**Systems Management - Session 9 - Seminar Activity 1: Security Tools and Controls**

**Links used:**

* <https://www.wireshark.org/>
* <https://jvns.ca/blog/2018/06/19/what-i-use-wireshark-for/>

**What Wireshark is and how it can be used:**

* Wireshark is the world’s foremost and widely used network protocol analyser. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.
* [Wireshark](https://www.wireshark.org/) is a graphical network packet analysis tool. It can be used to debug networking problems in production.

**PART A:**

* Instructions have been followed successfully
* I see that it is possible to gain form data from packet capturing
* It is quite dangerous, as anyone who connects to the network and fills in their private data, will be left vulnerable to cyber fraudsters

**PART B:**

* Wireless network transmission waves can be seen by outsiders, this possesses many security risks.
* WEP is the acronym for Wired Equivalent Privacy. It has security flaws which make it easier to break compared to other security implementations.
* WPA is the acronym for Wi-Fi Protected Access. It has  security compared to WEP
* Intrusion Detection Systems can help detect unauthorized access
* A good security policy can help protect a network.
* **Cain and Abel** (often abbreviated to **Cain**) is a password recovery tool for [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows).
* It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks