NETWORK INTRUSION DETECTION: DESIGN AND IMPLEMENTATION OF NIDS [NETWORK INTRUSION DETECTION SYSTEM] WITH THE USE OF SNORT and ANALYZING FLOOD PACKETS WITH WIRESHARK

Tools: KALI LINUX {threat actor}, UBUNTU { victim}
Site :

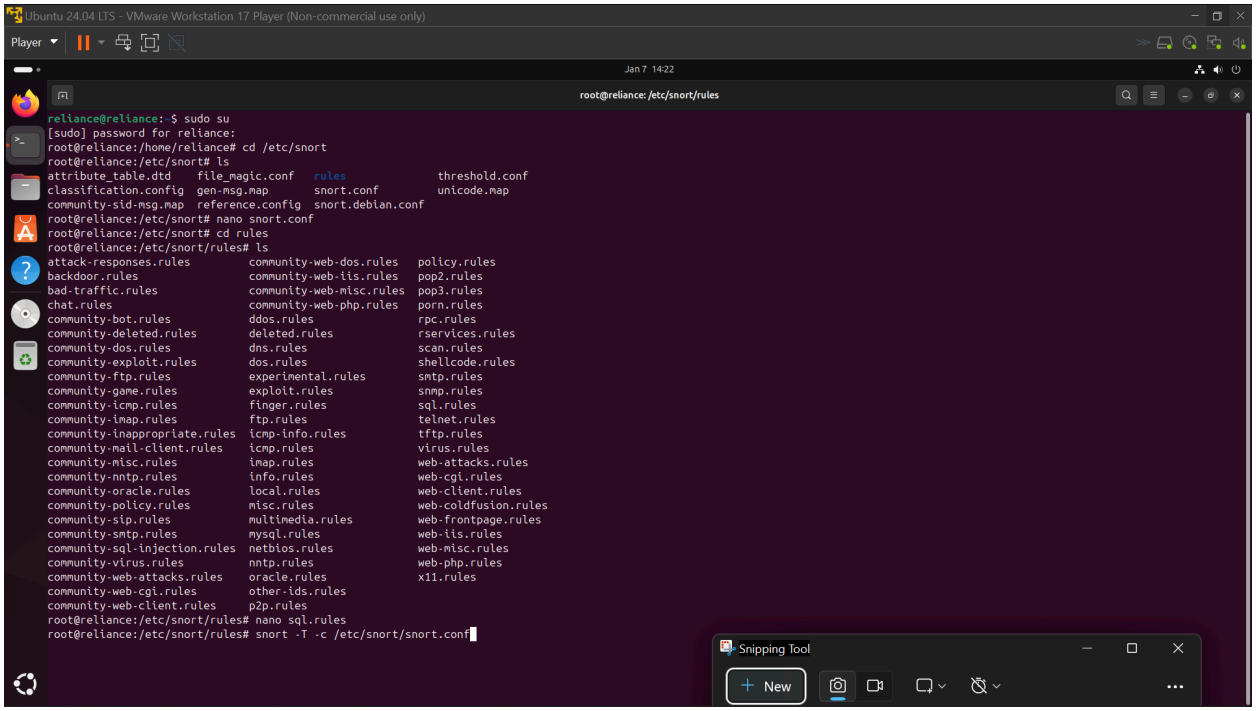
Snort is a powerful open-source network intrusion detection and prevention system (IDS/IPS) that is widely used in cybersecurity.

