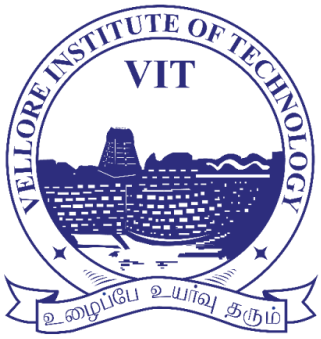


VIT®

Vellore Institute of Technology

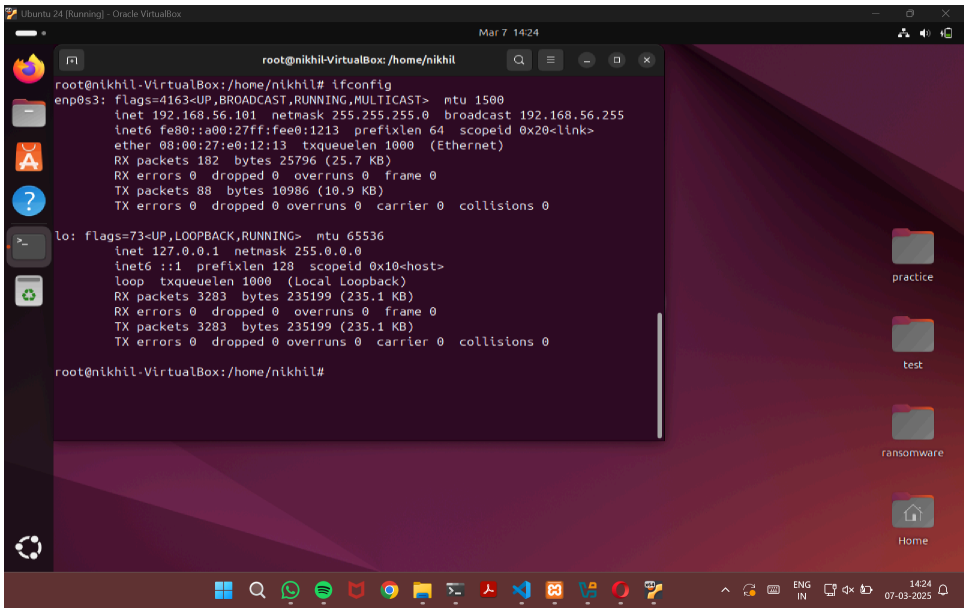
(Deemed to be University under section 3 of UGC Act, 1956)

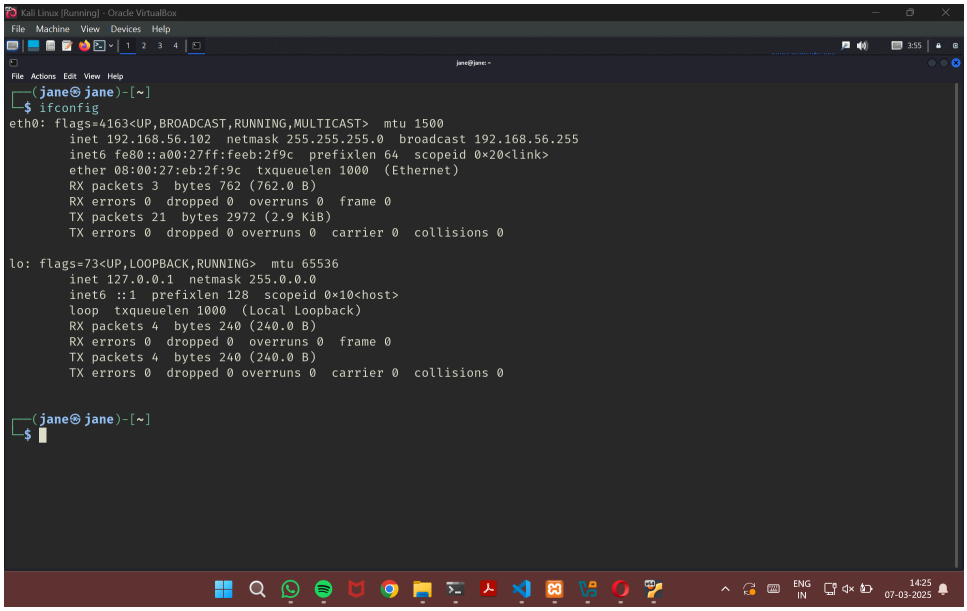
SNORT DEMO

NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

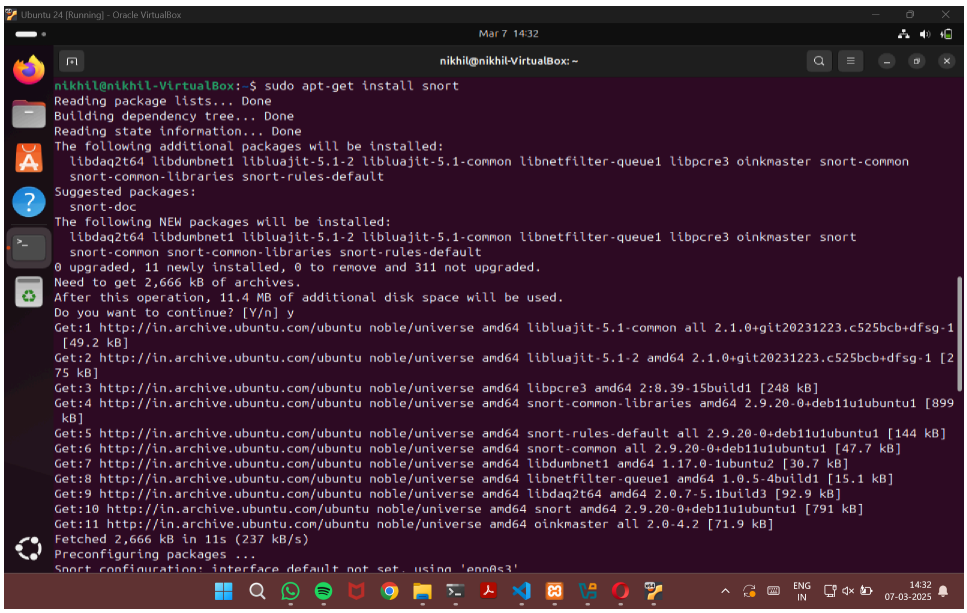
1. IP addresses of the Kali Linux and Ubuntu virtual machines



