**snort**

Download snort.exe and snort snapshort.tar

Install snort;

Check in cd > dir

Cd snort

Cd bin

Check if available

Go check windows exploration c:; etc, snort,…

Copy snapshort extracted to snort in windows explroration

Extract to the rules in snort

Go to to snort .conf and do the change.

Cmd snort/bin > snort -w /interfaces

Snort -i 4 -c c:\snort\etc\snort.cont -T for checking error

Config the white.list and black.list

Local.rules

Alert icmp any any -> any any (msg:”testing ICMP alert”; sid:1000001;)

Alert udp any any -> any any (msg:”testing udp alert”; sid:1000002;)

Alert tcp any any -> any any (msg:”testing tcp alert”; sid:1000003;)

Snort -I 5 -c c:\snort\etc\snort.conf -A console

|  |  |  |
| --- | --- | --- |
| line | Before change | After change |
| 45 |  | ipvar HOME\_NET 192.8.0.0/24 |
| 48 |  | ipvar EXTERNAL\_NET !$HOME\_NET |
| 104 |  | var RULE\_PATH c:\snort\rules |
| 105 | # | #var SO\_RULE\_PATH ../so\_rules |
| 106 |  | var PREPROC\_RULE\_PATH c:\snort\preproc\_rules |
| 113 |  | var WHITE\_LIST\_PATH c:\snort\rules |
| 114 |  | var BLACK\_LIST\_PATH c:\snort\rules |
| 186 | (REMOVE) # AND ADD SOME… | config logdir: c:\snort\log |
| 247 |  | dynamicpreprocessor directory C:\Snort\lib\snort\_dynamicpreprocessor |
| 250 | CHANGE path and name of file | dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll |
| 253 | comment | #dynamicdetection directory /usr/local/lib/snort\_dynamicrules |
| 265-269 | Comment all | #preprocessor normalize\_ip4  #preprocessor normalize\_tcp: ips ecn stream  #preprocessor normalize\_icmp4  #preprocessor normalize\_ip6  #preprocessor normalize\_icmp6 |
| 335 | # | #preprocessor bo |
| 418 | Remove comment | preprocessor sfportscan: proto { all } memcap { 10000000 } sense\_level { low } |
| 511 | Change line and create white.list and save it in rules | whitelist $WHITE\_LIST\_PATH\white.list, \ |
| 512 | Change line and create black.list and save it in rules | blacklist $BLACK\_LIST\_PATH\black.list |
| C:\ | C:\snort\rules\black.list | # Snort blacklist file  # List IP addresses here, one per line  # |
| C:\ | C:\snort\rules\white.list | # Snort whitelist file  # List IP addresses here, one per line  # |
| 546-661 | Change slash/ | \ |
| 659-661 | No comment/remove # | include $PREPROC\_RULE\_PATH\preprocessor.rules  include $PREPROC\_RULE\_PATH\decoder.rules  include $PREPROC\_RULE\_PATH\sensitive-data.rules |