Final Year B.Tech. (CSE) – II [2022-23]

Cryptograpy and Network Security Lab

PRN: 2019BTECS00077

Full name: Avinash Vishnu Biradar

Batch: B7

Assignment No. 15

Title:

Snort Intrusion Detection System (IDS)

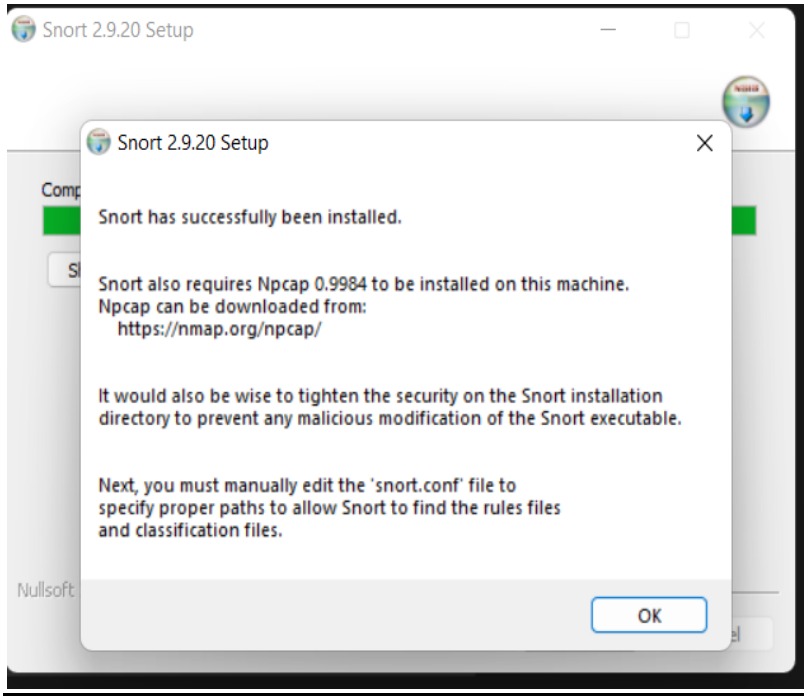
Aim:

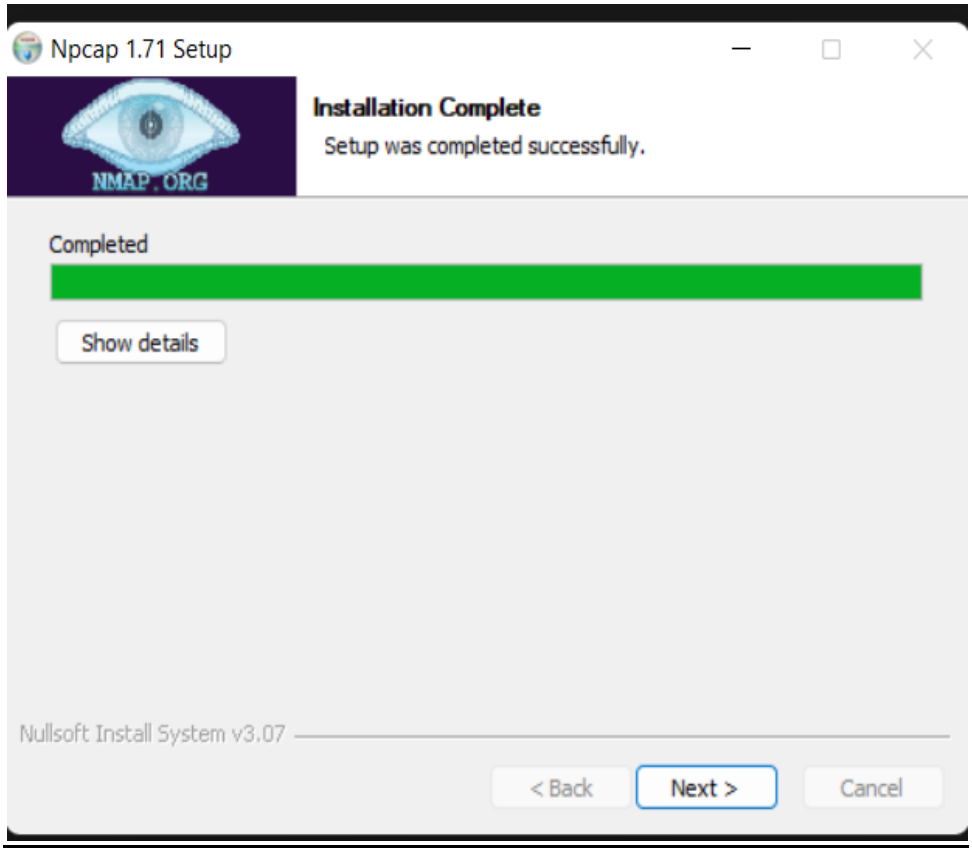
To Installing snort**.**

Theory:

Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Long a leader among enterprise intrusion prevention and detection tools

Process:


Snort 2.9.20 Setup
Snort 2.9.20 Setup
Snort has successfully been installed.
Snort also requires Npcap 0.9984 to be installed on this machine.
Npcap can be downloaded from:
https://nmap.org/npcap/
It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.
Next, you must manually edit the 'snort.conf' file to specify proper paths to allow Snort to find the rules files and classification files.
OK
Nullsoft


Npcap 1.71 Setup
NMAP.ORG
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel

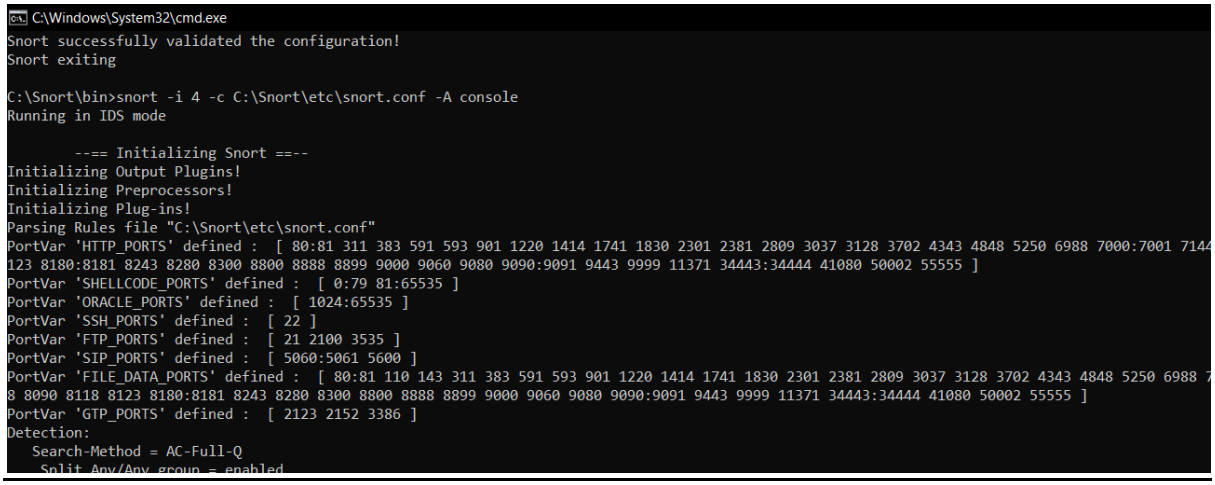
Output:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.

C:\Snort\bin>snort -i -1 -c C:\Snort\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine c:\Snort\lib\Snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor
Log directory = c:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
```

```
C:\Windows\System32\cmd.exe - snort -i 4 -c C:\Snort\etc\snort.conf -A console
11/29-14:25:09.813045  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0012:0000:0000:0000:0000:0239:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59115
11/29-14:25:09.813045  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0012:0000:0000:0000:0000:0239:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59115
11/29-14:25:09.813337  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59115 -> 2620:01ec:0012:0000:0000:0000:0000:0239:443
11/29-14:25:09.815053  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0012:0000:0000:0000:0000:0239:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59115
11/29-14:25:09.815116  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59115 -> 2620:01ec:0012:0000:0000:0000:0000:0239:443
11/29-14:25:09.923845  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:58926 -> 52.168.112.66:443
11/29-14:25:09.932453  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:53514 -> 239.255.255.250:1900
11/29-14:25:09.939733  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:54259 -> 20.198.119.84:443
11/29-14:25:10.120998  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 20.198.119.84:443 -> 192.168.43.2:54259
11/29-14:25:10.173461  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:54259 -> 20.198.119.84:443
11/29-14:25:10.720817  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:10.720978  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:10.955360  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59018 -> 2a03:2880:f26e:00c2:face:b00c:0000:0167:443
11/29-14:25:11.035537  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 3.232.1.102:443 -> 192.168.43.2:59101
11/29-14:25:11.035537  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 3.232.1.102:443 -> 192.168.43.2:59101
11/29-14:25:11.076323  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:11.138117  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a03:2880:f26e:00c2:face:b00c:0000:0167:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59018
11/29-14:25:11.344007  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a03:2880:f26e:00c2:face:b00c:0000:0167:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59018
11/29-14:25:11.387417  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59018 -> 2a03:2880:f26e:00c2:face:b00c:0000:0167:443
11/29-14:25:12.933765  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:53514 -> 239.255.255.250:1900
11/29-14:25:13.060922  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:13.061082  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:13.337801  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:50755 -> 239.255.255.250:1900
11/29-14:25:13.401227  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 3.232.1.102:443 -> 192.168.43.2:59101
11/29-14:25:13.401398  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 3.232.1.102:443 -> 192.168.43.2:59101
11/29-14:25:13.402606  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59101 -> 3.232.1.102:443
11/29-14:25:13.715449  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:13.800515  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 3.232.1.102:443 -> 192.168.43.2:59101
11/29-14:25:14.030461  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.2:59127 -> 13.107.21.200:443
11/29-14:25:14.119606  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.119778  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.120292  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.296847  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:58451 -> 192.168.43.1:53
11/29-14:25:14.297101  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:65059 -> 192.168.43.1:53
11/29-14:25:14.327191  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 13.107.21.200:443 -> 192.168.43.2:59127
11/29-14:25:14.327191  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.327191  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.327191  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.327426  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.331011  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.331011  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.331011  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.331181  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.331342  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125
11/29-14:25:14.331385  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.332362  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0042:0000:0000:0000:0000:0132:443 -> 2409:4042:0d85:09b8:9555:3248:e2d6:3614:58998
11/29-14:25:14.338116  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2409:4042:0d85:09b8:9555:3248:e2d6:3614:59125 -> 2620:01ec:0c11:0000:0000:0000:0000:0200:443
11/29-14:25:14.357042  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.43.2:50755 -> 239.255.255.250:1900
```



Conclusion:

Snort Analyze the traffic and generate the log file

Cmd –

snort -i -1 -c C:\Snort\etc\snort.conf -T

snort -i 4 -c C:\Snort\etc\snort.conf -A console