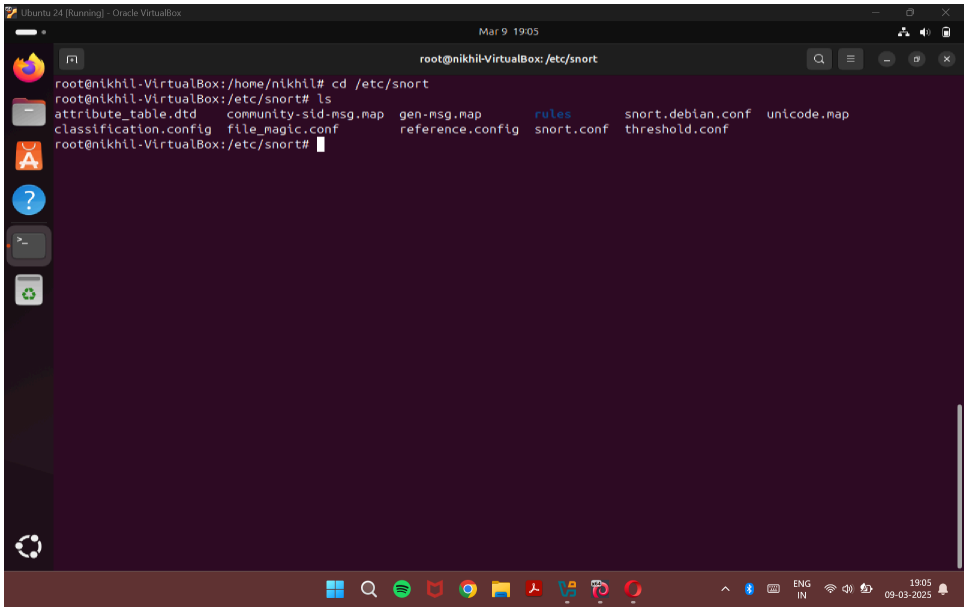


22BCE0826
Dhevatha S P

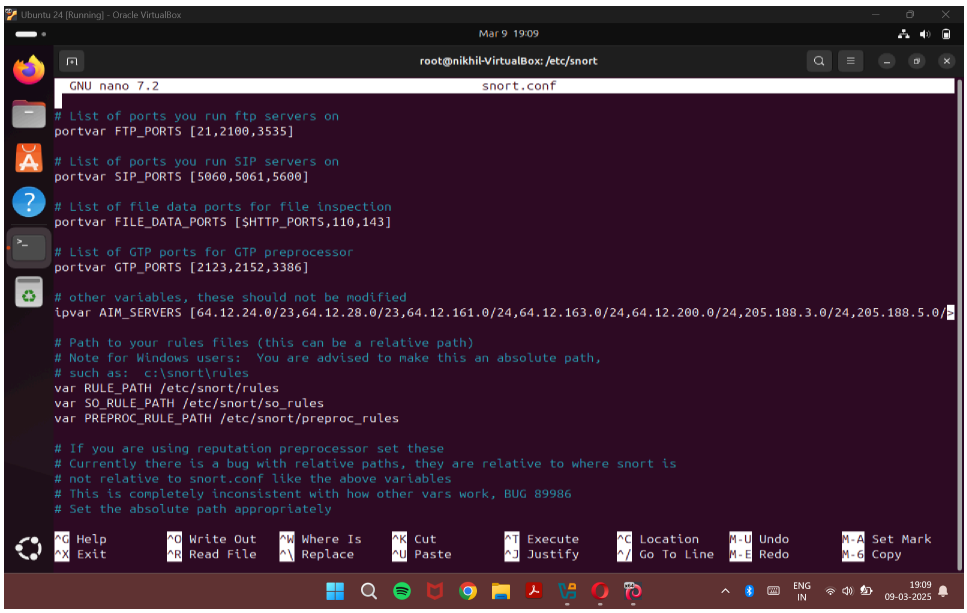
2. Installing SNORT in Ubuntu machine

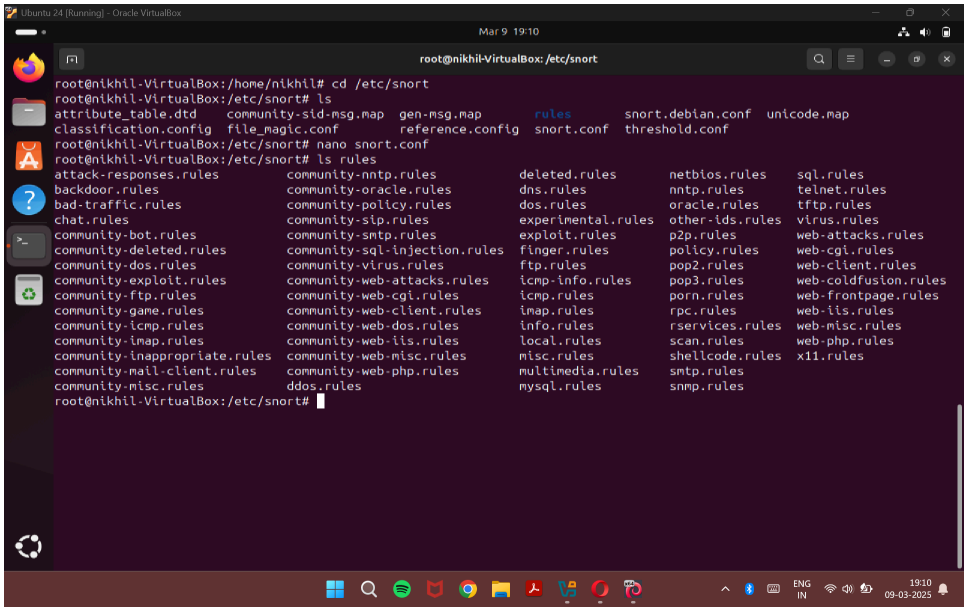


3. Locating the SNORT directory and the snort.conf file. And the rules directory.



