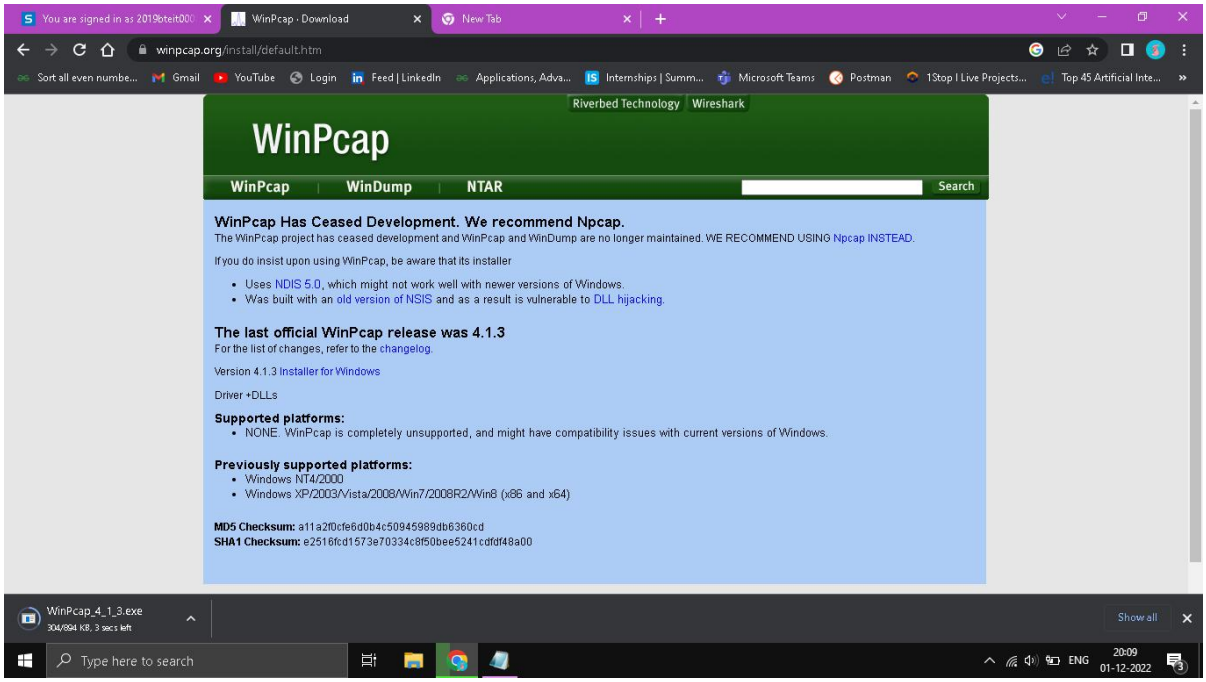
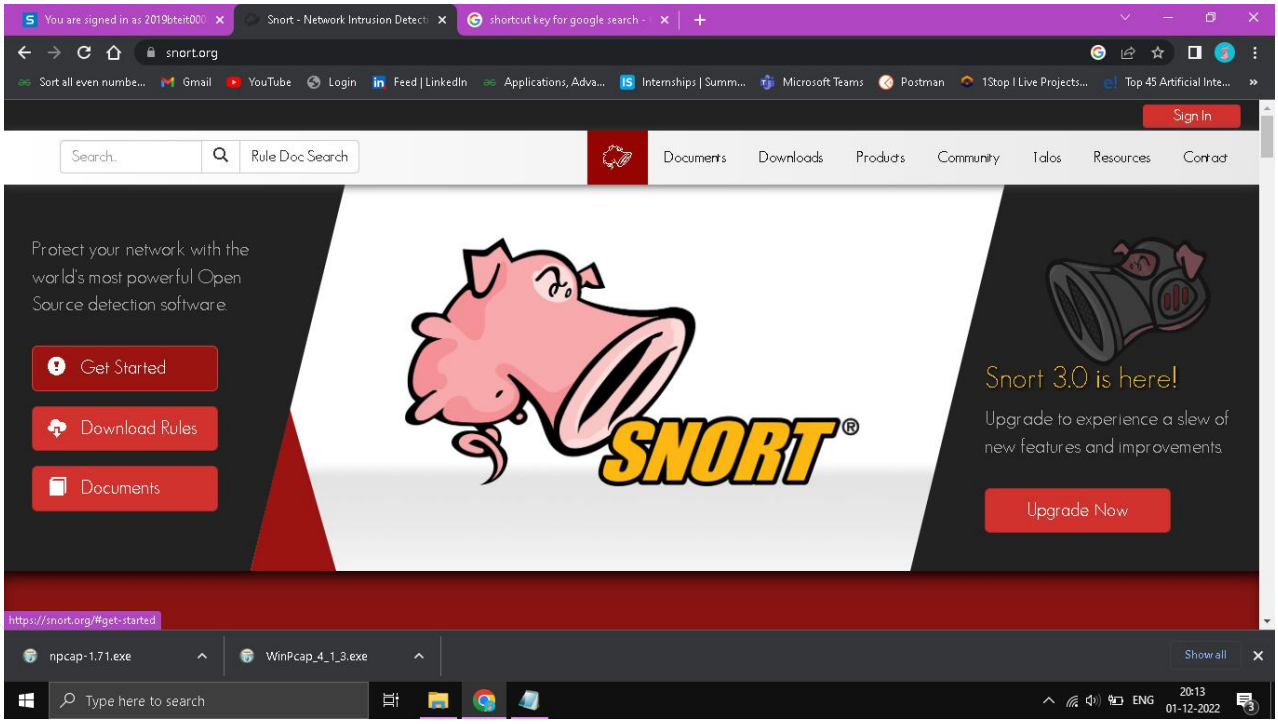
Final Year B. Tech., Sem VII 2022-23
Cryptography & Network Security Lab
PRN: 2020BTECS00205
Full Name: Monika .V. Chitrakathi
Batch: B8

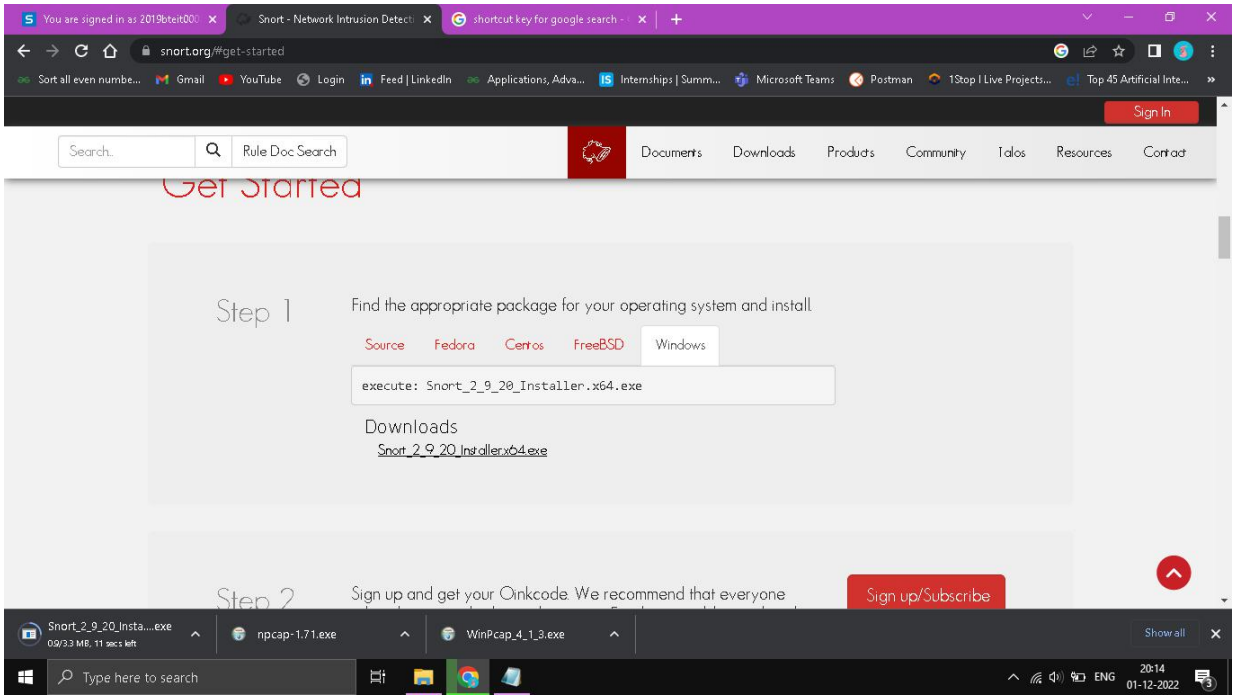
Assignment - Snort Intrusion Detection System (IDS)

