Name: Siddhi Lokhande
PRN NO: 2019BTECS00014

Title: Snort Intrusion Detection System (IDS)

Aim: To install and configure Snort Intrusion Detection System (IDS)

Objectives:

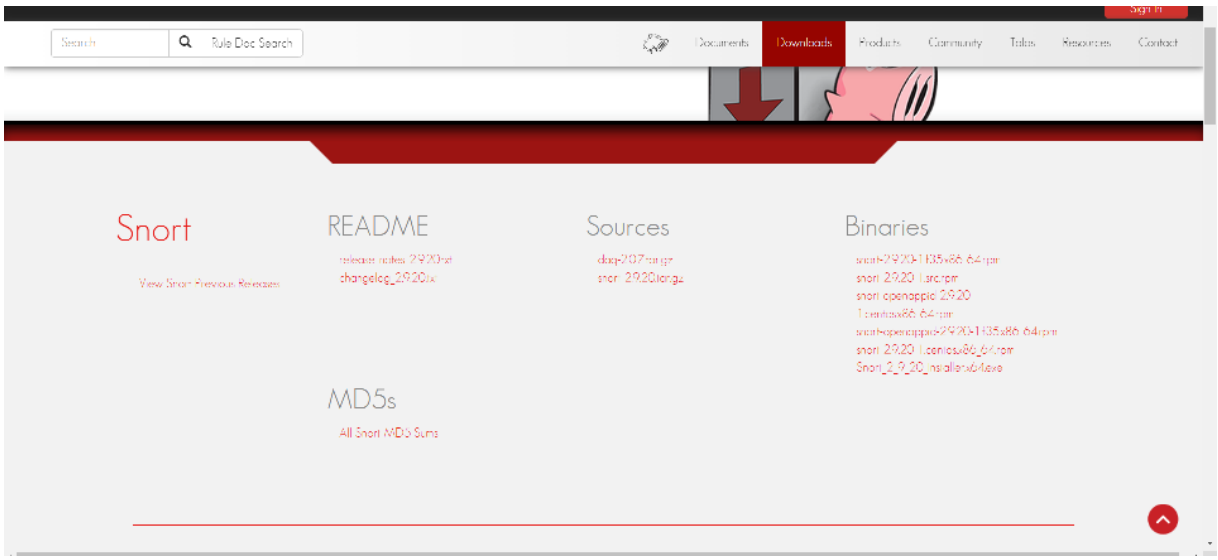
- To install snort ids
- To configure snort ids

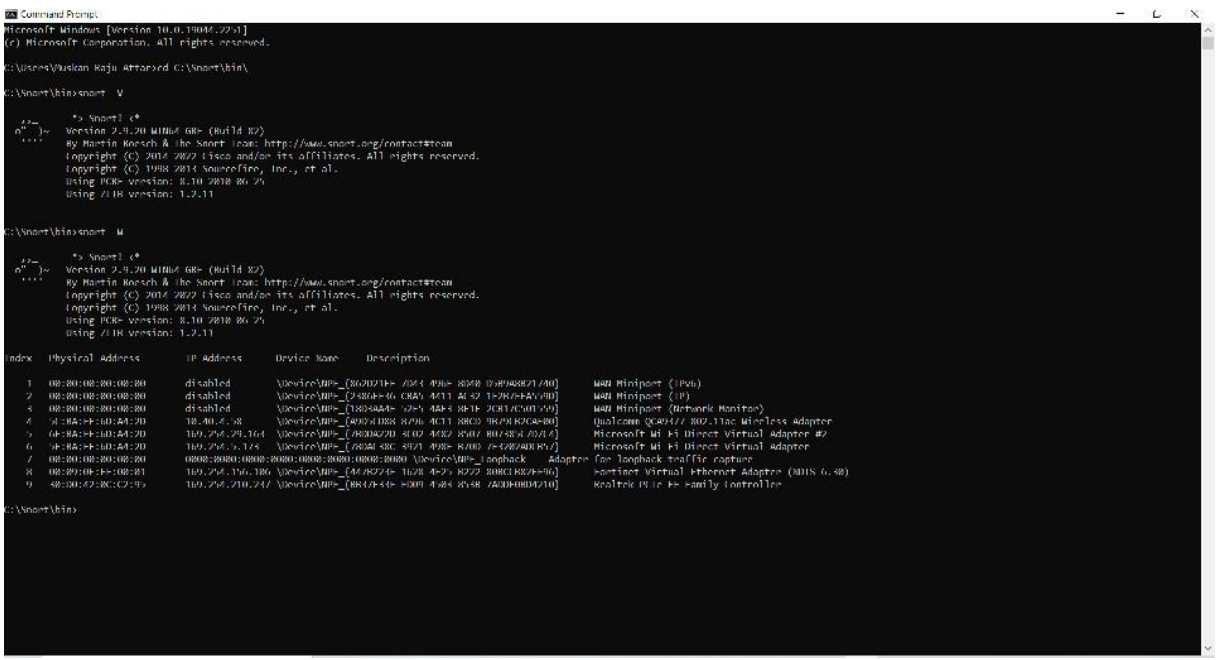
Theory:

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

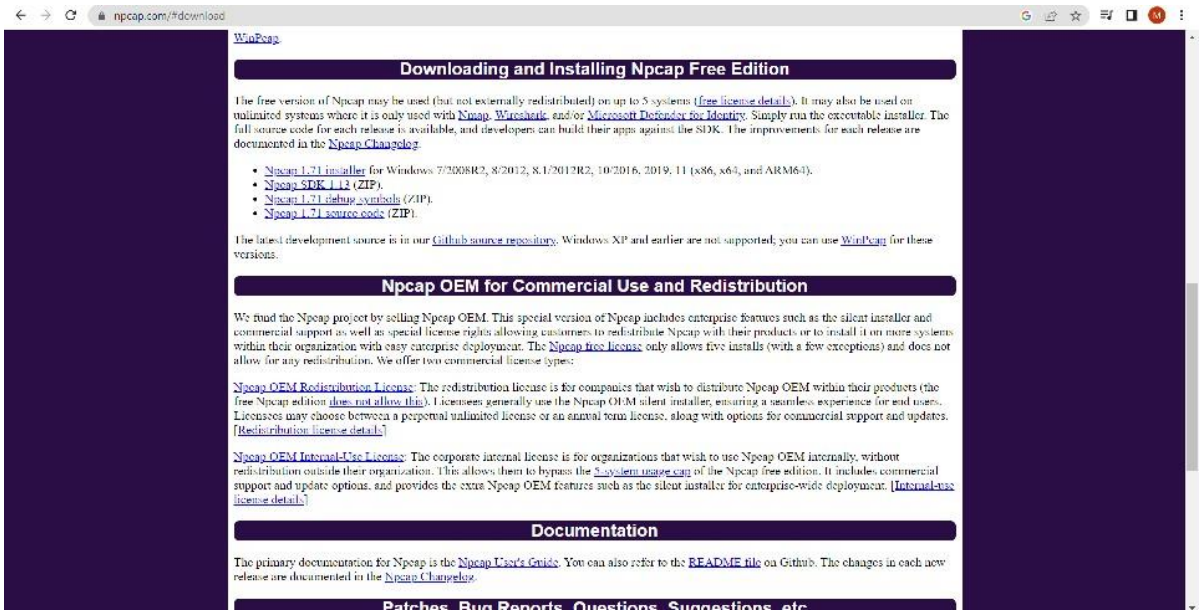
Snort installation:



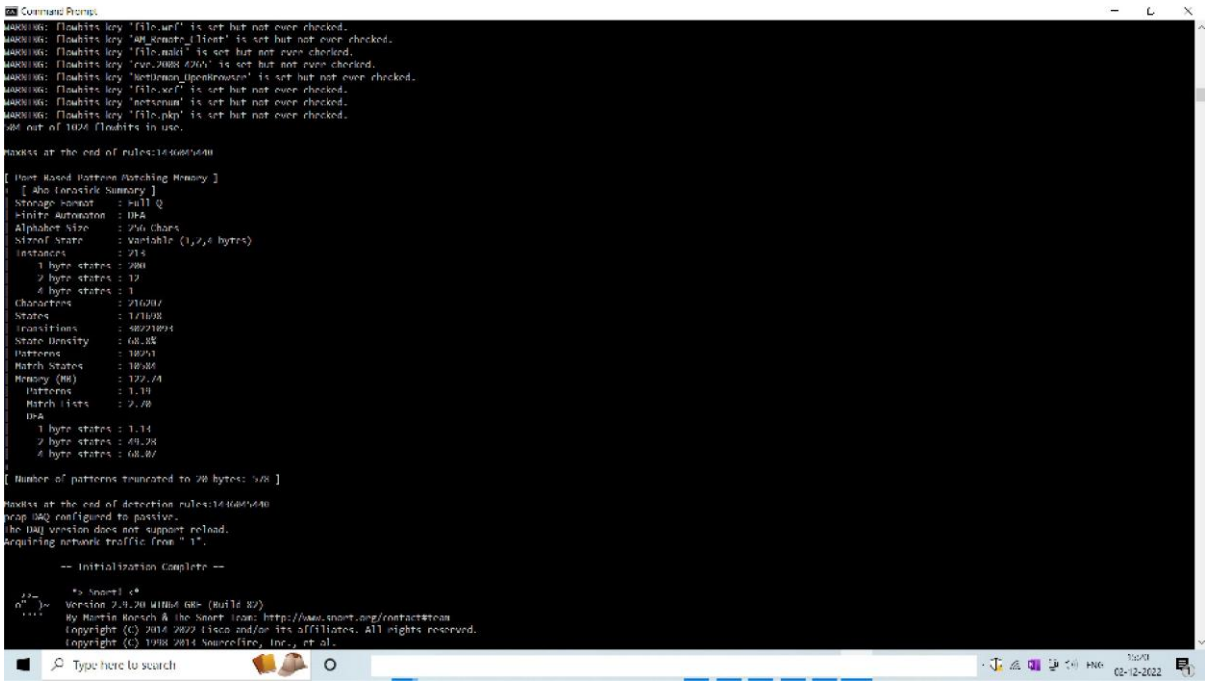


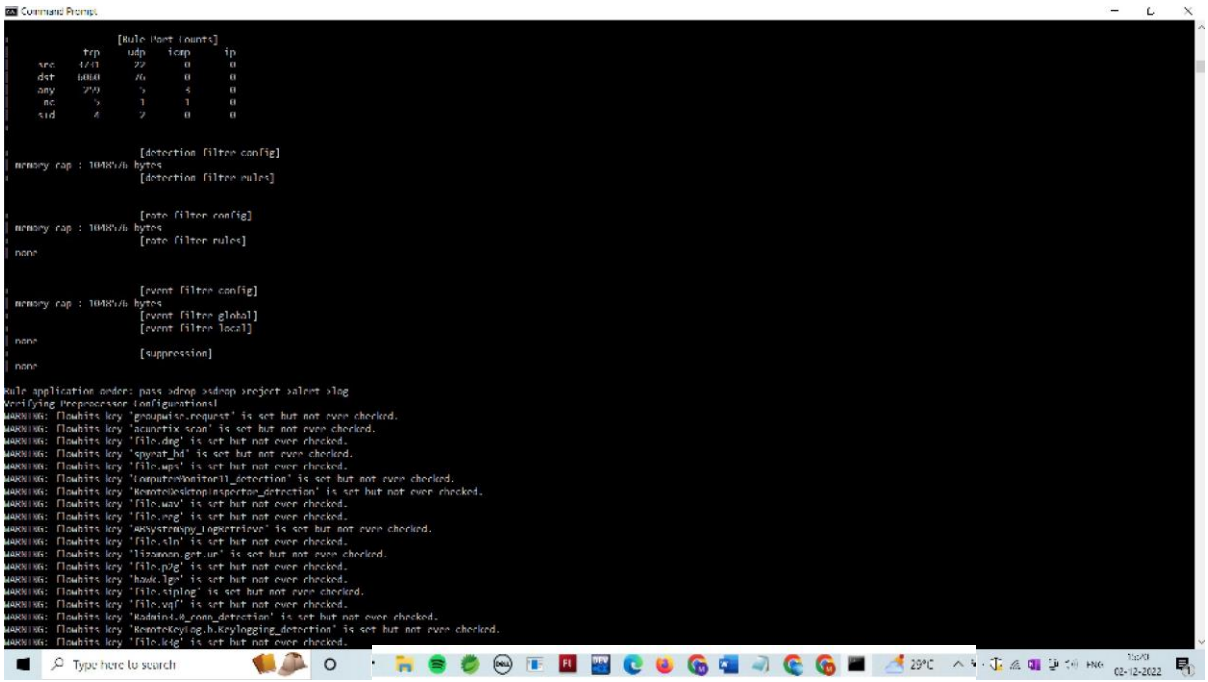
Downloading and Installing Npcap:

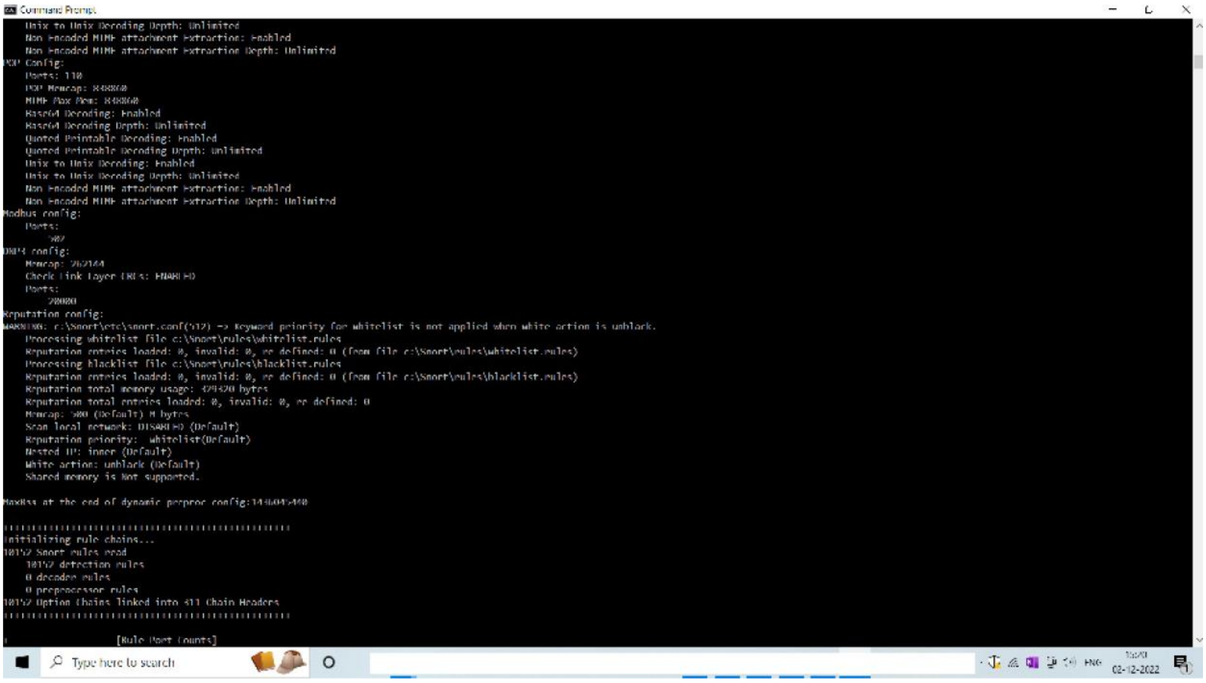
Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

