SHELL SHARE

A PROJECT REPORT

Submitted by

LUCKY PATHAN S.
VASU RAKHOLIYA D.
SWET PATEL R.

In Partial fulfillment for the award of
the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

Under the Guidance of

SHERYA DHOLARIA

Department of Computer Science & Engineering
Parul University, Vadodara

February, 2023

PARUL UNIVERSITY

CERTIFICATE

This is to Certify that Project - 1-Subject code 203105328 of 6th Semester entitled "**Shell Share** " of Group No. PIET_CSE_2 has been successfully completed by

LUCKY PATHAN S. – 210303105790
VASU RAKHOLIYA D. – 210303105794
SWET PATEL R. – 210303105787

under my guidance in partial fulfillment of the Bachelor of Technology (B.TECH) in Computer Science and Engineering of Parul University in Academic Year 2022-2023.

Project Guide
Shreya Dholaria

Project Coordinator

Prof. Yatin Shukla

Head of Department,
CSE
Dr. Amit Barve

External Examiner

II

ACKNOWLEDGEMENT

We would like to express our profound gratitude to Dr. **Amit Barve** (HOD) , of CSE department, and Dr. **Vipul Vekariya** (Dean) of PIET (Parul Institute of Engineering and Technology) for their contributions to the completion of my project title **SHELL SHARE**.

We would like to express our special thanks to our mentor Asst. Prof. **Shreya Dholaria** for her time and efforts she provided throughout the year. Your useful advice and suggestions were really helpful to us during the project's completion. In this aspect, We are eternally grateful to you.

Place: Vadodara

Date:

Lucky Pathan S. (210303105790)

Swet Patel R. (210303105787)

Vasu Raknoliya D. (210303105794)

ABSTRACT

As we all know the current cyber security crimes are increasing day by day. We need to create a faster way to test the system to secure them. Our tool SHELL SHARE will help company's cyber security team to coordinate in a better way. This tool help's a team to connect in a single network in which they can share their progress, any bug's, file's, and a log of every step of each user. If any member is successful to break into the system , He can share the details to other group members. As a successful break into a system, the log files can be retrieving for better documentation of the bug. We cannot rely on automation tools like NESSUS, so to ease the manual testing SHELL SHARE can be deployed. It's a python-based tool which can work on Linux system with some dependency's, we create the first user as an server host and use this device IP address and PORT with a random password to let other member's connect together . User can connect to the server will a command specifying 2 parameters (IP:PORT & Password) as user connect , the host will get a notification on the users IP and he can allow/denied the connection request.

Keywords: Server Creation ,Log File Generation , LAN networks, Manual Testing of Network

Contents

CHAPTER 1
Introduction

Our project is regarding a cyber security, as manual testing in company is very time consuming and all the work-load is derived to a employees. Our tool SHELL SHARE will help the user to group up as in a network and try to find the bugs, as a user find bug it gets register in the logs and other members in the network also get updated on the bug found.

1.1 Problem statement

As we know how manual testing of the network can be a big work-load on the cyber security team. So we need something that can give a proper management of the bugs found and the employees working on the current bug. As a employee finds bug its hard to backtrack the steps and the necessary data for the report found on the bug. As an group of team works on bug finding, its easy to get overlap on a same network part. As this make both of their time wasted. As we need to connect with the team to get them know about the new discovered bugs.

1.2 Scope

All the company's need a cyber security team to secure their digital assets and from a strong and secure website. So our tool will help the team to communicate batter and automatic form the logs file need to gather necessary information to generate the bug report.

1.3 Aim and Objectives

Aim of out project is create a python tool which can help cyber security teams to clear a network with less hassle and form a super easy to communicate with other group members. First we need to create a manual command line code for the special commands that we will implement in this project for ease of report generation and bug found list.

CHAPTER 2
Literature Review

In this chapter, we have given our critical evaluation & summary of all research papers that we read related to our project. After reading many reference papers we studied the latest existing model and found some flaunt. All those details are given below.

2.2 Research Paper Evaluation Table

Sr. No	Author	Title	Dataset	Method	Result	Future Work
01	Nwauba Nnaemeka Kennedy	Design And Implementation Of Network Security	Bank Network Packet	Basic encryption network with host identification	Ensure bank Network & Security	Add higher encryption
02	Lokesh Rao	Active Network Monitor/Net Tracer	Network error rate	Network monitoring tool	Clear bottlenecks in the existing networks	Enhance Network scanning
03	Pietro Grandinetti	Server deployment with Python	-	operations to get the server a manual config	Create server with host data management	Make a custom server for request and response
04	Tshepang Lekhonkhobe	Argparse Tutorial Python	Python Library	command-line options, arguments and sub-commands.	Understanding the components of the Argparse	-

05	Nathan Jennings	Socket Programming in Python (Guide)	-	Socket Programming	Create server with custom request perimeters.	-
06	Adeyinka, Victor, Adebiyi, Winifred, Olaitan	Packet sniffer for user end network performance monitoring using python	-	Promiscuous mode, TCP/IP header	Dada is being transmitted in form of packets with several no of failure.	Add encryption on files transfer
07	Yaser Mowlaiwzadah	Analyzing and simplifying log files using python	-	FN Log Analysis tool, YM log Analyzer tool ,GUI tool	Program successfully picking log files and these files daily stored in system .	Build database to store the log file
08	Asswini Swain, Het Sheth, Pratik kanani	Remote method invocation using python	PYRO Library(Library use in Python)	RMI model, RPC tool	Complete end to end RMI system, Successfully implemented RMI in python	Cross network connection
09	V.Neethidevan, G.Chandrasekaran	Web Automation with Python	Selenium Library	Selenium web driver, Web automation	GUI testing for web based application, cross browsers testing in different browsers	window components handling
10	Aditi Shrivastava, Nitin Shukla	Extracting Knowledge from user access logs	-	Server log files, web usage mining tool	Program successfully tracking logs files of user,	

					extract information of users with date and time	-
11	Hataw Jalal Mohammed, Kamaran Faraj	A Python-WSGI and PHP-Apache Web Server Performance Analysis by Search Page Generator	Search Page Database	Python, Server Analysis	New modifications have occurred in web servers	Improving response time
12	Xia Qing	Network Security Management Platform System Design and Implementation	-	Data encryption, Access control, Data backup, Anti-virus	To ensure data and system security in open network environment	Event collection data set improvements
13	Liu Zhijun	Computer network security virtual experiment system design and implementation	SQL database, system design plans	VPN, IDS	Construct platform for network attack and defense	Create more robust system design
14	HUANG Zhikun	The Design and Implementation of Security Network System Based on Web	Database server, Web server	ADO.Net	from the network between the transport layer and application layer, designed a network security	Create a VLAN for large deployment

15	Dabin Sun, Bowei Wang	Research on the Design of the Implementation Plan of Network Security Level Protection of Information Security	Network Traffic Logs	scheme design, Python,	the correct security protection level protection design, and improve the security awareness and management level	Coordination and cooperation between departments and relevant personnel at all levels to promote the construction

Table 2.1 Research Summery Table

2.2 Critical Evaluation of Journal paper

Paper 1 : Design And Implementation Of Network Security

Student Name :	Lucky Pathan S.		
Enrollment No	210303105790	Branch :	CSE
Title of Journal Paper	Design And Implementation Of Network Security		
Authors	Nwauba Nnaemeka Kennedy		
Journal / Conference :	Department Of Computer Science And Information Technology, Caritas University		
Volume / Issue	1	Pages :	48

Purpose of the research paper is to improve the security that flexible communication infrastructures which provide a diverse set of operations. Understanding the network data flow to manage data packages. Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources, logical resources, or digital resources. In this document authors mention bank low level network security and plans to improve it by adding encryption and access control for user verification. Bank has no security from attacks like eavesdropping, loops, and

traffic amplification. To overcome from this problem we uses challenge-responses and erasure-coding, for minimum security of the bank network.

