Tim Reilly

Professor Memo

Data Science Fundamentals

11 December 2019

Tracking slackers at work

This program was designed to track the internet usage of users, ultimately to determine how likely they are to slack at work and visit malicious sites at work. I believe that most people at work tend to not focus on the work that they are supposed to be doing and will like to slack off and look at sites they should not be using on company time. To combat this I have created a program that analyzes wireshark data captures, and analyzes them compared to a list of disapproved sites and approved sites. The website queries made will determine if the user is therefore a responsible employee or a slacker at work. They may also be a danger at work which is why the user’s traffic will also be compared to a list of known dangerous sites that contain malware and other harmful code. Tracking websites visited will be able to decide what people that use your network will aid system administrators in deciding privileges of users.

To track users a wireshark packet capture will analyze tcp and udp packets sent over port 53 to find standard queries. This can track data such as what sites the user is visiting and how many times per day they visit it. A list of unapproved sites are hardcoded into the program to determine what sites the user visits that will categorize them as a danger to the network or if they will slack off at work. To analyze this data and graph it matplotlib was used to visualize the hits of bad websites as a bar graph. The results of this will vary as the data changes from network to network and the approved and blocked sites should be based on a companies group policy which are able to change at any time. For further data analysis the user could collect data over a period of time on a network and track the time that users are most likely to slack at work. An example could be if on Fridays at 3pm everyone starts to look at Facebook to see what their friends are doing over the weekend rather than work. If this is the case an organization can block access to facebook at that time to prevent users from being less productive.

After analyzing data produced from my own home network I will be able to see what users on the network are likely to be looking at internet sites other than doing homework to determine which one of the users is not doing their homework. It is important to take away from this exercise that your network traffic is able to easily be tracked and viewed by any company or institution that the internet is used. This information can be used in a variety of ways such as tracking trends of workers productivity so the company can be more productive, or used for malicious intents such as tracking the traffic of internet users so that advertisers can gather data about what websites are frequently visited in order to target advertisements.