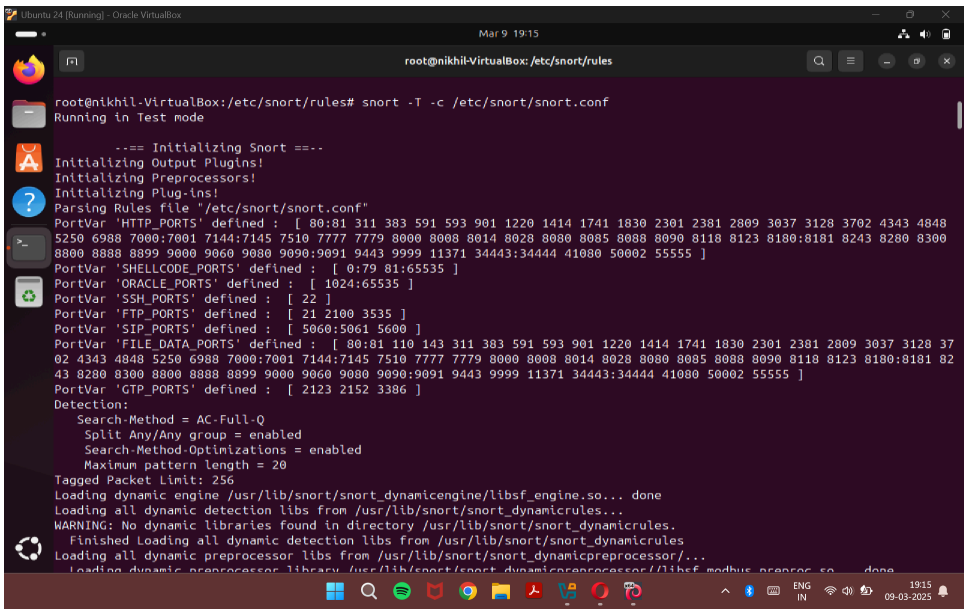
22BCE0826
Dhevatha S P



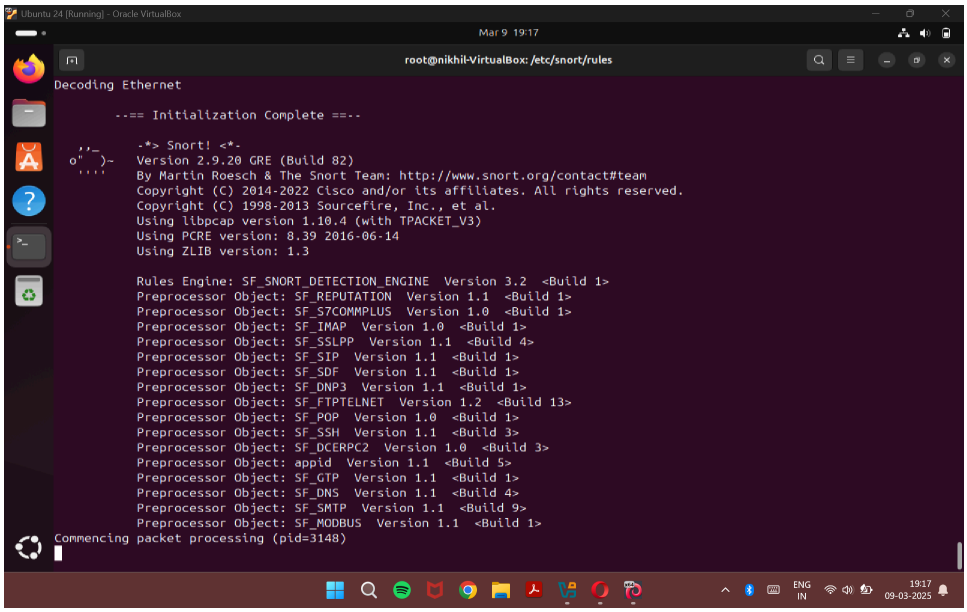


22BCE0826
Dhevatha S P

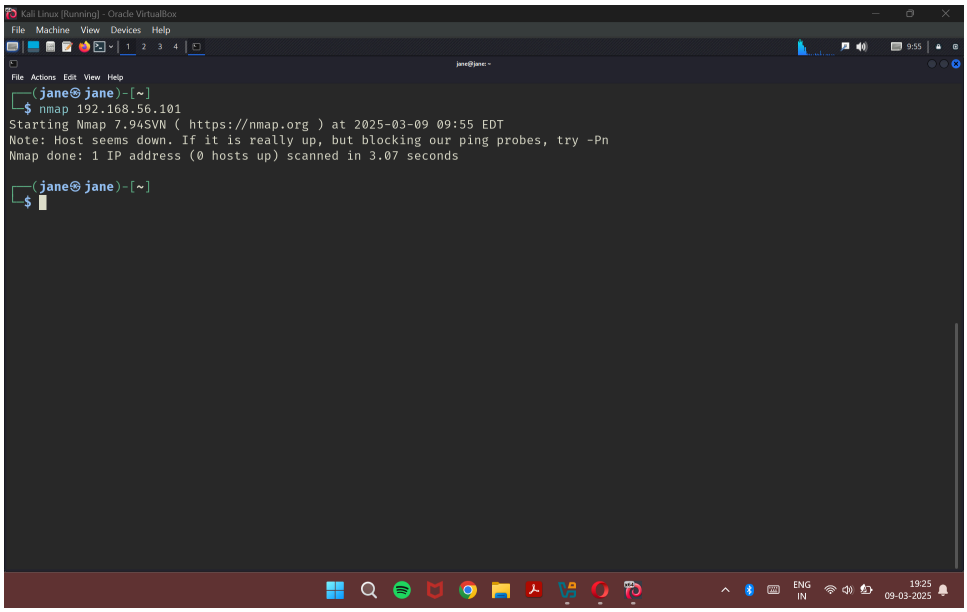
4. Testing the snort.conf

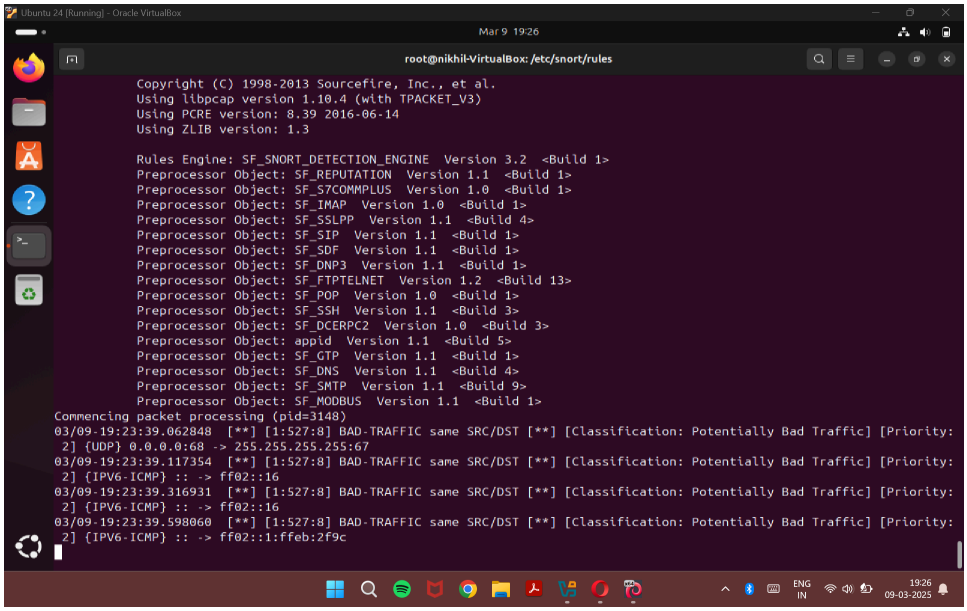


