

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:

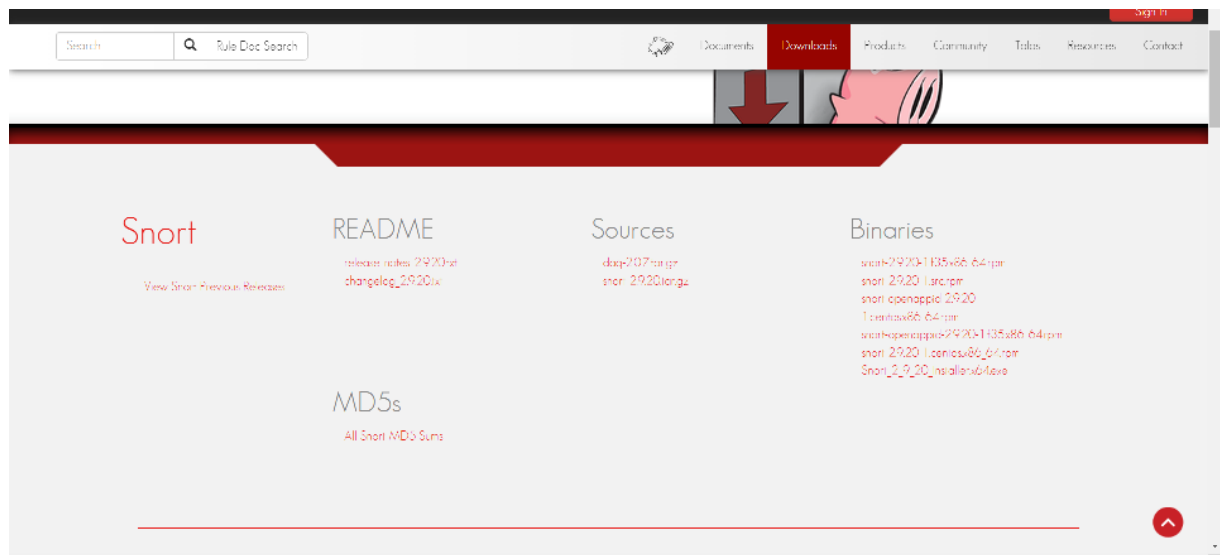
Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

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.