In this project , Administration is an aspect of running the organization by devising systems which will run smoothly. The goal of authentication is to first verify that the user, either a person or system, which is attempting to interact with your system is allowed to do so. Gathering basic host information, such as its location and security aspects of its connection, is critical. After all process done, inputs are stripped off with headers and all output is the information which is inside the headers and outputs are in human readable form. Several strategies are implemented like User id and Password , Physical security device, Biometric Identification and more. Based on research we use the network creation and network monitoring data to get multiple hosts with their ID's and User Profiles.

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems. Identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in. Authorization determines what a subject can do. Accountability identifies what a subject (or all subjects associated with a user) did. Based on this research paper , authors described Network Security is essential part of organization.

Critical Analysis:

It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. The main purpose of this project is to design a NETWORK SECURITY that will assist bank in the area of ensuring effective security measures. A security context is the collection of roles that a user is associated with. The security context is often defined as part of the authentication process. Depending on the technology used a security context is maintained by the system. Credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor .Credentials can be passed around, thus subverting the access control list

Paper 2 : Active Network Monitor/Net Tracer

Student Name :	Lucky Pathan S.		
Enrollment No	210303105790	Branch :	CSE
Title of Journal Paper	Active Network Monitor/Net Tracer		
Authors	Lokesh Rao		
Journal / Conference :	BSC-IT Project – Demonstration		
Volume / Issue	1	Pages :	3

Purpose of the research paper is to monitoring the router on the network monitoring tool to help the Network Administrator to find the bottlenecks in the existing networks. Helps to measure the error rate in the communication if present and inform the Administrator. The monitoring of the network implies gathering basic features and characteristics of network such as number of interfaces which are connected to the network. Incoming and outgoing bytes of data, bandwidth, CPU utilization, memory utilization, system uptime etc. It helps us to measure the error rate in the communication if present and inform the Administrator.

In this project, monitor the routers on the network monitoring tool is run. Gathering basic network information, such as its users and number of interfaces. After all process done, most used interface can be given more data bandwidth to adjust the data requirement of them. Based on research we use the network monitoring tool to generate the logs for users and help take note of each users steps with all the possible outcomes they may have encounter.

Critical Analysis:

The aim of project is to help the Network Administrator to find the bottlenecks in the existing networks. The monitoring of the network implies gathering basic features and characteristics of network such as number of interfaces which are connected to the network, incoming and outgoing bytes of data, bandwidth, CPU utilization, memory utilization, system uptime etc. It helps us to measure the error rate in the communication if present and inform the Administrator. Based on this research paper , authors described Network to be analyzer with

a network monitoring tool to get the assumption of the network bottleneck. Tools collet the basic features and characteristics of network such as number of interfaces, incoming and outgoing bytes of data, bandwidth, CPU utilization, memory utilization, system uptime etc. As we can use this tool we can get user notation and trace user data , and also create log files of user.

Paper 3 : Server deployment with Python

Student Name :	Lucky Pathan S.		
Enrollment No	210303105790	Branch :	CSE
Title of Journal Paper	Server deployment with Python		
Authors	Pietro Grandinetti		
Journal / Conference :	Data Science & Optimization		
Volume / Issue	1	Pages :	24

Purpose of the research paper is to illustrate how to configure a server to run a web application with no other tool than Python. Learned what are the components of a server's configuration for web deployment. Got a reproducible Python template, via GitHub gist's. A manual deployment in a vanilla server is a must-do for a developer. At least once in your lifetime, spin up a vanilla machine in any cloud provider do a full-fledged production deployment. It will give you a pretty good understanding of what is happening in the remote machine! Knowledge always matters.

In this project, author divides the steps in 3 part . Step 1 - Basic machine configuration. Step 2 - Install your application. Step 3 - Run the app!. Based on research we use the components of a server's configuration for our server deployment of hosts connection. We can create a server with all the basic operations to get the server a manual config. with preferred request/response results and also track each user steps and data on network for log generation.

Critical Analysis:

As author gets the setup explain he cut it to 3 steps with each step showing all the as a brief. After we make a detail view to modify the requests and manipulate the hosts throughput with

all the data flow management. Create a server with a basic templet of Flask web deployment, with python deployment and manage it with only python library.

Paper 4 : Argparse Tutorial Python

Student Name :	Lucky Pathan S.		
Enrollment No	210303105790	Branch :	CSE
Title of Journal Paper	Argparse Tutorial Python		
Authors	Tshepang Lekhonkhobe		
Journal / Conference :	Python Library		
Volume / Issue	3.2	Pages :	17

Purpose of the research paper is parser for command-line options, arguments and sub-commands. Understanding of the argparse package. Learning of Positional arguments, Optional arguments, Short options, Combining Positional and Optional arguments and more combination of the all. This tutorial is intended to be a gentle introduction to argparse, the recommended command-line parsing module in the Python standard library. There are two other modules that fulfill the same task, namely getopt (an equivalent for getopt() from the C language) and the deprecated optparse. Note also that argparse is based on optparse, and therefore very similar in terms of usage.

In this report, author teaches us the basic feature of the package Argparse. He shows how powerful this tool is to get the host command inputs with precise variable matching and the use it to run a simple terminal command with all the user defined perimeters . As this package gives a link data structure to the commands input into the terminal will be used as an log file creation also. Based on research we use the components of the Argparse to get the custom command lines for the easier host privileges.

Critical Analysis:

Explanation of a python package Argparse, with its super handy features and all basic operation it can perform with relative ease to get the programmer a smooth code for the custom command and parameter creation. The argparse module offers a lot more than shown in this document. Its docs are quite detailed and thorough, and full of examples. Having gone

through this tutorial, you should easily digest them without feeling overwhelmed. We get to learn about the python package Argparse with all the fundamental options it provide, Introducing Positional arguments, Introducing Optional arguments, Short options, Combining Positional and Optional arguments, Getting a little more advanced(instead uses verbosity level to display more text instead), Conflicting options.

Paper 5 : Socket Programming in Python (Guide)

Student Name :	Lucky Pathan S.		
Enrollment No	210303105790	Branch :	CSE
Title of Journal Paper	Socket Programming in Python (Guide)		
Authors	Nathan Jennings		
Journal / Conference :	Python Guide / web-dev		
Volume / Issue	1	Pages :	68

Purpose of the research paper is to make a, A simple socket server and client. An improved version that handles multiple connections simultaneously. A server-client application that functions like a full-fledged socket application, complete with its own custom header and content. Looked at the low-level socket API in Python's socket module and saw how it can be used to create client-server applications. Built a client and server that can handle multiple connections using a selectors object. Created your own custom class and used it as an application-layer protocol to exchange messages and data between endpoints.

