Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Intrusion Detection System for Intranet Security

Mr. Premchand B. Ambhore
Research Scholar Government College of Engg.
India-444604

Dr. Bandu B. Meshram
Head and Professor Computer Engg.
V.J.T.I. Matunga, Mumbai, India

Abstract: Intrusion Detection System is the major aspect of network computer security. Unlike firewall, it does not block particular data but keeps track of incoming data and determines whether any intrusion is underway or not. it also has records of previous attacks for future reference. IDS prevent the intrusion in first place itself. And if not possible notifies the user and brings system back on track. We went to analysis and design phase of paper. We tried to understand scope of our project and tried to analysis different aspects, identified real life entities that may be considered for project. We have drawn EER diagram, Data flow diagram and component diagram. We have implemented an Intrusion Detection System to detect various well known attacks. Intrusion Detection approach, that we have used is NIDS (Network Intrusion detection System). So our system captures network data using Win Dump and detects attacks based on captured packet header information. There is other approach called Host based Intrusion Detection System. This approach makes extensive use of system log file and detects system attacks such as failed login attempts, suspicious file data changes etc. As we have used only NIDS approach to implement IDS our IDS cannot detect attacks such as unauthorized data access, unauthorized system logins etc. To make the system immune to this type of attack we can implement Host based IDS that is able to detect such attacks. This will make system more secure. As we can understand any one approach (either Host based or Network IDS) is never going to be enough to provide the complete security for the system. So we need to implement Hybrid Intrusion detection approach. Hybrid Intrusion Detection makes use of both NIDS and Host based IDS. Both the approaches used together will provide complete safety to user (at least best possible security). Our Intrusion Detection System is implemented for single computer machine.

Keyword: IDS, LAN, Protocol, Security

I. INTRODUCTION

Intrusion detection systems, or IDSs, have become an important component in the Computer Security. IDS do exactly as the name suggest: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection of intrusion. An IDS, installed on a network, provides much the same purpose as a burglar alarm system installed in a house. Both detect an intruder/burglar, and subsequently issue some type of alert so that further action can be taken. But burglar alarm is hardware circuit where as network intrusion detection system is a software implementation for detection of possible attacks on the system from internet or LAN. Although IDSs may be used in conjunction with firewalls, which aim to regulate and control the flow of information into and out of a network, the two security tools should not be considered the same. Firewalls can be thought of as a fence or a security guard placed in front of a house.

Statement of the Problem: The aim of the problem is to build comprehensive Intrusion Detection that can protect the computer from outside threats, monitor data packets that flow into, alerts administrator about the possible intrusion. A user having administrative privileges, thus, can take possible steps so as to safeguard the system integrity. Intrusion detection system should capture data packet headers from network, analyze that header, and classify it according to the protocol used. It, then, should check this data for presence of intrusion by applying some set of rules that can be predefined. The port scanning utility will be an added advantage in determining the various intrusion attempts on the system. The module of the projects contains the following Design and implementation of user interface. Data collecting and formatting module. Attack detecting module. The modules are explained below Design and implementation of user interface: The user interface being the primary module interacting with user need to be complete and easy to use. As this product is being targeted for average users, the user interface should be perceived to be efficient and intuitive by the users. In other words, user interface should be responsive to the user needs. Data collecting and formatting module these modules takes data collected by WinDump software and classify according to different protocols. Attack detecting module this takes formatted data and then applies different rules for detecting any malicious behavior. If it is found, this module gives appropriate alert to administrator so that he can take necessary action.

II. LITERATURE SURVEY

As the paradigm shifts toward pervasive networking, security challenges get harder. One of the most important aspect of security is to detect and prevent attacks in real-time. Computers undergo many attacks. Attacker may exploit vulnerability to achieve its aim. There are 5 major types of attacks that are observed over the period of time: Each of this type troubles user in different ways. Each type of attack has its own motive and signature depending on the particular attack.