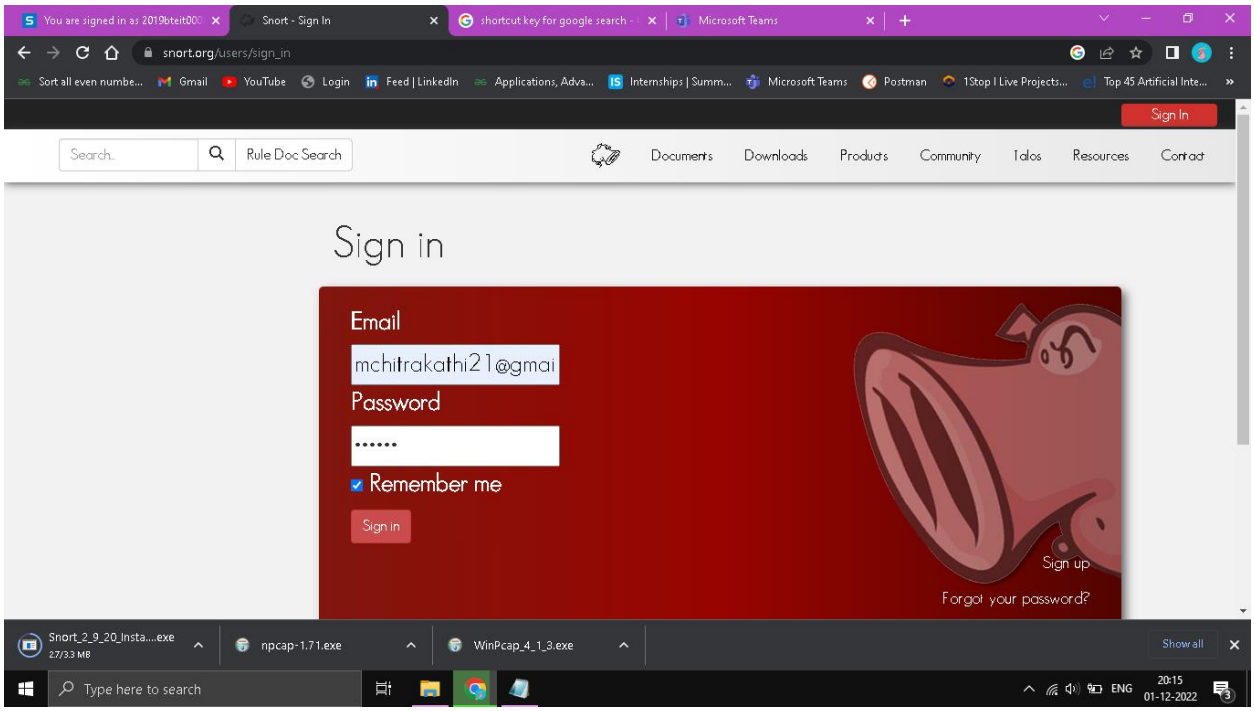
Lab Assignment Description

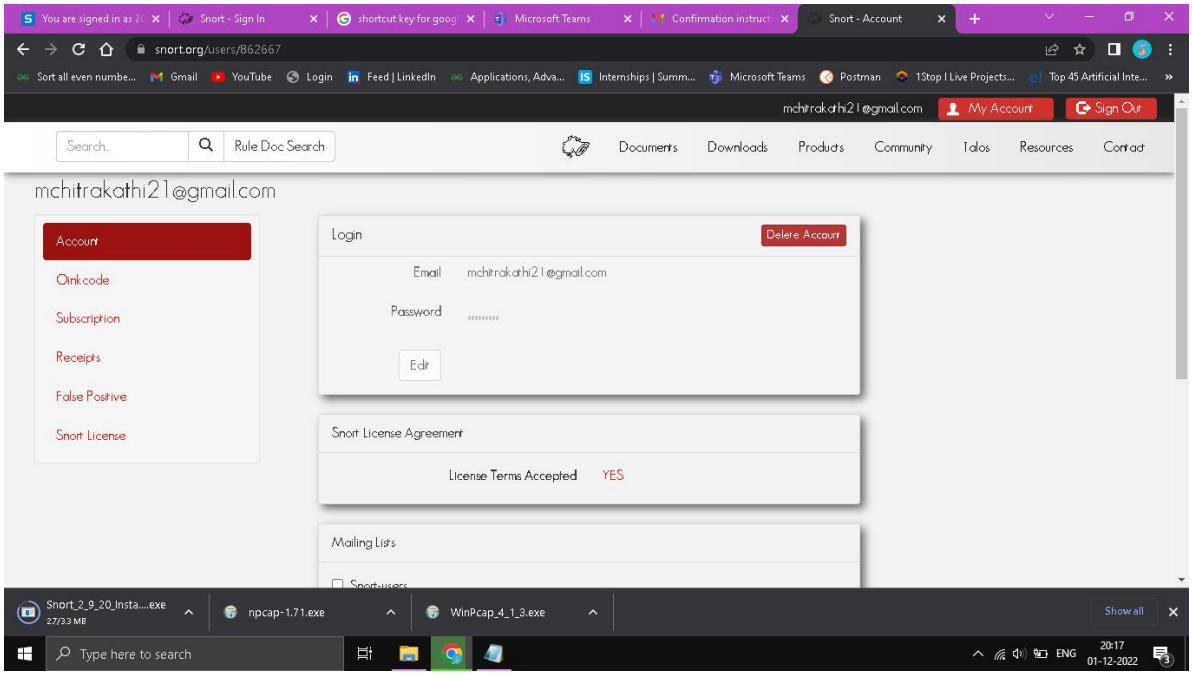
In this lab we will explore the Snort IDS. This is a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger, however we won't be doing that in this lab. Snort has multiple modes of operation, for the lab we will use snort as a packet sniffer, not inline.

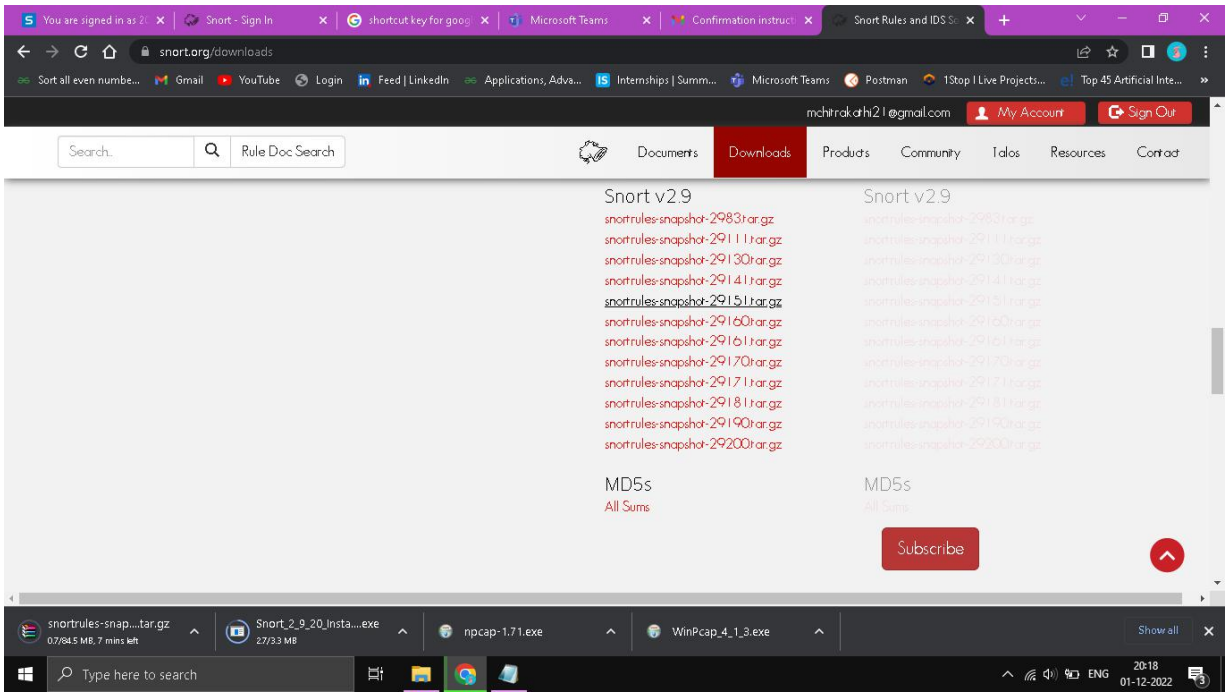

WinPcap
WinPcap | WinDump | NTAR
Search
WinPcap Has Ceased Development. We recommend Npcap.
The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. WE RECOMMEND USING Npcap INSTEAD.
If you do insist upon using WinPcap, be aware that its installer
Uses NDIS 5.0, which might not work well with newer versions of Windows.
Was built with an old version of NSIS and as a result is vulnerable to DLL hijacking.
The last official WinPcap release was 4.1.3
For the list of changes, refer to the changelog.
Version 4.1.3 Installer for Windows
Driver +DLLs
Supported platforms:
NONE. WinPcap is completely unsupported, and might have compatibility issues with current versions of Windows.
Previously supported platforms:
Windows NT4/2000
Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)
MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd
SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cdfdf48a00
WinPcap_4_1_3.exe
Type here to search

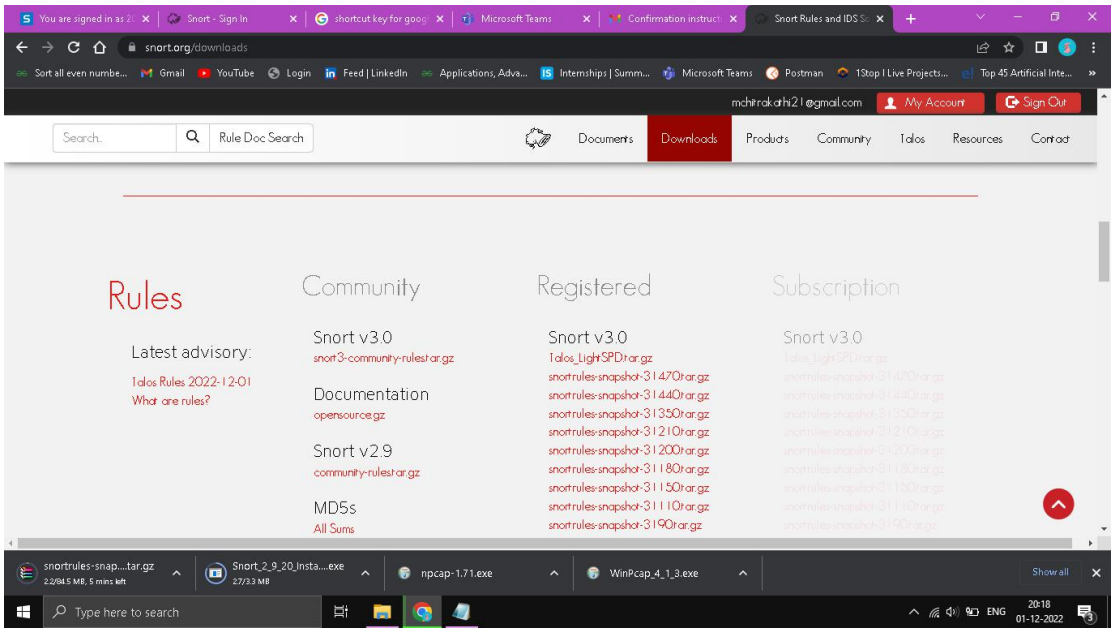

snort.org
Sign In
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
Protect your network with the world's most powerful Open Source detection software
Get Started
Download Rules
Documents
SNORT®
Snort 3.0 is here!
Upgrade to experience a slew of new features and improvements
Upgrade Now
https://snort.org/#get-started
npcap-1.71.exe
WinPcap_4_1_3.exe
Type here to search