Edit with WPS Office

Snort installation:



```

C:\Command Prompt>
Microsoft Windows [Version 10.0.19044.223]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Judson Kaju Attard> cd C:\snort\bin\

C:\snort\bin> V

    %> snort -e
    %> ~
    ****
    Version 2.9.20 MINIMAL GSN (Build 82)
    By Martin Kesch & the Snort team: http://www.snort.org/contactteam
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2014 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2018 06-25
    Using JLIB version: 1.2.11

C:\snort\bin> M

    %> snort -e
    %> ~
    ****
    Version 2.9.20 MINIMAL GSN (Build 82)
    By Martin Kesch & the Snort team: http://www.snort.org/contactteam
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2014 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2018 06-25
    Using JLIB version: 1.2.11

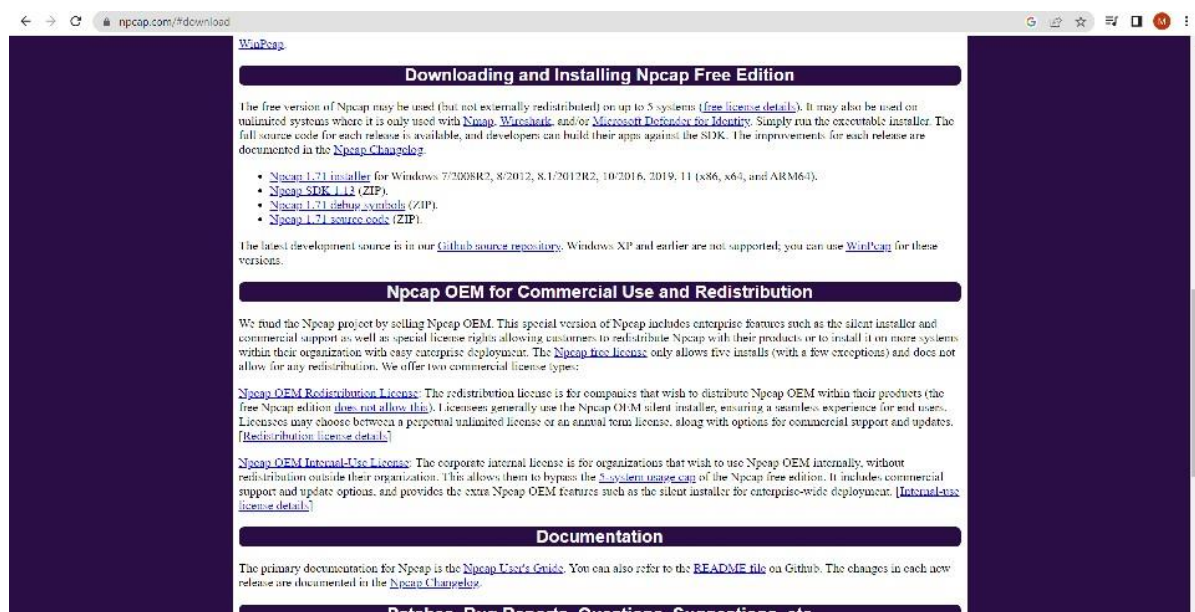
index Physical Address IP Address Device Name Description
1 08:00:00:00:00:00 disabled VmwareVMX_["3620211e-2024-490e-8050-009048021700"] WAN Miniport (IPv6)
2 08:00:00:00:00:00 disabled VmwareVMX_["22864546-C865-4513-A142-11-2826E55A90D"] WAN Miniport (IP)
3 08:00:00:00:00:00 disabled VmwareVMX_["187856d5-52e3-4244-881e-20242c00109d"] WAN Miniport (Bluetooth)
4 4-8A54-10-A1-A1-20 10.0.0.0/8 VmwareVMX_["007410B8-8A96-4C11-88C0-0014782C8401"] Qualcomm QCA9377 802.11ac Wireless adapter
5 4-8A54-10-A1-A1-20 192.168.1.164 VmwareVMX_["08030427D0-4102-4582-8047-804843422454"] Microsoft Wi-Fi Direct Virtual Adapter #2
6 4-8A54-10-A1-A1-20 192.168.1.154 VmwareVMX_["C820418C-9921-498b-8A00-78-2282940B5572"] Microsoft Wi-Fi Direct Virtual Adapter
7 08:00:00:00:00:00 0800:0800:0800:0800:0800:0800 VmwareVMX_["eapback"] Adapter for loopback traffic capture
8 08:00:00:00:00:00 192.168.16.190 VmwareVMX_["44-892746-1127-8-272-208C82B28560"] Realtek Virtual Ethernet Adapter (RTL8101E 6.80)
9 80:00:02:00:02:02 192.168.210.247 VmwareVMX_["08147456-3009-4284-8048-7420100D3710"] Realtek PCIe GbE Family controller

C:\snort\bin>

```

Downloading and Installing Npcap:

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



Snort Configuration :

```
Command Prompt
4400186: Pcapbits key 'file.wf' is set but not even checked.
4400186: Pcapbits key 'an_remote_host' is set but not even checked.
4400186: Pcapbits key 'file.midi' is set but not even checked.
4400186: Pcapbits key 'cve.2008.4201' is set but not even checked.
4400186: Pcapbits key 'hackermapopenbrowser' is set but not even checked.
4400186: Pcapbits key 'file.scf' is set but not even checked.
4400186: Pcapbits key 'hackermap' is set but not even checked.
4400186: Pcapbits key 'file.php' is set but not even checked.
all out of 1024 Pcapbits in use.

Results at the end of rules:1636005000

[ Host Based Signature Matching Memory ]
[ Also for signature Summary ]
Storage format : Full Q
Initial Automaton : DFA
Alphabet Size : 256 Chars
String State : Variable (1,2,4 bytes)
Instances : 214
1 byte states : 200
2 byte states : 19
4 byte states : 5
Characters : 216007
States : 171008
Transitions : 48291094
State density : 68.88
Patterns : 10251
Match States : 10385
Memory (MB) : 122.74
Patterns : 1.10
Match lists : 2.78
DFA
1 byte states : 1.14
2 byte states : 49.28
4 byte states : 68.87

[ Number of patterns truncated to 20 bytes: 508 ]

Results at the end of detection rules:1636005000
pcap apg reconfigured to parser.
the DAPI version does not support reload.
Acquiring network traffic from "1".

-- Initialization Complete --

C:\> %* %* %* %* %*
C:\> Version 2.9.20 (MIB4 GR- (Build 82))
By Martin Roesch & the Snort team (http://www.snort.org/contactteam)
Copyright (C) 2006-2022 Snort and/or its affiliates. All rights reserved.
Copyright (C) 1998-2014 Sourcefire, Inc., et al.
```

```
Command Prompt

[Rule Count (counts)]
src 1/1 22 0 0
dst 1000 26 0 0
any 255 5 5 0
nc 5 1 1 0
sid 8 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
[expression]
none

rule application order: pass sdrop sdrop sreject salent xlog
config/propose/propose (unconfigured)
4400186: Pcapbits key 'smtp.request' is set but not even checked.
4400186: Pcapbits key 'acumatrix scan' is set but not even checked.
4400186: Pcapbits key 'file.dag' is set but not even checked.
4400186: Pcapbits key 'sgent_hf' is set but not even checked.
4400186: Pcapbits key 'file.wps' is set but not even checked.
4400186: Pcapbits key 'capitroninspection_detection' is set but not even checked.
4400186: Pcapbits key 'hackermapopenbrowser_detection' is set but not even checked.
4400186: Pcapbits key 'file.wav' is set but not even checked.
4400186: Pcapbits key 'file.rpg' is set but not even checked.
4400186: Pcapbits key 'keylogger_loggers' is set but not even checked.
4400186: Pcapbits key 'file.sln' is set but not even checked.
4400186: Pcapbits key 'h3xmon.get.un' is set but not even checked.
4400186: Pcapbits key 'file.pjs' is set but not even checked.
4400186: Pcapbits key 'hackermap' is set but not even checked.
4400186: Pcapbits key 'file.siplog' is set but not even checked.
4400186: Pcapbits key 'file.vq' is set but not even checked.
4400186: Pcapbits key 'hackermap_remote_detection' is set but not even checked.
4400186: Pcapbits key 'hackermap_remote_detection' is set but not even checked.
4400186: Pcapbits key 'file.kg' is set but not even checked.
```

```
Command Prompt
Unix to Unix decoding depth: unlimited
Non encoded MIME attachment extraction: enabled
Non encoded MIME attachment extraction depth: unlimited
VSP Config:
Ports: 110
Max Mmap: 80000
MIME Max Pw: 80000
Hex2id decoding: enabled
Hex2id 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:
VSP
VSP config:
Mmap: 20000
Check link layer (RS): HMMH0
Ports:
VSP
Reputation config:
WARNING: c:\snort\etc\snort.conf(332) -> Required priority for whitelist is not applied when white action is unblock.
Processing whitelist file c:\snort\etc\whitelist.rules
Reputation entries loaded: 0, invalid: 0, re defined: 0 (from file c:\snort\etc\whitelist.rules)
Processing blacklist file c:\snort\etc\blacklist.rules
Reputation entries loaded: 0, invalid: 0, re defined: 0 (from file c:\snort\etc\blacklist.rules)
Reputation total memory usage: 0x000 bytes
Reputation total entries loaded: 0, invalid: 0, re defined: 0
Mmap: 400 (default) 0 bytes
Scan local network: DISAB0 (Default)
Reputation priority: whitelist(Default)
Reset on: inner (Default)
White action: unblock (Default)
Shared memory is not supported.
Headers at the end of dynamic processor config:14404540
*****
initializing rule chains...
101% Snort rules read
101% detection rules
0 decoder rules
0 preprocessor rules
101% Option (chains linked into all chain headers)
*****
[Rule Post Counts]
```

```
Command Prompt
Max Response line length: 65535
X link/State Alert: Yes
Drop on X link/State Alert: No
Alert on commands: none
Alert on unknown commands: on
Snort Mmap: 80000
MIME Max Pw: 80000
Hex2id decoding: enabled
Hex2id 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 Mail TO addresses: enabled
Log Mail Headers: enabled
Mail Headers log depth: 1000
SNM config:
Autodetection: HMMH0
Challenge Response DoS/Flow Alert: HMMH0
SNM (RS) alert: HMMH0
Server Version String DoS/Flow Alert: HMMH0
Protocol Mismatch Alert: HMMH0
Bad Message Injection Alert: DISAB0
Bad Upload Size Alert: DISAB0
Unrecognized Version Alert: DISAB0
Max Encrypted Packets: 20
Max Server Version String length: 100
Max Linetypes: 1000 (default)
Ports:
??
X2/RFC 2 Preprocessor Configuration
Global Configuration
DoS/RFC DoS/Preprocessor: enabled
Mmap: 1000000
Ports: 0
SNM Fingerprint policy: disabled
Server Default Configuration
Policy: none
Detect ports (Pw)
SNM: 10000
LLP: 100
LLP: 100
RRC over HTTP server: 000
RRC over HTTP proxy: none
Autodetect ports (Pw)
SNM: none
```

```
Command Prompt

rpc_decode arguments:
  Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779
  alert_fragments: INACTIVE
  alert_large_fragments: INACTIVE
  alert_incomplete: INACTIVE
  alert_multiple_requests: INACTIVE
  MaxKills at the end of static preproc config:0
FTPtelnet Config:
  GLOBAL CONFIG
    Inspection Type: stateful
    Check for unencrypted traffic: Yes alert: NO
    Continue to check encrypted data: YES
  TELNET CONFIG:
    Ports: 23
    Are You There Threshold: 20
    Normalize: YES
    Detect Anomalies: YES
  FTP CONFIG:
    FTP Server: default
    Ports (PAF): 21 2100 3535
    Check for Telnet Cnids: YES alert: YES
    Ignore Telnet Cmd Operations: YES alert: YES
    Ignore open data channels: NO
    FTP Client: default
    Check for Bounce Attacks: YES alert: YES
    Check for Telnet Cnids: YES alert: YES
    Ignore Telnet Cmd Operations: YES alert: YES
    Max Response Length: 255
SMTP Config:
  Ports: 25 465 587 691
  Inspection Type: Stateful
  Normalize: ATRN AUTH BOAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK TIME TURN TURNME VERB VRFY X-EXPS XAER XAUTH XCIR
  XECHO50 XGEN XLICENSE X-LINKSTATE XQUE XSTA XTRN XUSER CHARKING X-ADAT X-ORCP X-ERCP X-EXCH50
  Ignore Data: No
  Ignore TLS Data: No
  Ignore SMTP Alerts: No
  Max Command Line Length: 512
  Max auth Command Line Length: 1000
  Max Specific Command Line Length:
    ATRN:255 AUTH:246 BOAT:255 DATA:246 DEBUG:255
    EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
    ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
    IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
    QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
    SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
    TURN:246 TURNME:246 VCRB:246 VRFY:255 X-EXPS:246
    XAER:246 XAUTH:246 XCIR:246 XECHO50:246 XGEN:246
    XLICENSE:246 X-LINKSTATE:246 XQUE:246 XSTA:246 XTRN:246
    XUSER:246
  Max Header Line Length: 1000
```

```
Command Prompt

Gzip Compress Depth: 65535
Gzip Decompress Depth: 65535
Normalize Random Nulls in Text: NO
DEFAULT SERVER CONFIG:
  Server profile: All
  Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1810 2301 2381 2800 3037 3128 3702 4343 4848 5250 6088 7000 7001 7144 7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8181 8
  241 8280 8300 8880 8888 8899 9000 9060 9080 9090 9091 9441 9999 11371 34441 34444 41080 50002 55555
  Server Flow Depth: 0
  Client Flow Depth: 0
  Max Chunk Length: 580000
  Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
  Max Header Field Length: 750
  Max Number Header Fields: 100
  Max Number of WhiteSpaces allowed with header folding: 200
  Inspect Pipeline Requests: YES
  URI Discovery Strict Mode: NO
  Allow Proxy Usage: NO
  Disable Alerting: NO
  Oversize Dir Length: 500
  Only inspect URI: NO
  Normalize HTTP Headers: NO
  Inspect HTTP Cookies: YES
  Inspect HTTP Responses: YES
  Extract Gzip from responses: YES
  Decompress response files:
  Unlimited decompression of gzip data from responses: YES
  Normalize Javascripts in HTTP Responses: YES
  Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP responses: 200
  Normalize HTTP Cookies: NO
  Enable XFF and True Client IP: NO
  Log HTTP URI data: NO
  Log HTTP Response data: NO
  Extended ASCII code support in URI: NO
  ASCII: YES alert: NO
  Double Decoding: YES alert: NO
  MUI Encoding: YES alert: YES
  Bare Byte: YES alert: NO
  UTF 8: YES alert: NO
  IIS Unicode: YES alert: NO
  Multiple Slash: YES alert: NO
  IIS Backslash: YES alert: NO
  Directory Traversal: YES alert: NO
  Web Root Traversal: YES alert: NO
  Apache Whitespace: YES alert: NO
  IIS Delimiter: YES alert: NO
  IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
  Non-ASCII Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
  Whitespace Characters: 0x09 0x0B 0x0C 0x0D
  Legacy mode: NO
rpc_decode arguments:
```


Conclusion:

Successfully installed and configured IDS in system.



Edit with WPS Office