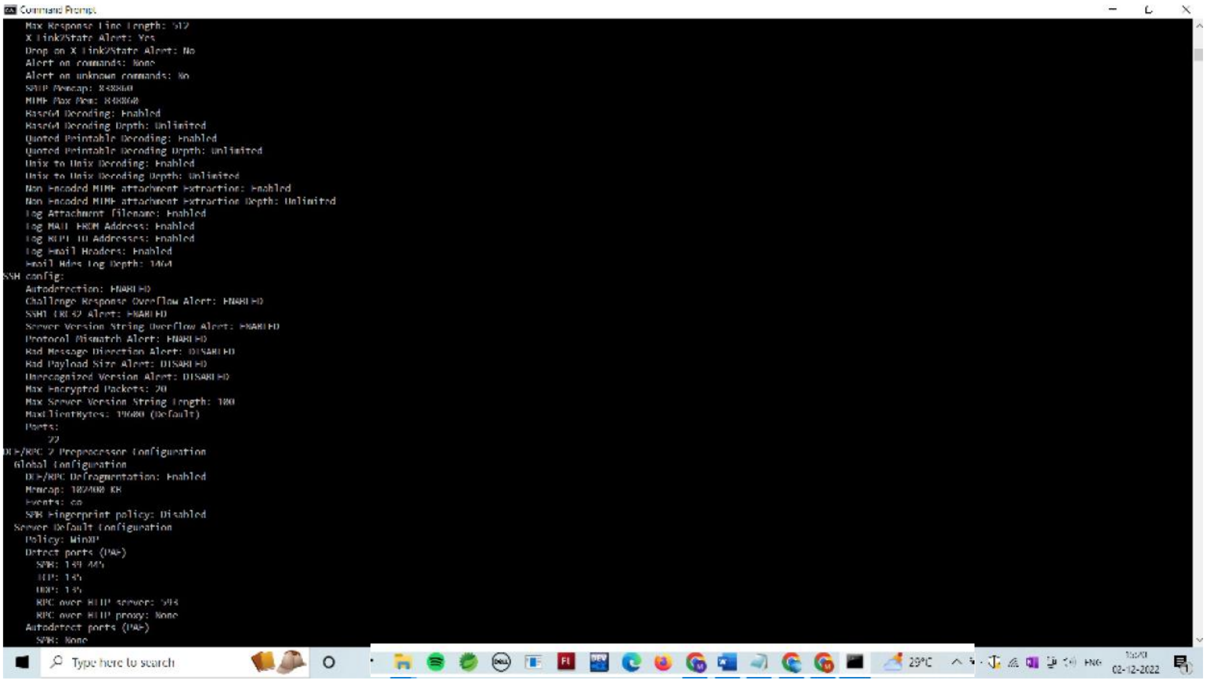


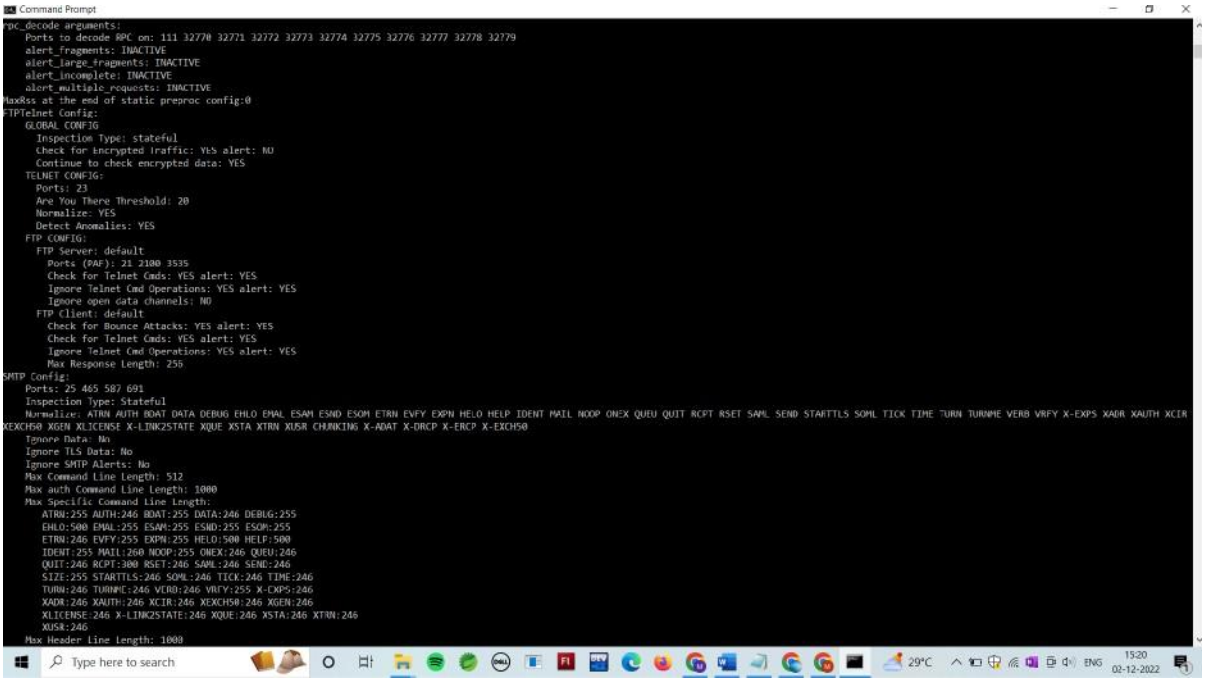
Snort Configuration :

