IT FOR SOCIETY, Vol. 04, No. 02
ISSN 2503-2224

NETWORK DEFENSE SYSTEM MONITORING THROUGH A MOBILE APPLICATION

Lalu Muhammad Aryandi Azrin[1]
Abdul Ghofir[2]
President University
Bekasi, Indonesia
[1]lalumaa@gmail.com
[2]geoff@president.ac.id

Abstract - This paper proposed a way to secure and protect pc or laptop remotely via mobile device. These two device communicate by exchanging information or data using database connection. There will be two applications that are developed, windows-based application and mobile application. The proposed scheme used some firewall configuration and log management to complete the process. The firewall configuration will block computer attacks such as Denial of Service. Log management is to generate a specific log file if there is a possible threat. It will then invoke. the windows application to update the database which is regularly accessed by mobile application. It then alerts user on possible attack or threat.

1. Introduction

SYN-Flood is a serious threat for everyone, it could take a server down within a minute. To block this threat, it could be done by configuring a one of firewall chain. This firewall chain is filter rule, this chain is in charge of inspecting or filter every incoming connection in the network. If there is a SYN-Flood attack, the firewall will block the attack, at the same time it will generate a log file. This log file will be processed by windows application. The windows application is java based application which is created using jee eclipse IDE. The application has a feature to send an information into the database. As for Mobile application is created using Android Studio. The mobile application has features such as notify the user of incoming attacks and shutdown the connected device in this case computer or laptop. The application is also using MySQL and php to connect into database. There are some limitations of this research which are listed below:

- Need additional application to generate a required log file.
- The firewall configuration cannot block every kinds of DoS and DDoS attack that is exist right now. Only one type of attack.

2. Method

The method approach taken in this thesis in order to execute all objective by implementing a filter rule in the firewall by configuring the filter chain. For database usability, the application using MySQL.

Firewall Rule in Mikrotik.

MikroTik Router is an operating system that can be used as a reliable network router, including a variety of full features for network and wireless[1]. Mikrotik has many features to choose from, each feature has its own purpose and impact within the network itself. Firewall is one of the features in mikrotik, it use to filter every packet that coming or leaving the network.

This feature have three rule to be set up first, these three rule are Filter Rule, NAT(Network Address Translation), and Mangle. For each rule there is a parameter as the bridge to every rule so it will synchronized properly, this parameter is called chain. The parameter function is to determine what type of traffic is currently in the firewall, which later will be handled by three rule.

Filter Rule, shown at figure 1,is a first stage when the packet is entering the network. This rule decide either allowed or not allowed the packet is to go into the next rule. In Filter Rule there is three chains, which is Forward, Input, and Output. The forward chain determine that the packet is just passing the router.

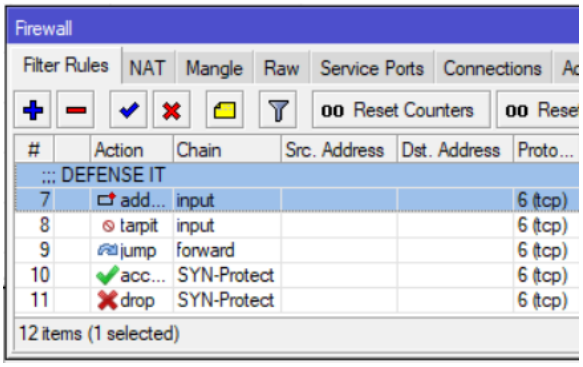

Figure 1 Firewall Filter Rule.

Input chain is used to process the data packet that is coming into the router through interface of the router and the IP address destination is available in the router. Output chain job is to process the outcome of data packet from router.

3. Experimental Result

In order to evaluate the outcome or result of the designed method in previous section, there will be a testing phase where every feature in the application will be tested. Testing is crucial in order to examine or verify the program to determine its functionality and accuracy. This section will consist of the Application testing and Firewall testing.

3.1 Windows Application

This testing section could be done by running the windows application first, then toggling protection button. After that the user could see the computer information by clicking show device info button. Windows Application section will be evaluated in Table 1 that shows the testing scenarios, and system response.