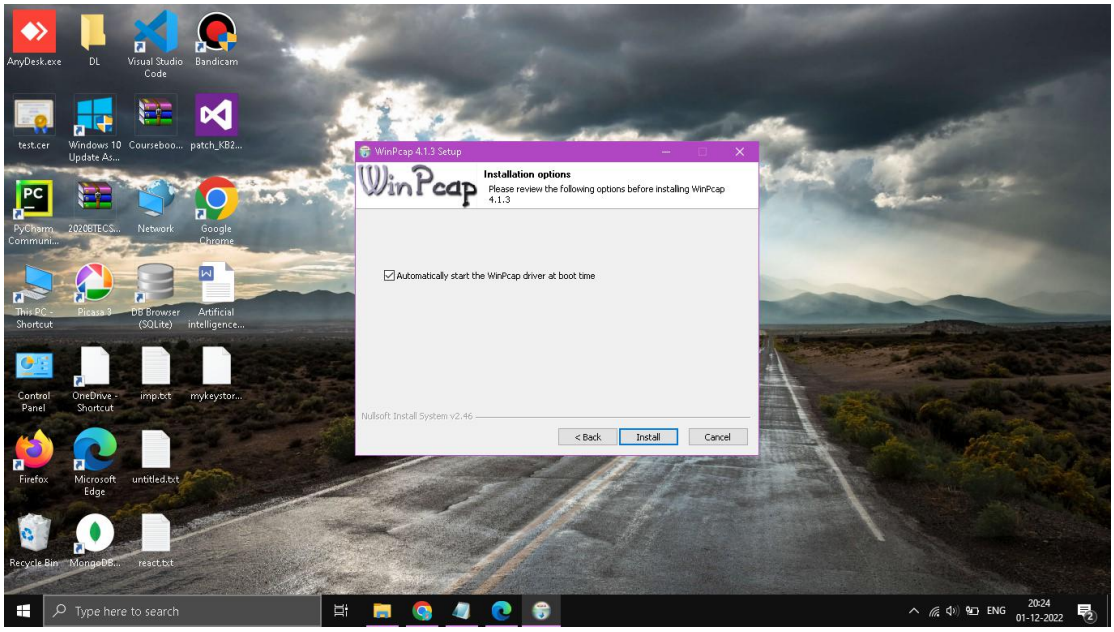

snort.org/#get-started
Sign In
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
Get Started
Step 1
Find the appropriate package for your operating system and install.
Source
Fedora
Centos
FreeBSD
Windows
execute: Snort_2_9_20_Installer.x64.exe
Downloads
Snort_2_9_20_Installer.x64.exe
Step 2
Sign up and get your Oinkcode. We recommend that everyone
Sign up/Subscribe
Snort_2_9_20_Insta....exe
0.9/3.3 MB, 11 secs left
npcap-1.71.exe
WinPcap_4_1_3.exe
Show all
Type here to search
ENG
20:14
01-12-2022

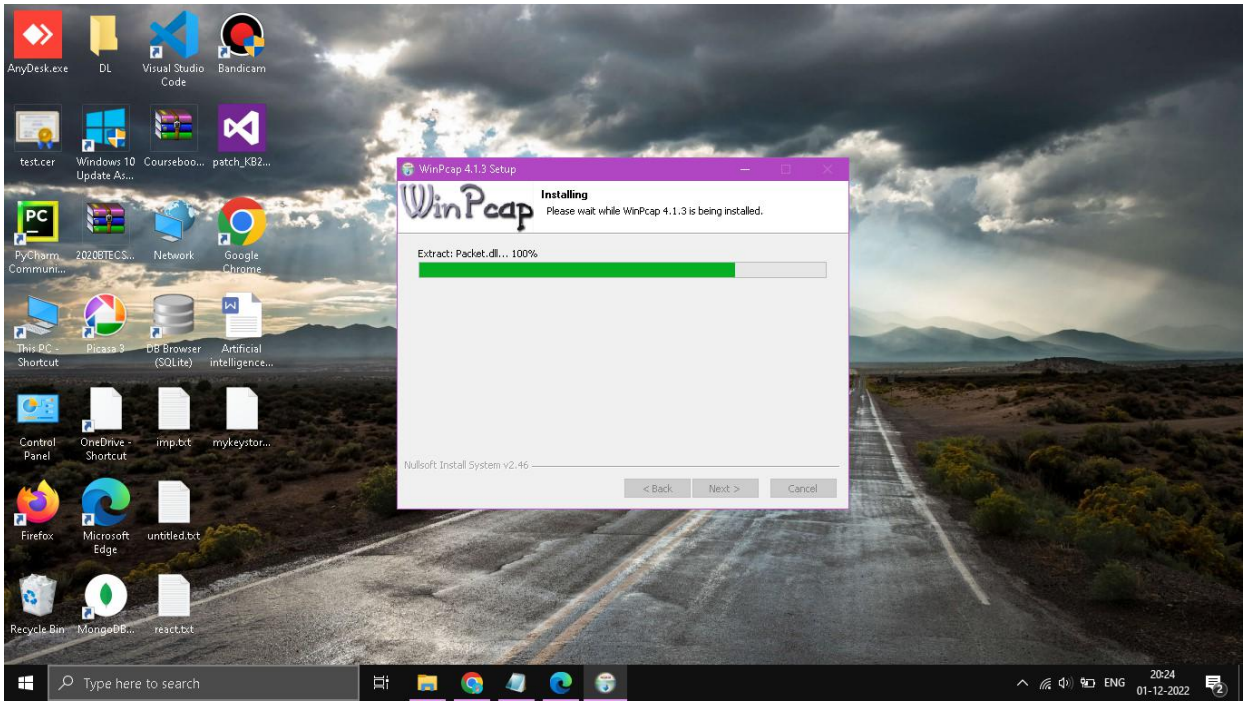

snort.org/users/sign_in
Sign In
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
Sign in
Email
mchitrakathi21@gmai
Password
Remember me
Sign in
Sign up
Forgot your password?
Snort_2_9_20_Insta....exe
2.7/3.3 MB
npcap-1.71.exe
WinPcap_4_1_3.exe
Show all
Type here to search
ENG
20:15
01-12-2022

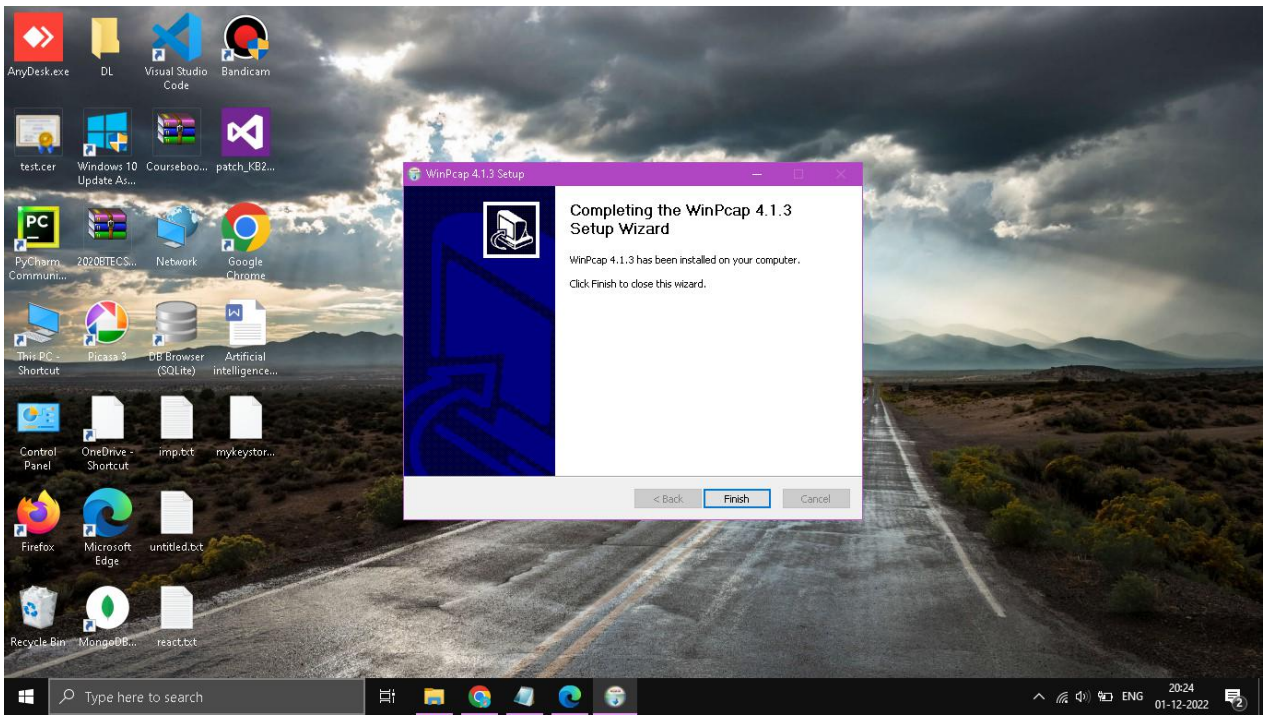

snort.org/users/862667
mchitrakathi21@gmail.com
My Account
Sign Out
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
mchitrakathi21@gmail.com
Account
Oink code
Subscription
Receipts
False Positive
Snort License
Login
Delete Account
Email
mchitrakathi21@gmail.com
Password
Edit
Snort License Agreement
License Terms Accepted
YES
Mailing Lists
Snort_2_9_20_Insta....exe
27/33 MB
npcap-1.71.exe
WinPcap_4_1_3.exe
Show all
Type here to search
ENG
20:17
01-12-2022