Architecture of Intrusion Detection System

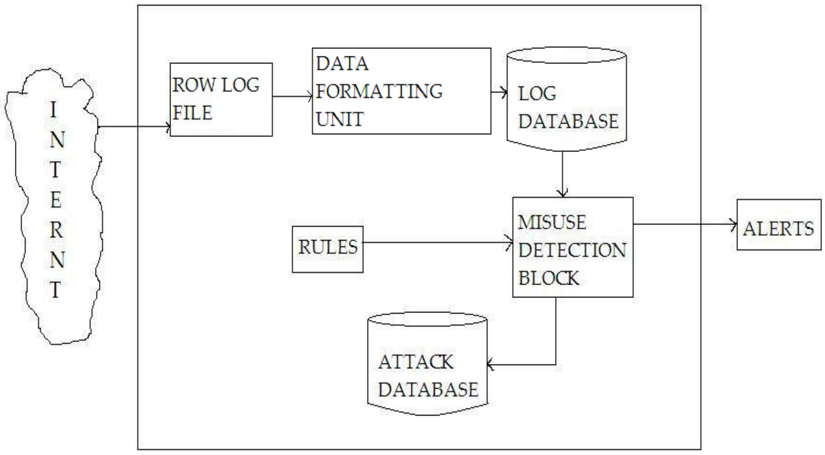


Fig. 1 Block Diagram of Intrusion Detection System

The figure shows the block diagram of Intrusion Detection System. It consists of following blocks: **Log File:** Packet sniffer Win Dump collects packet headers of data coming from internet or LAN. Data captured from WinDump is redirected to a file. This file is called as log file. **Data Formatting Unit:** Data collected in log file is classified according to various fields in the packet header. Protocols used for different packets are identified using some specific fields or predefined values of these fields. **Log Database:** It contains different tables according to different protocols (like TCP/IP, UDP, ICMP, and ARP). For each protocol there is one table. Each table consists of attributes related to that particular protocol. Formatted Data is stored in the database. **Misuse Detection Block:** Misuse Detection technique is used for detection of known attacks. Many computer attacks have fix signature. These attack signatures can be used to identify particular attack. We use predefined rules and compare the captured data packet header with them. If pattern matches, intrusion detection system declares it as intrusion and alerts administrator about it. **Attack Database:** Attack database also contains tables for different protocols as in case of log database. The entries from log database which are declared as attacks are stored in attack database. This database can be referred in future for drawing some conclusions or as a table showing statistics of past attacks on the system.

III. IMPLEMENTATION OF INTRUTION DETECTION SYSTEM

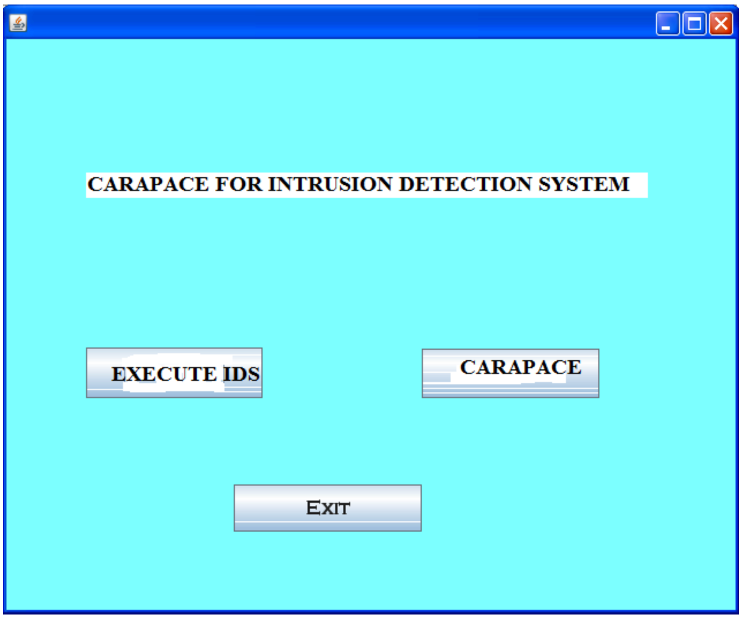
Environmental Setup: As introduced MS Access is the back end and java is used as front end. IDS are implemented for windows environment. IDS have following requirements: Windows 95/98/2000/XP, RAM 128 MB, Space requirement (on disk) 50 MB, Intel/AMD processor, Win Dump, MS Access, Net Beans, JDK 1.5.0 Installation and executable files created using free source software istall4j and exe4j respectively. Along with installation file user requires the Win Dump to collect the traffic data.

