Vulnerabilities 26

Figure 5.4: Scan Report in html format 32

Figure 5.4.1: Scan result in raw 33

Chapter 1: Introduction

1.1 Introduction

The increasing popularity of information technology services has resulted in an increase in cyber-attacks. The absence of security expertise, as well as improperly configured and inferior resource management, pose a threat to our information technology environment.

In this pandemic companies must now adapt to a new operations strategy in which working remotely has become the "new normal" in the wake of the coronavirus epidemic, which has posed a number of new obstacles. As businesses accelerate their digital transformation, cyber security is becoming an increasingly important problem. It is possible that failing to address cyber security threats will have significant consequences in terms of reputation, operational efficiency, legality, and compliance. An example is the SolarWinds Attack, which occurred recently in the United States government and large organizations and is becoming more lethal by the day.

To bring this problem under control, several cyber security strategies must be implemented. Increase the speed with which essential systems are patched. By shortening patch cycles for systems that are critical for remote working, which includes virtual private networks (VPNs), end-point encryption, and cloud interfaces, firms can eradicate vulnerabilities as soon as they are discovered, allowing them to focus on other aspects of their business. It is especially important to pay attention to patches that protect distant infrastructure. Increase the use of multifactor authentication.

In our current project, we are developing a collection of automated tools that analyze local networks and web assets for security gaps and aggregate those threats in a logical and organized manner.

1.2 Motivation

Typically, this occurs when an ethical dilemma is involved, such as when a large website's database is compromised. Because of their corporate style of thinking, companies are more concerned with their reputation, customer relationships, stock price, and profit. Because of this, they spend a lot of money on security. However, small businesses and organizations cannot afford to spend that much money and manpower on security. As we all know, small businesses are an important part of our domestic and global economies. Because of the lack of budget, skilled manpower, and policies, small businesses are more vulnerable to cyber-attacks than large corporations are. If we take a glance at the Internet world, we can notice that there are numerous security companies that provide Cyber Security Solutions. We were also influenced by the Security Operations Center.

From them, such as Pentest-Tools (.) com and cobalt (.) io, we aim to construct comparable tools but with a new approach, and we deliver these tools for Web & network-based solutions, as well as for mobile solutions.

1.3 Objectives

As previously stated, the primary goal of Cyber Security and this initiative is to achieve these three characteristics (Confidentiality, Integrity, and Availability), which are together known as the CIA Triad. It is critical for any firm to defend its data and information by utilizing appropriate tools.

Only authorized subscribers should be able to obtain confidential information, which can be characterized as keeping the data secret and protected at all times.

In a similar vein, Integrity is extremely crucial in order to ensure that data has not been altered during transmission or access.

The institution also focuses on availability to ensure that services, tools, workflows, information, and other resources are available at all times to ensure that the business can run effectively and that the impact of a disaster is kept to a minimum.

Zero-day attacks are carried out using zero-day malware. This zero-day malware exploits a previously unknown vulnerability that has not been addressed or patched. Since the zero-day vulnerability is previously not known, the zero-day exploits often occur without the consent of the users as there will be no patches available at the time of infection. We are aiming to give as much update as possible about the fresh CVE's

So that it can patch those before it spread.

Notorious cyber-attacks such as in the Goldeneye, WannaCry ransomware outbreaks have devastated some firms and prompted many others to close their doors permanently. After these sophisticated cyber-attacks and security compromises, security has taken center stage in the minds of executives from companies of all kinds. There are new versions. New strategies are being implemented. Cyber-threats are always evolving. Have perhaps we seen a growth in the number of cyber-attacks on organizations and individuals, but the complexity with which those cyber-attacks have been carried out has also increased. In the years to come, cyber-attacks will become much more sophisticated, employing new technologies, targets, and motivations.

As a part of this project, the goal is to protect a company or individual from cyberattacks. Those reports were also arranged in a logical manner. The goal is to automate this so that Big Asset will not be an issue and it saves us time.

1.4 Expected Outcomes

Because we have to provide any IP or web address to our systems for recons, we expect the results of this operation to be fairly straightforward. At first, it will scan all available ports to identify potentially dangerous ones, and then it will begin the process of identifying further vulnerabilities. After the scan is completed, it will transmit the results to the developer and programmers for further investigation and correction. The goal is to exploit as many loopholes as possible on that asset.

Reporting to the team after a thorough recon will expedite the process in terms of a timely patch, and alerting on very new CVEs regarding their details, severity, and other essential information will expedite the process. Because of this, the organization will be up to date on the situation, which will lessen the likelihood of a mass attack.

Inspire client confidence - If you can demonstrate that your company is properly protected against all types of cyber intrusions, you will be able to instill confidence in your clients that their private data will be kept safe.

1.5 Project Management and Finance

It is the planning and organizing of project resources that allows a given work, event, or obligation to be completed on time and within budget. Employees, finances, technology, and creative works are all managed as part of this process, which might be a one-time initiative or a continuous operation.

Project management is frequently connected with professions such as engineering and construction, as well as information technology (IT), because these fields typically involve a complicated set of components that must be completed and integrated in a specific manner in order to produce a functional product. We know that it is a project that is being developed for security reasons, and as such, it can be overseen by the organization's security engineers or team, the information technology team, or the web administrator. Because of its straightforward and user-friendly design, it is simple to maintain and customize.

In order to benefit mid-range businesses and organizations, this project was created to be open source and cost-effective. The VPS and VPN will be the most expensive parts of this project, and the cost will vary depending on the size and assets of the particular organization.

Chapter 2: Background

2.1 Preliminaries/Terminologies

The rapid expansion of Internet-based services and applications has reshaped our working and personal lives. This will allow us to do so much more in our work, as well as provide a secret door for intruders. This project is concerned with the security of the web and networks. Taking part in this program will assist enterprises and people in reducing the likelihood of experiencing data breaches and other intruder activities on their systems. Because of its design and operating process, it has the potential to function as an early alarming defensive system. It will monitor and attempt to detect vulnerabilities in various parameters of a particular asset, and it will report the findings to the system administrator or the security engineers in charge of the asset. Notifications are sent out via slack and email by default, but the user can personalize this by adding his or her own favorite services to the list of those who will receive notifications. We have invested our academic and practical experience into this endeavor in order to increase overall security and keep the system safe from breaches of security.

2.2 Related Works

There are a few services that we noticed while working on this project that have done excellent work by some industry top organizations, and we wanted to share them with you.

Rapid7 is one of them. It is a well-known security solution provider that is devoted to providing services and products to protect, detect and respond to security incidents. Rapid7 has been recognized as one of the fastest growing security companies by Inc.It is up to date with a security matters/updates from the Internet, it has dashboards giving executive summaries of various security issues, it also has the capability of integrating with CIS Standards to further improve security posture of a business. It gives your insight on where to focus first.

Tenable also did an excellent job; they focused on vulnerability assessment and management, among other things. Advanced analytics, customizable dashboards, reports, and processes enable enterprises to better understand their risk and identify which vulnerabilities need to be addressed first. The Tenable.sc platform, which is based on industry-leading Nessus technology, collects and analyzes vulnerability data from many Nessus scanners spread throughout your enterprise and then displays vulnerability behaviors over time to help you mitigate risks and highlight vulnerabilities.

In addition, AT&T security, formerly known as AlienVault, is a cloud-based security management system that is designed to accelerate and centralize thread detection, incident response, and enforcement management security. It has enabled us to gain a better understanding of what is going on within our organization's network by providing us with a more complete picture of what is going on. Our exposure too many more activities than we were previously aware of has resulted from the events shown, and the addition of this component has just enhanced our exposure.

2.3 Comparative Analysis

In current scenario organizations and individuals looking for solutions or services to get rid of from cyber-attacks or data breaches, and so many big tech giants and security firms step forward but the some of the services are so complicated and expensive also
Which need specific hardware and more manpower and this will accept by the big organizations and first world countries , But underdeveloped country like Bangladesh can’t afford this kind of services especially small organization can’t allocated so many manpower to this specific area and don’t have heavy equipment , Our initiative focus this issues and make easier to handle and monitor this and don't need heavy equipment , it can be deploy and managed from anywhere , also this tools build as community based project where we can use this free of cost and make it more sophisticated by developing its mechanism by all together

2.4 Scope of the Problem

The most effective approaches to cyber security go much beyond the aforementioned fundamentals. These modest defenses can be bypassed by any advanced hacker. As a business grows, so does the challenge of maintaining a secure network. A Fortune 1000 corporation has a far larger 'attack surface' than a small to medium-sized organization. The growing overlap of information transmission between the online and offline platforms is another concern in cyber security. The IoT and Bring Your Own Device (BYOD) regulations allow thieves to get greater access to cyber-physical systems. The list includes anything from automobiles and factories to your kitchen's smart fridge and toaster. If one of these devices is hacked, it could suggest that all of them are. Also there are shortages of skilled manpower and server cost could be an issue for this.