Table 1 Testing on Windows App.

No.	Scenario	System Response
1	Start Application	The application will start and user able to see toggle button and Show Device Info Button
2	Toggling the protection	The application will immediately starting to scan any log that contain the current attack that is happening and send data into the database.
3	Device Info Window screen	After user click on Device Info Button, the application will redirect user into another window screen containing the device information from database.

Figures 2 and 3 show some UIs of Windows Application.

3.2 Mobile Application

Mobile Application testing will be examine based on its functionality to evaluate incoming and outcoming process from the user activity and Windows Application outcome. The following scenario could be seen in Table 2.

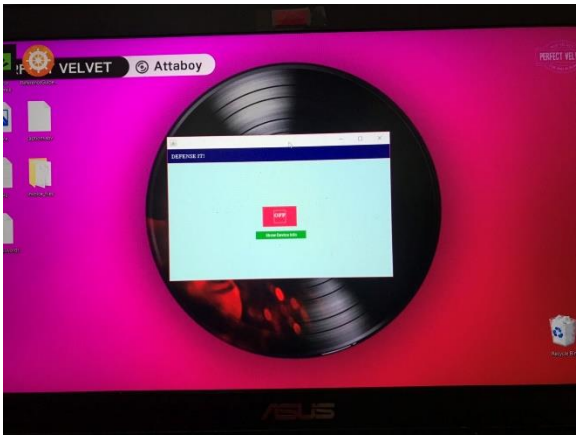

Figure 2. Windows Application Main

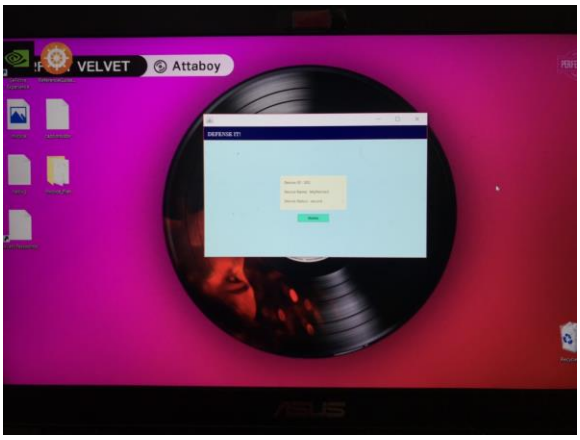

Figure 3. Windows Application Show Info

Table 2. Testing on Mobile App.

No.	Scenario	System Response
1	Start Application	The application will start and user able to see toggle button, Connect Button, and Shutdown Device Button.
2	Toggling the protection	The application will immediately starting to scan changing data of the device status in the database server.
3	Connect Device Screen	After user click on Connect Button, the application will redirect user into another application screen enabling user to connecting both device.
4	Shutdown Device	After user click on Shutdown device button, the application will change the data of the device status into shutdown then windows application will immediately shutting down device.
5	Connect Device	The Application will pop up a dialog box informing the user that the connection is success.

3.3 Firewall and Logging

Firewall and Logging testing will be examine based on its functionality to protect the device from incoming threat and also producing logging record of current event. The following scenario could be seen in Table 4.