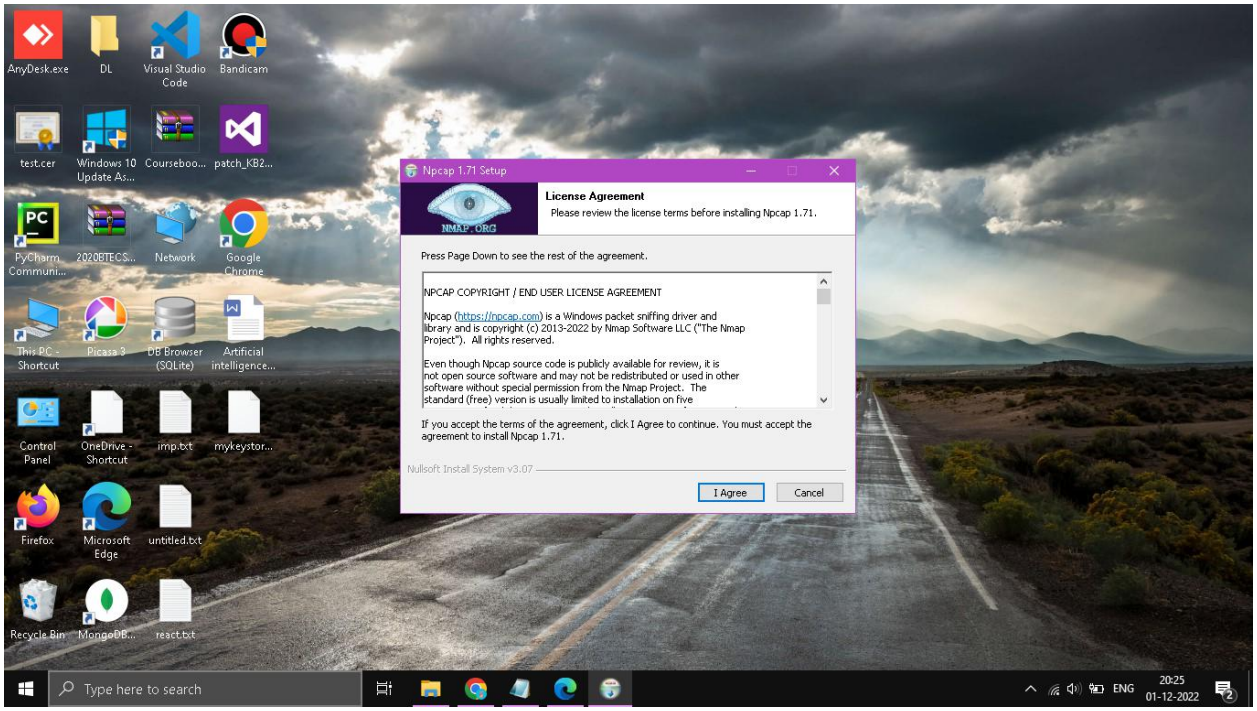

snort.org/downloads
mchitrakathi21@gmail.com
My Account
Sign Out
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
Snort v2.9
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-2911.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-2914.tar.gz
snortrules-snapshot-2915.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-2916.tar.gz
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-2917.tar.gz
snortrules-snapshot-2918.tar.gz
snortrules-snapshot-29190.tar.gz
snortrules-snapshot-29200.tar.gz
MD5s
All Sums
Subscribe
snortrules-snap....tar.gz
0.7/84.5 MB, 7 mins left
Snort_2_9_20_Insta....exe
27/33 MB
npcap-1.71.exe
WinPcap_4_1_3.exe
Show all
Type here to search
ENG
20:18
01-12-2022

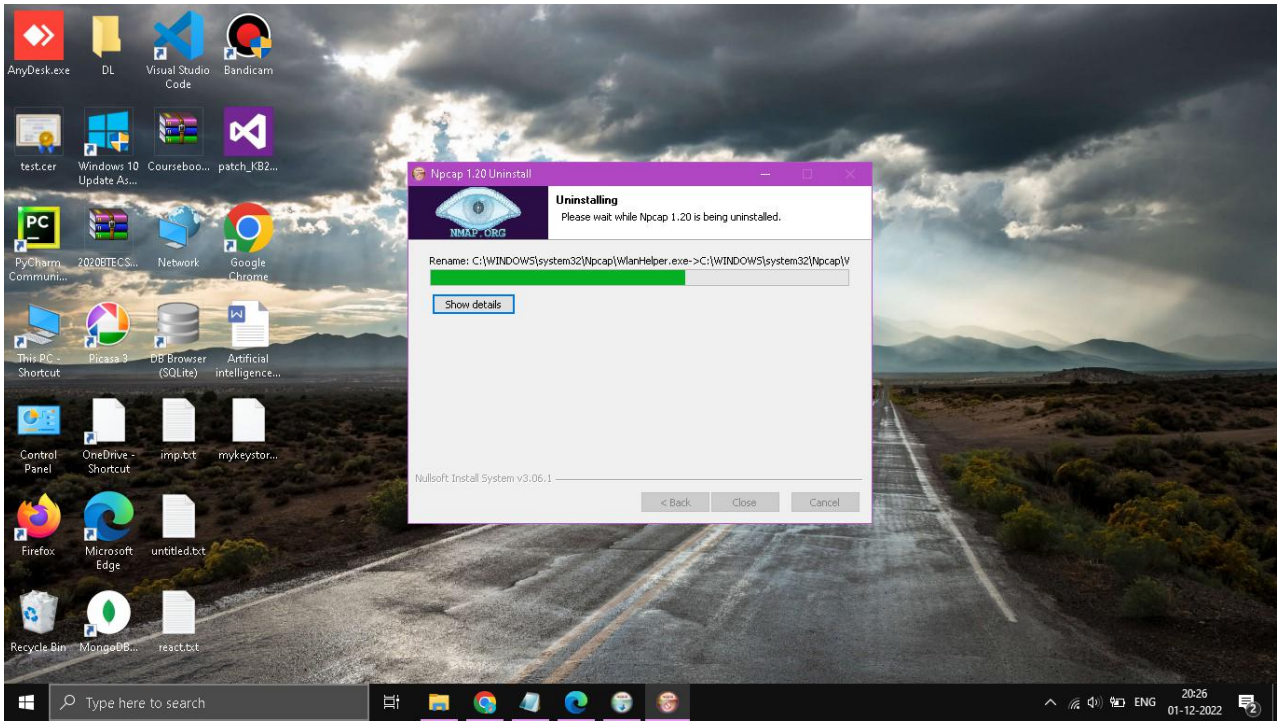

snort.org/downloads
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
My Account
Sign Out
Rules
Latest advisory:
Talos Rules 2022-12-01
What are rules?
Community
Snort v3.0
snort3-community-rules.tar.gz
Documentation
opensource.gz
Snort v2.9
community-rules.tar.gz
MD5s
All Sums
Registered
Snort v3.0
Talos_LightSPD.tar.gz
snortrules-snapshot-31470.tar.gz
snortrules-snapshot-31440.tar.gz
snortrules-snapshot-31350.tar.gz
snortrules-snapshot-31210.tar.gz
snortrules-snapshot-31200.tar.gz
snortrules-snapshot-31180.tar.gz
snortrules-snapshot-31150.tar.gz
snortrules-snapshot-31110.tar.gz
snortrules-snapshot-31190.tar.gz
Subscription
Snort v3.0
Show all
Type here to search
ENG
20:18
01-12-2022

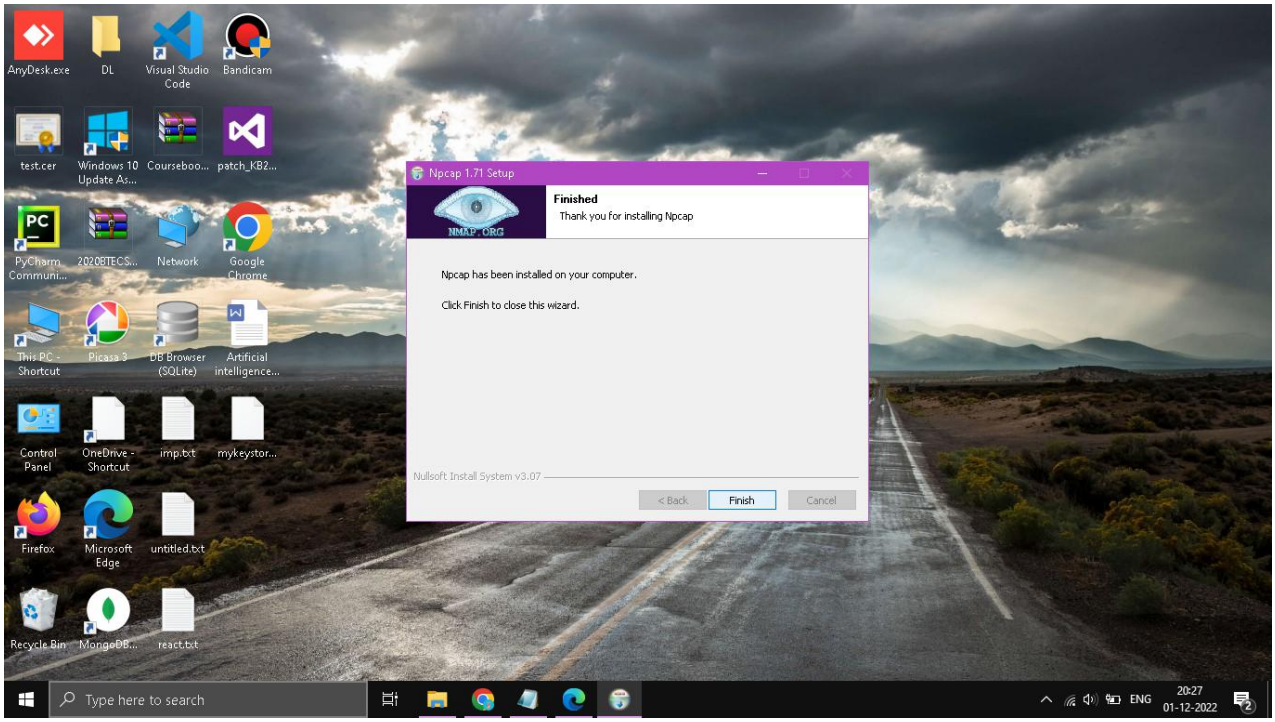

WinPcap 4.1.3 Setup
WinPcap
Installation options
Please review the following options before installing WinPcap 4.1.3
Automatically start the WinPcap driver at boot time
Nullsoft Install System v2.46
< Back
Install
Cancel
Type here to search
ENG
20:24
01-12-2022