2.5 Challenges

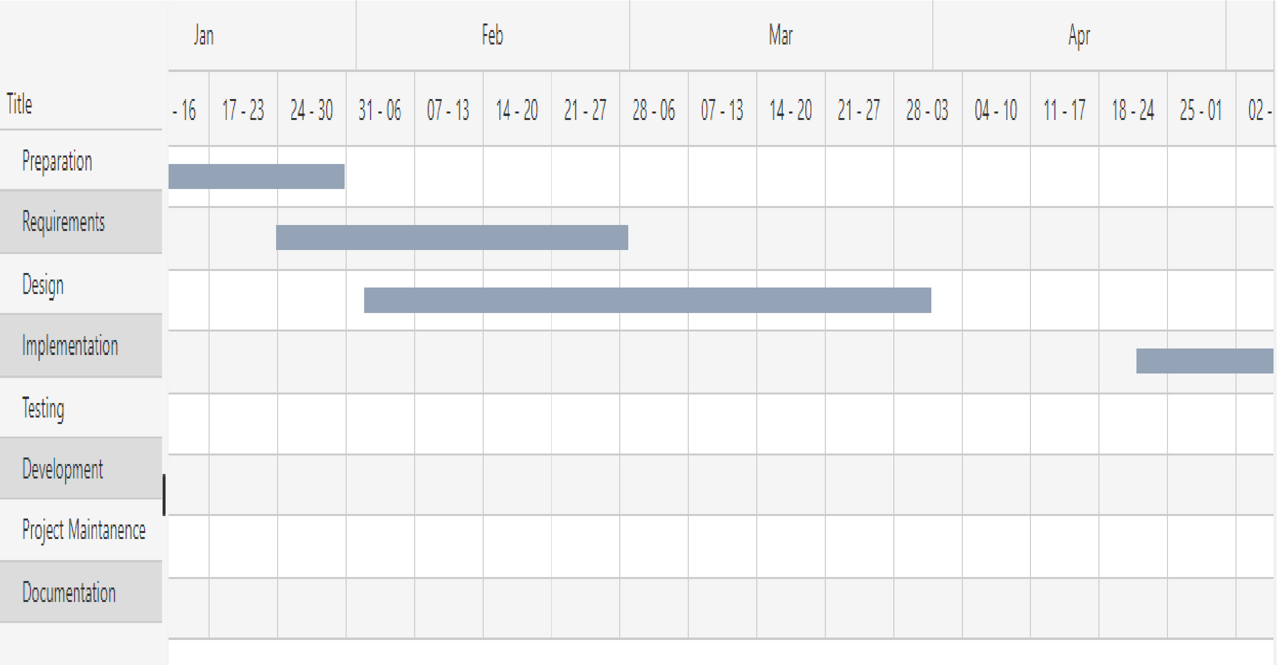
We have faced few challenges while working on this initiative, It’s a Cloud based project during the installation process sometimes cloud service provide can't fetch all libraries it will effect some specific workflow, we need to reinstall, one of the concerning things is processing power , if we want our output result faster this need multi thread processing.

Security monitoring is 24/7 work, so we have to maintain that protocol as well.

Chapter 3: Requirement Specification

3.1 Business Process Modeling

We started building this project as a community project and are trying to be open source and go with a simpler model. We like to use Business Process Modeling. We'll be able to use it for business purposes in the future. Business measure display is a top choice for us because it boosts productivity and is simple to use, ready to measure, and so on. It aids in a deeper understanding of how our cycle might work.



1Figure 3.1: Gantt chart

Figure 3.1: Gantt chart

3.2 Requirement Collection and Analysis

This project is established in the cloud so we need any protocol to communicate the server user can communicate from a device like mobile or pc's For smooth work this application requires very simple configuration. It is very easy to use with a user-friendly GUI to automate, arrange and handle all the task

Minimum Hardware required:

- 1 Core CPU
- 10 GB Storage
- 1 GB RAM

Platform:

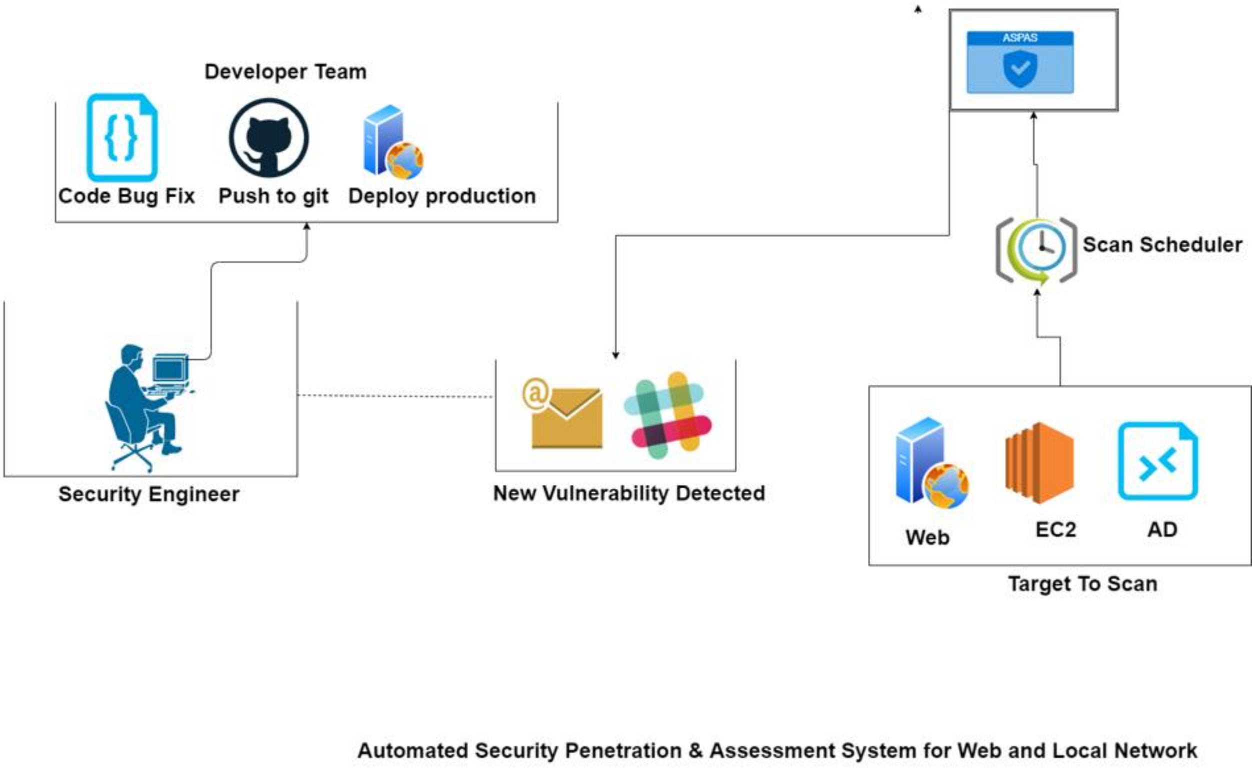
- Windows
- Linux
- Can be deployed on Dockers

Programming Language:

- Python
- Bootstrap, Angular JS

3.3 Use Case Modeling and Description

The figure we use in this section is pretty Self-explanatory, we have few sections that combine the full task properly done, and we can set the target AD, web then scan the target