The primary socket API functions and methods. To create a socket object using socket.socket(), specifying the socket type as socket.SOCK_STREAM. The default protocol that's used is the Transmission Control Protocol (TCP). This is a good default and probably what you want for its Is reliable and Has in-order data delivery. When using the loopback interface (IPv4 address 127.0.0.1 or IPv6 address ::1), data never leaves the host or touches the external network. In the diagram above, the loopback interface is contained inside the host. This represents the internal nature of the loopback interface and shows that connections and data that transit it are local to the host. This is why you'll also hear the loopback interface and IP address 127.0.0.1 or ::1 referred to as "localhost."

Critical Analysis:

In this report, author teaches us the Python interface is a straightforward transliteration of the Unix system call and library interface for sockets to Python's object-oriented style: the socket() function returns a socket object whose methods implement the various socket system calls. Parameter types are somewhat higher-level than in the C interface: as with read() and write() operations on Python files, buffer allocation on receive operations is automatic, and buffer length is implicit on send operations. Based on research we use the Multi-Connection Client and Server feature of the socket API, which will help us to connect the users in a LAN network. Here we have covered a lot of ground in this tutorial! Networking and sockets are large subjects. New to networking or sockets. There are a lot of pieces to become familiar with in order to understand how everything works together. However, just like Python, it start to make more sense as you get to know the individual pieces and spend more time with them.

Paper 6 : Packet Sniffer for Users End Network Performance Monitoring using Python Programming

Student Name :	Rakholiya Vasu D.		
Enrollment No	210303105794	Branch :	CSE
Title of Journal Paper	Packet Sniffer for Users End Network Performance Monitoring using Python Programming		
Authors	Adeyinka A. Adewale, Victor O. Matthews, Adebiyi A. Adelakun, Winifred Amase,Olaitan Alashir		
Journal / Conference :	International Journal of Current Trends in Engineering & Research (IJCTE)		
Volume / Issue	4	Pages :	11

Purpose of the research paper is to monitoring of data and information which is transmitted over network due to increase malicious attacks and continuously grows and complexity on network. Main results of these research papers is to understand implementation of packet sniffer using python programming language and monitor performance over the local campus computer network .based on that we can identify error rate and how many packets loss on

network. in this document authors mention about different packet size perform different role on network and it creates problem . example: if packets sixes is short than it will load on device, if packet size is high than it will load on network. Second drawback is packet response time, due to buffer packet did not arrive at NIC and it can't save so there is chances to packet loss. Many time administrators in order to increase performance they will replace servers with high end servers and increase bandwidth ,but this plan is only short-term planning.

In this project , first all raw packets are obtained from networks and store in buffer. After that buffer will be strips off with various headers of packet into TCP/IP header. After packets arrived all packets are analyzed first and their output will be update with latest information which is come from later process. After all process done, inputs are stripped off with headers and all output is the information which is inside the headers and outputs are in human readable form. Based on research we use promiscuous mode using that node we can track packets from internet using MAC address. And we use buffer to stored raw packets from network. In the results each packets sender and receiver address, port numbers ,headers are broken and all are converted in human readable form. the data is being transmitted ,one or more packets are failed to reach their destination.

Critical Analysis:

Based on author conclusion, packets sniffer software has been developed using python and implemented in windows OS ,since previous packet software developed using python and implemented in Linux OS. In windows packets sniffer precisely captures data and converts it and display data into proper format that enables to reading traffic and minimize difficulty to navigating through previous one and the performance which carried out by packets loss ratio and TCP packets loss ratio. Based on this research paper , authors described due to rapidly growth in networks and increasing users. Network become very huge and complex .because of that malicious attacks chances are increase if we can't monitor traffic on network it may lead disaster too .The main aim of authors to continuously monitor packets which are transmitted from overall network . to monitor traffic on network they used promiscuous mode ,in this mode only those packets are transmitted on NIC which has own MAC address. Others all packets are discard. First they collect all raw packets from network and stored in buffer after that they stripped off all various types of headers into TCP/IP headers and start analysis ,after analyze output file with update with latest information and convert into human readable

format. based on implementation we can see that when we increase the total no of packets the chances of losing packets are decrease.

Paper 7 : Analyzing and Simplifying Log Files using Python

Student Name :	Rakholiya vasu D.		
Enrollment No	210303105794	Branch :	CSE
Title of Journal Paper	Analyzing and Simplifying Log Files using Python		
Authors	Yaser Mowlaiwzadah, Master Degree Student ,ECE Department, REVA university, Bangalore , India		
Journal / Conference :	International Journal of Engineering Research & Technology (IJERT)		
Volume / Issue	Vol.9/Issue 05	Pages :	4

Objective of research paper is to simplifying and analyzing log files ,by using YMlog and analyzer tool to prevent unauthorized access from third party users. This research more focus on server base logs like DNS(Domain Name Systems), FTP(File Transfer Protocol), DHCP(Dynamic Host Control Protocol), Authentication etc. In the results, this program has two versions: Script version, this version has no GUI. these version are use in server. Graphic version, this version are used for desktop user. using this tool administrator can easily find what happening in system and realize importance of log files in system security. In this document authors are mentioned, why log files are important for user. it carry sensitive and important data through internet. This log file are playing key role to find information about attackers and unauthorized access.

This program developed in Linux operating system it cannot be used by another operating system. this method contain two separate files: GUI file:this is main file for local system with graphical user interface access. Server-based file: this file contains the code for non-GUI environment and server environment where there is no access to GUI interfaces, this file also works same as the before file except that it is not having GUI interface. Based on this document ,we use two separate files one file for host user which is GUI file using that file network host can see and observe that logs. another file is non-GUI files that used for server side to track

logs.

In this document GUI(graphical user interface) contain two parts. which is local and server parts. in local parts logs are located on own local system it can be search and analyzed. Server part is used for future work, if anyone want to work and develop it user can easily change, preliminary login page is developed. Using GUI interface administrator can analyze the data. Server data are stored on server side so in future is user want to change or work on it user can easily do. Because of GUI user can easily perform operation on different ports like DHCP,FTP,DNS etc. Administrator user can easily find what happening in network and also realize importance of log file. Based on analysis from tool we can easily identify and receive information about logs ,on the local system we can get information about logs using DNS name and we can select month to find particular data. On the server side using particular user IP address, username and password administrator can search data.

Critical Analysis:

In this documentation authors mention why log files is important for any user log files are carries out sensitive data and travel on internet using log files administrator can identify if any attacks or unauthorized access perform on network. authors also mentioned various types of log tools which is made how they tools are work and what is drawbacks of that tools. This tools which made by authors can only work on Linux operating systems. this tool contain two parts local files is GUI files which will be used on client-side administrator use this file to monitor and analyze log files on network by using different ports. Server side used for identify other user logs which are on host network by using user IP, username, password .there is predesigned page which are used for future work.

