**PROJECT SYNOPSIS**

**SYSLOG SERVER**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DEPARTMENT | Computer Science & Engineering | | | |
| TITLE OF THE PROJECT | Syslog Server | | | |
|  |  | | | |
| STUDENT NAMES/ USN/ PHONE/ MAIL ID | Madhulika Singh | Madugundu Lingesh Rohith | Mahantesh Masali |  |
| 1DS20CS113 | 1DS20CS114 | 1DS20CS115 |  |
| 9461165611 | 8147120063 | 7349727709 |  |
| madhulikarathore02@gmail.com | rohithml0588@gmail.com | vishalmasali759@gmail.com |  |
| PROJECT TIMELINE  (Tentative Start date- End Date) | Sept 2022 to Jan 2023 | | | |
| PROJECT GUIDE | Dr. Nagaraj J | | | |
|  |  | | | |
| PROJECT - Domain | Computer Networks | | | |
| Introduction | Syslog stands for **System Logging Protocol**and is a standard protocol used to **send system log or event messages to a specific server**, called a syslog server.  It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.  Monitoring numerous logs over an equally numerous number of routers, switches, and systems would be time consuming and impractical. Syslog helps solve this issue by forwarding those events to a centralized server.  Traditionally, Syslog uses the UDP protocol on port 514 but can be configured to use any port. In addition, some devices will use TCP 1468 to send syslog data to get confirmed message delivery.  The syslog servers have the following components: Syslog listener, database, Management and filtering software. | | | |
| Application/s | Event monitoring & Network monitoring. Also used for troubleshooting or rolling back the system after a failure accident. | | | |
| Challenges in the CURRENT WORK | • One major limitation of the syslog protocol is that the device being monitoring must be up and running and connected to the network to generate and send a syslog event. A critical error from the kernel facility may never send an error at all as the system goes offline.  • As syslog messages are sent via UDP, so messages aren’t acknowledged or guaranteed to arrive.  • There is no mechanism to poll the syslog data. | | | |
| PROJECT Problem STATEMENT | Design, simulate and analyze a sys log server in order to send the log information of all our network devices such as interface status, system restarts etc. to one centralized place. | | | |
| OBJECTIVEs OF THE PROJECT | Syslog server provides :   * Security * Authentication * Monitoring | | | |
| Proposed Solution | The syslog server can be used to configure alerts to notify us of problems coming through syslog. Syslog traffic can be encrypted using TLS which provides mutual authentication between the remote server and the clients, thereby preventing man-in-the-middle attacks. | | | |
| PlaTform that will be used for implementation  (Name the hardware and Software tools and Development Environment  that you will be using for implementation) | Software :  Cisco Packet Tracer Simulation Tool  Hardware :  None | | | |
| Demonstration Details | ( UI ) | | | |
| References | [1] K. Slavicek, J. Ledvinka, M. Javornik and O. Dostal, "Mathematical Processing of Syslog Messages from Routers and Switches," 2008 4th International Conference on Information and Automation for Sustainability, 2008, pp. 463-468, doi: 10.1109/ICIAFS.2008.4783957.  <https://ieeexplore.ieee.org/document/4783957>  [2] Shenglin Zhang et al., "Syslog processing for switch failure diagnosis and prediction in datacenter networks," 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), 2017, pp. 1-10, doi: 10.1109/IWQoS.2017.7969130.  <https://ieeexplore.ieee.org/document/7969130>  [3] Nadean H. Tanner, "Managing Logs," in Cybersecurity Blue Team Toolkit , Wiley, 2019, pp.109-124, doi: 10.1002/9781119552963.ch9.  <https://ieeexplore.ieee.org/document/9823036> | | | |