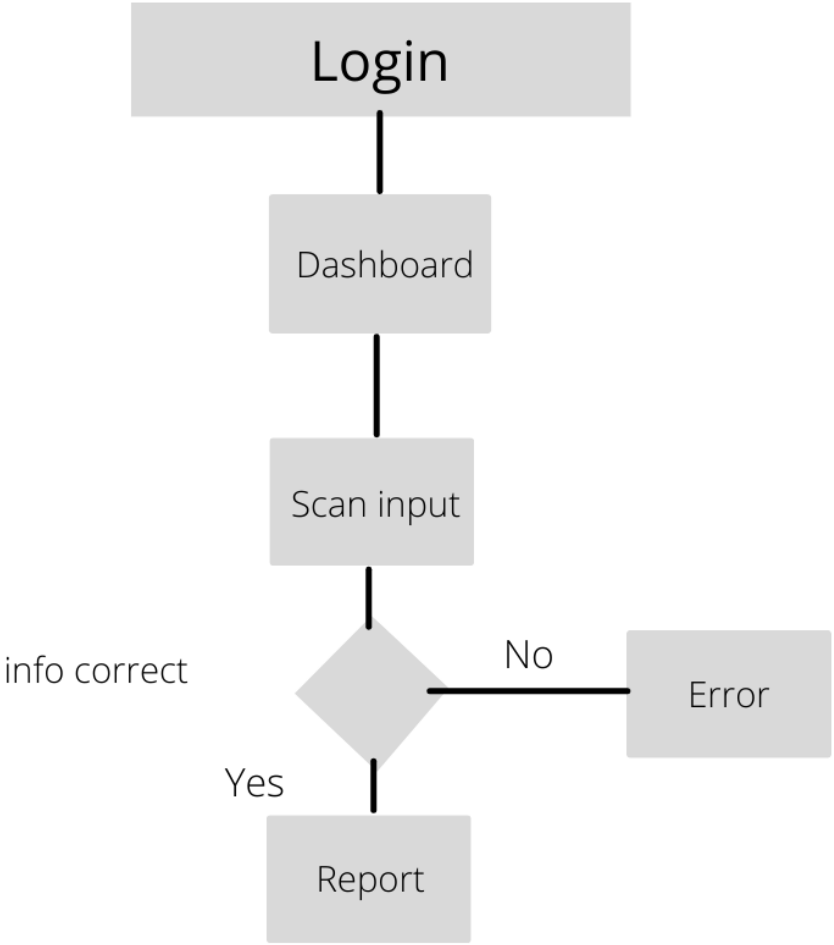
2 *Fig 3.3: system diagram*

Fig 3.3: system diagram

And then process the output and send it to the engineer via slack and email then those vulnerabilities go to developer sections for fix.

3.4 Logical Data Model

This is the logic behind the task. After login with correct credentials, we can access the dashboard where we can find all the features and sections related to scan and reports output. It takes assets as in input and passes this to the scan process if it's correct the processed output comes out as a report.



3Fig 3.4: Logical Data Model

Fig 3.4: Logical Data Model

Chapter 4: Design Specification

4.1 Front-end Design

Front-end web development, sometimes referred to as client-side development, is the process of creating HTML, CSS, and JavaScript for a website or Web application so that a user can see and interact with it directly. The difficulty with front end development is that the tools and techniques used to produce the front end of a website change all the time, necessitating the developer's ongoing awareness of how the field evolves.

The goal of website design is to guarantee that when users visit the site, they view material in an easy-to-read and relevant format. This is exacerbated even further by the fact that visitors today use a wide range of devices with different screen sizes and resolutions, prompting the designer to consider these factors while creating the site. They must ensure that their site works properly in a variety of browsers (cross-browser), operating systems (cross-platform), and devices (cross-device), which necessitates careful planning on the developer's part.

4.1.1 Front-end Program

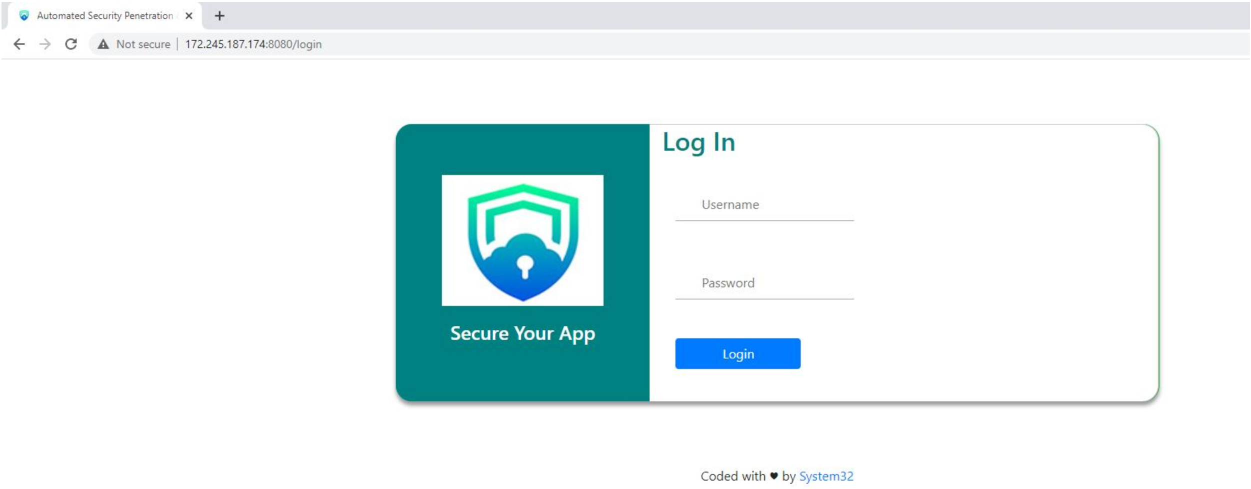
Hypertext Markup Language (HTML): HTML stands for Hypertext Markup Language. It is a markup language that is used to design the front-end portion of web pages. HTML is a markup language that combines hypertext with markup. The term "hypertext" refers to the link between web pages. Within the tag that specifies the structure of web pages, the markup language is used to create the text documentation.

CSS stands for Cascading Style Sheets, which is a simple language designed to make the process of making web pages presentable easier. Styles can be applied to web pages using CSS. More crucially, CSS allows you to do so without having to worry about the HTML code that makes up each web page.

JavaScript is a well-known programming language that is used to create magic on websites in order to make them more interactive for users. It's utilized to improve a website's functionality and run exciting games and web-based software.

The front-end design of the Automated Security Penetration & Assessment System for Web and Local Network Applications is a Login Page where a Security Engineer or Organization may login and manage their target site assessment.

Login page for Automated Security Penetration & Assessment System for Web and Local Network has Email & Password Box for Login, as well as a Submit Button to go Dashboard.

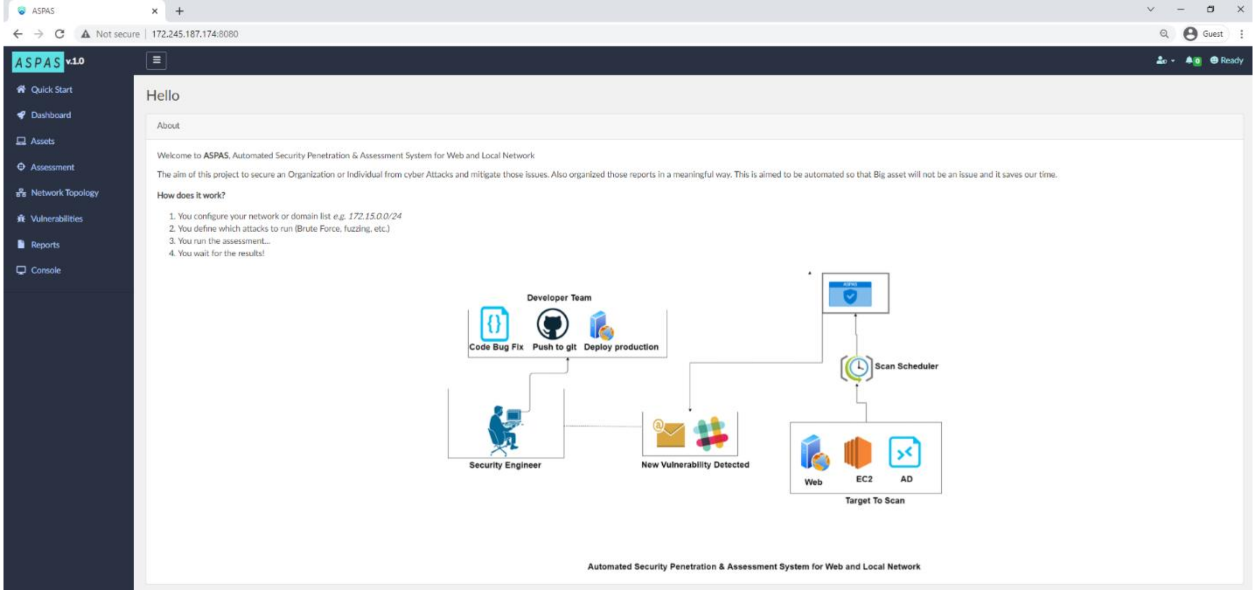

Automated Security Penetration
Not secure | 172.245.187.174:8080/login
Secure Your App
Log In
Username
Password
Login
Coded with ♥ by System32

4Fig 4.1.1: Login Page

Fig 4.1.1: Login Page

4.2 Back-end Design

Server-side development is referred to as back-end design. Databases, scripting, and website architecture are all covered. It describes the operations that take place behind the scenes when a user performs a specific activity on a website. It could be logging into an account or purchasing anything from an internet retailer. Back-end developers write code that allows browsers to communicate with database information.