Paper 8 : Remote Method Invocation Using Python

Student Name :	Rakholiya vasu D.		
Enrollment No	210303105794	Branch :	CSE
Title of Journal Paper	Remote Method Invocation Using Python		
Authors	Ashwini Swain , Het Sheth , Pratik Kanani		
Journal / Conference :	INTERNATIONAL JOURNAL OF ADVANCED STUDIES IN COMPUTER SCIENCE AND ENGINEERING,IJASCSE		

Volume / Issue	Vol.6/issue 11	Pages :	4

The objective of document is distributing computing which is widely used ,which help in efficient storage and transmission data over the network. using distributed computing we can transmitted data over high-speed data in short time. In this system one single system are connected with multiple computers with high-speed network, the main idea behind is to send and receive data in short amount of time and get better throughput compare to single processor system. In this research RPC(Remote Procedure Cell),RPC model is similar to LPC(Local Procedure Call) model .this both model used for transfer data and control it within program. In this document we use RPC, but its use structured programming approach which can be improved by using object-oriented models. using this approach objects which are in different procedures can communicate with each other through RMI. We implement RMI in python, advantage of using Python is readability and we can build with limited lines of codes.

In this research we implement RMI using socket programming, in this first user request are converted into objects and these objects are invoke methods all over network .but its required high-level programming ,reduce this effort we use PYRO library . PYRO automatically create objects and locate port and it can create efficient distributed system, so many people can connect. From this research we use RMI to connect objects with each other and use RPC to transfer and control data over the network. we also use PYRO library so we can easily implement and reduce code and we can easily implement distributed programming.

In this document authors use RPC to transfer and control data over the network, RMI used for invoke objects over the network and that objects are talk with each other. and use PYRO library to create objects and locating port also can implement distribute programming. Its written in python language so its platform independent. It can work on different operating system at same time. It can accept any return type of value and method. Using PYRO user can easily write code and automatically create object and assign port. Using objects we can perform distributed programming. In this documentation authors perform complete end to end RMI system. they also succeeded in implementation of RMI .although we can't compare implementation of RMI in java with implementation of RMI in python but with ever increasing community python maybe supplant java in the field of distributed programming.

Critical Analysis:

Based on the documentation author are clearly mentioned how we can use different methods and tools to perform distributed programming using python. in this research author use different tools like RPC ,RMI and PYRO library to create and locate objects with different port numbers. that all objects are talk with each other and responsible for transfer and control data all over the internet . Using this technique user can easily transfer data with high speed and short amount of time, also we use pyro library so we can create application which are work on RMI easily . Developers no need high level coding to create object and allocating port it automatically done by RMI.

Paper 9 : Web Automation using Selenium Web driver Python

Student Name :	Rakholiya vasu D.		
Enrollment No	210303105794	Branch :	CSE
Title of Journal Paper	Web Automation using Selenium Web driver Python		
Authors	V.Neethidevan, G.Chandrasekaran		
Journal / Conference :	International Journal of Recent Technology and Engineering (IJRTE)		
Volume / Issue	Vol.7/issue 6s	Pages :	3

In this research author performed web automation testing using selenium web driver python. cross browser testing done with various browsers to check performance of application as expect. The web-based application is tested with Selenium web driver with Python code. In this document authors building testing system using selenium, this tool used for testing software automatically. using selenium driver testers can perform testing more effectively. Current days user interface testing consume more times because it has more no of elements and more time dedicated for this by developer team. To under user interface testing, testing team members must understand the various specification of system. testing should start from day one itself. Similar to involvement of customer in all phases of software system, this team also should be involved from day one.

In this research authors performs cross browsers testing using selenium driver, the main objective of cross browser testing is to ensure application performs its intended operations across different browsers. each software need to perform multi browser testing to ensure that

application work correctly on different browsers. testers are ensured that components like AJAX requests, Applets, Flash, etc. work perfectly on different browsers. From this document we use web automation so our application can work on any web browsers without any error. and we use selenium web driver to perform automatic testing of our software. In this project we use selenium, Selenium is an open-source testing tool and it has web automation framework, used to perform automated website testing. It has the capability to do more automation work to simplify the testing process by the test engineer.

Critical Analysis:

Explanation of web automation and selenium software with its features and all basic operations. It can perform testing on various browsers and its done automatically .user no need manual testing .it produce effective output in each browsers. This paper described how to perform GUI testing techniques for web-based application, also showing why selenium web driver important in python in web automation. Also discussed about the importance of cross browser testing and it implemented in chrome and Firefox. Based on the paper author described what problem in manual testing of software and it's taking too much time to test software. to avoid difficulty testers use selenium tool to perform automatic testing in web-based software. Also use web automation to perform testing in various browsers so application perform effectively and get result as expect.

Paper 10 : Python-WSGI and PHP-Apache Web Server Performance Analysis by Search Page Generator

Student Name :	Swet Patel R.		
Enrollment No	210303105787	Branch :	CSE
Title of Journal Paper	Python-WSGI and PHP-Apache Web Server Performance Analysis by Search Page Generator (SPG)		
Authors	Hataw Jalal Mohammed , Kamaran Hama Ali Faraj		
Journal / Conference :	University of KURDISTAN Hewler		
Volume / Issue	Vol.5/Issue 1	Pages :	7

The web servers (WSGI-Python) and (PHP-Apache) are in middleware tier architecture. Middleware architecture is between frontend tier and backend tier, otherwise it's a

connection between frontend tier and backend tier for three tier architecture. The eLearning systems are designed by two different dynamic web technologies. First is by PythonWSGI and the second is by Personal Home Page (PHP-Apache). The two websites were designed with different open source and cross platform web technologies programming language namely; Python and PHP in the same structure and weight will evaluate perform over two different operating systems (OSs): 1) Windows-16 and 2) LinuxUbuntu 20.4. Both systems run over the same computer architecture (64bit) as a server side with a common backend MySQL web database for both of them.

The software (SW) and hardware (HW) for web servers and E-management are an essential factor, but this paper concentrates on software and application. Since web application is a crucial part of every functioning web application system designed in different web technologies, Python and PHP with different web applications are WSGI-Python and Apache-PHP and benchmarked. The benchmark has been developed to assist society in its practice of delivering quality improvement (QI). QI for the proposed system is two different web servers (i.e., WSGI and Apache). Other sections in the paper investigate which web server is enhanced and is calculated by handwriting codes for SPG. The enhanced QI illustrates the results in this paper for the mentioned technologies of a search page generator in milliseconds.

Critical Analysis:

WBRP stands for "Web Base Response Performance" which is an aspect of measuring the speed of web technology XAMPP over the different OS. This, in turn, is related to the design and developments, as the faster website is shown to enhance visitor attention, loyalty, and satisfaction for XAMPP, which is currently the widespread web technology application software and support web servers of Apache (Othman et al., 2020). The Web Server Gateway Interface (WSGI) is a standard interface between web servers and Python web application frameworks. By standardizing behavior and communication between web servers and Python web frameworks, WSGI makes it possible to write portable Python web code that can be deployed in any WSGI-compliant web server. WSGI is documented in PEP 3333.

Paper 11 : Extracting Knowledge From User Access Logs

Student Name :	Rakholiya vasu D.		
Enrollment No	210303105794	Branch :	CSE
Title of Journal Paper	Extracting Knowledge From User Access Logs		
Authors	Aditi Shrivastava, Nitin Shukla		
Journal / Conference :	International Journal of Scientific and Research Publications		
Volume / Issue	Vol.2/issue 4	Pages :	4

Now in the world web are increasing with no of users ,it very essential for website owners to better understand their customers so they can provide better services also enhance the quality of website. to achieve this they will depend on log files. in this files web server contain information each time when user request resources from sites. In this study we learn about web access log files and information which can mine from logs which is useful to understand user behavior. this information use for restructuring and redesigning website. In this world accessing information is most frequent task. every day we have to go through many information influenced both users website owners and visitors. Website owners reach their audience nationally and internationally also provide 24X7 customer service .other site website visitors also increase rapidly. To mine information ,data mining techniques will be applied ,but website are unstructured so we cannot directly apply mining techniques, but we use web mining which applied on data.