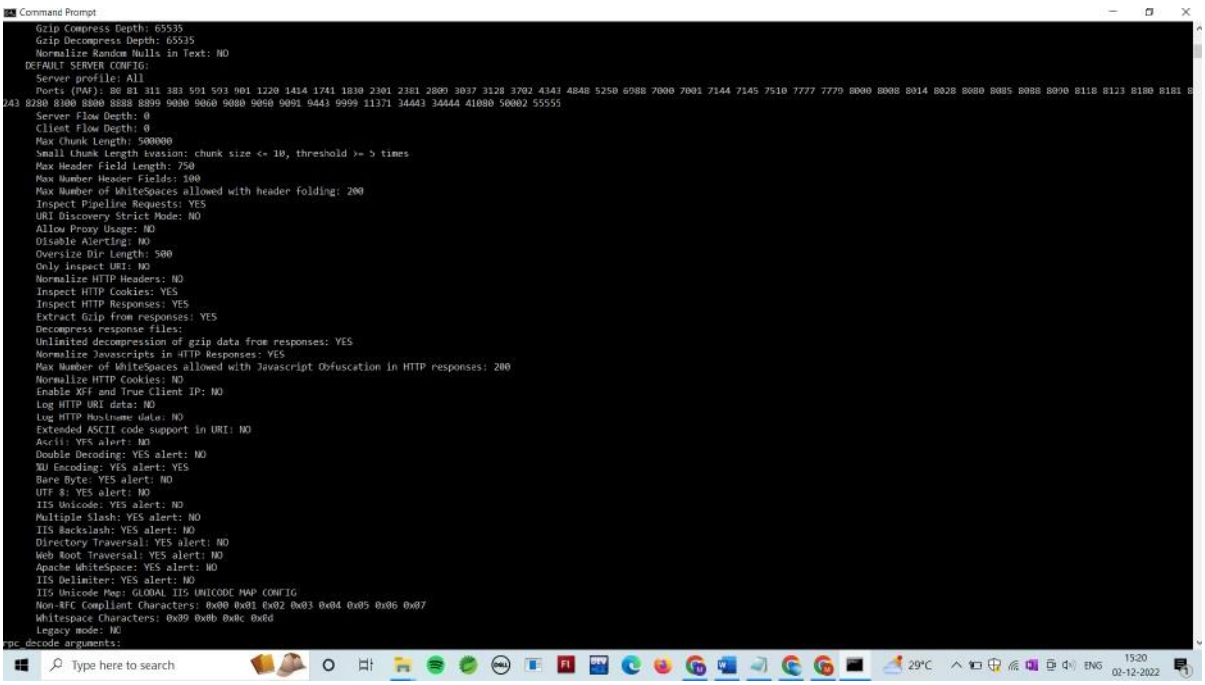

Command Prompt
WARNING: flowbits key 'file.wrf' is set but not ever checked.
WARNING: flowbits key 'AM_Remote_Client' is set but not ever checked.
WARNING: flowbits key 'file.maki' is set but not ever checked.
WARNING: flowbits key 'cve.2008_4250' is set but not ever checked.
WARNING: flowbits key 'NetDemon_UpenRevshell' is set but not ever checked.
WARNING: flowbits key 'file.xcf' is set but not ever checked.
WARNING: flowbits key 'netsenum' is set but not ever checked.
WARNING: flowbits key 'file.pkp' is set but not ever checked.
500 out of 1024 flowbits in use.
MaxBAS at the end of rules:1048576x40
[Port Based Pattern Matching Memory]
[Aho-Corasick Summary]
Storage Format : Full Q
Finite Automaton : DFA
Alphabet Size : 256 Chars
Sizeof State : Variable (1,2,4 bytes)
Instances : 214
1 byte states : 200
2 byte states : 12
4 byte states : 1
Characters : 216202
States : 171038
Transitions : 40271094
State Density : 68.8%
Patterns : 10251
Match States : 10588
Memory (MB) : 122.74
Patterns : 1.19
Match Lists : 2.78
DFA
1 byte states : 1.14
2 byte states : 49.76
4 byte states : 68.87
[Number of patterns truncated to 20 bytes: 578]
MaxBAS at the end of detection rules:1048576x40
Snap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "1".
-- Initialization Complete --
> Snort! <
Version 2.9.20 WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998 2013 Sourcefire, Inc., et al.
Type here to search
02-12-2022