Hello

About

Welcome to **ASPAS**, Automated Security Penetration & Assessment System for Web and Local Network

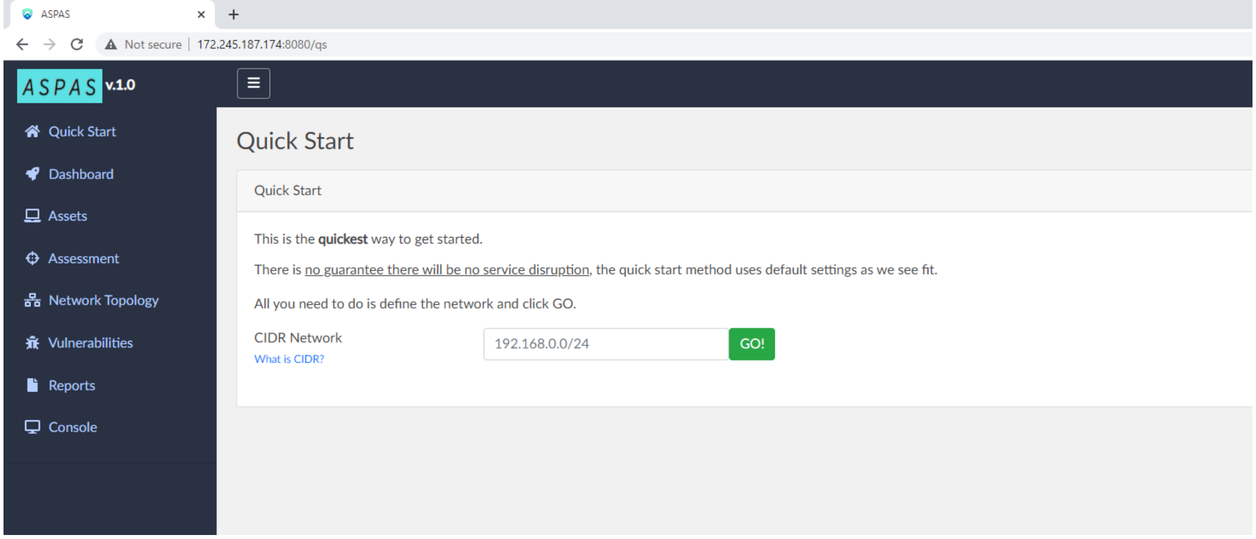
The aim of this project to secure an Organization or Individual from cyber Attacks and mitigate those issues. Also organized those reports in a meaningful way. This is aimed to be automated so that Big asset will not be an issue and it saves our time.

How does it work?

1. You configure your network or domain list *e.g. 172.15.0.0/24*
2. You define which attacks to run (Brute Force, fuzzing, etc.)
3. You run the assessment...
4. You wait for the results!

5*Fig 4.2.1: Dashboard*

Fig 4.2.1: Dashboard



Quick Start

Quick Start

This is the **quickest** way to get started.

There is no guarantee there will be no service disruption, the quick start method uses default settings as we see fit.

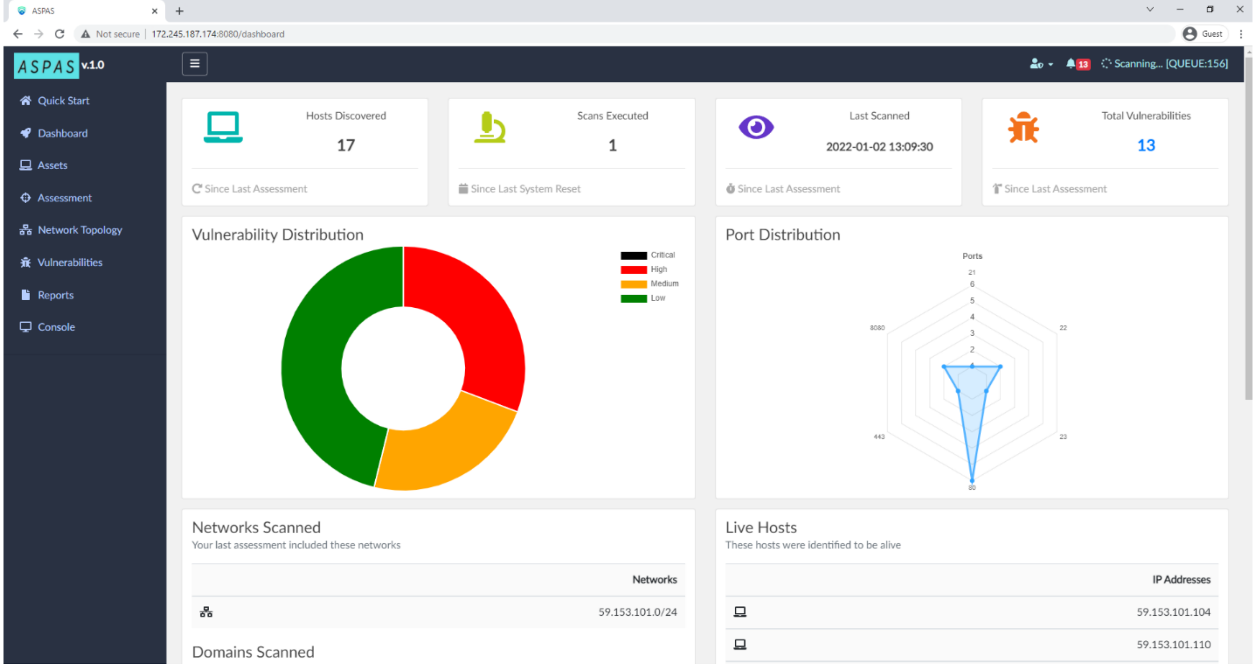
All you need to do is define the network and click GO.

CIDR Network: 192.168.0.0/24 GO!

What is CIDR?