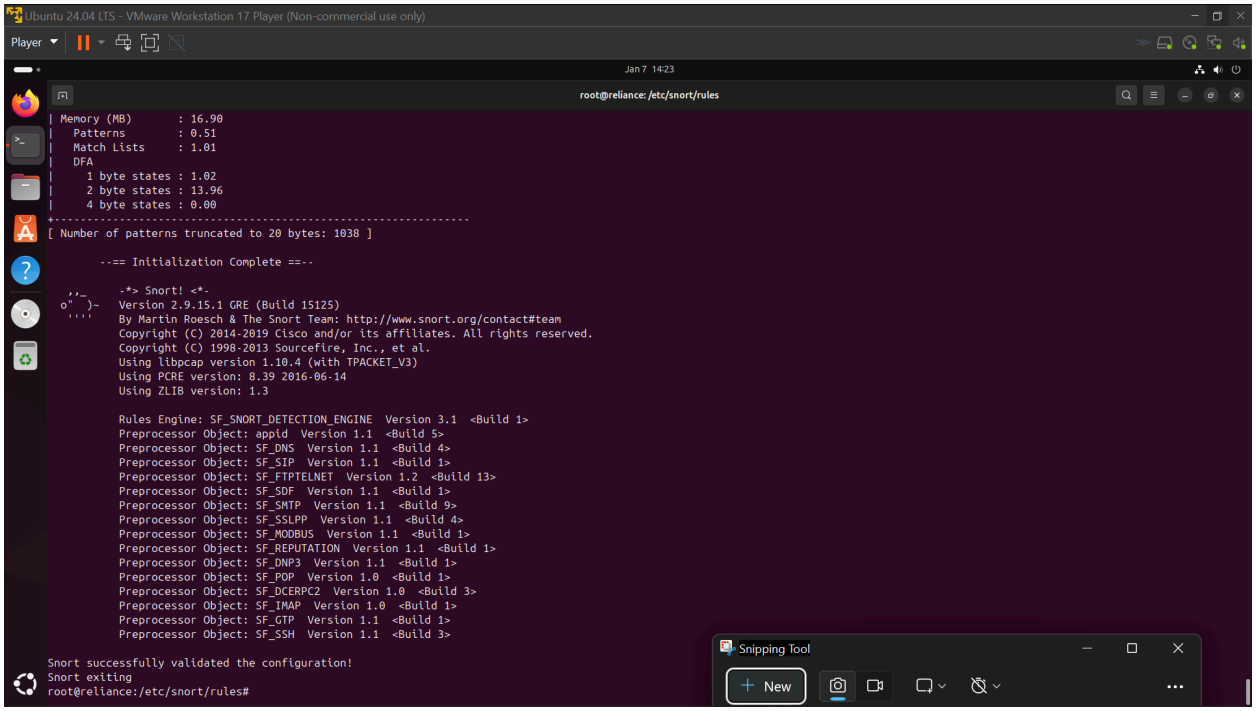
USING KALI LINUX FOR THE ATTACKING AND UBUNTU FOR THE VICTIM, here we set up snort and used it to detect incoming traffic from a threat actor.

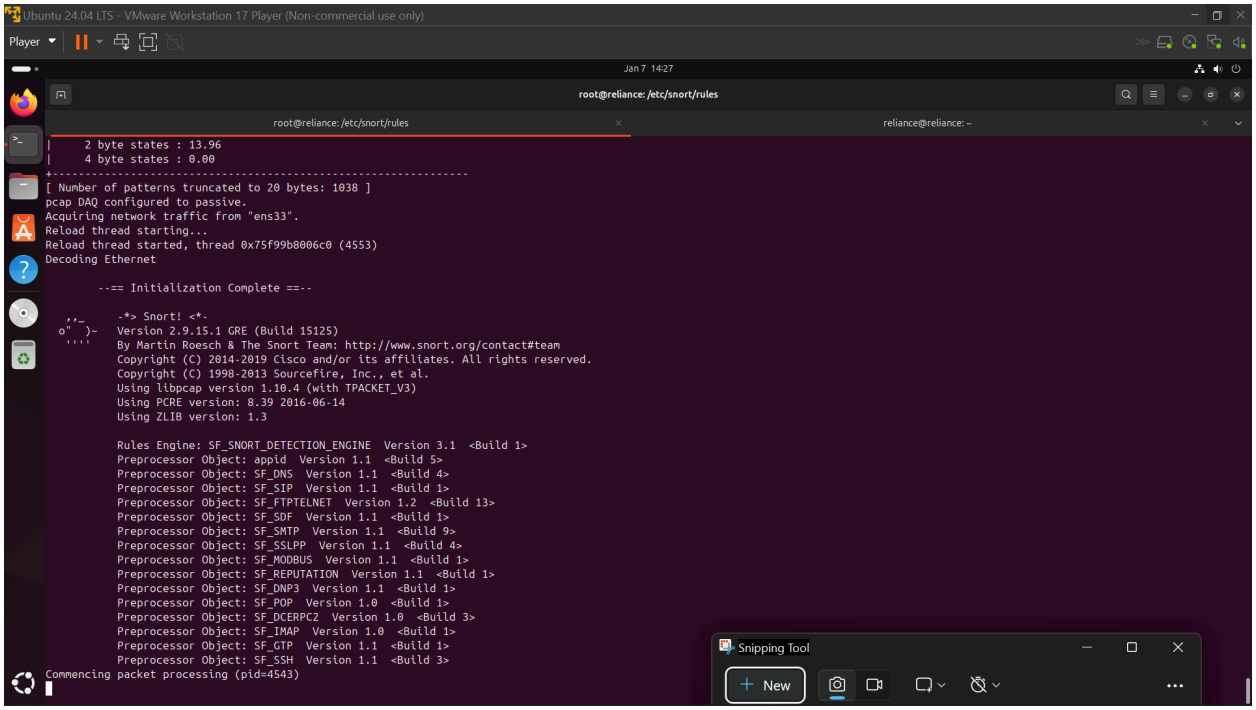
These are the attacks that was performed and how SNORTalong with WIRESHARK captured the packets :

