Network Intrusion Detection and Prevention in Organizations

Mohammed Al Madhi and Daniel Kearl

Final Project Team 14

University of Louisville - College of Business

Proposal

The focus of our project is on Network Intrusion Prevention and Detection. We plan to introduce the idea of network vulnerabilities and describe those that can be common in the workplace, then move on to describe methods of detection and prevention of these threats. There is also a small portion over recovery methods and topics that should be considered immediately after a threat has been brought under control. Finally, we will wrap up our research by attempting to relate it to the average employee, describing what they should be doing to keep their workplace network as secure as possible.

The following table of contents has been created with the paper and the presentation in mind, so if all goes to plan then both will be following it, though the presentation will likely do so more loosely. Our general plan is to approach this topic with the average person (as an employee of a business) in mind, hence the overview of networking and network vulnerabilities and tying things back into the average employee's contribution to security.

Network security and intrusion prevention systems are never perfect, but with multiple layers of security, an organization is better protected against threats of network intrusion. Network intrusion occurs when someone attempts to gain access to the organization's network for nefarious purposes, whether it is only to disrupt or to infiltrate. Well, how do we stop it? Using an Intrusion Detection and Prevention System (IDPS), the purpose of which is to prevent, identify, and report and harmful activities, is crucial to the information security of a business or other organization. In the case of an intrusion, the attacker might have gained access to data that may include clients' and employees' private information, highlighting the importance of detecting and preventing intrusion attempts in such an environment.

TABLE OF CONTENTS