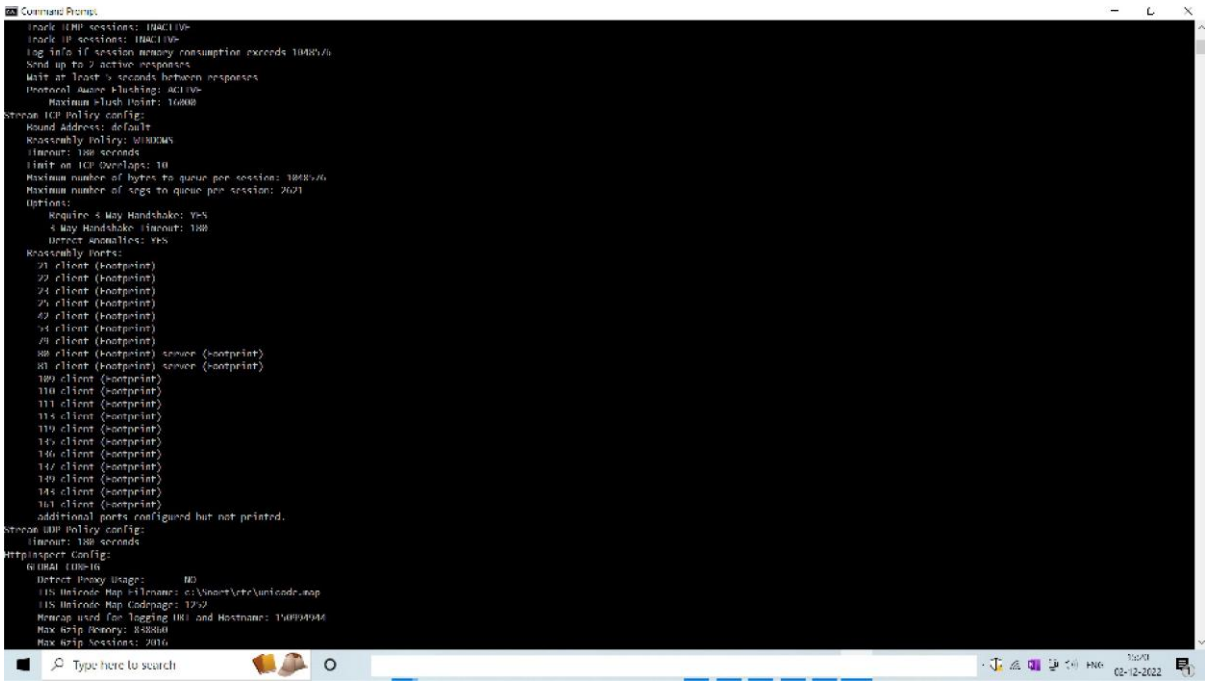

Command Prompt
[Rule Port Counts]
tcp udp icmp ip
src 1703 22 0 0
dst 6888 76 0 0
any 299 5 4 0
nc 5 1 1 0
sid 4 2 0 0
[detection filter config]
memory cap : 1048576 bytes
[detection filter rules]
[rate filter config]
memory cap : 1048576 bytes
[rate filter rules]
none
[event filter config]
memory cap : 1048576 bytes
[event filter global]
[event filter local]
none
[suppression]
none
Rule application order: pass drop sdrop reject alert log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'gpoupwin.request' is set but not ever checked.
WARNING: flowbits key 'acunetix_scan' is set but not ever checked.
WARNING: flowbits key 'file.dmg' is set but not ever checked.
WARNING: flowbits key 'spyeye_bd' is set but not ever checked.
WARNING: flowbits key 'file.wps' is set but not ever checked.
WARNING: flowbits key 'ComputerMonitor11_detection' is set but not ever checked.
WARNING: flowbits key 'RemoteDesktopInspector_detection' is set but not ever checked.
WARNING: flowbits key 'file.wav' is set but not ever checked.
WARNING: flowbits key 'file.org' is set but not ever checked.
WARNING: flowbits key 'AmSystemSpy_logRetrieve' is set but not ever checked.
WARNING: flowbits key 'file.sln' is set but not ever checked.
WARNING: flowbits key 'lizamoon.get.ur' is set but not ever checked.
WARNING: flowbits key 'file.p2g' is set but not ever checked.
WARNING: flowbits key 'hook.lg4' is set but not ever checked.
WARNING: flowbits key 'file.stplog' is set but not ever checked.
WARNING: flowbits key 'file.vqf' is set but not ever checked.
WARNING: flowbits key 'Radmin4.0_conn_detection' is set but not ever checked.
WARNING: flowbits key 'RemoteKeyLog.h.Keylogging_detection' is set but not ever checked.
WARNING: flowbits key 'file.ktg' is set but not ever checked.
Type here to search
29°C
02-12-2022