6*Fig: 4.2.2: Quick Start*

Fig: 4.2.2: Quick Start



Hosts Discovered 17 — Since Last Assessment

Scans Executed 1 — Since Last System Reset

Last Scanned 2022-01-02 13:09:30 — Since Last Assessment

Total Vulnerabilities 13 — Since Last Assessment

Vulnerability Distribution

Port Distribution

Networks Scanned

Your last assessment included these networks

Networks
59.153.101.0/24

Live Hosts

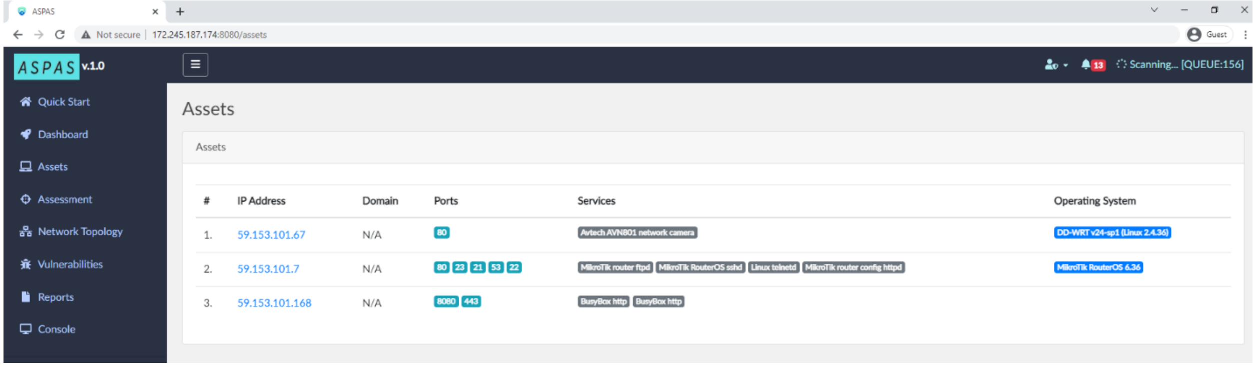
These hosts were identified to be alive

IP Addresses
59.153.101.104
59.153.101.110

Domains Scanned

7Fig: 4.2.3: Dashboard with Scan Result Details

Fig: 4.2.3: Dashboard with Scan Result Details

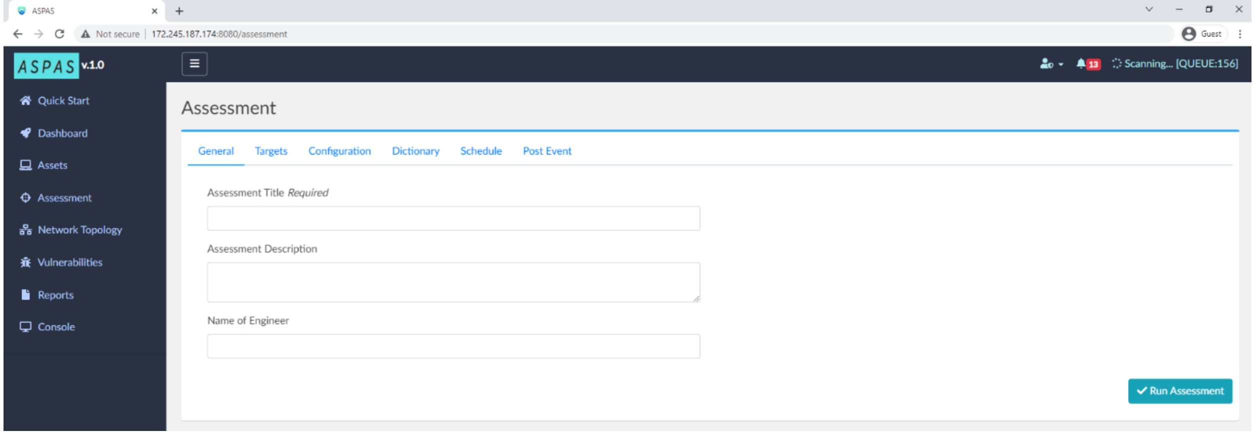


Assets

Assets

#	IP Address	Domain	Ports	Services	Operating System
1.	59.153.101.67	N/A	80	Avtech AVN801 network camera	DD-WRT v24-sp1 (Linux 2.4.36)
2.	59.153.101.7	N/A	80 23 21 53 22	MikroTik router ftpd MikroTik RouterOS sshd Linux telnetd MikroTik router config httpd	MikroTik RouterOS 6.36
3.	59.153.101.168	N/A	8080 443	BusyBox http BusyBox http	