Web usage mining is research field that focus on development and tools which use to study users web navigation behavior. A server log is logging file that automatically created and manipulated by a server to actively performed it. its file where web server writes information ,each time a user request for resources from the particular site .it represents activity for every user for long time. From this document we use server log files, which is created and manipulated automatically, and server actively performed it. we also use web usage mining to gather log files to get information of their action. this file is only several megabytes.

Critical Analysis:

This document contain server log files which are used for mining and collecting important user information of each request ,website owner use this data to understand customer. Also use log analysis which is used to collect data from server to get relevant information. Log file are generated with date and time of transaction. It also contains particular client IP which are request on site. Once user logged on user name include in log files. Show different status of particular requests. Also showing how much byte sent and received from server. Also showing time duration. Web is most important medium to conduct business and commerce. That's why design web pages is very important for system administrator and web designers. this feature can impact on great no of visitors. so web analyzer has to analyze data with server log files to detect pattern. In this study we understanding web server logs, discovering such information that can used to improve business performance. In this documentation authors described about log files ,like how log files are created in website what are use of that log files. They also explain about server logs and logs analysis. In they explain why logs are important for website owners and how they used this data to understand their audience also do improvement in their website so more customer are join and interact with them. They also explain one log file how many different type of data contain. Ex: user logged in detail. time stamp, server IP and port .they also described types of logs and explain in detail.

Paper 12 : Network Security Management Platform System Design and Implementation

Student Name :	Swet Patel R.		
Enrollment No	210303105787	Branch :	CSE
Title of Journal Paper	Network Security Management Platform System Design and Implementation		
Authors	Xia Qing, Library, Huaihai Institute of Technology ,Lianyungang, China		
Journal / Conference :	International Conference on Computer Engineering and Technology		
Volume / Issue	Vol.7/Issue 2	Pages :	4

With the rapid development of the Internet age and the growing popularity of Internet, network security has become increasingly prominent, so how to ensure data and system security in open network environment becomes an issue concerned by many people in the

industry. Firewall technology is special networking equipment used to strengthen the access control between the networks to prevent the external network users to enter the internal network through an external network with illegal means and access to internal network resources, thus to protect the internal network operating environment.

Security event collection subsystem uses C/S structure, including security event collection and formatting two parts. The first part uses SYSLOG and SNMP protocols to collect security incidents, and the second part is to store the collected security incidents in the security information database after formatting, to provide data basis for the entire network security management platform system. Data management subsystem uses B/S structure, including: integrated display, alarm management, device management, event management, emergency management, report management, system management, expansion management and other functions, the various functions through security event analysis layer operates the data in security information database, and displays the data through pages display and statistical reports two ways.

Critical Analysis:

Data management subsystem is mainly to apply the security event information collected by the security event acquisition subsystem, comprehensively display the information useful to users, and carry out configuration management for the security devices, to generate security event reporting and other functions. Data management subsystem is to extract data (security events, other data) from the security information database to show, or store in it after the corresponding operation. Security information database is used to store most of the system data (security events, other data), and a small part of the system data is stored in the XML file.

Paper 13 : Computer network security virtual experiment system design and Implementation

Student Name :	Swet Patel R.		
Enrollment No	210303105787	Branch :	CSE
Title of Journal Paper	Computer network security virtual experiment system design and implementation		
Authors	Liu Zhijun, Zhejiang Textile & Fashion Vocational College		

Journal / Conference :	International Conference on Intelligent Computation Technology and Automation		
Volume / Issue	-	**Pages :**	5

The network security is one of the important factors that influence the development of computer network, under the background of the virtual experiment system is studied in this paper, on the Visual c + + 6.0 and Visual Studio2005 platform was designed and implemented a "network security" virtual experiment system, the system each function module in detail the design idea and implementation methods of description, also gives a design method of database. With the continuous development of the Internet and growing, it has brought more and more convenient for the user's life and benefits. But to network security problems are also let people suffering from the worry, ongoing network security incident to the safety of the rapid development of Internet has brought great threat. Through the computer network security virtual experiment system can through the real feelings on the experimental process, the user understand the dangers of network security problem, and master a certain defense network attack method.

The experiment mainly use Trojan scanner this virtual host Trojans scanning, and then will scan the Trojan removal individually, not all hosts can when performing Trojan scan results, these Trojans are in side Trojan attacks by injection in the attack end only after operation is successful. From the database query, only trojan event readout in the table are consistent with the machine virtual IP trojan ID, trojan name, trojan detail and so on, respectively the Trojan ID number, name and the information such as the harm to the host, when users choose to remove this Trojan is corresponding to delete the selected Trojan information in the database. In the attack end defense SYN FLOOD, there are three parameters available for users to set: TcpMaxPortsExhausted (TCP connection requests),

Critical Analysis:

TcpMaxHalfOpen and TcpMaxHalfOpenRetried. Including TepMaxPortsExhausted valid values in the range of 0-65535, suggested value of 5; TcpMaxHalfOpen valid values in the range of 100-65535, it is recommended that the value is 500, TcpMaxHalfOpenRetried valid values in the range of 80-65535, recommended value is 400. When three parameters, were more than any one, start the SYN protection mechanism. In TCP concurrent connections to attack

defense, there are two parameters for the experimenter Settings: the threshold and the maximum number of simultaneous connections, threshold said when other hosts on the machine on the number of TCP connections when it reaches the threshold start the TCP concurrent connections to protect, will all connections for source IP address, destination address, p source port, destination port, packet size information such as the monitoring; Maximum number of simultaneous connections to say when the number of connections than this value, the host will no longer accept any other host on the machine by a TCP connection, so as to achieve the purpose of protecting the host. The DMZ domain (isolation) is one or more network. Located in the area of the host or server is called a bastion host. Generally can be placed in the isolation zone Web server, E-mail server, etc. Isolation for the network users usually have access to, this way let the network users can access enterprise information publicly, but I don't allow them to access enterprise the protected internal network.

Paper 14 : The Design and Implementation of Security Network System Based on Web

Student Name :	Swet Patel R.		
Enrollment No	210303105787	Branch :	CSE
Title of Journal Paper	The Design and Implementation of Security Network System Based on Web		
Authors	HUANG Zhikun1, Wuhan Polytechnic, Hubei Wuhan 430074, China		
Journal / Conference :	IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)		
Volume / Issue	-	Pages :	3

The computer network technology is developing rapidly, and the development of Internet technology is more quickly, in this case, people more aware of the importance of network security. Due to the information system in the application of the need for security protection, therefore, the study of computer network security problems are always revolved around the information system. Nowadays, the global computer network security companies and scientific research departments are trying to study and solve the problem of network security, not only developed a variety of maintenance network security hardware and software products, and launched a variety of security of network communication standards and

specifications. This article is from the network between the transport layer and application layer, designed a network security system based on Web, and implements a truly safe Internet network.