Algorithms' used: Data Capture: Two ways to Capture Data: 1) Redirecting to a Text file. e.g. D:\windump folder>Win Dump>filename.txt This will create a file named "filename" in the same directory where Win Dump is placed and the greater than operator will make the data captured by Win Dump to put in that text file. This method uses ">" operator as a redirection operator which converts binary data in the human readable format.

IV. CONCLUSION

Intrusion Detection System is the major aspect of network computer security. Unlike firewall, it does not block particular data but keeps track of incoming data and determines whether any intrusion is underway or not. it also has records of previous attacks for future reference. IDS prevent the intrusion in first place itself. And if not possible notifies the user and brings system back on track. We went to analysis and design phase of paper. We tried to understand scope of our project and tried to analysis different aspects, identified real life entities that may be considered for project. We have drawn EER diagram, Data flow diagram and component diagram. We have implemented an Intrusion Detection System to detect various well known attacks. Intrusion Detection approach, that we have used is NIDS (Network Intrusion detection System). So our system captures network data using Win Dump and detects attacks based on captured packet header information. There is other approach called Host based Intrusion Detection System. This approach makes extensive use of system log file and detects system attacks such as failed login attempts, suspicious file data changes etc. As we have used only NIDS approach to implement IDS our IDS cannot detect attacks such as unauthorized data access, unauthorized system logins etc. To make the system immune to this type of attack we can implement Host based IDS that is able to detect such attacks. This will make system more secure. As we can understand any one approach (either Host based or Network IDS) is never going to be enough to provide the complete security for the system. So we need to implement Hybrid Intrusion detection approach. Hybrid Intrusion Detection makes use of both NIDS and Host based IDS. Both the approaches used together will provide complete safety to user (at least best possible security). Our Intrusion Detection System is implemented for single computer machine. Many times it is desirable for organization to monitor their whole Local Area Network for any possible intrusion. In that case it is more suitable to have one dedicated Intrusion Detection server machine that monitors complete the Local Area network for intrusion. This keeps the centralized track of any intrusion rather than having to worry about intrusion on every single machine separately. Also keeping single centralized server updated is comparatively easy task. In big organization this becomes helpful since it is easy for administrator to keep track of single dedicated Intrusion detection server. Also there can be separate official to monitor the server and keep it updated.

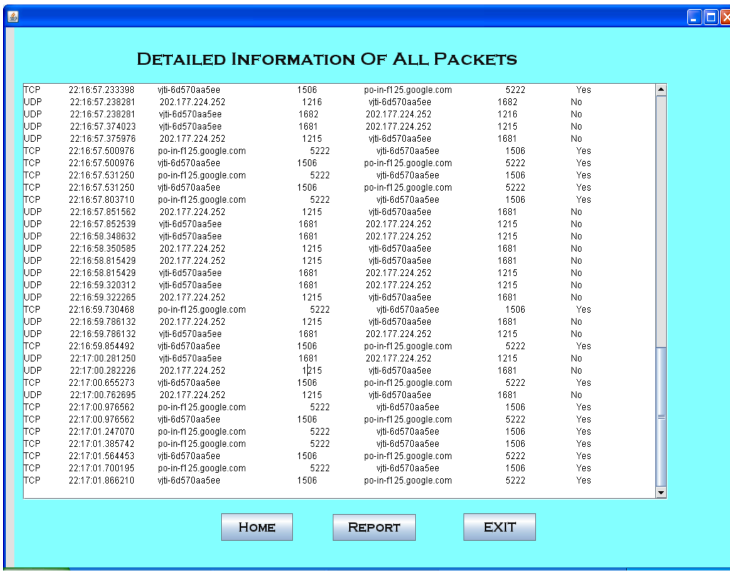
APPENDIX -A



SCREEN SHOT 4.1 Home window

It has three buttons RUN IDS, ATTACKS, EXIT. If you click RUN IDS, IDS will start scanning data and check if there is some malicious behavior. While running simultaneously, it will display information about captured packets in a separate window. This window is as shown below:

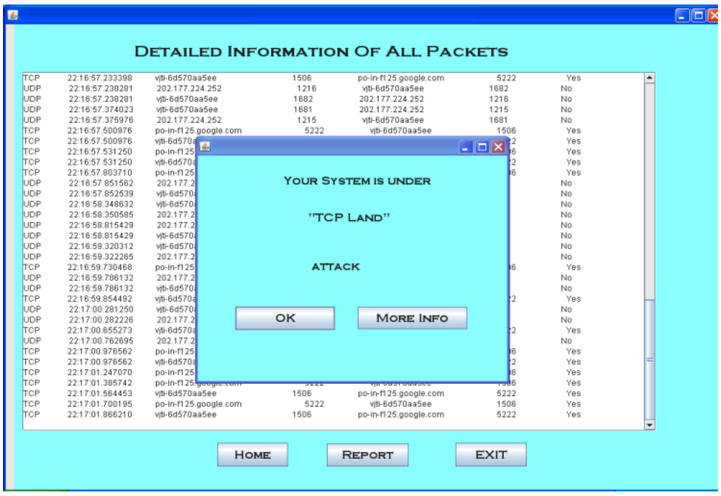
APPENDIX-B



SCREEN SHOT 4.2 Captured Packet Info window

If IDS finds some intrusion it will give alert. This window gives alert to administrator that the system is under attack and it also give the name of particular attack. Alert window is as shown below:

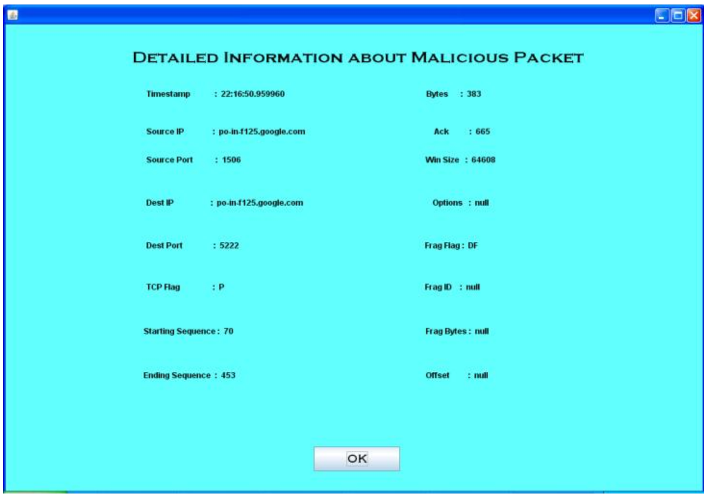
APPENDIX-C



SCREEN SHOT 4.3 Alert Window

If OK button is clicked, Alert window is removed and IDS. If MORE INFO button is clicked, it will take to Malicious Packet Info window. This window will show content of packet header of malicious packets. Malicious packet window is as shown below:

