Minor Project- Report

Aug 2021 – Jan 2022

Course Faculty: SWAPNA MAM Course Name & code: Computer Networks Semester: 5 Date:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TITLE OF THE PROJECT | **Intrusion Detection System** | | | |
|  |  | | | |
| STUDENT NAME | **XITIZ VERMA** | **YUKTA N SHETTIGAR** | **BHARGAVI S** | **YASHASWINI SHREE** |
| USN | **1DS19CS193** | **1DS19CS197** | **1DS19CS198** | **1DS19CS196** |
| INDIVIDUAL  CONTRIBUTION |  |  |  |  |
| GUIDE | **SWAPNA MAM** | | | |
|  |  | | | |
| PROJECT ABSTRACT : | **Intrusion Detection System** is a software or a device that can monitor all the suspicious activities in the network or that activities that violates its policy.  IDS is very popular system to protect the networks from different types of attacks. Any intrusion activity or violation is reported or informed either to administrator or this information can be centrally collected in a system called SIEM (Security Information and Event Management). It collects and combine information from different sources and it uses alarm filtering techniques.  There are two most common types of IDS  - (NIDS) Network based Intrusion detection system and  - (HIDS) Host based Intrusion detection system.  **HIDS** is used for monitoring important operating system files and **NIDS** are used to analyze incoming network traffic. Here's how IDS work, IDS when placed at a strategic point or points within a network to monitor traffic to and from all devices on the network, an IDS will perform an analysis of passing traffic, and match the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behaviour is sensed, the alert can be sent to the administrator.  **Modern Networked Business Environments** require a high level of security to ensure safe and trusted communication of information between various organizations.  An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber-attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats. | | | |
|  |  | | | |
| Introduction | An IDS is basically a software or device that is categorised into two common parts one is NID i.e. Network Intrusion Detection and second is HID i.e. Host Intrusion Detection. The work of both the NID & HID is same but their level is different. But IDS are categorised into 5 types - NIDS, HIDS, PIDS, Hybrid IDS & APIDS. Work is same to detect intrusions but they are used at different levels.    In the above Figure we are now clear that where HIDS are used and where NIDS are used.  In this project we have implemented **Intrusion Detection System** by creating 3 different networks as in Figure. Implementing the IDS is very challenging task as it needs the implementor to have proper knowledge with prior knowledge with some common and special network devices and ethernet cables. One have to know that how to deal with the CLI i.e. Command Line Interface. As we are performing this project on Cisco Packet Tracer – the best available simulation tool which allows users to see the working of network in real time.  A layout of the network should be made prior to the implementation of IDS as we are implementing NIDS. There are various parameters which are to be kept in mind while We designed network and configure IDS. Here are some 'can's and can not's about the IDS :  - CAN recognize and report alterations to data.  - CAN detect when your system is under attack.  - CAN detect errors in your system configuration.  - CAN NOT analyse all the traffic on a busy network.  - CAN NOT prevent system from that attack which it detects.  - CAN NOT deal with some of the modern network hardware and features. | | | |
|  |  | | | |
| LAYOUT AND Design | **Goals and Specifications**  The Design goal of this project is to implement and test a stable and secure IDS that can be used to secure any type of network. It also has the ability to immediately inform the administration about the intrusion or any suspicious activity. It collects all the different protocols and traffic information directly to the admin of the network and after informing the admin the work of the IDS is completed, next admin decides what to do with this traffic, whether to continue the traffic or block.  The Final IDS design after all the configurations it should meet the following specifications:  1. The IDS must be capable of detecting the type of traffic which admin assigned to it.  2. The IDS must be capable of informing admin about any suspicious activity related to the signatures assigned by the admin.  