With the rapid development of science and technology, the enormous increase of network information, the requirement of increasing the user access speed of the web site, make the database access technology pays close attention to by more customers look forward to working with more and more, in the process of database link and access technology, database access technology of ADO.Net by more and more to the enterprise and the customers trust and praise. Security network system structure is a main consideration security mechanism and security, security object mainly include network security, information security, equipment security, system security, database security, information security and computer virus prevention and cure of medium etc.

Critical Analysis:

In order to ensure that the balance of information, the protection of all aspects of the network information to conduct a comprehensive, thus make the barrel principles of network information security. Barrel principle on the system of security vulnerabilities and security threats of every aspect, in the aspect of prevention to ensure that each to break into the weakest place in the system can be found, the design of information security system, evaluation and testing of any part is not to be missed. Put an end to the most common attack means successfully breached the security of the system is a security mechanism and security service design original motivation, but from another perspective, is essentially in order to ensure the safety of the whole system performance, will be safe low coefficient increases. Safety plan must be architecture in science and security network system architecture, because the security architecture is the foundation of security scheme design and analysis.

Paper 15 : Research on the Design of the Implementation Plan of Network Security

Level Protection of Information Security

Student Name :	Swet Patel R.		
Enrollment No	210303105787	Branch :	CSE
Title of Journal Paper	Research on the Design of the Implementation Plan of Network Security Level Protection of Information Security		
Authors	Dabin Sun, Bowei Wang		
Journal / Conference :	International Symposium on Mechatronics and Industrial Informatics (ISMII)		
Volume / Issue	-	Pages :	5

Information security is a widely discussed topic in the era of big data. With the rapid development of computer networks, various information security issues have frequently occurred. How to improve the level of computer network information security protection through the implementation of network security level protection is the direction that network security should focus on. Based on the existing security technology and products combined with the information security level protection system, this paper analyzes the relevant technical management requirements of the scheme design, and studies the design method and design process.

We divide the information system into five levels according to the severity of the damage to the social order, public interest, and national security after the information system is damaged. The corresponding information system security level protection is also divided into five levels. The basic requirements for information system security level protection include technical requirements and management requirements. Among them, the technical requirements are divided into five aspects: physical security, network security, host security, application security and information data security. The management requirements include safety management institutions, safety management systems, personnel safety management, system construction and system operation and maintenance management.

Critical Analysis:

The principle of autonomous protection. That is, the user unit of the information system should operate the information system strictly in accordance with national laws and regulations, independently determine the information system security protection level, and organize and carry out the information system security protection work by itself. Secondly, the principle of key protection. That is to say, the information system is classified according to the importance of the information system and the characteristics of the business. Then, different security protection plans are implemented after the implementation of different security protection schemes. This will give priority to protecting the information system of the core business and important key information resources. Thirdly, the principle of simultaneous construction.

CHAPTER 3
Project Flow and Methodology

3.1 Technologies

3.1.1   Python

Python is an extremely useful programming language for cybersecurity professionals because it can perform a multitude of cybersecurity functions, including malware analysis, scanning, and penetration testing tasks. Python is often recommended as the first language people new to cybersecurity should learn because of its wide use and minimal learning curve. As we use python as an core base of the project.

We will create custom user commands to be used for easer understanding of the commands. For the creation of this custom commands we use a python library **Argparse.** As there are two other modules that fulfill the same task, namely getopt (an equivalent for getopt() from the C language) and the deprecated optparse. Note also that argparse is based on optparse, and therefore very similar in terms of usage. When we use argparse.ArgumentParser() and parser.parse_args() . Running the script without any options results in nothing displayed to stdout. When we add a parser.add_argument("echo") in the command output.

```
$ python3 prog.py --help
usage: prog.py [-h] echo

positional arguments:
  echo

options:
  -h, --help  show this help message and exit
$ python3 prog.py foo
foo
```

Fig: 3.1.1.1 Custom Command Parser

As there will be a command for a new user to create new LAN server to get this team on it. So for the server creation we can use the python Library Socketserver. A server is a software that waits for client requests and serves or processes them accordingly. On the other hand, a client

is requester of this service. A client program request for some resources to the server and server responds to that request. Socket is the endpoint of a bidirectional communications channel between server and client. Sockets may communicate within a process, between processes on the same machine, or between processes on different machines. For any communication with a remote program, we have to connect through a socket port. The main objective of this socket programming is to get how socket server and client communicate with each other. This program is similar to the server program, except binding. The main difference between server and client program is, in server program, it needs to bind host address and port address together. So we create an INET, Steaming socket , socket.socket(socket.AF_INET, socket.SOCK_STREAM). . Now to connect to it we use s.connect(("**IP**", **PORT**)). When the connect completes, the socket s can be used to send in a request for the text of the page. The same socket will read the reply, and then be destroyed. We used socket.gethostname() so that the socket would be visible to the outside world. If we had used s.bind(('localhost', 80)) or s.bind(('127.0.0.1', 80)) we would still have a "server" socket, but one that was only visible within the same machine. s.bind(('', 80)) specifies that the socket is reachable by any address the machine happens to have.

3.1.2   Pryo Library

Pyro is a library that enables you to build applications in which objects can talk to each other over the network, with minimal programming effort. You can just use normal Python method calls, with almost every possible parameter and return value type, and Pyro takes care of locating the right object on the right computer to execute the method. It is designed to be very easy to use, and to generally stay out of your way. But it also provides a set of powerful features that enables you to build distributed applications rapidly and effortlessly. Pyro is a pure Python library and runs on many different platforms and Python versions. It works between different system architectures and operating systems. Can use IPv4, IPv6 and Unix domain sockets. Optional secure connections via SSL/TL.

Pyro is an advanced and powerful Distributed Object Technology system written entirely in Python, that is designed to be very easy to use. It resembles Java's Remote Method Invocation (RMI). It has less similarity to CORBA - which is a system and language independent Distributed Object Technology and has much more to offer than Pyro or RMI. But Pyro is small, simple, fun and free. It is a library that enables you to build applications in which objects can talk to

each other over the network, with minimal programming effort. You can just use normal Python method calls to call objects on other machines. Pyro is a pure Python library and runs on many different platforms and Python versions. Latest version of PYRO is PYRO4.its considered future complete and new development of PYRO is frozen. only some security issues will still made to PYRO4. improvements and new features will only be available in its successor Pyro5 . New code should use Pyro5 unless a feature of Pyro4 is strictly required.

Clears the global ParamStoreDict.

This is especially useful if you're working in a REPL. We recommend calling this before each training loop (to avoid leaking parameters from past models), and before each unit test (to avoid leaking parameters across tests).
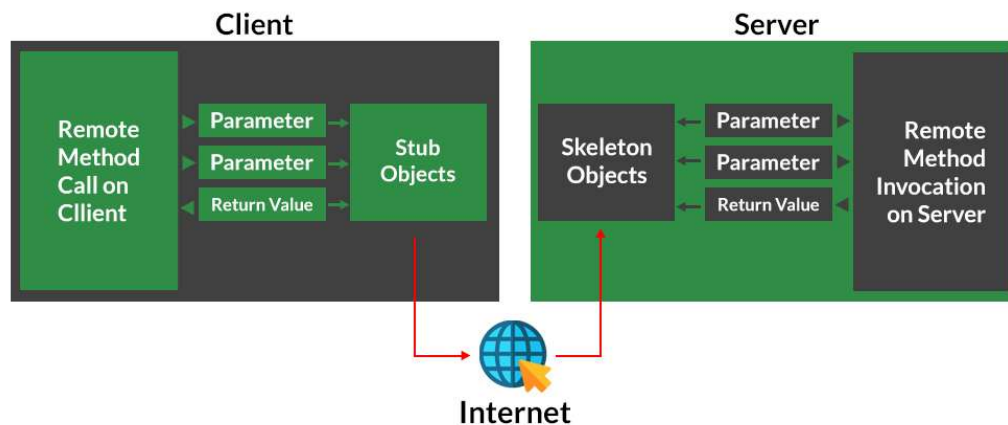
Fig 3.1.2.1 Working of RMI

3.1.3   Selenium WebDriver

Selenium WebDriver is a web framework that permits you to execute cross-browser tests. This tool is used for automating web-based application testing to verify that it performs expectedly.