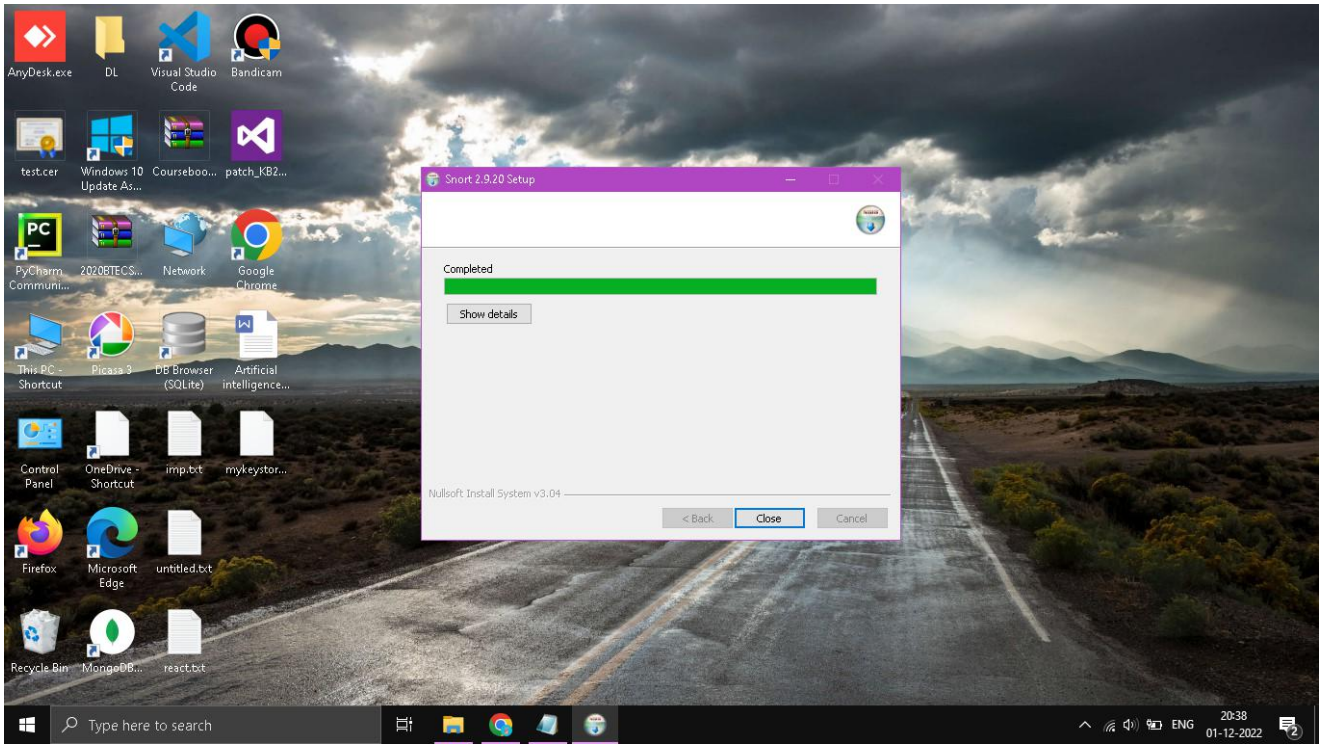

AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
WinPcap 4.1.3 Setup
WinPcap
Installing
Please wait while WinPcap 4.1.3 is being installed.
Extract: Packet.dll... 100%
Nullsoft Install System v2.46
< Back
Next >
Cancel
Type here to search
ENG
20:24
01-12-2022

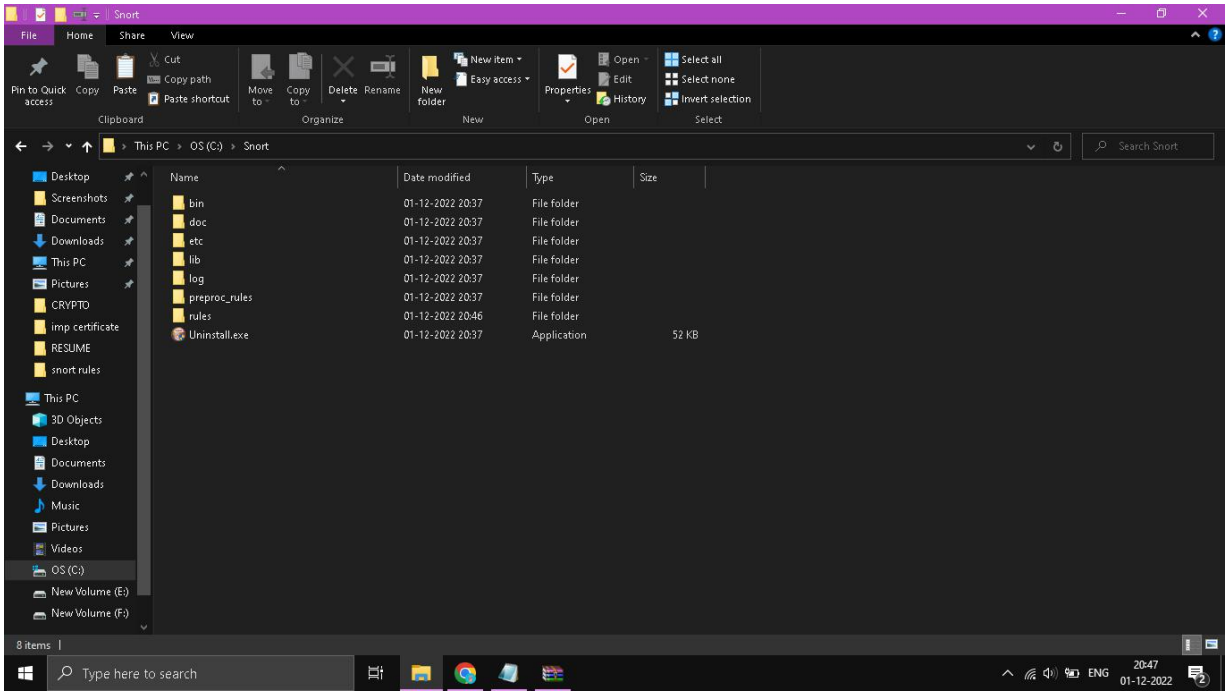

AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
WinPcap 4.1.3 Setup
Completing the WinPcap 4.1.3 Setup Wizard
WinPcap 4.1.3 has been installed on your computer.
Click Finish to close this wizard.
< Back
Finish
Cancel
Type here to search
ENG
20:24
01-12-2022

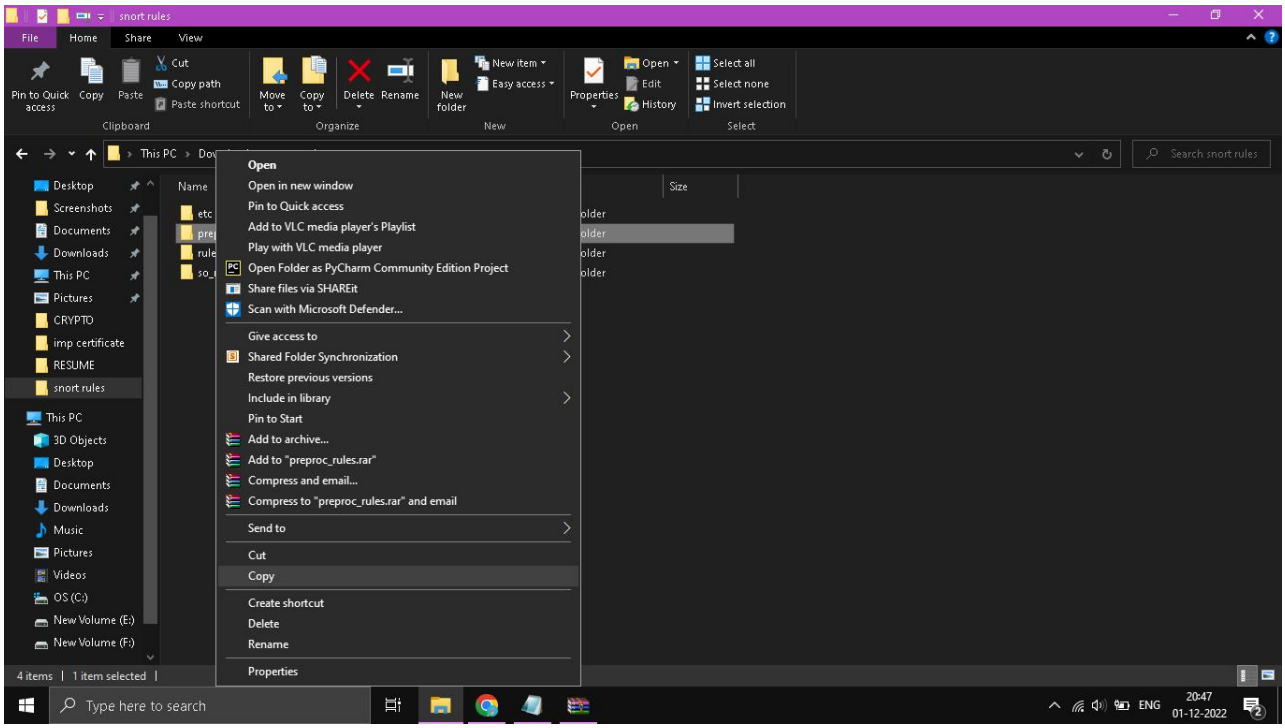

Npcap 1.71 Setup
License Agreement
Please review the license terms before installing Npcap 1.71.
NMAP.ORG
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.71.
Nullsoft Install System v3.07
I Agree
Cancel
AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
Type here to search
ENG
20:25
01-12-2022

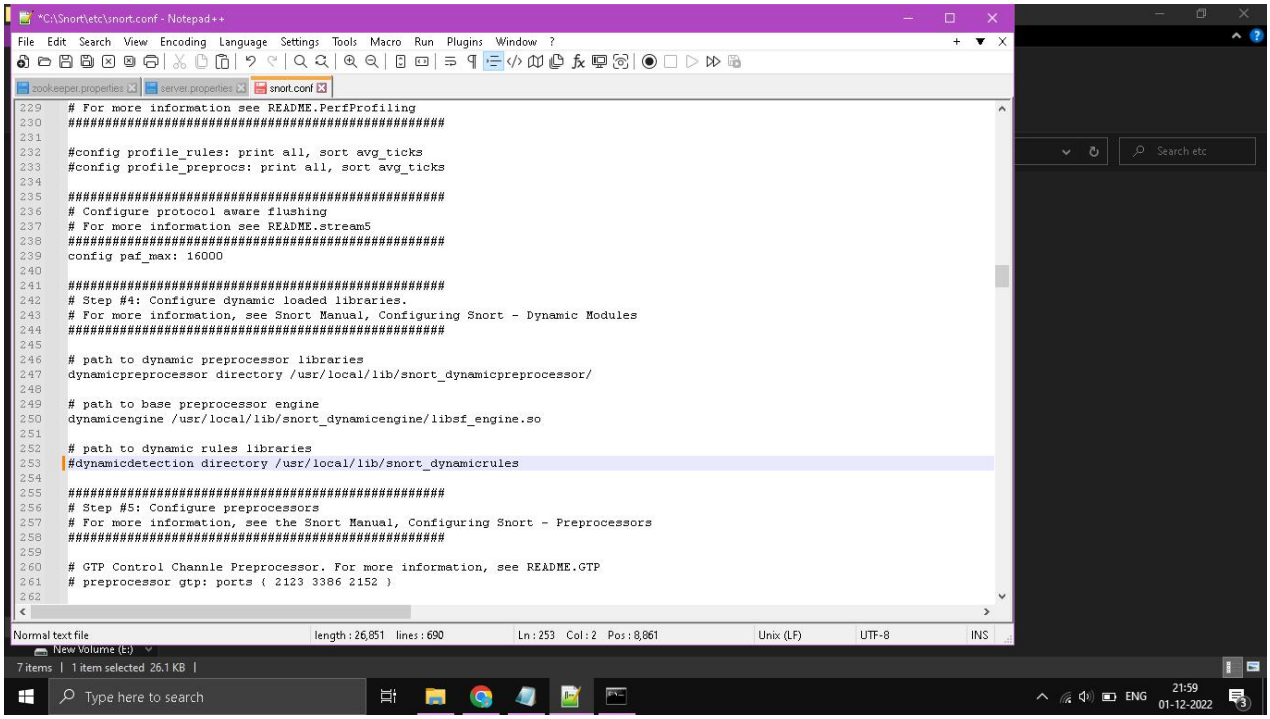

Npcap 1.20 Uninstall
Uninstalling
Please wait while Npcap 1.20 is being uninstalled.
NMAP.ORG
Rename: C:\WINDOWS\system32\Npcap\WlanHelper.exe->C:\WINDOWS\system32\Npcap\V
Show details
Nullsoft Install System v3.06.1
< Back
Close
Cancel
AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
Type here to search
ENG
20:26
01-12-2022

