Timothy Rine

ISDS 4120

Dr. Schwarz

Hands-On Assignment #6

1. There are a couple of main points to consider relating to the ethical issues of packet sniffing. First is a property issue. Who owns the right to the information and controls the access points? Packet sniffing allows an organization or company to control the intellectual property of its employees by monitoring them at an individual level. Another point to consider is whether or not packet sniffing is an invasion of privacy. Employees will likely form interpersonal relationships at work. If an organization decides to prohibit communication between employees, then can they use packet sniffing to find communication between employees and fire them for it?

2. I think that packets captured during a web page request could be useful for debugging communication between clients and servers in an organization. By analyzing the information received, an organization can fix bugs in their networking system which ultimately benefits the organization. Also, analysis of these packets can provide an entity with information about potential security risks.

3. The packet capturing process changes depending on whether the network uses hubs or switches. In a hub, data that is received at one port is transmitted to all of the others. This means that if you are viewing packets running at one port you will also see data sent throughout the entire hub. This is contrasted with a switch where you would only see packets from one machine and not the entire system.

4. Packet sniffing is more difficult over wired networks than wireless networks. In a wired network you need a physical connection and installed software to perform packet sniffing whereas over a wireless network a hacker or malicious user only needs to crack some passwords to get access to the network. I looked up packet sniffing software and found “Wireshark” and “Cain and Abel” as two programs that anyone can use.