Fig 4.2.4: Assets with Vulnerable IP and Device OS Info



Assessment

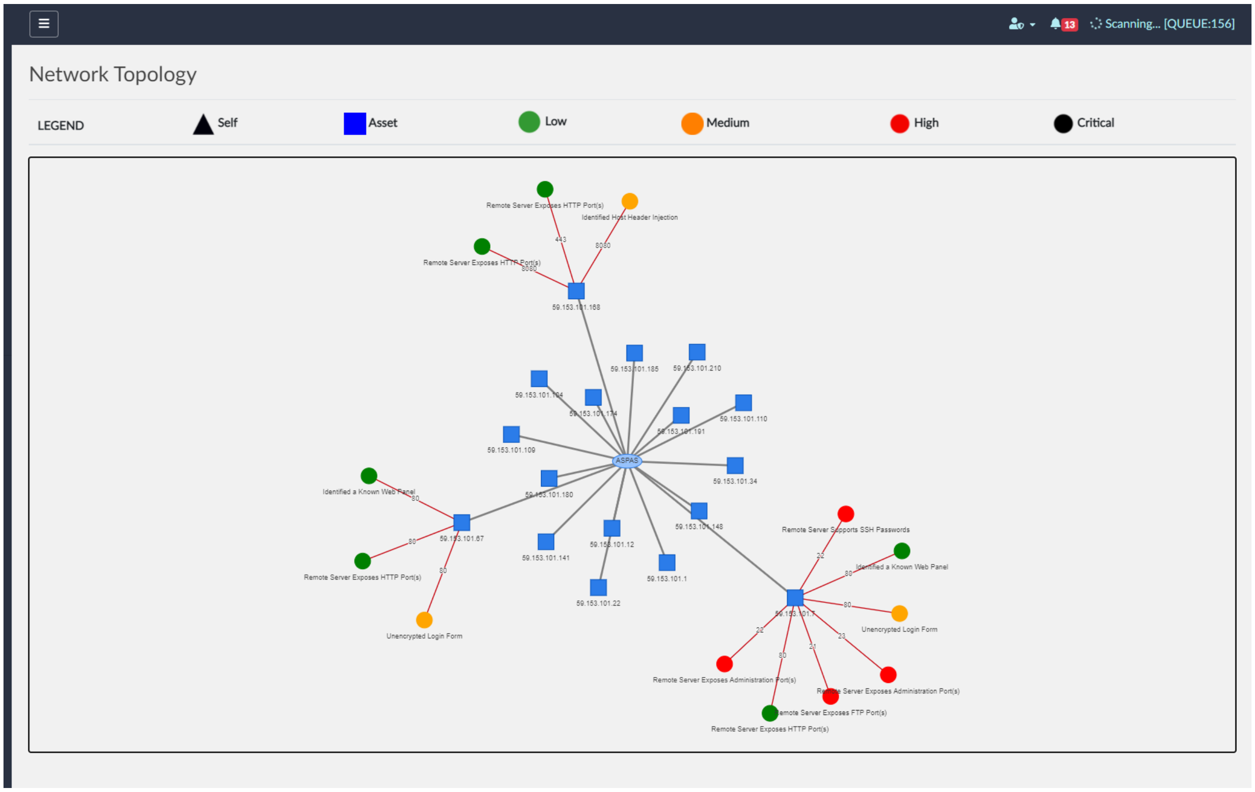
Assessment Title *Required*

Assessment Description

Name of Engineer

8Fig 4.2.5: Assessment

Fig 4.2.5: Assessment


13
Scanning... [QUEUE:156]

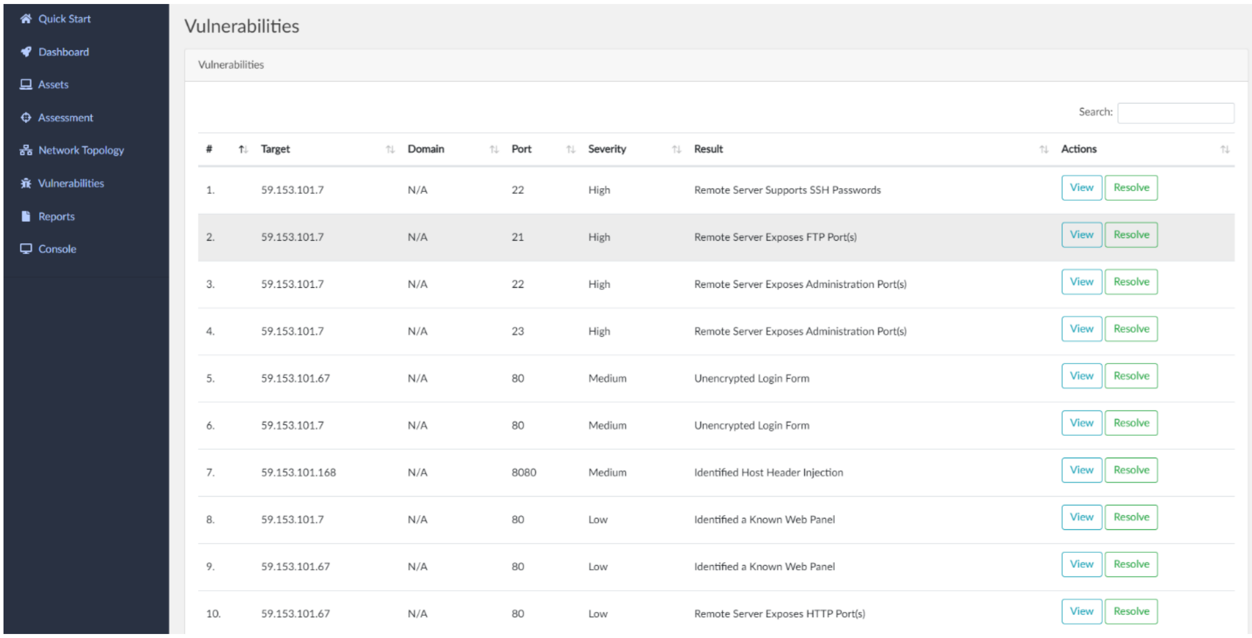
Network Topology

LEGEND ▲ Self ■ Asset ● Low ● Medium ● High ● Critical

Remote Server Exposes HTTP Port(s)
Identified Host Header Injection
443
8080
Remote Server Exposes HTTP Port(s)
8080
59.153.101.168
59.153.101.185
59.153.101.210
59.153.101.104
59.153.101.174
59.153.101.191
59.153.101.110
59.153.101.109
ASPAS
59.153.101.34
Identified a Known Web Panel
80
59.153.101.180
59.153.101.148
59.153.101.67
80
Remote Server Exposes HTTP Port(s)
80
59.153.101.141
59.153.101.12
59.153.101.1
59.153.101.22
Unencrypted Login Form
Remote Server Supports SSH Passwords
22
Identified a Known Web Panel
80
59.153.101.7
80
Unencrypted Login Form
22
23
80
21
Remote Server Exposes Administration Port(s)
Remote Server Exposes Administration Port(s)
Remote Server Exposes FTP Port(s)
Remote Server Exposes HTTP Port(s)

9Fig 4.2.6: Network Topology of targeted IP

Fig 4.2.6: Network Topology of targeted IP



#	Target	Domain	Port	Severity	Result	Actions
1.	59.153.101.7	N/A	22	High	Remote Server Supports SSH Passwords	View Resolve
2.	59.153.101.7	N/A	21	High	Remote Server Exposes FTP Port(s)	View Resolve
3.	59.153.101.7	N/A	22	High	Remote Server Exposes Administration Port(s)	View Resolve
4.	59.153.101.7	N/A	23	High	Remote Server Exposes Administration Port(s)	View Resolve
5.	59.153.101.67	N/A	80	Medium	Unencrypted Login Form	View Resolve
6.	59.153.101.7	N/A	80	Medium	Unencrypted Login Form	View Resolve
7.	59.153.101.168	N/A	8080	Medium	Identified Host Header Injection	View Resolve
8.	59.153.101.7	N/A	80	Low	Identified a Known Web Panel	View Resolve
9.	59.153.101.67	N/A	80	Low	Identified a Known Web Panel	View Resolve
10.	59.153.101.67	N/A	80	Low	Remote Server Exposes HTTP Port(s)	View Resolve

10Fig 4.2.7: Vulnerabilities

Fig 4.2.7: Vulnerabilities

4.2.1 Languages for the back end

Python: Python is a programming language that allows you to operate more quickly and efficiently with systems.

Radis as database: Redis is a NoSQL in-memory data structure store that can be persistently stored on disk. It can be used as a database, a cache, and more.

JavaScript: JavaScript is a programming language that may be used on both the front end and the back end.

Nmap: Nmap lets you scan your network for not only everything that's connected to it, but also a wealth of information about what's connected, what services each host is providing, and so on. It supports a variety of scanning protocols, including UDP, TCP connect (), OpenSSH, and FTP.

4.2.2 Frameworks for the back end

Python Flask Frameworks were utilized as the back-end software in the Automated Security Penetration & Assessment System for Web and Local Network.

4.3 Interaction Design and User Experience (UX)

Automated Web and Local Network Security Penetration & Assessment System can be installed on any operating system, and because our application is fully responsive, any Android or Chrome browser will have no trouble browsing it. We also welcome customer feedback in the dashboard.

Furthermore, once a consumer logs into the dashboard, we always provide a tour guide.

4.4 Implementation Requirements

Full Python-based Code So it can run any Cross-Device, anyone can Run it Linux Operating System or Windows System,

Automated Web and Local Network Security Penetration & Assessment System Full Compatible in Dockers and using Dockers any user can install it in any Dockers supported device. Minimal System Requirement is 1GB RAM 1 Core CPU and 1 Public IP address needs.

Chapter 5: Implementation and Testing

5.1 Implementation of Database

When a Security Engineer logs in to the dashboard, there is a QuickStart button that launches an IP scan. The IP vulnerability results are saved in a database, which can subsequently be used to generate a report. Assessment Options will display all vulnerable ports. In this process we use Redis database to make this process fast, even this database does not store any data in server it stores in ram then send full report to Security Engineer.

5.2 Implementation of Front-end Design

Automated Web and Local Network Security Penetration & Assessment System Front-end Design We use HTML Bootstrap CSS JavaScript. Login Page Available Only for That Origination Who have Install this Application in there Server so this Application need 1 Public IP To Reach that From anywhere in Internet. In Login Page Automated Web and Local Network Security Penetration & Assessment System Will ask A User to Put Username & Password. Other hand This Login Request Handel by POST Method.

5.3 Testing Implementation

5.3.1 Prerequisites

In the case that you opt for the Server setup (CentOS 7.x and Ubuntu 18.x were tested), ASPAS will install all prerequisites for you automatically (using the install/setup.sh script). For your convenience, it also includes a Dockerfile.

Keep in mind that the initial configuration of ASPAS on bare metal necessitates root access (package installation, etc).

Services and Packages required for ASPAS to run:

Web Server

Redis server

Nmap package

Inbound access on HTTP/S port

5.3.2 Deployment Recommendation

The ideal approach to use it is to run it against your infrastructure from many locations (for example, multiple instances of ASPAS in different countries) and select continuous mode to catch short-lived vulnerabilities in dynamic environments/cloud.

To thoroughly evaluate your infrastructure from an attacker's perspective, we normally recommend not whitelisting the IP addresses where ASPAS will be launching the scans.

To make ASPAS lightweight, there's no use of a database other than Redis.

We recommend using the Web hook functionality if you want to save your vulnerabilities for a long time. ASPAS will send a JSON payload to an endpoint of your choice at the end of each scan cycle, which you can then store in a database for future testing.

Setup ASPAS on 1 or more servers.

Make a script to retrieve your Cloud services (such as AWS, Azur Cloud.) If you have assets in a Datacenter, you might want to keep a static list of IP addresses.

Schedule a scan using the assets you acquired in step #2 by calling the ASPAS API (POST /api/scan/submit).

5.3.3 Deployment using Docker

Clone the repository

```
git clone https://github.com/Sajibekanti/ASPAS/aspas.git && cd aspas
```

Build the Docker image

```
docker build -t aspas .
```

Create a container from the image

```
docker run -e username="YourUsername" -e password="YourPassword" -d -p 80:8080 aspas
```

Now, launch Chrome or the other web browser of your choosing. After that, enter your IP address: 127.0.0.1 in the Admin Information field.

5.3.4 Deployment in VPS / Server

Navigate to /opt

```
cd /opt/
```

Clone the repository

```
git clone https://github.com/Sajibekanti/ASPAS/aspas.git && cd aspas
```

Run Installer (requires root)

```
bash install/setup.sh
```

Check ASPAS is running

```
systemctl status aspas
```

Now, launch Chrome or the other web browser of your choosing. After that, enter your IP address: 127.0.0.1:8080 in the Admin Information field.

5.3.5 Multi Node Installation

If you want to install ASPAS in a multi-Server deployment, you can follow installation process:

Change the config.py file on each Server

Change the server address of Redis RDS-HOST to point to a central Redis server that all ASPAS instances will report to.