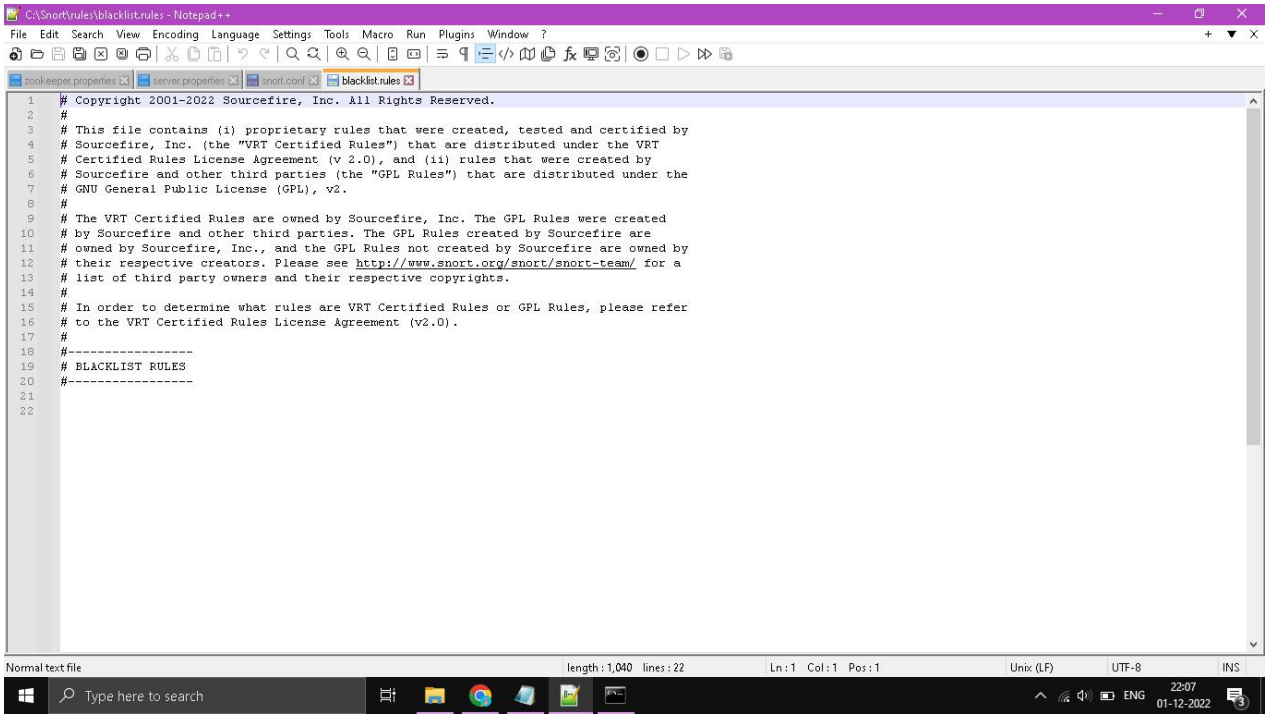

AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
Npcap 1.71 Setup
Finished
Thank you for installing Npcap
NMAP.ORG
Npcap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v3.07
< Back
Finish
Cancel
Type here to search
ENG
20:27
01-12-2022

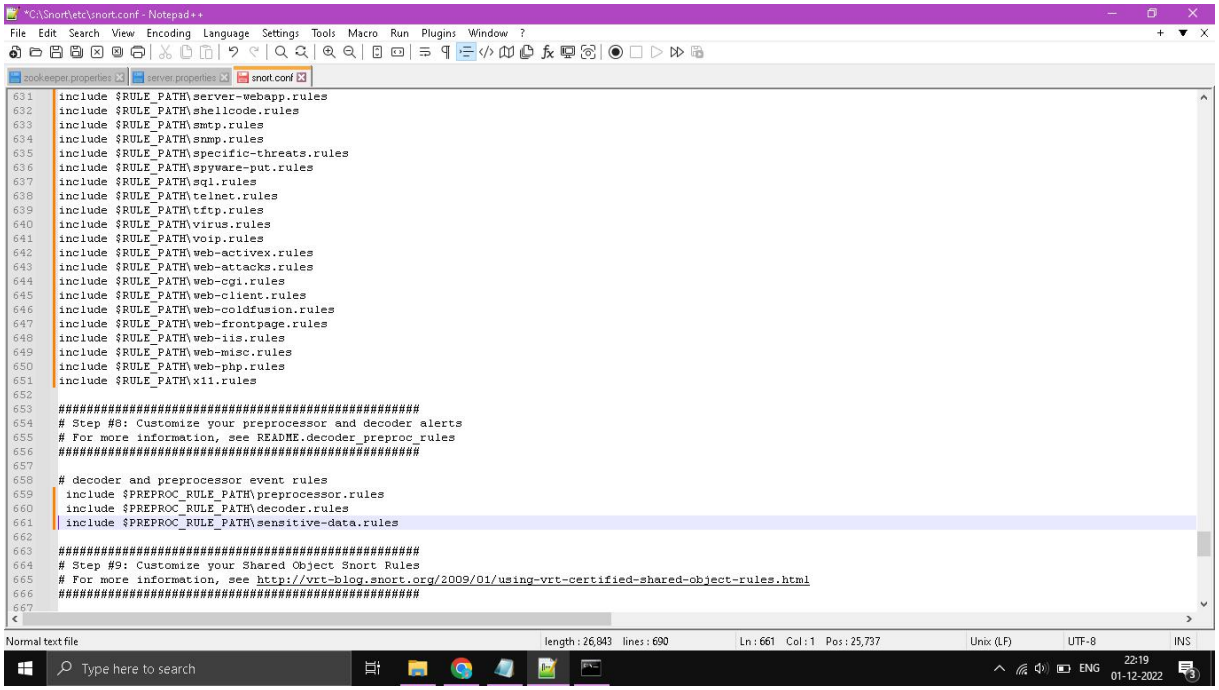

AnyDesk.exe
DL
Visual Studio Code
Bandicam
test.cer
Windows 10 Update As...
Courseboo...
patch_KB2...
PyCharm Communi...
2020BTECS...
Network
Google Chrome
This PC - Shortcut
Picasa 3
DB Browser (SQLite)
Artificial intelligence...
Control Panel
OneDrive - Shortcut
imp.txt
mykeystor...
Firefox
Microsoft Edge
untitled.txt
Recycle Bin
MongoDB...
react.txt
Snort 2.9.20 Setup
Completed
Show details
Nullsoft Install System v3.04
< Back
Close
Cancel
Type here to search
ENG
20:38
01-12-2022

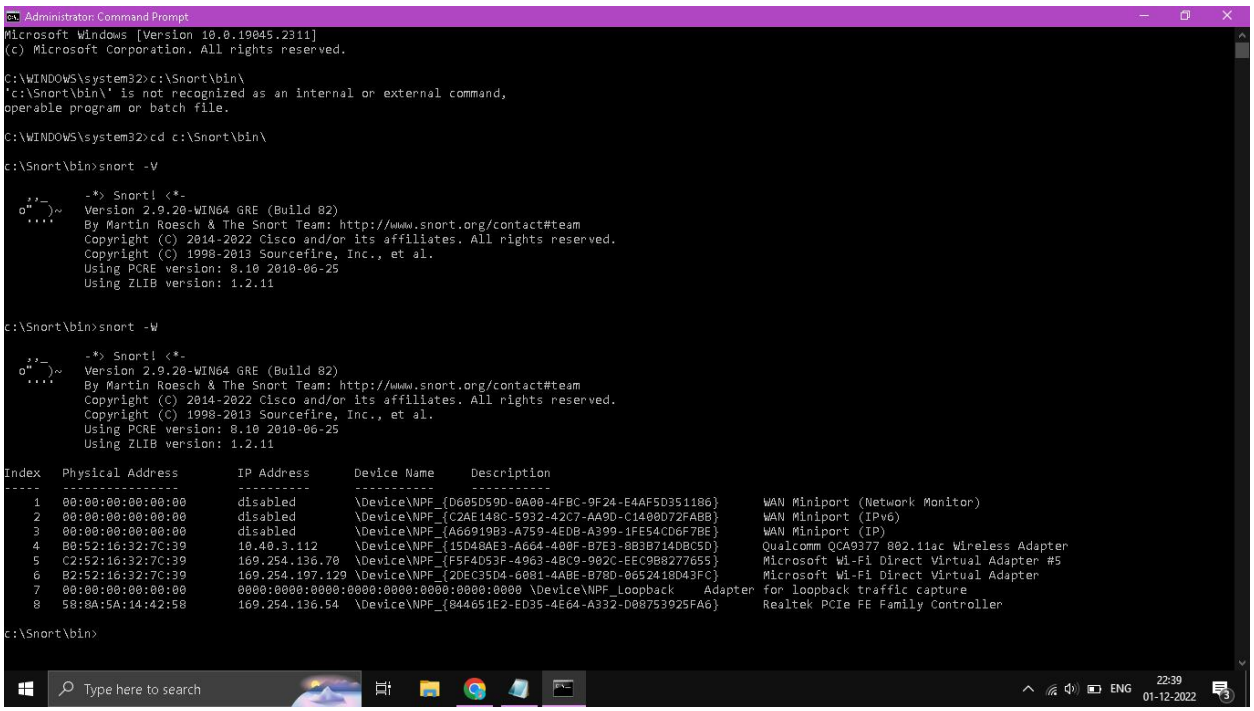

Snort
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
OS (C:)
Snort
Search Snort
Desktop
Screenshots
Documents
Downloads
This PC
Pictures
CRYPTO
imp certificate
RESUME
snort rules
3D Objects
Music
Videos
New Volume (E:)
New Volume (F:)
Name
Date modified
Type
Size
bin
doc
etc
lib
log
preproc_rules
rules
Uninstall.exe
01-12-2022 20:37
01-12-2022 20:46
File folder
Application
52 KB
8 items
Type here to search
ENG
20:47
01-12-2022