3. The IDS should create a log report in the server which is specifically meant for logging these activities.  4. The IDS must be capable of scanning the traffic which is entering inside the network.  **Project Layout Stage**  The network layout stage includes the whole network blueprint that on which type of network our IDS will be implemented. We are using 3 different types of networks which has some hosts and servers inside it.  **NETWORK 1**    **Devices in this Network 1 -**  - 4 Different PCs  - 1 SYSLOG Server  - I Printer  - 1 Switch as shown in Fig 3.1  The **First Network** is made of IPv4 Addressing having the IP addresses in the range of  192.168.10.2-192.168.10.8 Default Gateway for this Network is 192.168.10.1  **NETWORK 2**    **Devices in this Network 2 -**  - 4 Different PCs  - 1 FTP Server  - 1 Printer  - 1 Laptop  - 1 Switch as shown in Figure  The Third Network is made of IPv4 Addressing having the IP addresses in the range of  192.168.30.2-192.168.30.4  Default Gateway for this Network is 192.168.30.1  **NETWORK 3**    **Devices in this Network 3 -**  - 1 PC  - 1 Laptop  - 1 Switch as shown in Figure  3 (1941) Routers are used to connect all these 3 LANs together. Dynamic routing is used to route traffic all across 3 networks.  **Networks Connected with Router 1 (router0)**  - 192.168.1.0  - 100.0.0.0  - 10.0.0.0  **Networks Connected with Router 2 (router!)**  - 192.168.30.0  - 10.0.0.0  - 20.0.0.0  **Networks Connected with Router 3 (router2)**  - 192.168.10.0  - 20.0.0.0.  **Implementation of NIDS using CLI**  Now the main task has reached. We have to apply IDS into network for securing it.  Our IDS will be implemented on Router0 on interface (gigabit ethernet 0/0). Our IDS will scan all the ICMP traffic which is coming into the Network 1 from this interface.  For implementing IDS on router0 we have to firstly activate security package of that router. We have activated 'securityk9' package and IPS Signature 2004 as shown in Figure.  **Commands for Implementing IDS –**  There are various commands used for implementing and enabling IDS on that specific interface.    **Testing NIDS & SYSLOG -**  For our project we have used dynamic routing concept because it is more easy to use.  Another task for configuring this network was configuration of Servers i.e. Syslog, HTTP, FTP. For Syslog server I have turned down all the service except logging service called \*SYSLOG' so that it can focus only to logging information come from IDS. | | | |
| PLATFORM USED/ REQUIREMENTS  (HardWare and Software tools used) | To implement this project we have to meet some software and hardware requirements.  For **Software Requirement** it is required to have (CISCO PACKET TRACER) installed on the System. Every implementation is done on this tool.  For **Hardware Requirement** it is required to have the followings   * Intel Pentium 4, 2.53GHz or equivalent Processor * 2GB Ram * 1GB of free storage space * Display of resolution 1024\*768 * Language fonts supporting Unicode encoding * Latest video card and OS updates | | | |
|  |  | | | |
| Project Source Code Link (Github/ Google DRive) | ***https://github.com/XitizVerma/Intrusion-Detection-System*** | | | |
|  |  | | | |
| Conclusion /FUTURE ENHANCEMENT | **Future Work -**  In future reference we need to work on the Honeypot System to implement and work the Intrusion Prevention System along with the Intrusion Detection System.  **Summary -**  In this phase of the projects we delt with the difficulties that aroused from the testing and improving the IDS System, also we learnt how to use the command lines and use features of cisco like Syslog and Ping monitorisation.  **Conclusion -**  In this project of implementing an Intrusion detection System using Cisco Packet Tracer, we created a network using different components likes PC's, Routers, Switches, Servers, Connecting Wires, Hubs, etc.  After Connecting the network, we accessed the networks and allotted different protocols to different components like FTP, HTTP etc. to servers, IP's to all the devices in the network, And Shared ICMP packets through the network to ensure its flawless working.  Then we fed and flooded the network using Pings and monitored the ping, type of message and connection status. This was done to test the NIDS and implemented the IDS. | | | |
|  |  | | | |
| Ui sCreenshots | **IDS NETWORK TOPOLOGY** | | | |