**Module 5 Malware**

**5.2 Malware Lab Intro**

**Ports**

1. Connection/interface between devices
2. Includes network wired connections, wireless connections & OS processes

**Stinger**

1. Free tool from Mcafee that allows for detection & removal of viruses & other malware

**Currports**

1. Displays a listing of all current open TCP & UDP ports on local comp
2. Automatically marks suspicious TCP/UDP ports owned by unidentified apps
   1. It mas them in pink

**TCPView**

1. Shows you detailed list of all TCP & UDP endpoints on system including state of TCP connections

**What’s Running**

1. Shows you processes running on machine

**Hashcalc**

1. Allows you to generate hashes for file integrity

**Trojan Protection**

1. Stinger – Antivirus program
   1. Download & install Stinger (don’t, Mcafee sucks)
   2. Open cmd in stinger directory
   3. Type, stingerc.bat
      1. Initialised batch file
   4. Use stinger to scan machine
      1. Can check logs for scan info
2. Currports – give info on diff ports running on machine
   1. Run cports.exe
   2. Select protocols column header – sorts protocols
   3. Click process name then click local port name column headers
      1. Sorts processes & port names
   4. Can see all info of ports
      1. Name, listening or not etc.
      2. Can analyse if attacked
3. TCPView – similar to currports
   1. Run tcpview.exe
4. What’s Running – show processes & ports running
   1. Run setup.exe
   2. Processes tab – show what’s running on machine
   3. IP connections columns
      1. Can filter out processes
   4. can filter drivers, change startup processes, take snapshot etc.

**HashCalc**

1. Perform hash calculations
   1. This thing is outdated though, doesn’t have Bcrypt
2. Download & install hashcalc
3. In hashcalc under data, select hashcalc app file
   1. Keep default hash type selections & click calculate
4. Checking HMAC (Hash Message Authentication Code) will only allow specified number of hash types to be calculated
   1. Can give your own key value (the key is supposed to be kept secret)
5. Can change data format of input too