Figures 4 and 5 show some of UIs of Mobile Application

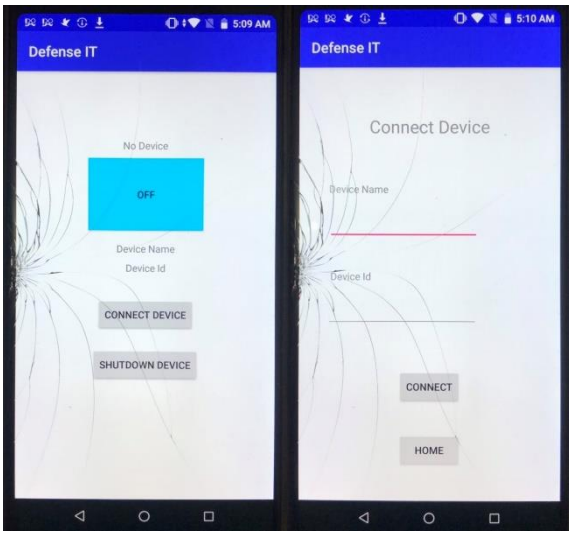

Figure 4. Mobile Application Interface 1

Table 4. Testing on Firewall

No.	Scenario	System Response
1	Block SYN-Flood	The firewall successfully blocking incoming syn-flood attack in connected device.
2	Logging record	The syslog server will automatically produce log file containing information of current attack.

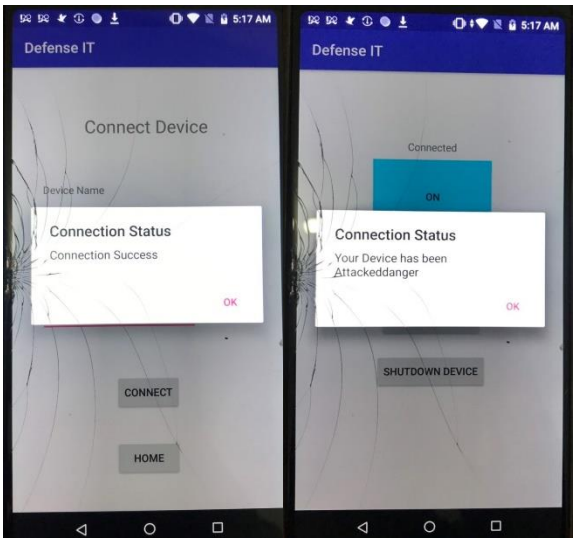

Figure 5. Mobile Application Interface 2

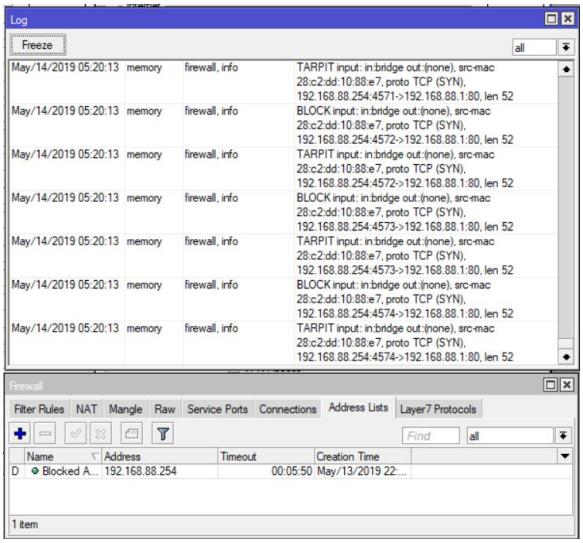

Figure 6. System Log

4. Conclusion

This thesis is aiming to provide a simple and easy way to protect and monitor the user device current status from far away. The main purpose of this thesis has been accomplished successfully which are to block SYN-Flood in windows device. By using this thesis, user do not to worry anymore of leaving their device in home, office and etc.

The protection method used in the firewall to block a syn-flood attack is using a packet filtering which is one of three firewall configuration. By using this method, any incoming syn-flood attack could be blocked by understanding the basic procedure of TCP/IP three way handshake. The SYN-Flood threat exploit this three way handshake drawback to attack server, device and etc.

References

[1] Khaled M. Elleithy, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison". SYSTEMICS, CYBERNETICS AND INFORMATICS, VOLUME 3 - NUMBER 1

[2] Qijun Gu, PhD., Peng Liu, PhD. , “Denial of Service Attacks”

[3] Mohammad Imran, Dr.AbdulrahmanA.Algamdi, Bilal Ahmad, “Role of firewall Technology in Network Security” International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Issue 12 December 2015

[4] Mr. Sachin Taluja1, Mr. Pradeep Kumar Verma, Prof. Rajeshwar Lal Dua, “Network Security Using IP firewalls” International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 8, August 2012