**LAB (2) – Configure Snort**

* <https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/>
* Download WinPCAP from <https://www.winpcap.org/install/default.htm> , then download snort from <https://www.snort.org/downloads> and select .exe file installer, install both of them
* Download rules from <https://www.snort.org/downloads> I download Snort v3 rules (requires sign in), copy the rules to c:\Snort\rules folder.
* cd c:\snort\bin then write the command snort –V command to show the snort version
* snort –W, to view all the connections
* snort -dev -i 6, interface number 6 is the currently running interface, (you have to configure your internal network range.
* Replace ipvar to var
* Change HOME\_NET any to HOME\_NET 127.0.0.1/24, var EXTERNAL\_NET !$HOME\_NET
* Change the rule path to c:\snort\rules
* Change PREPROC\_RULE\_PATH to “ var PREPROC\_RULE\_PATH c:\rules\preproc\_rules “
* Got to “step 4: configure dynamic libraries” and change the paths too, C:\Snort\lib\snort\_dynamicpreprocessor, C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll, C:\Snort\lib\snort\_dynamicrules
* You will find problem with WiFi connection because of WPA/WPA2 encryption
* Still check if you can still able to work the command, snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 6, where 6 is the interface index obtained from snort –W.
* Open rules and see its content.