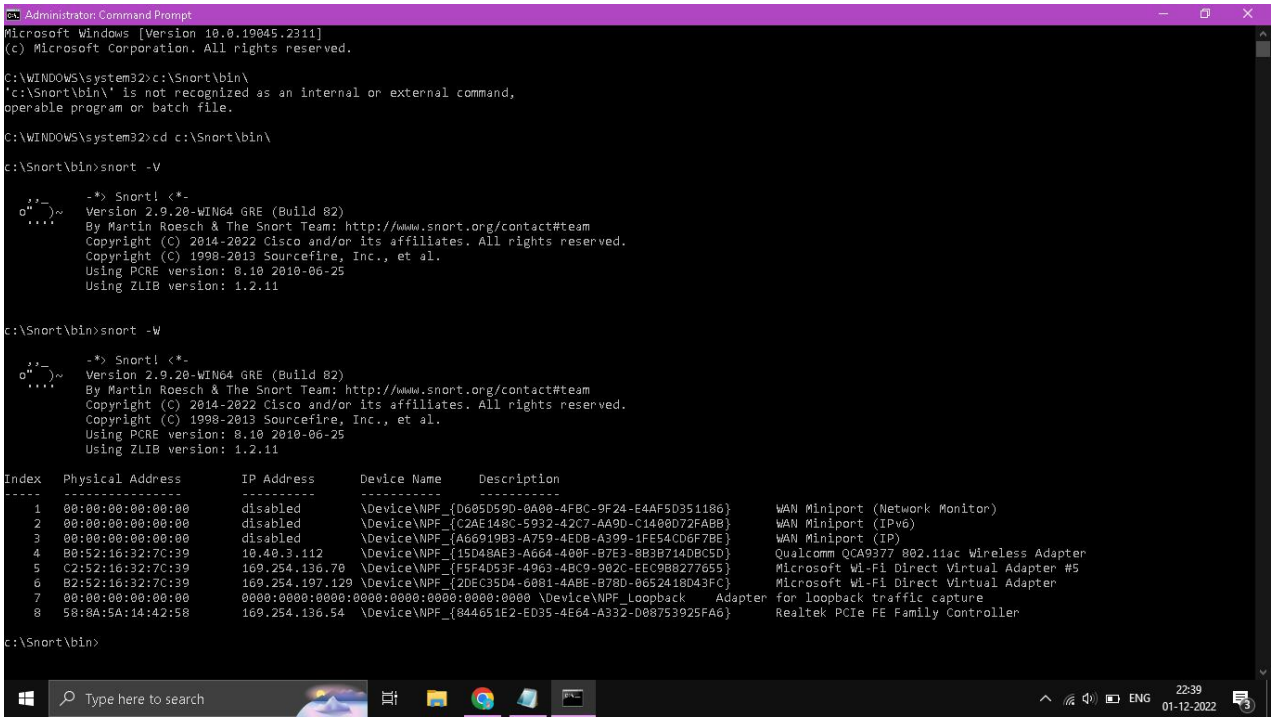

snort rules
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Search snort rules
Open
Open in new window
Pin to Quick access
Add to VLC media player's Playlist
Play with VLC media player
Open Folder as PyCharm Community Edition Project
Share files via SHAREit
Scan with Microsoft Defender...
Give access to
Shared Folder Synchronization
Restore previous versions
Include in library
Pin to Start
Add to archive...
Add to "preproc_rules.rar"
Compress and email...
Compress to "preproc_rules.rar" and email
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
4 items
1 item selected
Type here to search
ENG
20:47
01-12-2022

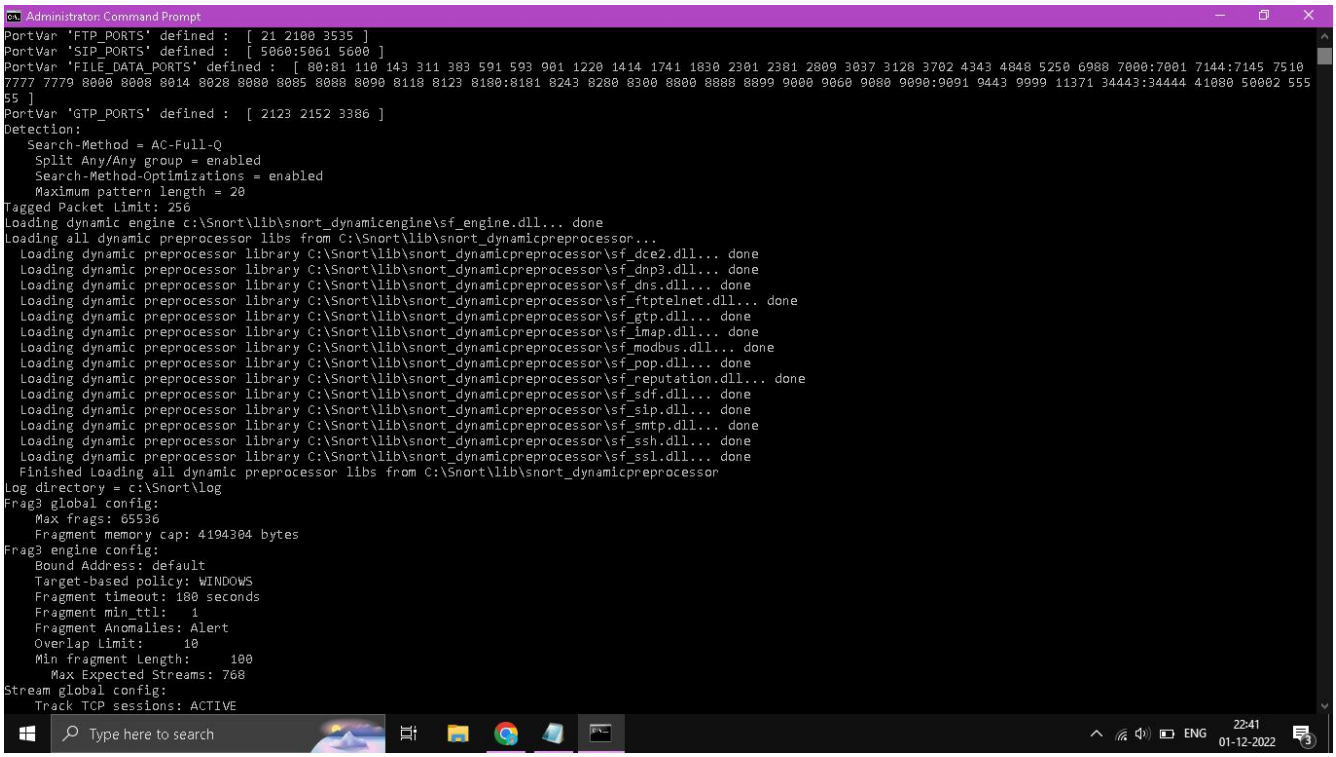

*C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
zookeeper.properties
server.properties
snort.conf
For more information see README.PerfProfiling
##
#config profile_rules: print all, sort avg_ticks
#config profile_preprocs: print all, sort avg_ticks
##
Configure protocol aware flushing
For more information see README.stream5
##
config paf_max: 16000
##
Step #4: Configure dynamic loaded libraries.
For more information, see Snort Manual, Configuring Snort - Dynamic Modules
##
path to dynamic preprocessor libraries
dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/
path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
path to dynamic rules libraries
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
##
Step #5: Configure preprocessors
For more information, see the Snort Manual, Configuring Snort - Preprocessors
##
GTP Control Channle Preprocessor. For more information, see README.GTP
preprocessor gtp: ports { 2123 3386 2152 }
Normal text file length : 26,851 lines : 690 Ln : 253 Col : 2 Pos : 8,861 Unix (LF) UTF-8 INS
New Volume (E:)
7 items | 1 item selected 26.1 KB
Type here to search
ENG 21:59 01-12-2022

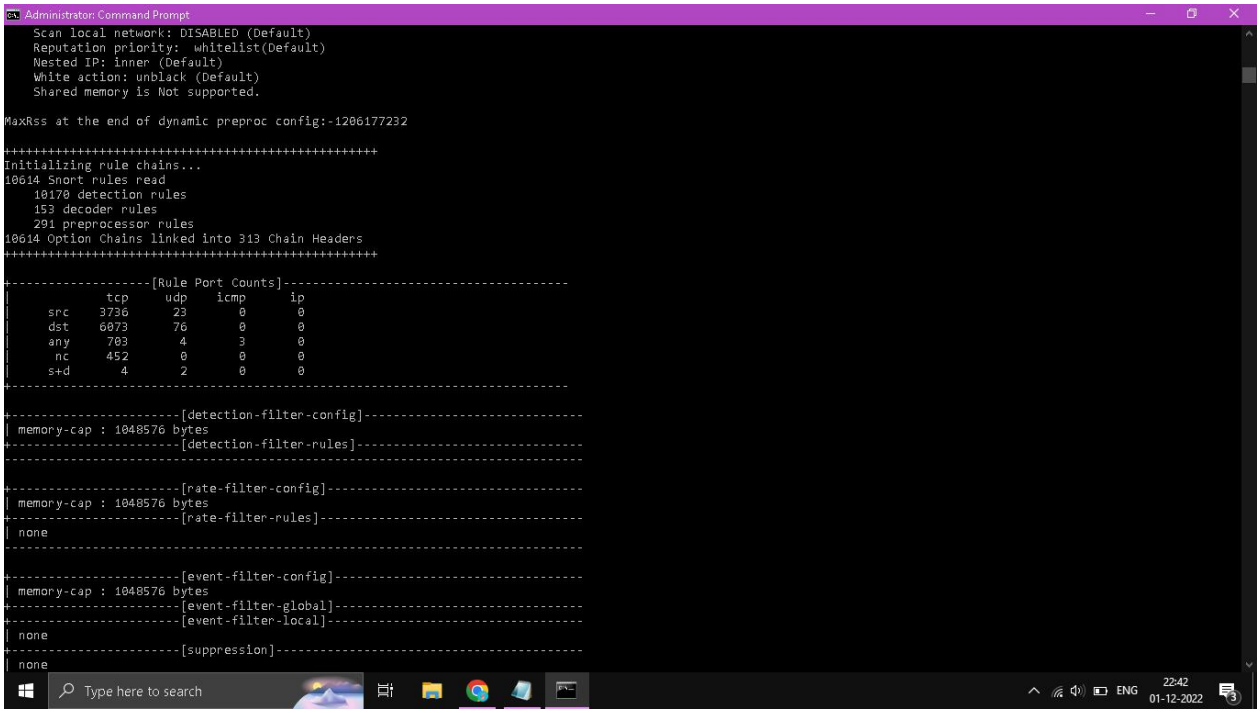

C:\Snort\rules\blacklist.rules - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
zookeeper.properties
server.properties
snort.conf
blacklist.rules
Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
This file contains (i) proprietary rules that were created, tested and certified by
Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
Sourcefire and other third parties (the "GPL Rules") that are distributed under the
GNU General Public License (GPL), v2.
#
The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
list of third party owners and their respective copyrights.
#
In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
to the VRT Certified Rules License Agreement (v2.0).
#
#------------------
BLACKLIST RULES
#------------------
Normal text file length : 1,040 lines : 22 Ln : 1 Col : 1 Pos : 1 Unix (LF) UTF-8 INS
Type here to search
ENG 22:07 01-12-2022