Selenium WebDriver allows you to choose a programming language to create test scripts. it is an advancement over Selenium RC to overcome a few limitations. Selenium WebDriver is not capable of handling window components, but this drawback can be overcome by using tools like Sikuli, Auto IT, etc.

Selenium provides support to multiple libraries such as Ruby, Python, Java, etc. as language bindings have been developed by Selenium developers to provide compatibility for multiple languages. For instance, if you want to use the browser driver in Python, use the Python Bindings. Selenium provides drivers specific to each browser and without revealing the internal logic of browser functionality, the browser driver interacts with the respective browser by establishing a secure connection. These browser drivers are also specific to the language which is used for test case automation like C#, Python, Java, etc.

The selenium.webdriver module provides all the WebDriver implementations. Currently supported WebDriver implementations are Firefox, Chrome, IE and Remote. The Keys class provide keys in the keyboard like RETURN, F1, ALT etc. The By class is used to locate elements within a document. The driver. Get method will navigate to a page given by the URL. WebDriver will wait until the page has fully loaded (that is, the "onload" event has fired) before returning control to your test or script. Be aware that if your page uses a lot of AJAX on load then WebDriver may not know when it has completely loaded. WebDriver offers a number of ways to find elements using the find element method. For example, the input text element can be located by its name attribute using the find element method and using By.NAME as its first parameter. Next, we are sending keys, this is similar to entering keys using your keyboard. Special keys can be sent using the Keys class imported from selenium.webdriver.common.keys. To be safe, we'll first clear any pre-populated text in the input field (e.g. "Search") so it doesn't affect our search results:
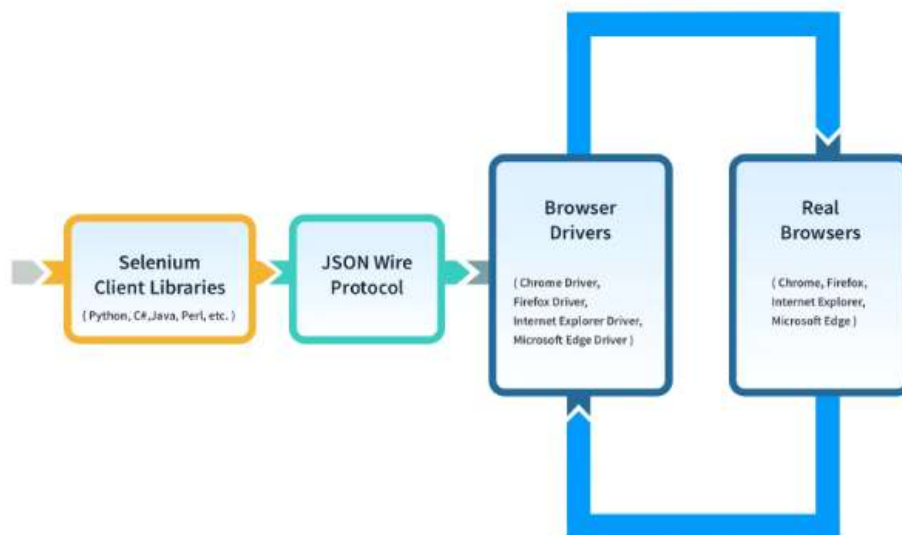
Fig 3.1.3.1 Selenium WebDriver

3.1.4   Log File

It is a file to which the Web server writes information each time a user requests a resource from that particular site. Log file data can offer valuable information insight into web site usage. It represents the activity of many users over a potentially long period of time . This logs collect data on the server in the files of specific formats. Measures hold information about web site usage by recording how users visit the web site and how active they are. Depending on the log format structure, different data is stored. Usually logs contain data such as: client's IP address, URL of the page requested, time when the request was send to server.
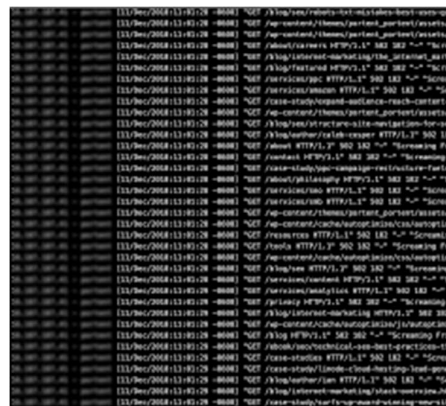
Fig 3.1.4.1 Server Generated Logs based on user request

When a user sends queries to the server, requested databases will be retrieved. At the same time ,the user session including the URL, Client's IP address, accessing date and time , query stem will be recorded in the server logs. These server logs can be preprocessed and mined in order to get some insight into the usage of a server site as well as the user's behavior. As it is said oil is no more the most important and valuable asset it is data that is more valuable than oil, and logs are one type of data that are having a big share of these data, anyone who is having access to this data would be able to do many things with it, so many researches are done on logs in all fields of computer systems not only networks but other parts also, as mentioned before after a system is facing a problem the first thing to be analyzed are logs so the system admin would be able to answer who or what was the problem cause, when it started, why did it happen, all sort of these things, and admin make sure that in future same thing never happens. For all above reasons logs are making a big part in systems troubleshooting, maintenance and security issues, so there is need for research in this field

which is widely done already and is being done every. Logs file will contain day at the present time, these researches on log processing are done on every field and type of subject