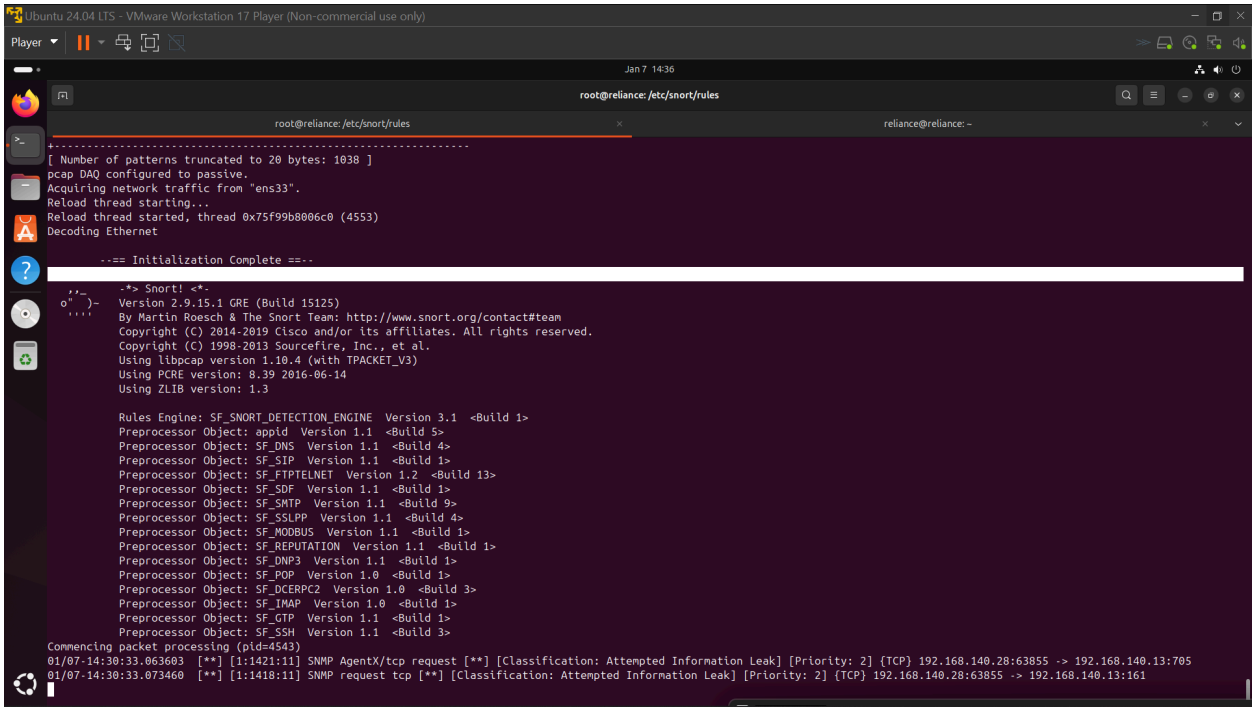
FTP
ICMP
SSH
PING FLOOD
SYN FLOOD
DOS AND DDOS

