

SNORT INSTALLATION AND CONFIGURATION IN WINDOWS

What is Snort?

Snort is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS). It functions as a network packet sniffer, using predefined rules to detect malicious network activities.

Key Features of Snort:

- Packet Sniffer
- Packet Logger
- Network Intrusion Detection and Prevention

Installation Requirements

Before setting up Snort, the following packages need to be downloaded:

1. Snort

<https://www.snort.org/downloads>

2. Snort Rules (Registered)

[Download Registered Rules](<https://www.snort.org/downloads>)

You will need to create an account, log in, and download the registered rules matching your version of Snort. To check your Snort version, open the command prompt and run the following commands:

```
>cd C:\snort\bin  
>snort -V
```

```

C:\Users\user>cd C:\snort\bin
C:\Snort\bin>snort -V

  _ _ _ _ _
  o"  )~
  '...'

-*> 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

C:\Snort\bin>

```

3. Zenmap

<https://nmap.org/zenmap/>

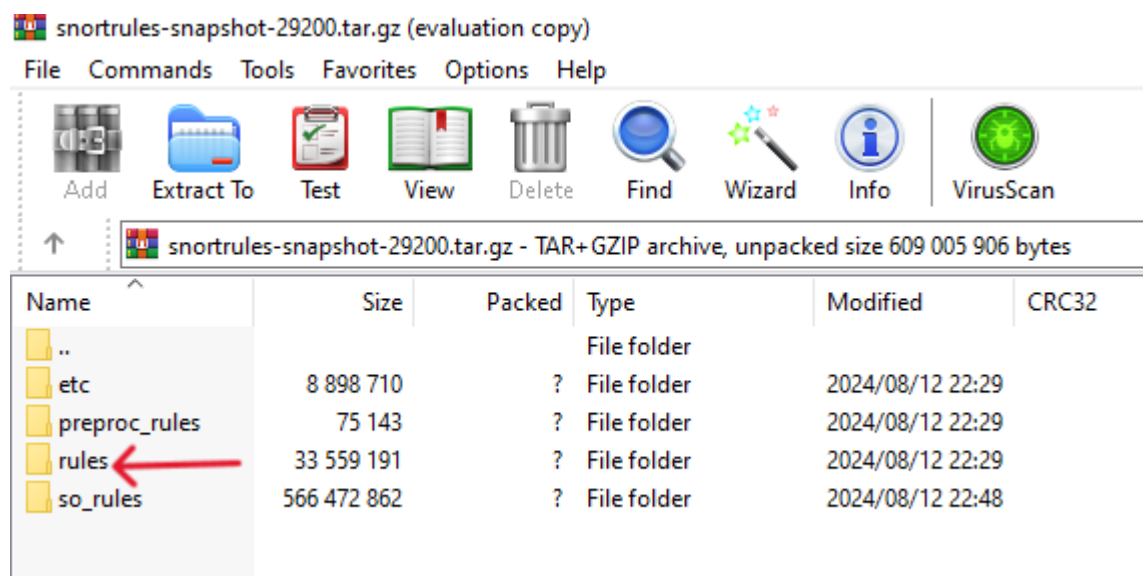
Adding Snort Rules

Once you've downloaded the rules, follow these steps to add them to Snort:

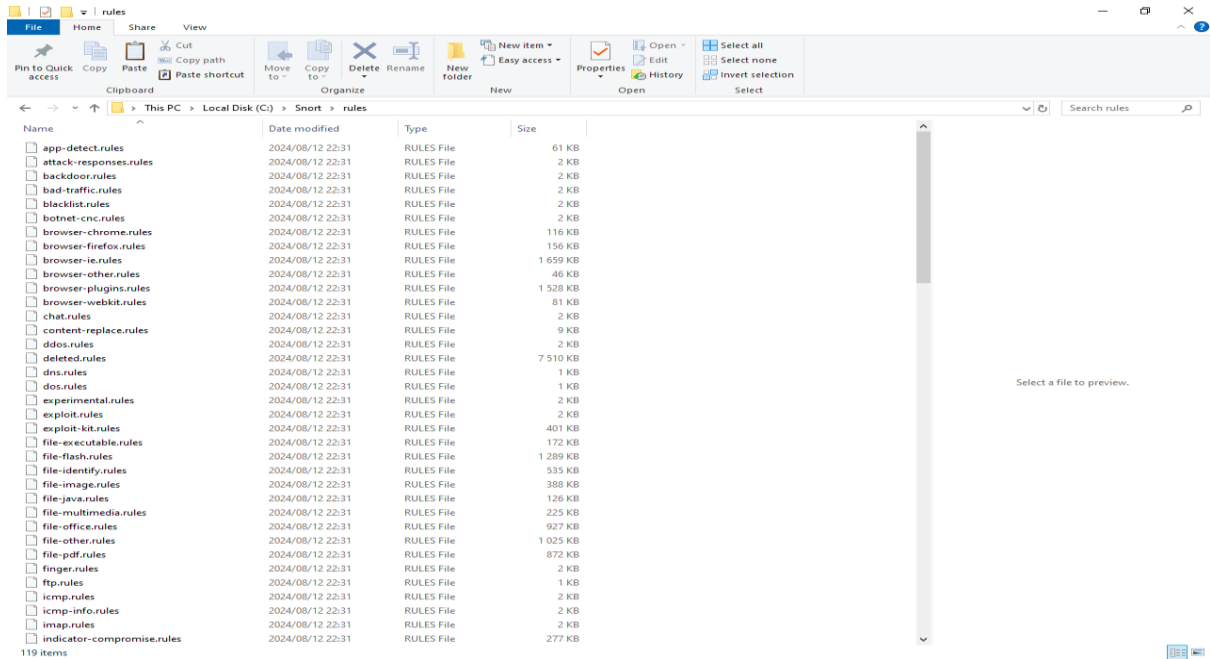
1. Navigate to the downloaded rules, then copy and paste them into the rules folder:

C:\snort\rules

Copy

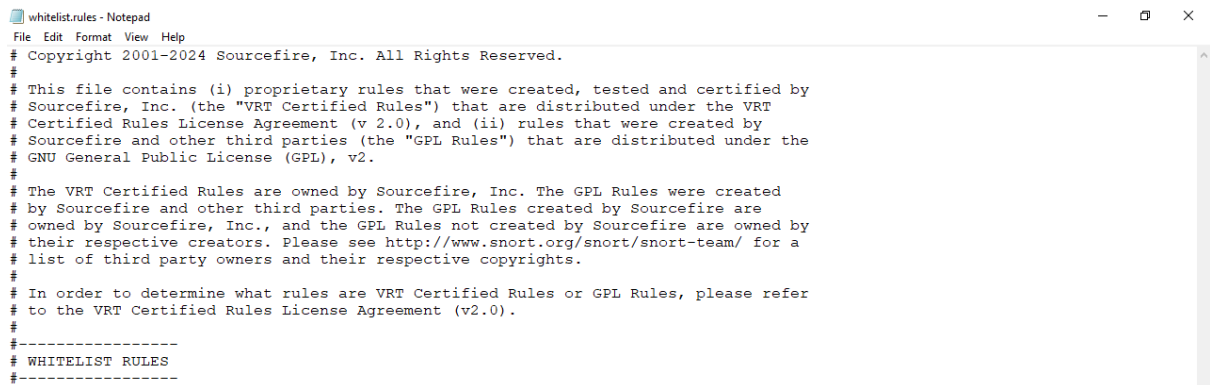


Paste



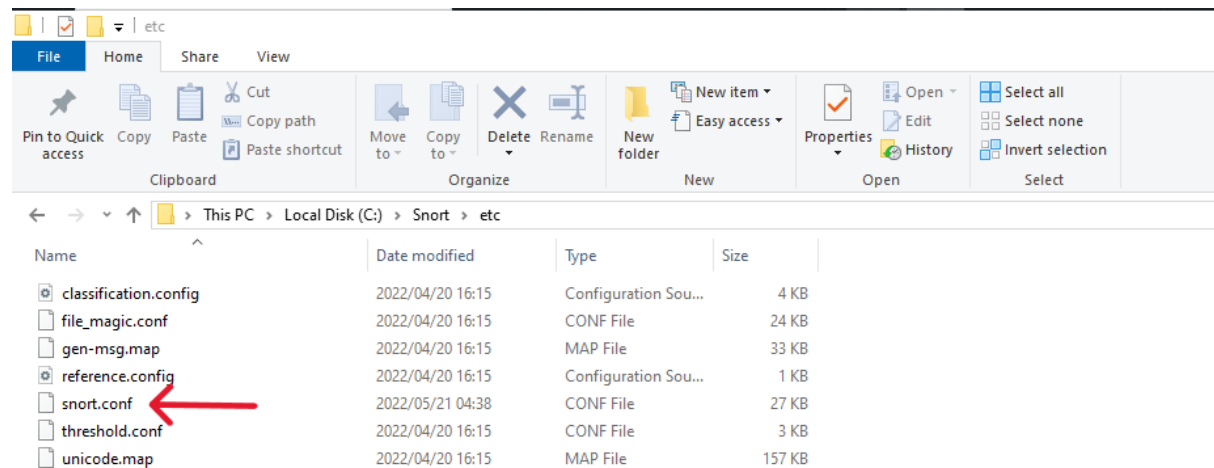
NB: Also replace the existing preproc_rules by copying the downloaded rules and pasting them in the snort folder 'C: Snort'

2. If the `whitelist.rules` file is missing, you can copy the `blacklist.rules` file from the same folder and rename it whitelist.rules.



Configuring the `snort.conf` File

1. Open the `snort.conf` file located in `C:\Snort\etc` using a text editor (e.g., Notepad).



2. There are several sections from the 9 steps that require editing in the `snort.conf` file. The following steps guide you through the necessary modifications:

```
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
```

STEPS

Step 1: Network Variables and Rules File Paths

Set the network variables by specifying the IP address of your Windows machine (use `ipconfig` in the command prompt to view your IP address).

1. Set the internal network address as `'\$HOME_NET` and configure the external network as `'\$EXTERNAL_NET = !\$HOME_NET`.

```
#####  
# Step #1: Set the network variables. For more informat:  
#####  
  
# Setup the network addresses you are protecting  
ipvar HOME_NET 192.168.8.143  
  
# Set up the external network addresses. Leave as "any" :  
ipvar EXTERNAL_NET !$HOME_NET
```

2. Update the path to the rules directory as follows:

```
var RULE_PATH C:\Snort\rules  
  
var PREPROC_RULE_PATH C:\Snort\preproc_rules  
  
var WHITE_LIST_PATH C:\Snort\rules  
  
var BLACK_LIST_PATH C:\Snort\rules
```

```
# Path to your rules files (this can be a relative path)  
# Note for Windows users: You are advised to make this an absolute path,  
# such as: c:\snort\rules  
var RULE_PATH C:\Snort\rules  
# var SO_RULE_PATH ../so_rules  
var PREPROC_RULE_PATH C:\Snort\preproc_rules  
  
# If you are using reputation preprocessor set these  
# Currently there is a bug with relative paths, they are relative to where snort is  
# not relative to snort.conf like the above variables  
# This is completely inconsistent with how other vars work, BUG 89986  
# Set the absolute path appropriately  
var WHITE_LIST_PATH C:\Snort\rules  
var BLACK_LIST_PATH C:\Snort\rules
```

Step 2: Log Directory

Set the path of the log directory as "C:\Snort\log"

Config logdir: C:\Snort\log

```
# Configure default log directory for snort to log to.
#
config logdir: C:\Snort\log
```

Step 3

No change

Step 4: Dynamic Libraries

Configure dynamic library paths as follows:

dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

dynamicengine C:\Snort\lib\snort_dynamicengine\sfe_engine.dll

Comment out the dynamic detection rule path by adding a # as follows:

dynamicdetection directory /usr/local/lib/snort_dynamicrules

```
#####
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Module
#####

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sfe_engine.dll

# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Step 5: Preprocessors

1. Comment out the following preprocessors as follows:

```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```

2. Configure preprocessors by removing the “\” and putting decompress_swf { deflate lzma } and decompress_pdf { deflate } in the comments.

```
u_encode yes \
webroot no
# decompress_swf { deflate lzma } \
# decompress_pdf { deflate }
```

3. comment out preprocessor bo

```
# Back Orifice detection.
# preprocessor bo
```

4. Put preprocessor sfportscan in the comments by removing the #

```
# Portscan detection. For more information, see README.sfportscan
preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }
```

Step 6

No change

Step 7: Rule Paths

1. Replace all forward slashes (`/`) with backslashes (`\\`) for all rule paths as per below image.

```
# site specific rules
include $RULE_PATH\local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
include $RULE_PATH\file-other.rules
include $RULE_PATH\file-pdf.rules
include $RULE_PATH\finger.rules
include $RULE_PATH\ftp.rules
include $RULE_PATH\icmp-info.rules
include $RULE_PATH\icmp.rules
include $RULE_PATH\imap.rules
include $RULE_PATH\indicator-compromise.rules
include $RULE_PATH\indicator-obfuscation.rules
include $RULE_PATH\indicator-shellcode.rules
include $RULE_PATH\info.rules
include $RULE_PATH\malware-backdoor.rules
include $RULE_PATH\malware-cnc.rules
include $RULE_PATH\malware-other.rules
include $RULE_PATH\malware-tools.rules
include $RULE_PATH\misc.rules
include $RULE_PATH\multimedia.rules
include $RULE_PATH\mysql.rules
include $RULE_PATH\netbios.rules
include $RULE_PATH\nntp.rules
<
```

2. Customize preprocessor and decoder alerts in Step 8 by replacing the forward slash “/” with backslash “\”

```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

Step 9

No change

Using Snort to Detect Malicious Activity

1. Check Available Network Interfaces:

Open the command prompt and run:

```
snort -W
```

This will list the available network interfaces. Select the appropriate interface index for Snort to monitor.

```
Command Prompt
C:\Users\user>cd C:\Snort\bin
C:\Snort\bin>snort -W

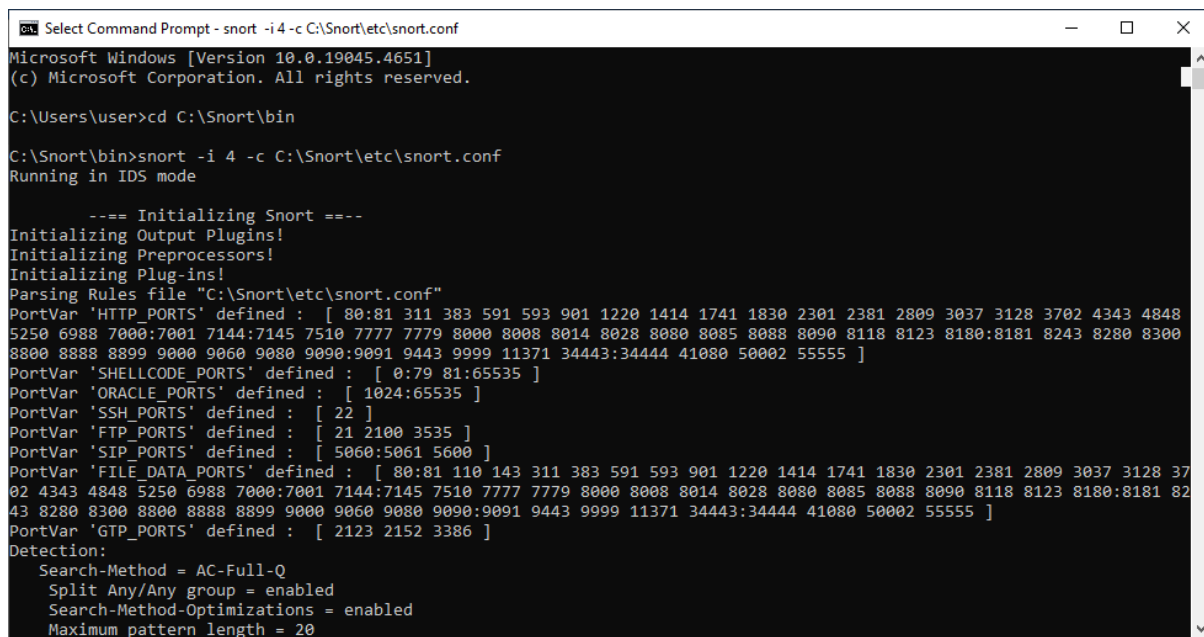
-*)> Snort! <*-
o"~
'""
'""
'""
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled      \Device\NPF_{2F525CEF-3081-4BE2-90F7-ADBCA5EA0D84}  WAN Miniport (Network Monitor)
2      00:00:00:00:00:00      disabled      \Device\NPF_{E9E0F617-0B28-45FE-929A-5E257C717D6F}  WAN Miniport (IPv6)
3      00:00:00:00:00:00      disabled      \Device\NPF_{5DCE51F2-98EB-4775-A011-F18F5DEDA21D}  WAN Miniport (IP)
4      78:8C:85:8A:FF:EC      192.168.8.143  \Device\NPF_{45015335-32C4-445B-8C28-5BCF26856E14}  TP-Link Wireless USB Adapter #2
5      78:8C:85:8A:FF:EC      169.254.21.189 \Device\NPF_{28623ECB-4ED2-4A89-9296-8558CBE423D9}  Microsoft Wi-Fi Direct Virtual Adapter #4
6      7A:8C:85:8A:FF:EC      169.254.106.43 \Device\NPF_{7A1A9454-47F2-4B10-9B22-6976D53A2B76}  Microsoft Wi-Fi Direct Virtual Adapter #3
```

2. Test Snort Setup:

Run the following command to test the configuration: Replace `4` with the correct interface number if needed. The `-T` flag tests the configuration file and the `C` is for identifying the configuration file (snort.conf)

```
snort -i 4 -c C:\Snort\etc\snort.conf -T
```



```
Select Command Prompt - snort -i 4 -c C:\Snort\etc\snort.conf
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>cd C:\Snort\bin

C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf
Running in IDS 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 8123 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 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 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
```

3. Navigate to rules and the open 'local.rules' with a text editor. Add custom rules to the 'local.rules' file to detect various types of attacks. Example rules:

```
alert tcp any any -> any any (msg: "SYN attack"; flags: S; sid: 10000005;)
```

```
alert udp any any -> 192.168.8.143 any (msg: "UDP Scan"; sid: 10001; rev: 1;)
```

```
alert icmp any any -> 192.168.8.143 any (msg: "PING Scan"; dsize: 0; sid: 10002; rev: 1;)
```

```
alert tcp any any -> 192.168.8.143 any (msg: "FIN Scan"; flags: F; sid: 10003; rev: 1;)
```

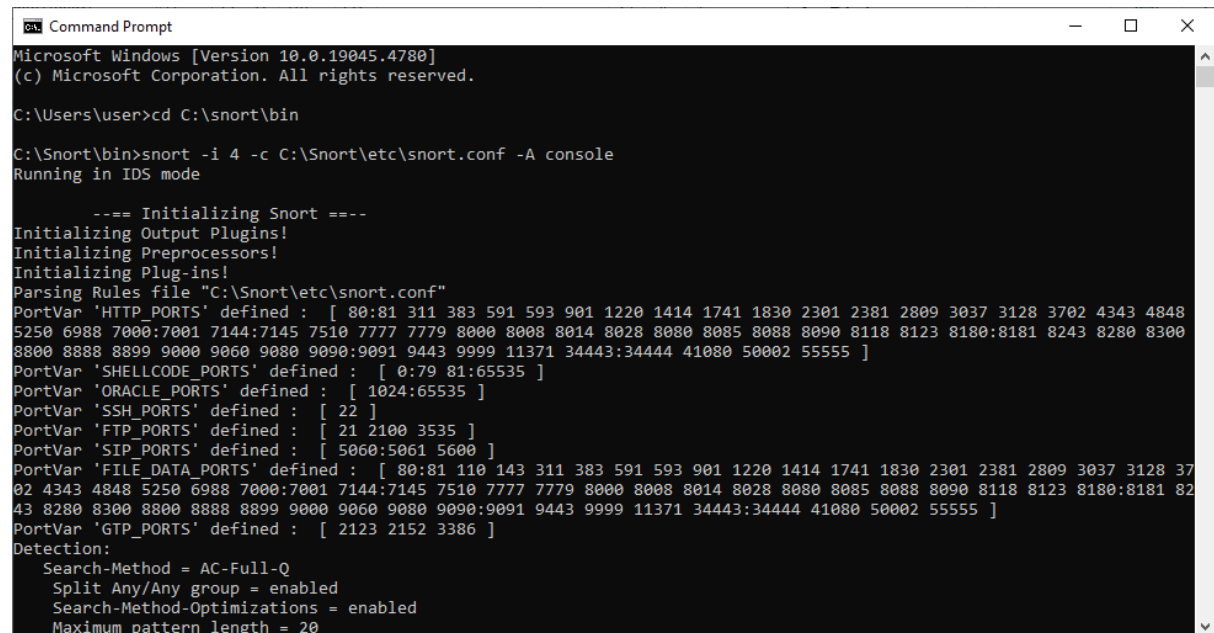
```
alert tcp any any -> 192.168.8.143 any (msg: "NULL Scan"; flags: 0; sid: 10004; rev: 1;)
```

```
alert tcp 192.168.8.143 any -> 192.168.8.143 22 (msg: "XMAS Scan"; flags: FPU; sid: 10005;
rev: 1;)
```

4. Run Snort in IDS Mode:

Execute the following command to start Snort in IDS mode and monitor traffic:

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



```
Command Prompt
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>cd C:\snort\bin

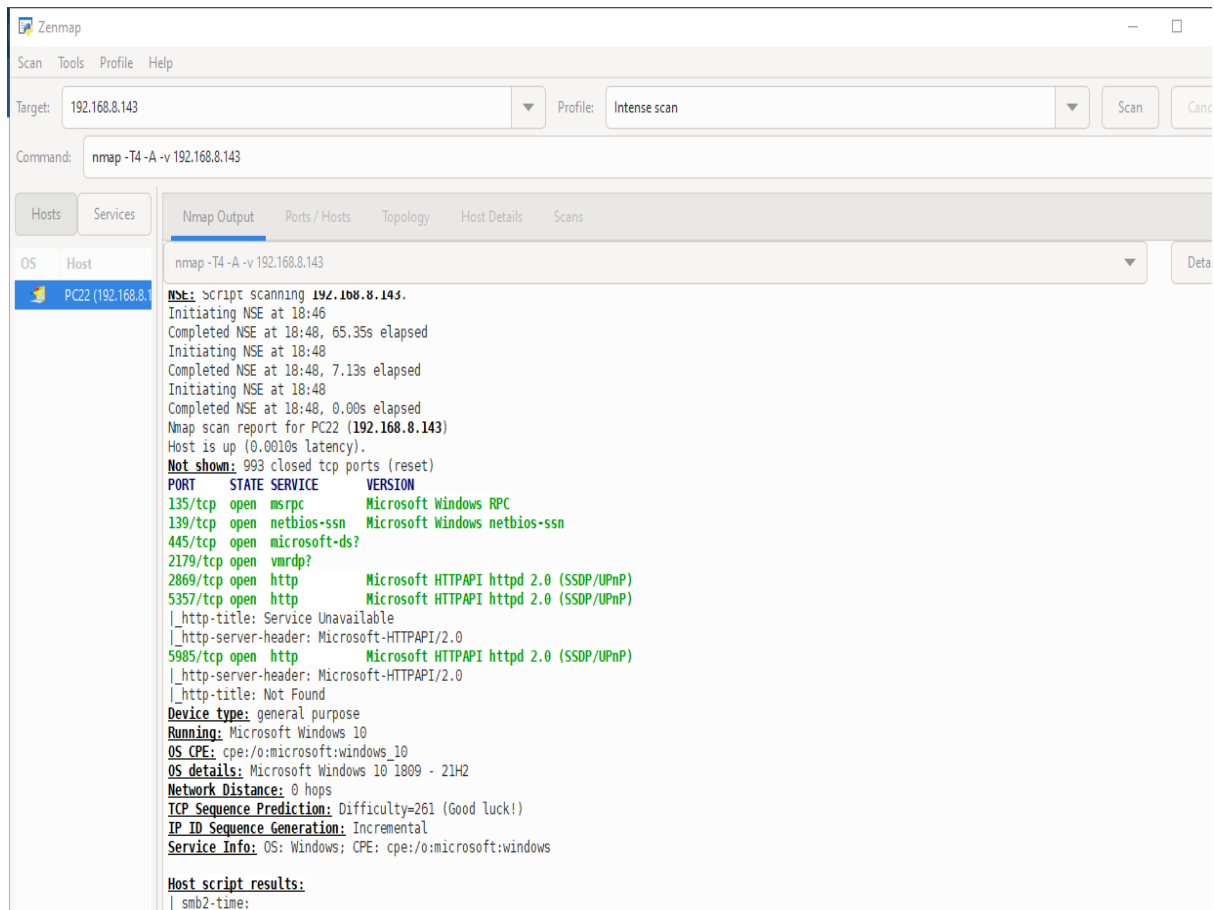
C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf -A console
Running in IDS mode

--== 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 8123 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 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 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
```

5. Testing with Zenmap

Perform network scanning attacks using Zenmap:

- Open Zenmap and select 'Intense Scan' to scan the target IP address.



Snort should detect these scans and log them accordingly.

```

C:\Windows\system32\cmd.exe
Commencing packet processing (pid=24780)
09/16-17:30:06.292671 09/16-17:30:06.292671 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.250.199.131:443 -> 192.168.8.143:63510
09/16-17:30:08.629098 09/16-17:30:08.629098 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.118:64400 -> 192.168.8.143:7680
09/16-17:30:13.395240 09/16-17:30:13.395240 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:13.655580 09/16-17:30:13.655580 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:13.657772 09/16-17:30:13.657772 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:13.710279 09/16-17:30:13.710279 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:16.331761 09/16-17:30:16.331761 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.168.8.1:53 -> 192.168.8.143:54354
09/16-17:30:16.338531 09/16-17:30:16.338531 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.143:20065 -> 41.21.235.75:443
09/16-17:30:16.492594 09/16-17:30:16.492594 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.8.143:20065 -> 41.21.235.75:443
09/16-17:30:16.584740 09/16-17:30:16.584740 [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.8.143:20065 -> 41.21.235.75:443
09/16-17:30:16.616676 09/16-17:30:16.616676 [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 41.21.235.75:443 -> 192.168.8.143:20065
09/16-17:30:16.783871 09/16-17:30:16.783871 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.105:56592 -> 192.168.8.143:7680
09/16-17:30:18.356780 09/16-17:30:18.356780 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.168.8.1:53 -> 192.168.8.143:53487
09/16-17:30:18.357675 09/16-17:30:18.357675 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.143:20070 -> 52.183.220.149:443
09/16-17:30:22.780076 09/16-17:30:22.780076 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:22.981254 09/16-17:30:22.981254 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:22.983558 09/16-17:30:22.983558 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:23.036081 09/16-17:30:23.036081 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 192.178.54.46:443 -> 192.168.8.143:61973
09/16-17:30:24.402885 09/16-17:30:24.402885 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.143:20075 -> 192.168.8.1:53
09/16-17:30:24.483864 09/16-17:30:24.483864 [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.8.143:20076 -> 192.168.8.1:53
09/16-17:30:24.487289 09/16-17:30:24.487289 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 142.251.47.132:443 -> 192.168.8.143:64467
09/16-17:30:24.634688 09/16-17:30:24.634688 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 142.251.47.132:443 -> 192.168.8.143:64467
09/16-17:30:24.634687 09/16-17:30:24.634687 [**] [1:10001:1] UDP Scan [**] [Priority: 0] {UDP} 142.251.47.132:443 -> 192.168.8.143:64467

```