5. Running the snort.conf with the cmd - snort -A console -c /etc/snort/snort.conf

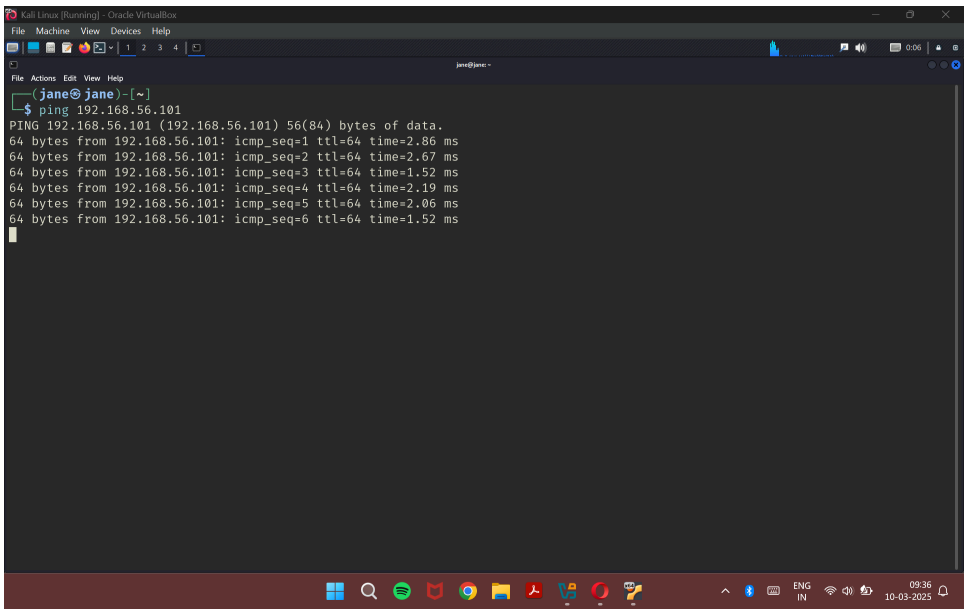


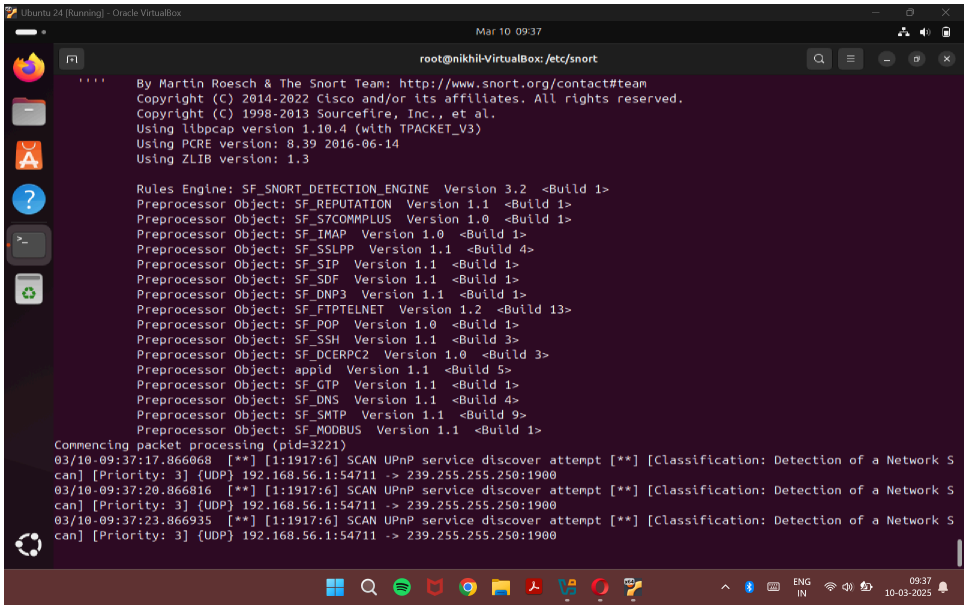
6. Performing NMAP scan from Kali Linux to Ubuntu while SNORT is still running



