CPE – 691 -- Project Proposal

Topic: State-of-the-art Intrusion Detection Systems (IDS) for Cloud Computing

Members: Lokesh Mishra, Rohan Karki & Sri Dhanush Reddy Kondapalli

Abstract: Intrusion Detection System (IDS) is a very crucial part of SOC, i.e., Security Operations Center, which plays a huge part in preserving system security for any organization. An IDS monitors a network for any malicious activity or security policy violations. Any such violation is reported and stored within a Security Information and Event Management (SIEM) system. The selected topic focuses on implementing this IDS onto cloud computing. The resulting research paper will initially explain the working of cloud system and then present the implementation of IDS to improve the level of security. Unlike the traditional computing system, cloud computing works on a different platform and uses different kinds of resources resulting in different types of security threats/vulnerabilities. In this state-of-the-art IDS, network traffic is mirrored, which then is inspected by a SOC team which will scan the network for threats. The system uses multiple VMs to inspect the network traffic on a cloud system and detects any lateral movement. Since cloud computing stands for scalability, elasticity, reliability and performance, the state-of-the-art IDS which is mentioned in this topic will satisfy all the mentioned requirements and provide ultimate security.