**“System Monitoring and Security”**

*Synopsis submitted*

*In*

*Partial fulfillment of requirement for the award of degree of*

**Master of Technology**

**In**

**Computer Science and Engineering**

By

**Komal Lawani**

Guide- Ms. Nisha Balani



**Department of Computer Science and Engineering**

**Jhulelal Institute of Technology, Nagpur(Rashatsant Tukadoji Maharaj**

**Nagpur University), Nagpur**

**SESSION 2016-2017**

1. **INTRODUCTION**

Monitoring system for any changes in specific file or folders is an important task now-a-days. Monitoring specific files has become important in order to prevent any modification without the user information. Also, monitoring network in order to prevent packets from specific IPs to your machine is important so that the intruders cannot attack your system.

This project will monitor specific files/folders on users’ machine. It will also block packets from specific machine to the users’ machine.

1. **LITERATURE SURVEY / RELATED WORK**

* **Network Security Using IP firewalls Mr. Sachin Taluja1 , Mr. Pradeep Kumar Verma2 , Prof. Rajeshwar Lal Dua (International Journal of Advanced Research in Computer Science and Software Engineering):**

This paperwork demonstrates the tasks needed to enhance the network security in Linux environment. The various security modules existing in Linux makes it different from other operating systems. we analyzing network packets using the most popular open source network protocol analyzer wire shark and on the basis of analyzing the packet work has been done on writing the script to block/allow the network traffic using IP firewall and after blocking traffic further capturing and analyzing of packets using wire shark.

* **Monitor file integrity using MultiHasher (London school of hygiene & tropical medicine – Library & Archives Service):**

This guide describes the use of MultiHasher, an integrity monitoring tool for Microsoft Windows that may be used to monitor data files for evidence of accidental or deliberate change. Unexpected file change may be a symptom of an underlying problem – that the storage media is beginning to fail, or that the system has been compromised and updates made by a non-authorized user. For this reason it is important to monitor the integrity of valuable files on a regular basis.

1. **OBJECTIVE**

This project will create a desktop based application for windows that will perform the following activities on a specific machine:

* **Monitor specified files/folders on your machine:**

                This will monitor the specified files/folders/directory for any changes including reading of the file, updating a file, adding any new file, deleting any file etc.

* **Block packets from a specified IP to this machine:**

                This will capture all the packets and analyze it to identify if the packet has arrived from the specific IP. If so, then block that packet. This will include working with drivers in order to capture the packets for analysis. After analysis the packet will either be dropped or accepted according to the analysis.

A GUI will be created for updating the list of files/folders to be analyzed and updating the list of IPs to be blocked. Only authorized users will be allowed for any modification via this GUI.

Another GUI will be created to display the events that are occurring in the system. This includes the type of event that has occurred (e.g.: File modified, packet blocked), time of the event etc.

1. **PROPOSED PLAN OF WORK**

|  |  |
| --- | --- |
| **Month** | **Proposed task** |
| August | Synopsis Submission |
| September | Study of the available products in the market |
| October | System study and Configuration |
| November | Module 1: GUI creation to set the folders to be monitored |
| December | Module 2: Implement the monitoring of specified folders with GUI creation. |
| January | Progress Paper Submission |
| February | Module 3: Study of packet blocking from specific IPs in the system. |
| March | Module 4: Implementation of packet blocking from specific IPs. |
| April | Thesis Submission |

1. **EXPECTED OUTPUT**

The application should be able to properly monitor the specified files/folders. Also it should be able to block packets from specific IPs to the machine.

1. **APPLICATIONS**

The project will provide security to the end user by blocking the packets from malicious clients. The project will also monitor the important files/folders for any modifications.

1. **CONCLUSION**

Need to create a desktop based application for windows that will do the following:

* + Monitor specified files/folders on your machine.
  + Block packets from a specified IP to this machine.

**REFERENCES**

* Network Security Using IP firewalls Mr. Sachin Taluja1 , Mr. Pradeep Kumar Verma2 , Prof. Rajeshwar Lal Dua (International Journal of Advanced Research in Computer Science and Software Engineering)

<https://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8/V2I800280.pdf>

* Monitor file integrity using MultiHasher (London school of hygiene & tropical medicine – Library & Archives Service)

<https://www.lshtm.ac.uk/research/researchdataman/store/multihasher_guide.pdf>

* Systems Security research at Politecnico di Milano by Federico Maggi and Stefano Zanero

<http://www.syssec-project.eu/m/page-media/3/maggi-syssec11.pdf>

* Distributed real-time task monitoring in the safety-critical system Melody by H.F. Wedde, J.A. Lind and G. Seghert

<http://ieeexplore.ieee.org/document/777462/authors>

* Network monitoring system design under LAN” by Liang Fan and Li Fei.

<http://ieeexplore.ieee.org/document/5451573/authors>

* Network Security Using Cryptographic Techniques by Sumedha Kaushik and Ankur Singhal

<http://www.ijarcsse.com/docs/papers/12_December2012/Volume_2_issue_12_December2012/V2I12-0132.pdf>

* Controlling IP Spoofing through Inter domain Packet Filters by Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar.

<http://ieeexplore.ieee.org/document/4358709/authors>

* IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending Against Internet DDoS Attacks by Minho Sung and Jun Xu, College of Computing Georgia Institute of Technology Atlanta

<http://www.ieee-icnp.org/2002/papers/2002-27.pdf>

* Design and Implementation of a Fast Dynamic Packet Filter by Zhenyu Wu, Mengjun Xie, Member, IEEE, and Haining Wang, Senior Member, IEEE.

<http://www.cs.wm.edu/~hnw/paper/ToN_swift.pdf>

* High-Speed Dynamic Packet Filtering by Luca Deri.

<http://luca.ntop.org/Blooms.pdf>

* Packet Filtering using Data Mining Algorithm by Neha Faxwala, Nishtha Dhar, Riya Avlani, Dilip Dalgade(International Journal of Advanced Research in Computer Science and Software Engineering)

<https://www.ijarcsse.com/docs/papers/Volume_5/3_March2015/V5I3-0566.pdf>

* Adaptive Early Packet Filtering for Defending Firewalls against DoS Attacks by Adel El-Atawy , Ehab Al-Shaer and Tung Tran, Raouf Boutaba

<http://pub.cs.sunysb.edu/~ttran/infocom09.pdf>

**Name and Signature of Projectee Name and Signature of Guide**