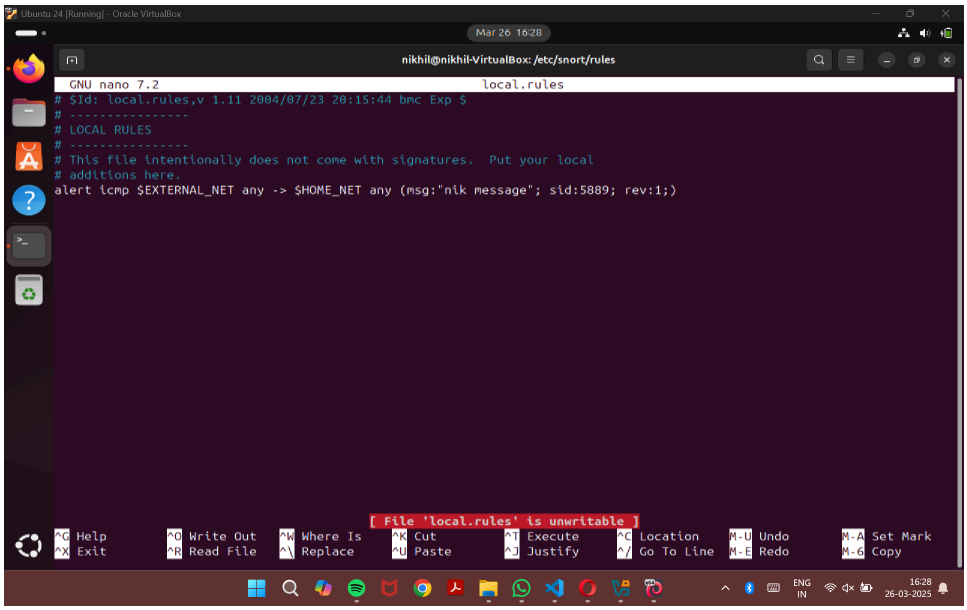


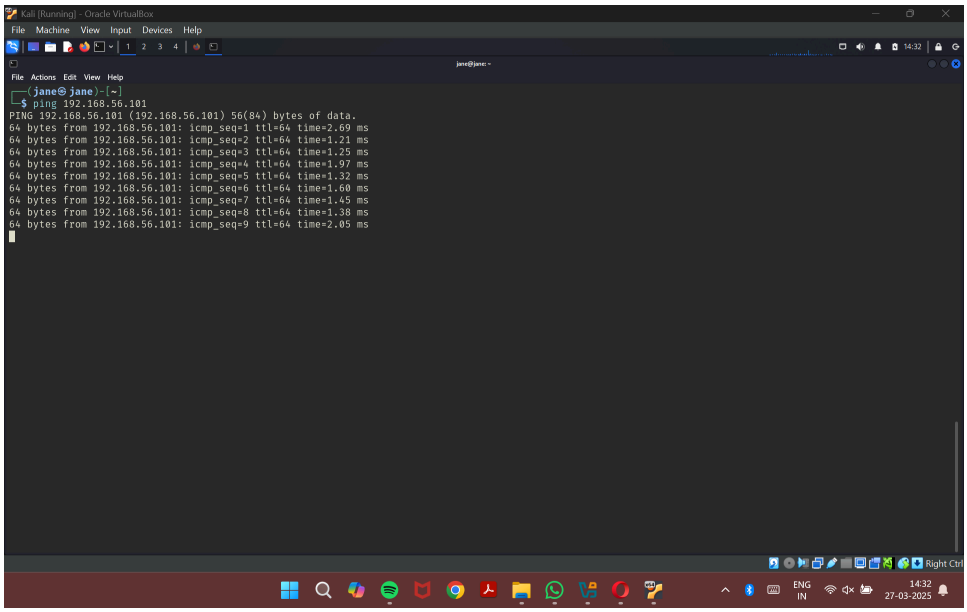
7. Pinging Ubuntu from Kali Linux

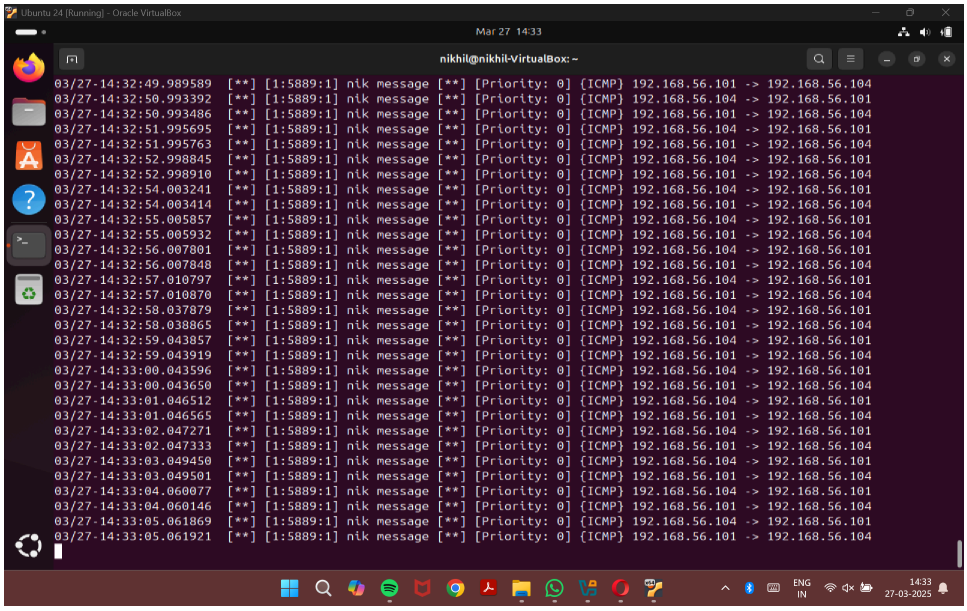