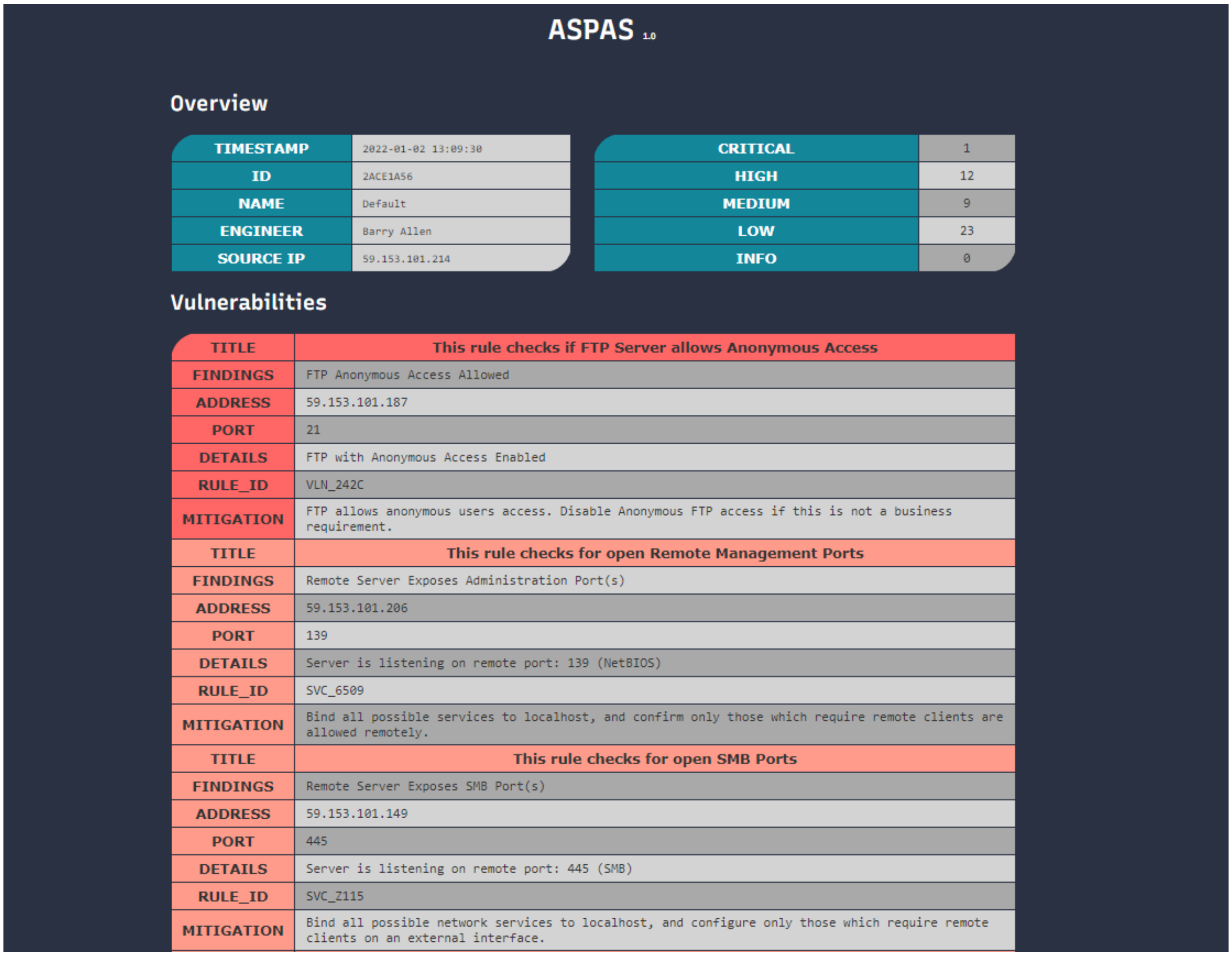
Run service aspas restart or systemctl restart aspas to reload the configuration Settings

Run apt-get remove redis / yum remove redis because each instance will no longer need to report to itself Make sure that the Redis instance allows port 3769 inbound traffic so that the ASPAS instances can connect with it.

5.4 Test Results and Reports

We use three types of reports in our test results and reports: HTML, CSV, and TXT files, so that any user may understand them. Have that type of format in the report section.

View the Report You can obtain an overview of the target, the vulnerability, the severity of the vulnerability, the source IP, the engineer's name, the project's name, the time, and the data.



ASPAS 1.0

Overview

TIMESTAMP	2022-01-02 13:09:30
ID	2ACE1A56
NAME	Default
ENGINEER	Barry Allen
SOURCE IP	59.153.101.214

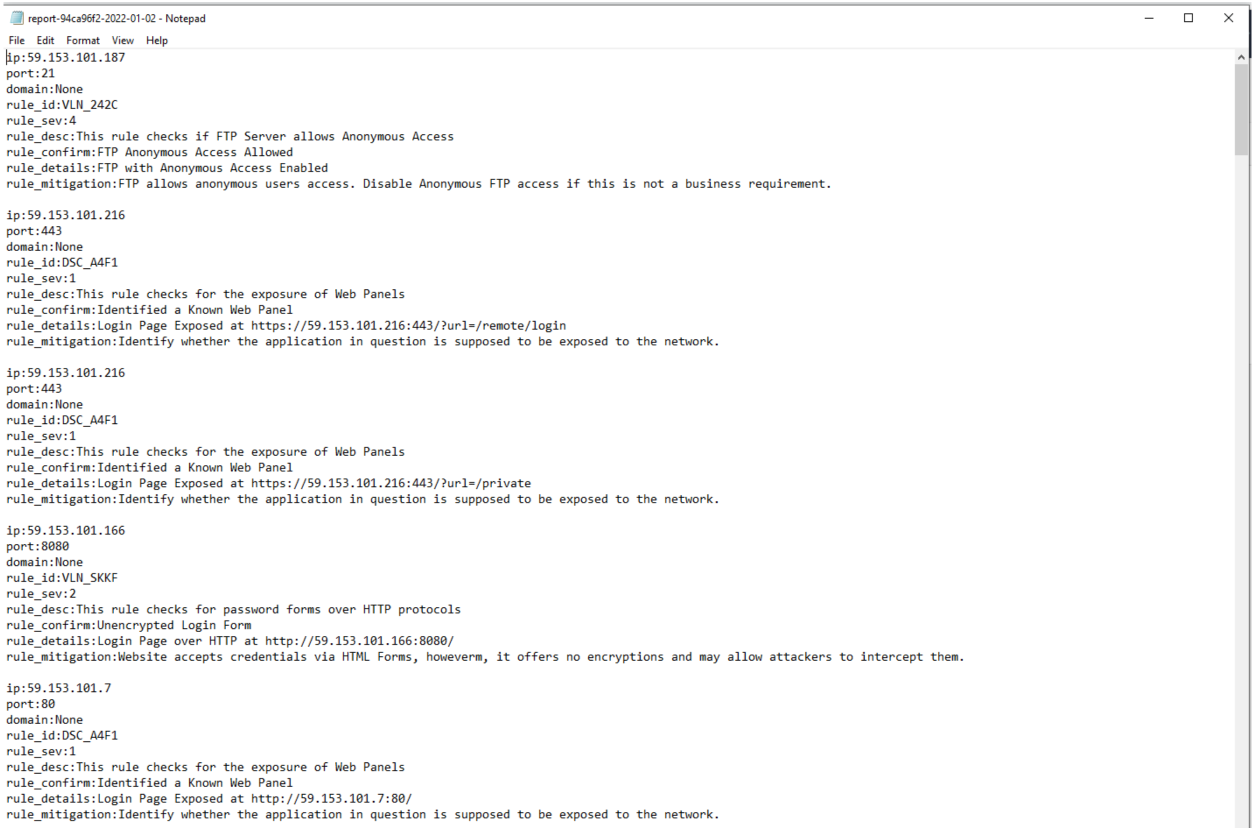
CRITICAL	1
HIGH	12
MEDIUM	9
LOW	23
INFO	0

Vulnerabilities

TITLE	This rule checks if FTP Server allows Anonymous Access
FINDINGS	FTP Anonymous Access Allowed
ADDRESS	59.153.101.187
PORT	21
DETAILS	FTP with Anonymous Access Enabled
RULE_ID	VLN_242C
MITIGATION	FTP allows anonymous users access. Disable Anonymous FTP access if this is not a business requirement.
TITLE	This rule checks for open Remote Management Ports
FINDINGS	Remote Server Exposes Administration Port(s)
ADDRESS	59.153.101.206
PORT	139
DETAILS	Server is listening on remote port: 139 (NetBIOS)
RULE_ID	SVC_6509
MITIGATION	Bind all possible services to localhost, and confirm only those which require remote clients are allowed remotely.
TITLE	This rule checks for open SMB Ports
FINDINGS	Remote Server Exposes SMB Port(s)
ADDRESS	59.153.101.149
PORT	445
DETAILS	Server is listening on remote port: 445 (SMB)
RULE_ID	SVC_Z115
MITIGATION	Bind all possible network services to localhost, and configure only those which require remote clients on an external interface.

