104346575@student.swin.edu.au

User Manual for Running the Attack Detection Program

Prerequisites

1. **VirtualBox:**
   - Install VirtualBox on your host machine.
   - Create a new virtual machine in VirtualBox and install Ubuntu (or any operating system) on it.
2. **XAMPP Installation:**
   - Download and install XAMPP on your system.
   - Start Apache and MySQL services from the XAMPP control panel.
3. **DVWA Setup:**
   - Clone the Damn Vulnerable Web Application (DVWA) repository into the htdocs directory of XAMPP:

     ```
     cd /opt/lampp/htdocs : git clone https://github.com/digininja/DVWA.git
     ```

   - Set up DVWA by configuring the config.inc.php file and setting up the database.

Steps to Run the Attack Detection Program

1. **Clone the Attack Detection Scripts:**
   - Clone the attack detection scripts from GitHub into a directory on your Ubuntu machine:

     ```
     git clone https://github.com/104202994/PROJECT-2-TAP.git
     ```

2. **Navigate to the Directory:**
   - Open a terminal and navigate to the directory where you cloned the scripts:

     ```
     cd /path/to/your/cloned/repository
     ```

3. **Configure Slack Webhook:**
   - Create a Slack Incoming Webhook URL:

        - Go to your Slack workspace and create a new Incoming Webhook in the app settings.
        - Copy the webhook URL.
    - Update the SLACK_WEBHOOK_URL in the slack_alert.py file:

```
SLACK_WEBHOOK_URL = 'https://hooks.slack.com/services/your/webhook/url'
```

    - Replace 'https://hooks.slack.com/services/your/webhook/url' with your actual Slack webhook URL.

4. **Run the Attack Detection Program:**
    - Use the following command to run the attack detection script:

```
sudo python3 detectAttacks.py
```

    - The script will start monitoring the Apache access logs for various attack patterns:
        - **Brute Force Attacks**
        - **Directory Traversal**
        - **Denial of Service (DoS)**
        - **File Inclusion (RFI/LFI)**
5. **Monitoring & Alerts:**
    - The program will continuously monitor the Apache access logs.
    - If an attack is detected, the offending IP address will be blocked using iptables, and a notification will be sent to the configured Slack channel.
    - The logs and alerts will be displayed in real-time in the terminal.
6. **Automated Self-Healing:**
    - The system will attempt to self-heal by modifying security settings and restarting services as needed when specific attacks are detected.

Troubleshooting

- **Permission Issues:**
    - Ensure that you are running the script with sudo to allow it to modify system settings like iptables.

- **Slack Notification Issues:**
  - If Slack notifications are not being sent, check the webhook URL and your internet connection.
- **Log Monitoring:**
  - Ensure that the path to the Apache access logs (/opt/lampp/logs/access_log) is correct and accessible.

Additional Information

- **Custom Thresholds:** You can adjust the thresholds for attack detection in each script (e.g., ATTEMPT_THRESHOLD for brute force detection).
- **Script Customization:** You can modify the scripts to detect additional types of attacks or integrate with other notification services.