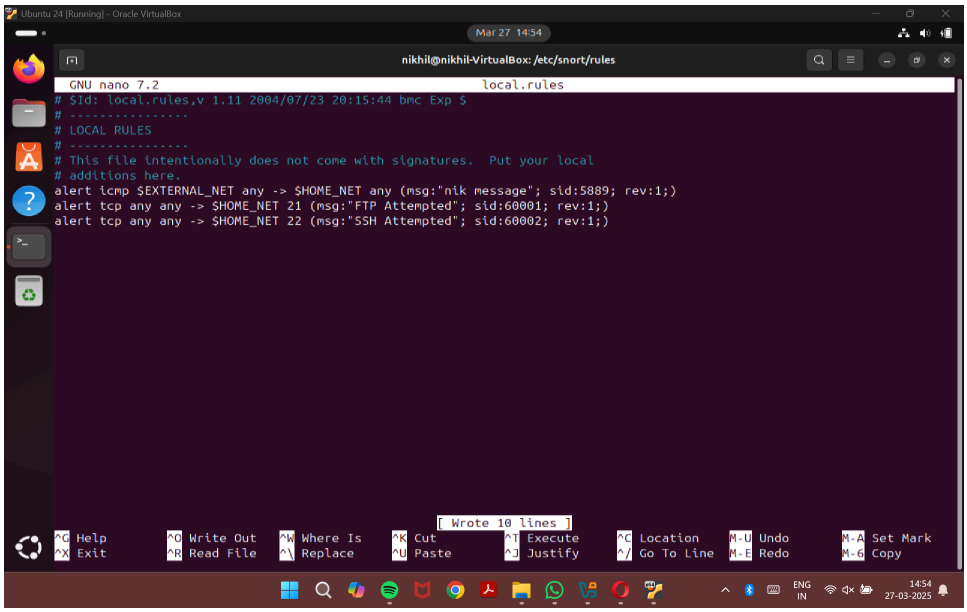
8. Adding rules to local.rules and testing validation
    a. Alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:”nik message”; sid:5889;rev:1;)