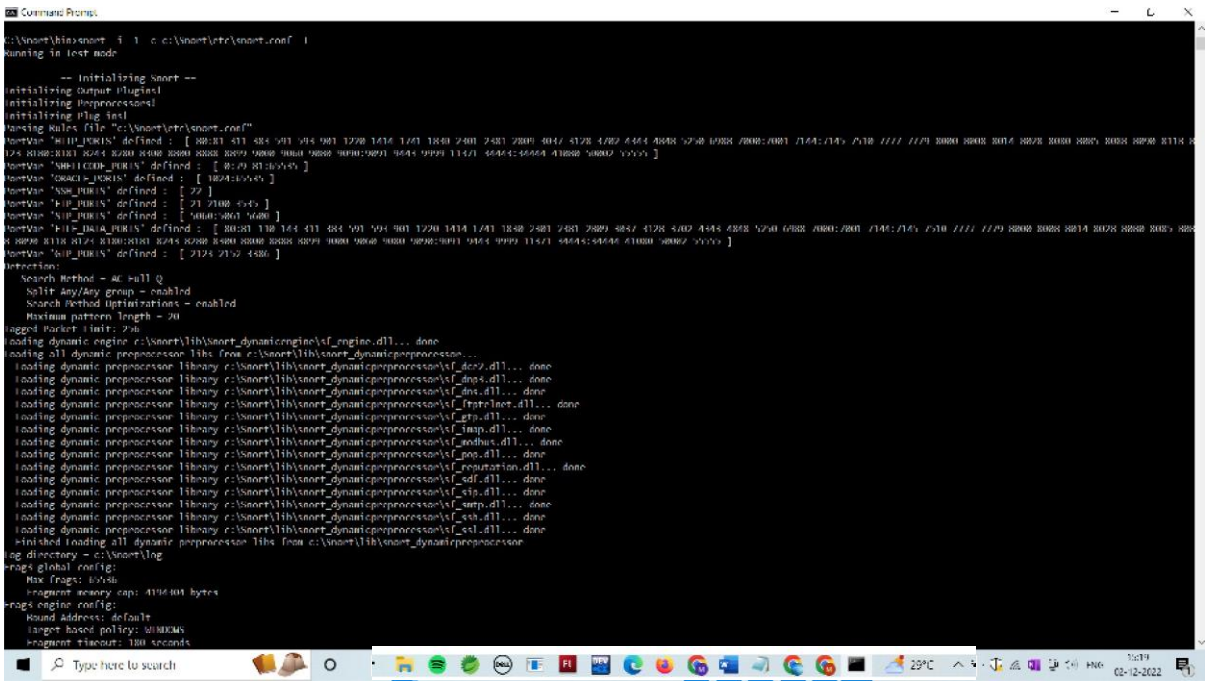

Command Prompt
Unix to Unix Decoding Depth: Unlimited
Non Encoded MIME attachment Extraction: Enabled
Non Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
Ports: 110
POP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted Printable Decoding: Enabled
Quoted Printable Decoding Depth: Unlimited
Unix to Unix Decoding: Enabled
Unix to Unix Decoding Depth: Unlimited
Non Encoded MIME attachment Extraction: Enabled
Non Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
Ports:
502
DNP3 config:
Memcap: 262144
Check Link Layer CRCs: ENABLED
Ports:
20000
Reputation config:
WARNING: c:\Snort\etc\snort.conf(512) => Keyword priority for whitelist is not applied when white action is unblack.
Processing whitelist file c:\Snort\rules\whitelist.rules
Reputation entries loaded: 0, invalid: 0, re defined: 0 (from file c:\Snort\rules\whitelist.rules)
Processing blacklist file c:\Snort\rules\blacklist.rules
Reputation entries loaded: 0, invalid: 0, re defined: 0 (from file c:\Snort\rules\blacklist.rules)
Reputation total memory usage: 429320 bytes
Reputation total entries loaded: 0, invalid: 0, re defined: 0
Memcap: 500 (Default) M bytes
Scan local network: DISABLED (Default)
Reputation priority: whitelist(Default)
Nested IP: inner (Default)
White action: unblack (Default)
Shared memory is Not supported.
MaxRss at the end of dynamic preproc config:143604540
Initializing rule chains...
10152 Snort rules read
10152 detection rules
0 decoder rules
0 preprocessor rules
10152 Option Chains linked into 311 Chain Headers
[Rule Port Counts]
Type here to search
ENG
02-12-2022

