5.3 INPUT DESIGN

Input design is a process of converting a user-oriented description of inputs to a computer-based program-oriented specification. The main objective is to create a input layout that is easy to follow and avoid entering data incorrectly.

The goal of input design is to make input data entry as easy and error free. Input screen takes care to filter the invalid data from becoming an operational data at data entry phase.

If data going into the system is incorrect then processing and output will magnify these errors.

Objective during the input design is as follows:

- Setting up the virtual labs
- Access the system log-ng
- Working with the juniper router
- Confirm the IP address
- Login the tool Hydra to perform brute force against SSH
- Access the Nmap

Several stages that was included in the input design during the brute force attacks:

In the login with system log input design includes :

- Install the software using IP address
- Software updation
- Set the default configuration
- Logs from another machine or device
- Check the status configuration

In the access with the Juniper router:

- Login the physical router
- Configure the router interfaces
- Confirm the interface IP address
- Configure logging for R3
- Test connectivity from R3

In the accessing tool of Hydra to perform against SSH the input architecture are as follows:

- Create a list of usernames with hydra
- Check the usernames in SSH
- Trim the file to view or delete in SSH
- Perform Hydra
- View the syslog

5.4 OUTPUT DESIGN

The output design defines the output required and the format in which it is to be produced. Care must be taken to present the right information so that right decisions are made and to how the command are performed in the UBUNTU terminal window:

Designing the output for a brute force attack detection system involves presenting information in a clear and actionable format for security personnel to analyze and respond effectively.

In the syslog-ng to update the software using the SSH

```
ssh apnic@192.168.30.10
```

To SSH into the server at the specified IP address (192.168.30.10) with the username After entering this command, it will be prompted to enter the password for the user account on the server

Install the software using the command terminal

```
sudo apt-get install -y nano tree syslog-ng syslog-ng-core
```

- nano: A simple and easy-to-use text editor for the command line.
- tree: A command-line utility that displays directory structures in a tree format.
- syslog-ng: A flexible and highly configurable logging system for Linux.
- syslog-ng-core: The core components of the syslog-ng logging system.

Using the -y flag with apt-get install will automatically answer "yes" to any prompts, enabling a non-interactive installation process

Setting the Default Configuration file in the output design:

```
sudo less /etc/syslog-ng/syslog-ng.conf
```

The command sudo less /etc/syslog-ng/syslog-ng.conf will allow to view the contents of the syslog-ng configuration file located at /etc/syslog-ng/syslog-ng.conf. The less command is a pager that enables to scroll through the contents of a file in your terminal.

Check the status of the configuration using the command:

```
sudo systemctl restart syslog-ng
sudo systemctl status syslog-ng
```

- sudo systemctl restart syslog-ng: This command restarts the syslog-ng service. After restarting, syslog-ng will reload its configuration and apply any changes made to its configuration files.

- sudo systemctl status syslog-ng: This command checks the status of the syslog-ng service. It will provide information about whether the service is running, any errors encountered, and other relevant details

The output design of the juniper router command architecture are as:

The output of the juniper router is to login the router through the command and IP address of the SSH. After then configure the router interfaces for R3 it will show as the following:

```
configure
top edit interfaces
set ge-0/0/0 unit 0 description "Link to Remote syslog"
set ge-0/0/0 unit 0 family inet address 192.168.30.3/24
```

These commands will set the description of interface ge-0/0/0 to "Link to Remote syslog" and assign it the IP address 192.168.30.3/24

After that to interface the IP address using the UBUNTU in command terminal :

```
show interface terse
```

The command "show interface terse" is used in Juniper devices to display a terse summary of all interfaces and their current status. This command will output a summary of interfaces and other relevant information such as MAC addresses and IP addresses.

In the process of the juniper router resources Test connectivity from R3 to the syslog-ng Server in the command terminal

```
ping 192.168.30.10 count 2
```

The command you provided is used to ping a specific IP address (192.168.30.10) with a specified count of packets (2).When you execute this command, your system will send ICMP echo request packets to the specified IP address (192.168.30.10). If the destination is reachable and responds to ICMP echo requests, it should receive ICMP echo reply packets back, indicating successful communication.

After accessing with the juniper router then to perform the Brute force attacks with the tool Hydra

To create a list of usernames in addition with obtain a password list from various sources. In the ubuntu terminal window installed a usernames

```
cd ~
cat ssh-usernames.txt
```

The commands provided are used to change the directory to the user's home directory (cd ~) and then to view the contents of a file named ssh-usernames.txt (cat ssh-usernames.txt).

cd ~: This command changes the current directory to the user's home directory. The ~ symbol is a shorthand representation of the home directory.

cat ssh-usernames.txt: This command displays the contents of the file named ssh-usernames.txt. cat is a command used to concatenate and display the content of files.

Then to view the usernames are in the file SSH sernames.txt

```
wc -l ssh-usernames.txt
```

The command wc -l ssh-usernames.txt is used to count the number of lines in the file named ssh-usernames.txt. In the command it will taken 55 usernames

Then to perform the Brute force attack in the Hydra :

```
hydra -L ssh-usernames.txt -e n -t 1 ssh://192.168.30.3
```

L	the path to a wordlist file that contains a list of possible usernames to try.
-e n	use a null password (i.e., an empty password) for the login attempt.
-t 1	use a single thread for the attack, which can help to reduce the load on the target system.
ssh://	use the SSH protocol for the attack.
<target IP>	the IP address of the target SSH server.

Finally the output shows the Data attacking the SSH.