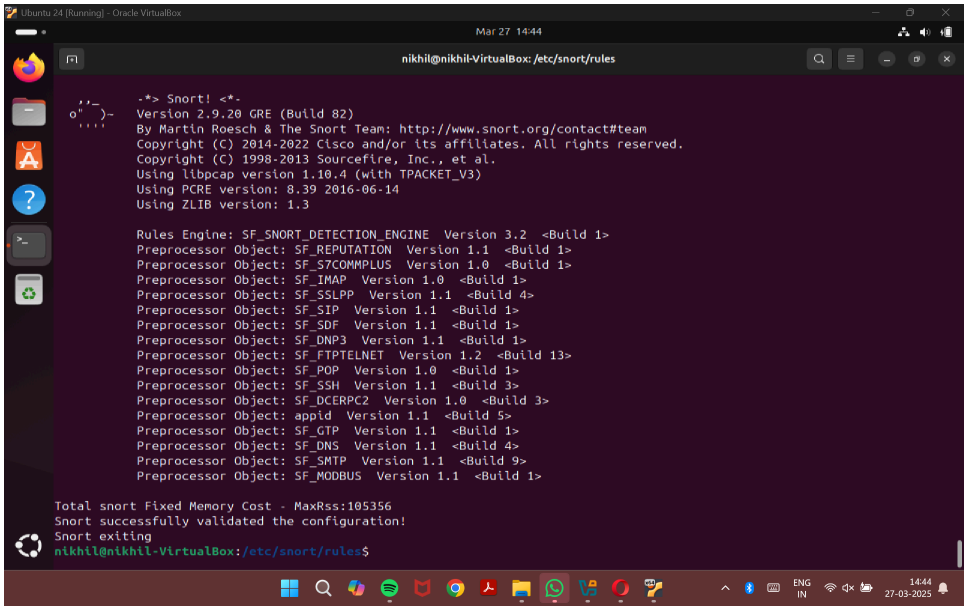


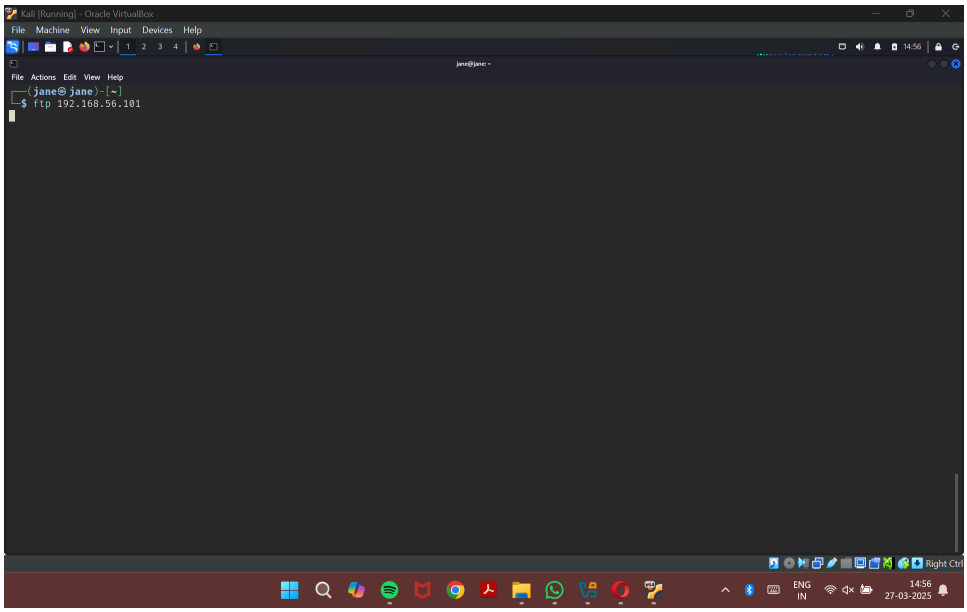


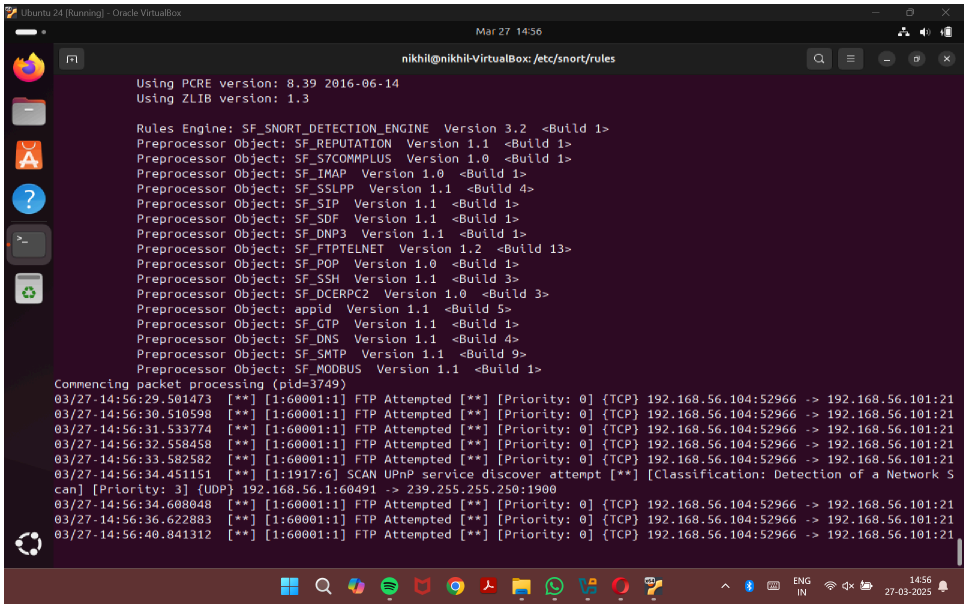


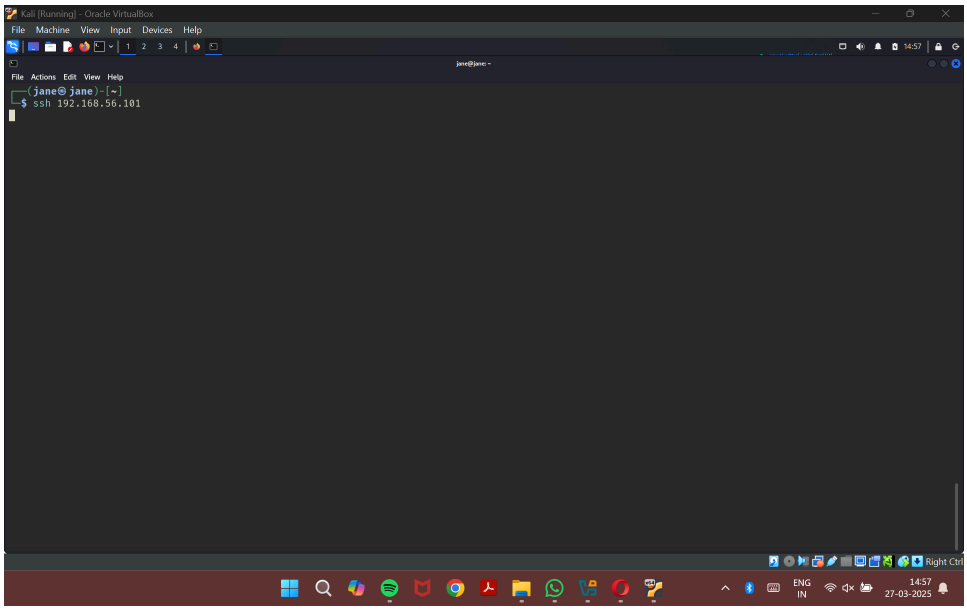
b. alert tcp any any -> $HOME_NET 21 (msg:"FTP Attempted"; sid:60001;rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH Attempted"; sid:60001;rev:1;)

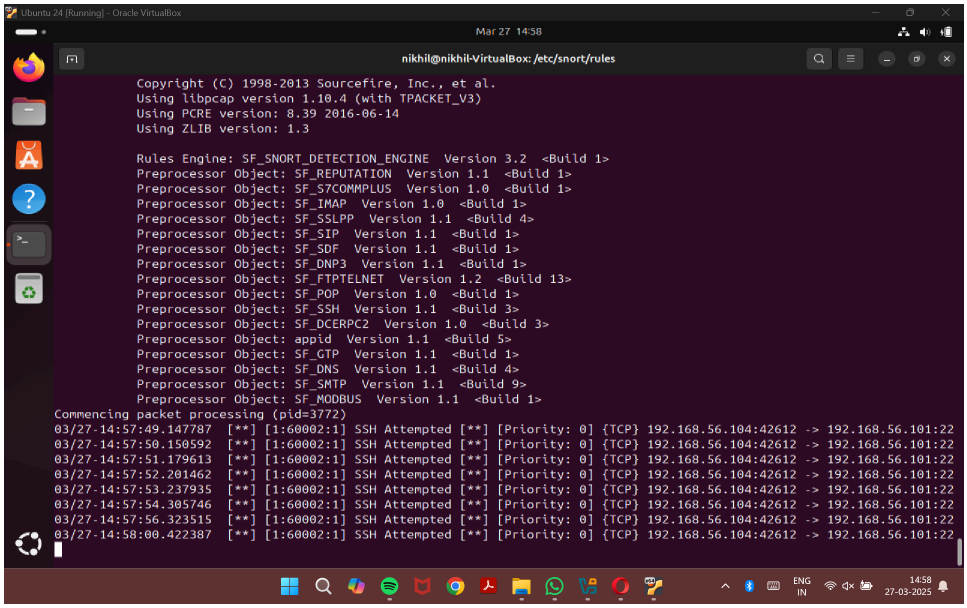



Ubuntu 24 [Running] - Oracle VirtualBox
Mar 27 14:44
nikhil@nikhil-VirtualBox: /etc/snort/rules
-*> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Total snort Fixed Memory Cost - MaxRss:105356
Snort successfully validated the configuration!
Snort exiting
nikhil@nikhil-VirtualBox:/etc/snort/rules$
ENG IN
14:44
27-03-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(jane㉿jane)-[~]
$ ftp 192.168.56.101
Right Ctrl
ENG IN
14:56
27-03-2025


Ubuntu 24 [Running] - Oracle VirtualBox
Mar 27 14:56
nikhil@nikhil-VirtualBox: /etc/snort/rules
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Commencing packet processing (pid=3749)
03/27-14:56:29.501473 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:30.510598 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:31.533774 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:32.558458 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:33.582582 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:34.451151 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.1:60491 -> 239.255.255.250:1900
03/27-14:56:34.608048 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:36.622883 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:40.841312 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
ENG IN
14:56
27-03-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(jane㉿jane)-[~]
$ ssh 192.168.56.101
Right Ctrl
ENG IN
14:57
27-03-2025


Ubuntu 24 [Running] - Oracle VirtualBox
Mar 27 14:58
nikhil@nikhil-VirtualBox: /etc/snort/rules
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Commencing packet processing (pid=3772)
03/27-14:57:49.147787 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:50.150592 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:51.179613 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:52.201462 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:53.237935 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:54.305746 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:56.323515 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:58:00.422387 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
ENG
IN
14:58
27-03-2025