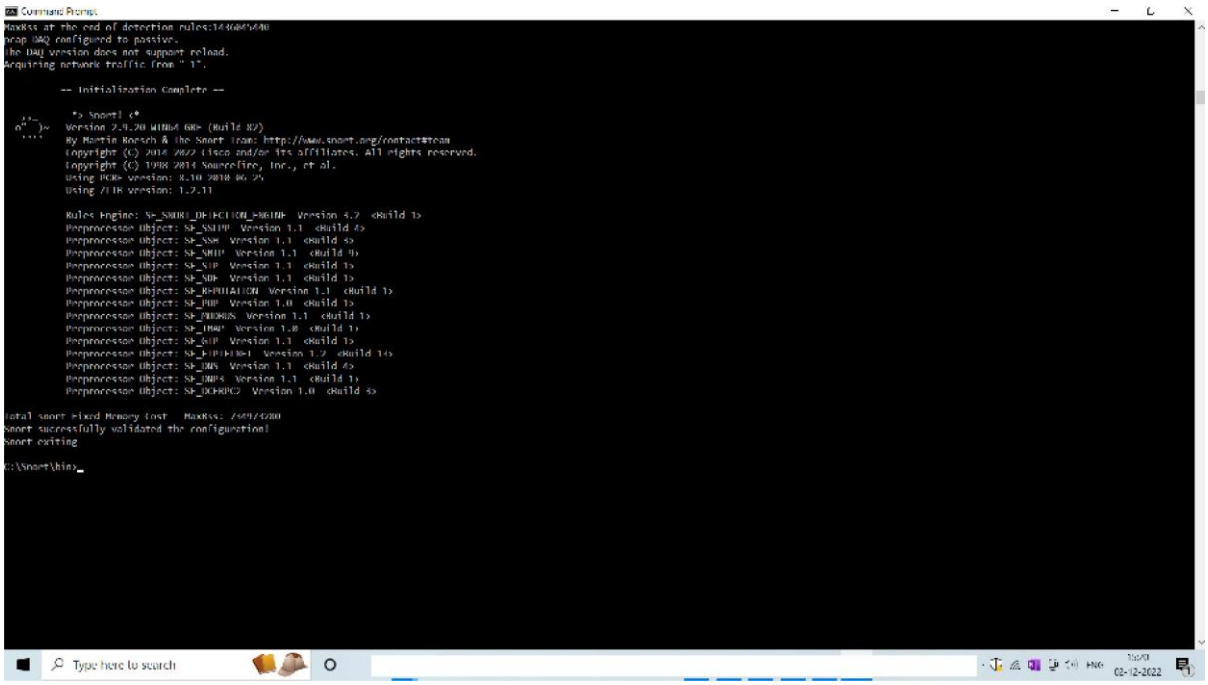

Command Prompt
Max Response Line Length: 512
X Link2State Alert: Yes
Drop on X Link2State Alert: No
Alert on commands: None
Alert on unknown commands: No
SMTP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted Printable Decoding: Enabled
Quoted Printable Decoding Depth: Unlimited
Unix to Unix Decoding: Enabled
Unix to Unix Decoding Depth: Unlimited
Non Encoded MIME attachment Extraction: Enabled
Non Encoded MIME attachment Extraction Depth: Unlimited
Log Attachment filename: Enabled
Log MAIL FROM Address: Enabled
Log RCPT TO Addresses: Enabled
Log Email Headers: Enabled
Email Hdrs Log Depth: 1464
SSH config:
Autodetection: ENABLED
Challenge Response Overflow Alert: ENABLED
SSH1 CRC32 Alert: ENABLED
Server Version String Overflow Alert: ENABLED
Protocol Mismatch Alert: ENABLED
Bad Message Direction Alert: DISABLED
Bad Payload Size Alert: DISABLED
Unrecognized Version Alert: DISABLED
Max Encrypted Packets: 20
Max Server Version String Length: 100
MaxClientBytes: 19600 (Default)
Ports:
22
DCE/RPC 2 Preprocessor Configuration
Global Configuration
DCE/RPC Defragmentation: Enabled
Memcap: 102400 KB
Events: co
SMB Fingerprint policy: Disabled
Server Default Configuration
Policy: WinXP
Detect ports (PAF)
SMB: 139 445
TCP: 135
UDP: 135
RPC over HTTP server: 593
RPC over HTTP proxy: None
Autodetect ports (PAF)
SMB: None
Type here to search
29°C
ENG
02-12-2022

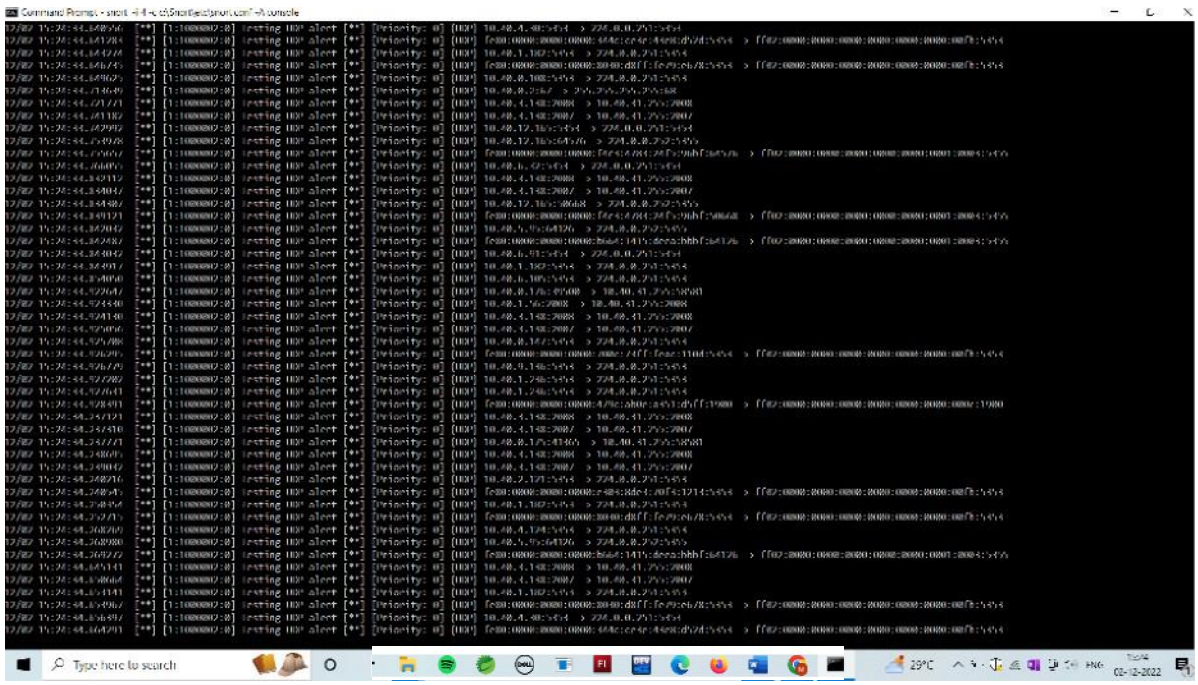





Command Prompt
Type here to search
02-12-2022


Command Prompt
Type here to search
02-12-2022


Command Prompt
Maxkss at the end of detection rules:1440805440
Snap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "1".
-- Initialization Complete --
> Snort! <
Version 2.9.20 WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_PROFILER Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Total snort Fixed Memory Cost - MaxRss: 2689/6280
Snort successfully validated the configuration!
Snort exiting
C:\Snort\bin>
Type here to search
02-12-2022


Command Prompt - snort -i 4 -c c:\Snort\etc\snort.conf -A console
Type here to search
29°C
02-12-2022

Conclusion:

Successfully installed and configured IDS in system.