11*Fig 5.4: Scan Report in html format*

Fig 5.4: Scan Report in html format



report-94ca96f2-2022-01-02 - Notepad
File Edit Format View Help

```
ip:59.153.101.187
port:21
domain:None
rule_id:VLN_242C
rule_sev:4
rule_desc:This rule checks if FTP Server allows Anonymous Access
rule_confirm:FTP Anonymous Access Allowed
rule_details:FTP with Anonymous Access Enabled
rule_mitigation:FTP allows anonymous users access. Disable Anonymous FTP access if this is not a business requirement.

ip:59.153.101.216
port:443
domain:None
rule_id:DSC_A4F1
rule_sev:1
rule_desc:This rule checks for the exposure of Web Panels
rule_confirm:Identified a Known Web Panel
rule_details:Login Page Exposed at https://59.153.101.216:443/?url=/remote/login
rule_mitigation:Identify whether the application in question is supposed to be exposed to the network.

ip:59.153.101.216
port:443
domain:None
rule_id:DSC_A4F1
rule_sev:1
rule_desc:This rule checks for the exposure of Web Panels
rule_confirm:Identified a Known Web Panel
rule_details:Login Page Exposed at https://59.153.101.216:443/?url=/private
rule_mitigation:Identify whether the application in question is supposed to be exposed to the network.

ip:59.153.101.166
port:8080
domain:None
rule_id:VLN_SKKF
rule_sev:2
rule_desc:This rule checks for password forms over HTTP protocols
rule_confirm:Unencrypted Login Form
rule_details:Login Page over HTTP at http://59.153.101.166:8080/
rule_mitigation:Website accepts credentials via HTML Forms, howeverm, it offers no encryptions and may allow attackers to intercept them.

ip:59.153.101.7
port:80
domain:None
rule_id:DSC_A4F1
rule_sev:1
rule_desc:This rule checks for the exposure of Web Panels
rule_confirm:Identified a Known Web Panel
rule_details:Login Page Exposed at http://59.153.101.7:80/
rule_mitigation:Identify whether the application in question is supposed to be exposed to the network.
```

12*Fig 5.4.1: Scan result in raw*

Fig 5.4.1: Scan result in raw

Chapter 6: Impact on Society, Environment and Sustainability

6.1 Impact on Society

Every day, the world of cyber security evolves, and cybercriminals try to take advantage of it in order to obtain as much money and influence as possible. As the Internet expands, more individuals join it from all over the world. The goal is to determine how important cyber security is and how cyber-criminals might use the cyber world for their own personal gain.

Automated Security Penetration & Assessment System for Web and Local Network Will Protected Organization from Cyber Attack, This Application will Scan Organization All Local Device that is connected on Internet, every network Infrastructure has many devices that have an open port, many times those available port are vulnerable for cyber-attack this application help to identify those port and make fix notification. As a result, we can say these Security tools impact our society as a whole.

6.2 Impact on Environment

The Security Application we developed has no significant environmental impact. This application will not change the environment, will not contaminate the ecosystem, and will not improve ecological awareness in any way. In other words, there isn't a single feature in this Application that is related to the environment. As a result, we can conclude that it has no environmental impact.

6.3 Ethical Aspects

While developing this application, I had to consider ethical considerations and ensure that there were no security flaws or loopholes. Still, if any Security Issue Found, any User can Report it through GitHub project Issue Page. I tried my best not to follow any unethical patterns that may mislead users into providing personal information. I've also made sure that the application does not have access to the user's Server root access, PC Access, Storage Access, Network Access, or any storage files and that it doesn't ask for permission to do so. I attempted to keep the application as simple as possible so that it doesn't deceive the user into dealing with any sensitive or vulnerable topic by clicking any Application button. I took the most modern security and privacy precautions possible to ensure that data is stored in an end-to-end encrypted way, thus ensuring no chance of data loss possible through this application. So, the application remains user-friendly and easy to use with excellent security.

6.4 Sustainability Plan

When developing the application, I needed to ensure that it was long-lasting. So I attempted to make it future proof so that it might continue to deliver services in the near future while still retaining the ability to produce good results throughout time. As. Cyber-attacks are happening all the time in our world, and Security Engineers are constantly striving to deliver the appropriate justice to this world, so there is always a need for an application like this. It's not even like this is a one-time occurrence in which the need for this application fades in an instant. We will keep fighting for our Secure Cyber World, and this application will continue to serve the Organization in the future.

Chapter 7: Conclusion and Future Scope

7.1 Discussion and Conclusions

We all like to live a life that is simple is simple, uncomplicated, and pleasant. Life is more convenient in the Internet age. With a single finger click, we can access all information. Typically, we use the internet to see how the entire system is performing and what updates are available. We are quite excited to undertake this if we find any system to be comfortable. Communication has become easier as a result of our increased connectivity. We have made a discussion page in GitHub so that any user can leave a comment about our project and fix any code using GitHub pull requests.

7.2 Future work and Further Development

We intend to expand the functionality of this application. This system has a lot of room for improvement in the future to make it more user-friendly. We will include the Zero Days Exploit, which will allow us to automatically exploit any system. This application is currently only capable of scanning web domains and network ports.

Obviously, we need to add more dependable, appealing features to our user interface. In the future

Many features can be developed to make this Security tools more successful and user friendly for people:

- Zero Days Exploit
- Shodan Integration
- VirusTotal Integration
- OWSAP TOP 10 Vulnerability Scan
- SSRF Testing
- Blind XSS Testing

REFERENCES

[1]. Cyber security Important, available at << https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php>>, [last Accessed on August 25, 2021]

[2]. Rapid7, available at << https://www.rapid7.com/blog/post/2020/06/26/rapid7-managed-detection-and-response-mdr-the-service-that-never-sleeps/>>, [last Accessed on November 26, 2021]

[3]. Tenable, available at << https://www.tenable.com/products/nessus/nessus-professional>>, [last Accessed on November 26, 2021]

[4]. AT&T, available at << https://cybersecurity.att.com/>>, [last Accessed on November 26, 2021]

[5]. The Basics of Hypertext Markup Language HTML, available at <<https://capowebdesign.com/>>, [last Accessed on December 30, 2021]

[6]. Front-End vs Back-End Development, available at << https://msbcgroup.com/>>, [last Accessed on December 30, 2021]

[7]. Front-End Web Developer, available at << https://queued.at/>>, [last Accessed on December 30, 2021]

[8]. Items API Article, available at << https://softwarearchitech.wordpress.com/>>, [last Accessed on December 30, 2021]

Automated Security Penetration & Assessment System for Web and Local Network

ORIGINALITY REPORT

3 %	25%	1%	23%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	**Submitted to Daffodil International University** Student Paper	9%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	6%
3	hackersonlineclub.com Internet Source	4%
4	Submitted to Wawasan Open University Student Paper	3%
5	Submitted to Kensington College of Business - Brunei Student Paper	3
6	one.comodo.com Internet Source	1%
	Submitted to Bahrain Training Institute	1

7	Student Paper	%
8	Submitted to The University of the South Pacific Student Paper	1

9 Submitted to University of Dubai

Student Paper

10 resources.infosecinstitute.com

Internet Source

11 Submitted to Sir George Monoux College

Student Paper

12 Submitted to Birmingham City University International College

Student Paper

13 Submitted to CSU, San Jose State University

Student Paper

14 dspace.library.daffodilvarsity.edu.bd:8080

Internet Source

15 github.com

Internet Source