- Date&time

- Client IP address

- User authentication

- Server name

- Server IP address

- Server Port

- Status

- Time stamp

- Protocols

- Cookies

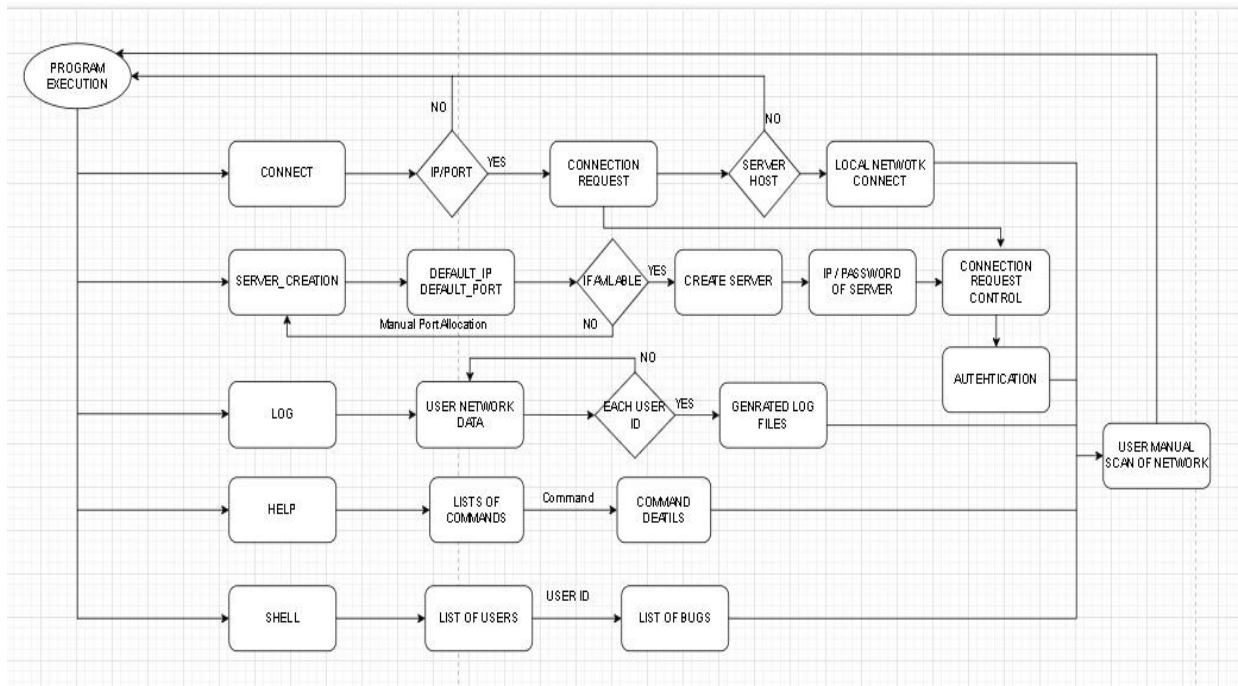Fig 3.1.4.2 Application Output Page

3.2 Project Flow

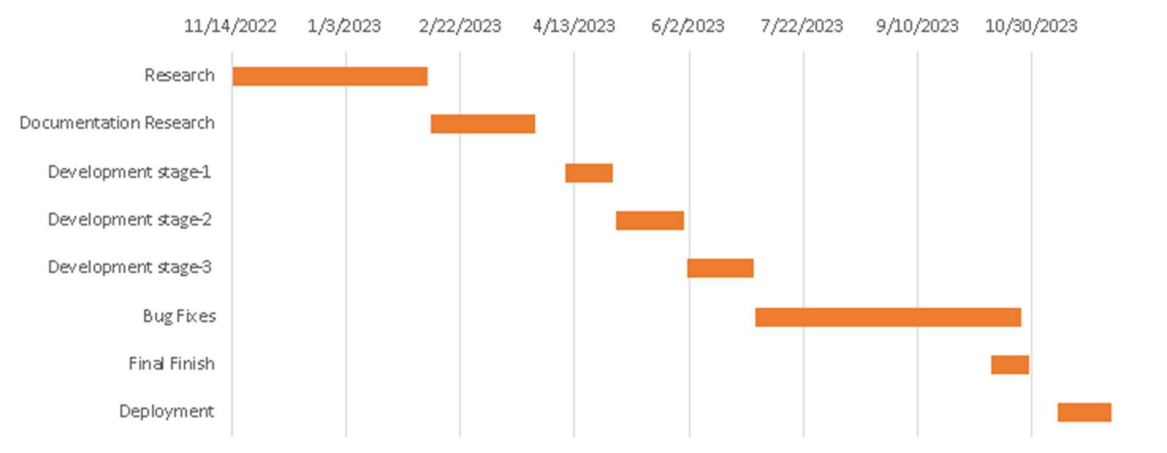Fig 3.2.1 Project Flow Diagram

3.3 TimeLine chart

Fig 3.3.1 Time Line Chart

CHAPTER 4

Future work

- Add a more detail log file creation.[Packet tracking & Finding]

- Add 5+ member's on LAN server

- Manual server configuration options

- GUI Interface

Reference

[1]Brandon Rhodes, John Goerzen & Tim Bower, 2023, Foundations of Python Network Programming , 2rd ed., Prentice- APress.

[2]Nathan Jennings, 2023 . Socket Programming in Python 1(1.2), pp. 0-30.

[3]Pietro Grandest, 2022. Server deployment with Python: From A to Z , Prentice- Codementor.

[4]Panagiotis Chartas, 2022. Villain Tool (Updated 12 January 2023) Available at: https://github.com/t3l3machus/Villain [Accessed 30 January 2023].

[5]Python Documentation , 2022 . argparse — Parser for command-line options, arguments and sub-commands (3.2), pp. 2-30.

[6] Adeyinka Ajao Adewale, Victor Olugbemiga Matthews, Adelakun Adebiyi, Olaitan Alashiri, 2021,packet-sniffer-for-users-end-network-performance-monitoring-using-python programming,, pp. 0-25.

[7] R. B. Manjula, P. I. Basarkod, Yaser Mowlaiwzadah, 2021, Analyzing and Simplifying Log Files using Python, Vol. 9 , Prentice- IJERT.

[8] Asswini Swain, Het Sheth, Pratik kanani, 2021, Remote Method Invocation Using Python, Vol. 6 , Prentice- International Journal Of Advanced Studies In Computer Science And Engineering,Ijascse.

[9] Adeyinka A. Adewale, Victor O. Matthews, Adebiyi A. Adelakun, Winifred Amase,Olaitan Alashir, 2019, Packet Sniffer for Users End Network Performance Monitoring using Python Programming, Prentice- International Journal Of Advanced Studies In Computer Science And Engineering,Ijascse.

[10] V.Neethidevan, G.Chandrasekaran, 2019, Web Automation using Selenium Web driver Python , Prentice- International Journal of Recent Technology and Engineering.

[11] Aditi Shrivastava, Nitin Shukla , 2019, Extracting Knowledge From User Access Logs , Prentice- International Journal of Scientific and Research Publications.

[12] Hataw Jalal Mohammed , Kamaran Hama Ali Faraj, 2019, Python-WSGI and PHP-Apache Web Server Performance Analysis by Search Page Generator, Prentice- University of KURDISTAN Hewler.

[13] Xia Qing, 2018, Network Security Management Platform System Design and Implementation, Vol. 7, Prentice- International Conference on Computer Engineering and

Technology.

[14] Liu Zhijun, 2017, Computer network security virtual experiment system design and implementation, Prentice- International Conference on Intelligent Computation Technology and Automation.

[15] HUANG Zhikuntt, 2017, The Design and Implementation of Security Network System Based on Web, Prentice- IEEE Workshop on Advanced Research and Technology in Industry Applications.

[16] Dabin Sun, Bowei Wang, 2017, Research on the Design of the Implementation Plan of Network Security Level Protection of Information Security, Prentice- International Symposium on Mechatronics and Industrial Informatics.

Links:

https://docs.python.org/3/howto/argparse.html

https://docs.python.org/3/library/http.server.html

https://docs.python.org/3/library/argparse.html#argumentparser-objects

https://www.codementor.io/@pietrograndinetti/server-deployment-with-python-from-a-to-z-1fjhy96qni

https://github.com/t3l3machus/Villain

https://realpython.com/python-sockets/

https://www.sourcecodester.com/python

https://realpython.com/python-sockets/#conclusion

https://docs.python.org/3/library/socket.html

https://www.researchgate.net/publication/341271544_Remote_Method_Invocation_Using_Python

ChatGPT