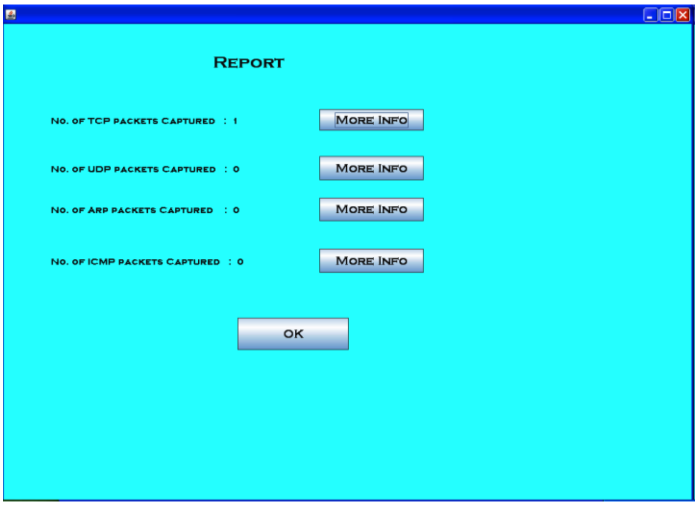
APPENDIX-D



SCREEN SHOT 4.4 Malicious packet window

If OK button is clicked, control will again return to Captured Data window. On Captured Data window, if REPORT button is clicked, Report window is displayed. Report window is as shown below:

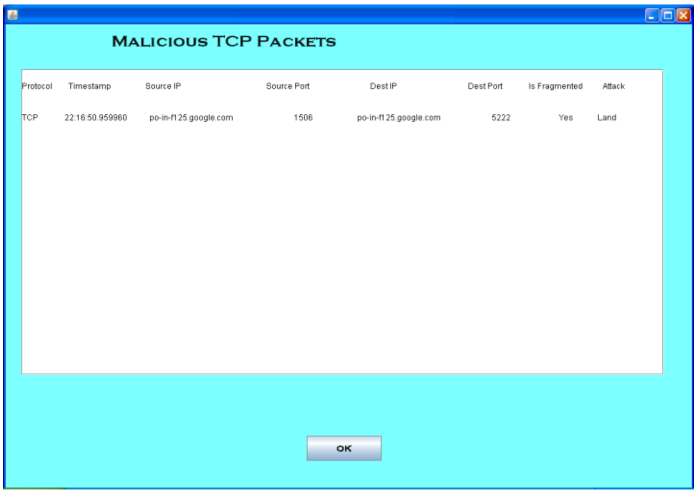
APPENDIX-E



SCREEN SHOT 4.5 Report window

This window shows count of total packets captured for each type of packet. If OK button is clicked, control will be returned to Captured Data Window. MORE INFO button will take to the new window, Malicious Report Window. This window shows information about all attacks occurred until now from particular type of packets. Malicious Packet Report window is as shown below:

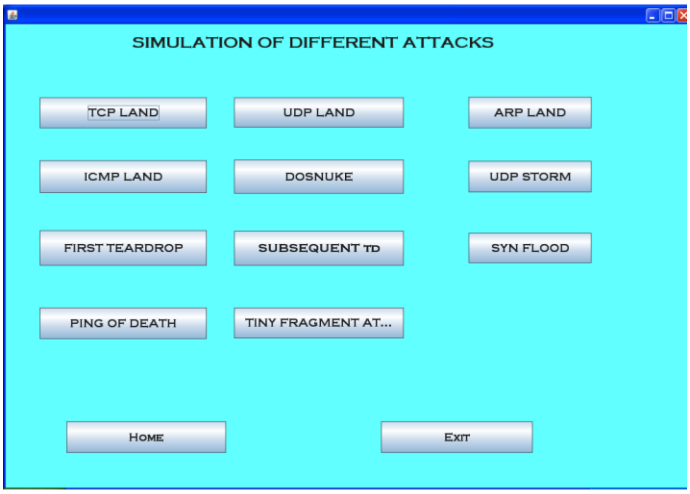
APPENDIX-F



SCREEN SHOT 4.6 Malicious Report Windows

If OK button is clicked it will return to Report window. Intrusion Detection System is running continuously but we cannot guarantee when attack will occur. Thus to check weather system is working properly we have simulated some of the attacks. To simulate attacks we have created some data files which already contain some malicious packet headers. These simulations can be done through Attack simulation window. In Home window there is ATTACKS button. If we click this button, this will take to Attack Simulation Window. This window contains many buttons each for one attack. If any one button is clicked, that type of attack is made on system and IDS will give appropriate alert. Attack Simulation window is as shown below:

APPENDIX-G



SCREEN SHOT 4.7 Attack windows

HOME button on any window will get control back to Home window. EXIT button on any window will tend to terminate IDS. After clicking EXIT button IDS will stop working.

