

**Computer Security**

**Tutorial 10:**

**Part 1: Open Source vs. Commercial**

For each of the following network security tool categories, locate a real world example, determine if the tool is open source or commercial, and write a brief description / purpose of the tool.

1. Packet sniffer / Protocol analyser
2. Network fingerprint tool
3. Vulnerability scanner
4. Network intrusion detection system
5. Honeypot / honeynet
6. Personal firewall

Should you wish to test or play around with any of the tools you find and download, it is recommended that you do so in an isolated environment or virtual machine, and scan the downloaded files for malware.

**Part 2: Home Network Security**

Home networks connected via an ADSL router/modem are notoriously poorly protected. Research and brainstorm the factors which make securing a home network difficult. Do some research on protecting a home network and compare this to the existing safeguards you have implemented on your own network.

**Part 3: Advanced Question**

Suppose you want to use an Internet cafe to login to your personal account on a bank web site, but you suspect that other computers in this cafe are infected with software keyloggers.

Assuming that you can have both a web browser window and a text editing window open at the same time, describe a scheme that allows you to type in your userID and password so that a keylogger, used in isolation of any screen captures or mouse event captures, would not be able to discover your userID and password.