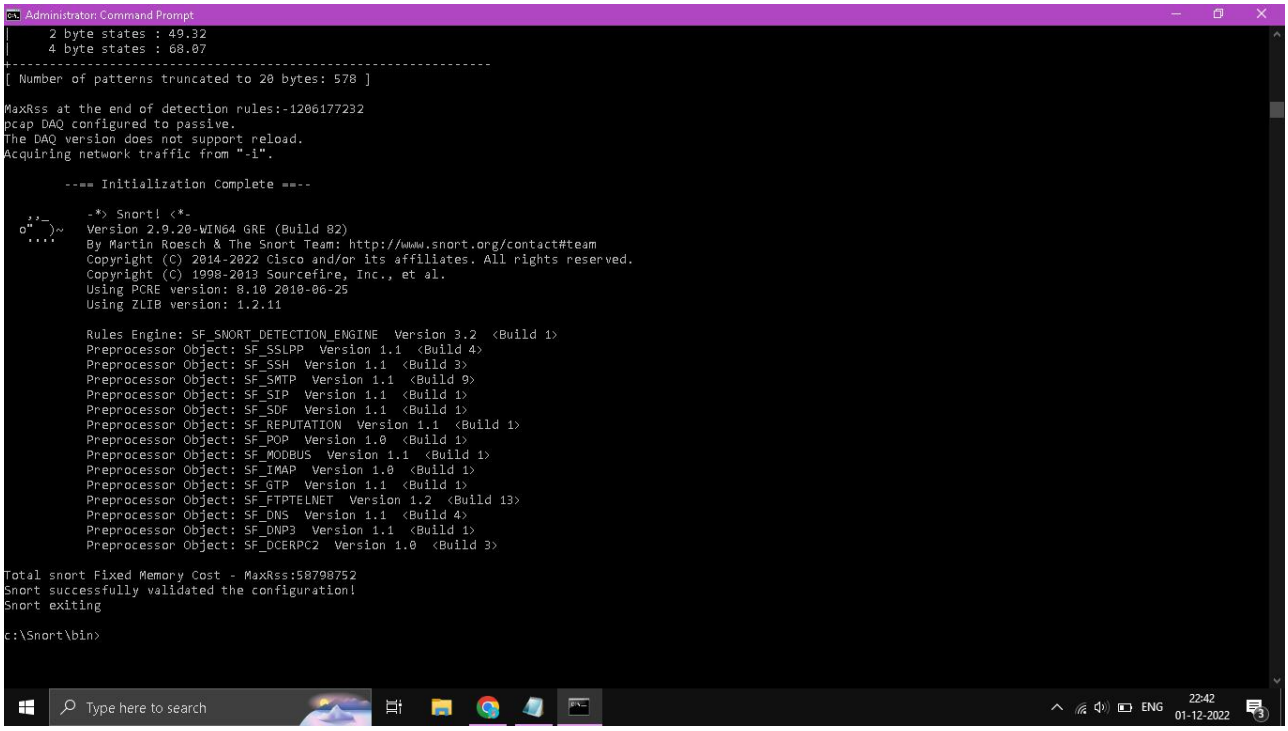

*C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
zookeeper.properties
server.properties
snort.conf
include $RULE_PATH\server-webapp.rules
include $RULE_PATH\shellcode.rules
include $RULE_PATH\smtp.rules
include $RULE_PATH\snmp.rules
include $RULE_PATH\specific-threats.rules
include $RULE_PATH\spyware-put.rules
include $RULE_PATH\sql.rules
include $RULE_PATH\telnet.rules
include $RULE_PATH\tftp.rules
include $RULE_PATH\virus.rules
include $RULE_PATH\voip.rules
include $RULE_PATH\web-activex.rules
include $RULE_PATH\web-attacks.rules
include $RULE_PATH\web-cgi.rules
include $RULE_PATH\web-client.rules
include $RULE_PATH\web-coldfusion.rules
include $RULE_PATH\web-frontpage.rules
include $RULE_PATH\web-iis.rules
include $RULE_PATH\web-misc.rules
include $RULE_PATH\web-php.rules
include $RULE_PATH\x11.rules
Step #8: Customize your preprocessor and decoder alerts
For more information, see README.decoder_preproc_rules
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: Customize your Shared Object Snort Rules
For more information, see http://vrt-blog.snort.org/2009/01/using-vrt-certified-shared-object-rules.html
Normal text file
length : 26,843 lines : 690
Ln : 661 Col : 1 Pos : 25,737
Unix (LF)
UTF-8
INS
Type here to search
ENG
22:19
01-12-2022


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2311]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>c:\Snort\bin\
'c:\Snort\bin\' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32>cd c:\Snort\bin\
c:\Snort\bin>snort -V
-*> 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>snort -W
-*> 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
Index Physical Address IP Address Device Name Description
1 00:00:00:00:00:00 disabled \Device\NPF_{D605D59D-0A00-4FBC-9F24-E4AF5D351186} WAN Miniport (Network Monitor)
2 00:00:00:00:00:00 disabled \Device\NPF_{C2AE148C-5932-42C7-AA9D-C1400D72FABB} WAN Miniport (IPv6)
3 00:00:00:00:00:00 disabled \Device\NPF_{A66919B3-A759-4EDB-A399-1FE54CD6F7BE} WAN Miniport (IP)
4 B0:52:16:32:7C:39 10.40.3.112 \Device\NPF_{15D48AE3-A664-400F-B7E3-8B3B714DBC5D} Qualcomm QCA9377 802.11ac Wireless Adapter
5 C2:52:16:32:7C:39 169.254.136.70 \Device\NPF_{F5F4D53F-4963-48C9-902C-EEC9B8277655} Microsoft Wi-Fi Direct Virtual Adapter #5
6 B2:52:16:32:7C:39 169.254.197.129 \Device\NPF_{2DEC35D4-6081-4ABE-B78D-0652418D43FC} Microsoft Wi-Fi Direct Virtual Adapter
7 00:00:00:00:00:00 0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture
8 58:8A:5A:14:42:58 169.254.136.54 \Device\NPF_{844651E2-ED35-4E64-A332-D08753925FA6} Realtek PCIe FE Family Controller
c:\Snort\bin>
Type here to search
ENG
22:39
01-12-2022


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2311]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>c:\Snort\bin\
'c:\Snort\bin\' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32>cd c:\Snort\bin\
c:\Snort\bin>snort -V
-*> 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>snort -W
-*> 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
Index Physical Address IP Address Device Name Description
1 00:00:00:00:00:00 disabled \Device\NPF_{D605D59D-0A00-4FBC-9F24-E4AF5D351186} WAN Miniport (Network Monitor)
2 00:00:00:00:00:00 disabled \Device\NPF_{C2AE148C-5932-42C7-AA9D-C1400D72FABB} WAN Miniport (IPv6)
3 00:00:00:00:00:00 disabled \Device\NPF_{A66919B3-A759-4EDB-A399-1FE54CD6F7BE} WAN Miniport (IP)
4 B0:52:16:32:7C:39 10.40.3.112 \Device\NPF_{15D48AE3-A664-400F-B7E3-8B3B714DBC5D} Qualcomm QCA9377 802.11ac Wireless Adapter
5 C2:52:16:32:7C:39 169.254.136.70 \Device\NPF_{F5F4D53F-4963-4BC9-902C-EEC9B8277655} Microsoft Wi-Fi Direct Virtual Adapter #5
6 B2:52:16:32:7C:39 169.254.197.129 \Device\NPF_{2DEC35D4-6081-4ABE-B78D-0652418D43FC} Microsoft Wi-Fi Direct Virtual Adapter
7 00:00:00:00:00:00 0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture
8 58:8A:5A:14:42:58 169.254.136.54 \Device\NPF_{844651E2-ED35-4E64-A332-D08753925FA6} Realtek PCIe FE Family Controller
c:\Snort\bin>
Type here to search
ENG
22:39
01-12-2022


Administrator: Command Prompt
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 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 555
55]
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:
Bound Address: default
Target-based policy: WINDOWS
Fragment timeout: 180 seconds
Fragment min_ttl: 1
Fragment Anomalies: Alert
Overlap Limit: 10
Min fragment Length: 100
Max Expected Streams: 768
Stream global config:
Track TCP sessions: ACTIVE
Type here to search
ENG
22:41
01-12-2022


Administrator: Command Prompt
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:-1206177232
Initializing rule chains...
10614 Snort rules read
10170 detection rules
153 decoder rules
291 preprocessor rules
10614 Option Chains linked into 313 Chain Headers
[Rule Port Counts]
tcp udp icmp ip
src 3736 23 0 0
dst 6073 76 0 0
any 703 4 3 0
nc 452 0 0 0
s+d 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
Type here to search
ENG
22:42
01-12-2022


Administrator: Command Prompt
2 byte states : 49.32
4 byte states : 68.07
[Number of patterns truncated to 20 bytes: 578]
MaxRss at the end of detection rules:-1206177232
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "-i".
--== 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_MODBUS 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:58798752
Snort successfully validated the configuration!
Snort exiting
c:\Snort\bin>
Type here to search
ENG
22:42
01-12-2022