References

1. Brian Kumar, Ronald Beekelaar, and Joern Wettern, PhD , (2003), Firewall for Dummies, Wiley Publishing, New 2.York.Andrew S. Tannenbaum, (2003), Computer Networks, Prentice hall publishing, New Jersey.Terry Ogletree, (2000), Practical Firewall, Prentice Hall Publishing, New Jersey
3. Margaret H. Dunham, (2008), Data Mining: Introductory and Advanced topics, Dorling Kindersley (India) Pvt. Ltd , New Delhi
4. XYZ, (200X), Firewall The Complete Reference, Tata McGraw Hill, New Delhi.
5. Korosh Golnabi, Richard K. Min, Latifur Khan, (2003), Analysis Of Firewall Policy Rules Using Data Mining Techniques,

6. http://www.google.co.in used for various purposes like finding various documentations and papers previously presented on firewall and data mining technique
7. Axelssion.intrusion Detection Systems: A Survey and Taxonomy.Technical Report 99-15, Department of Computer Engineering, Chalmers University,march 2000.8. Tcpdump: www.tcpdump.org
9. Y. Chen, Y. Li, X. Cheng, L. Guo, "Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detectio System", Inscrypt 2006.
10. http://kdd.ics.uci.edu/databases/ kddcup99/ task. Html. Accessed on Dec 1, 2007.
11. G. Stein, B. Chen, A.S. Wu, K.A. Hua, "Decision tree classifier for network intrusion detection with GA-based feature selection", In proceedings of the 43rd ACM Southeast Regional Conference - Volume 2, Kennesaw, Georgia, USA, March 2000.
12. Yan-heng Liu, Da-xin Tian, Da Wei, "A wireless intrusion detection method based on neural network", Proceedings of the 2nd IASTED international conference on Advances in computer science and technology, Puerto Vallarta, Mexico, January 200613.
13. T.M. Khoshgoftaar, S.V. Nath, S. Zhong N. Seliya, "Intrusion detection in wireless networks using clustering 2techniques with expert analysis", Proceedings of the FourthInte inational Conference on Machine Learning and Applications, December 2005
14. E. Al-Shaer and H. Hamed. "Firewall Policy Advisor for Anomaly Detection and Rule Editing." *IEEE/IFIP Integrated Management Conference (IM'2003)*, March 2003.
15. Li Hongwei, Yang Shoubao, Ren Anxi, etc. Research on IDS-based Distributed Firewall System [J]. Compute,Engineering.2005 Vol.31, http:Htech.sina.com.cn/2003-05-12/19153.html 560
16. Yuan Zhanting, Feng Tao, Yang Peng. Investigation of Integrated System of Distributed Intrusion With Firewall and It's Implementation [J]. Journal of Lanzhou University of Technology, 2005, Vol.3 1, No.1
17 D. Nayak, N. Rajendran, D.B. Phatak, V.P Gulati, "Security issues in mobile data networks", Vehicular Technology Conference VTC2004-Fall, 26-29 Sept. 2004.
18. Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, and Valtteri Niemi, UMTS Networks Architecture, Mobility and Services, 2nd Edition, John Wiley & Sons, Ltd., 2005.
19. www.keyfocus.net/kfsensor
20. http://www.shorewall.net
21. http://simonzone.com/software/guarddog
22. http://firewall-jay.sourceforge.net
23. http://www.privoxy.org
24. http://www.netnanny.com
25. http://www.cyberpatrol.com
26. http://www.lib.ru/SECURITY/gauntlet.txt#14
27. http://dansguradian.org
28. http://www.ipcop.org
29. http://smoothwall.org
30. Snort: www.snort.org
31. Tcpdump: www.tcpdump.org