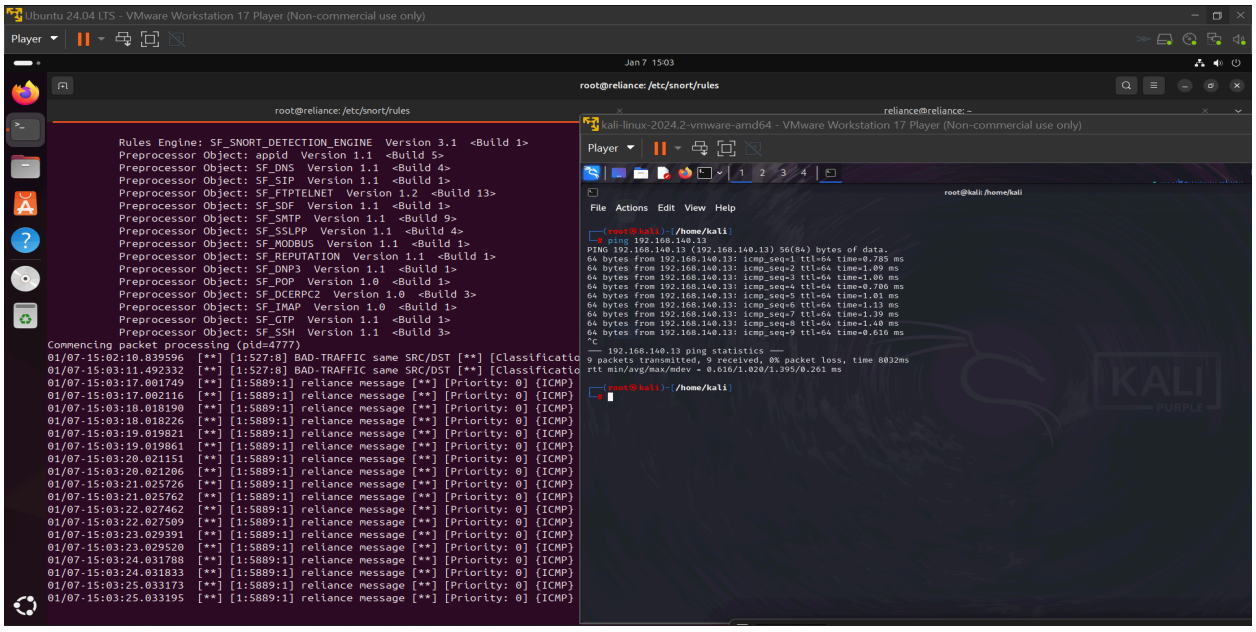
Input from the task :

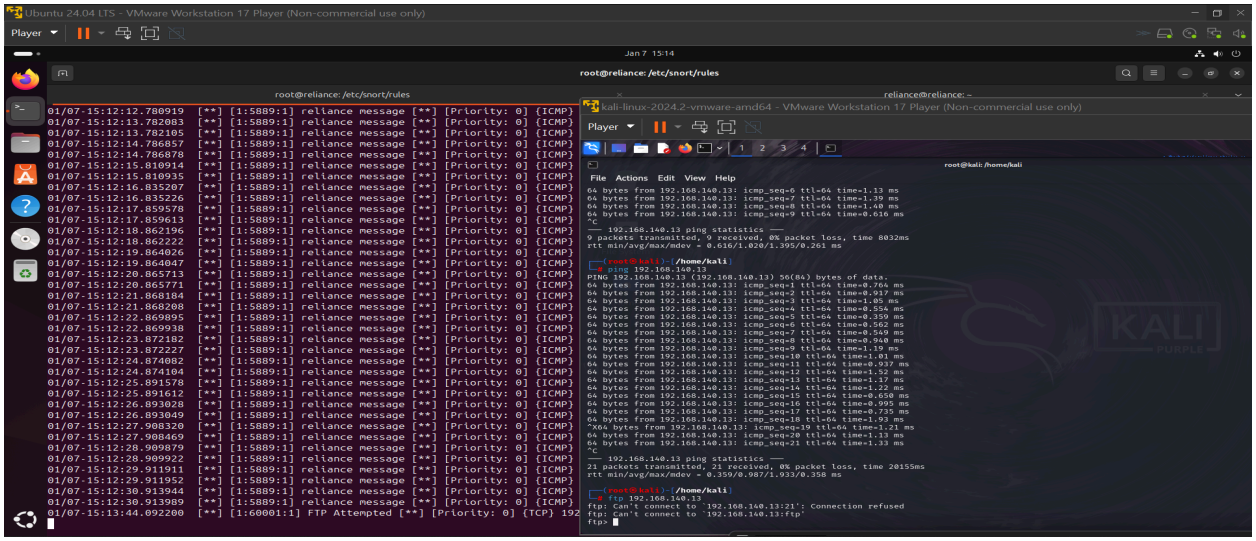


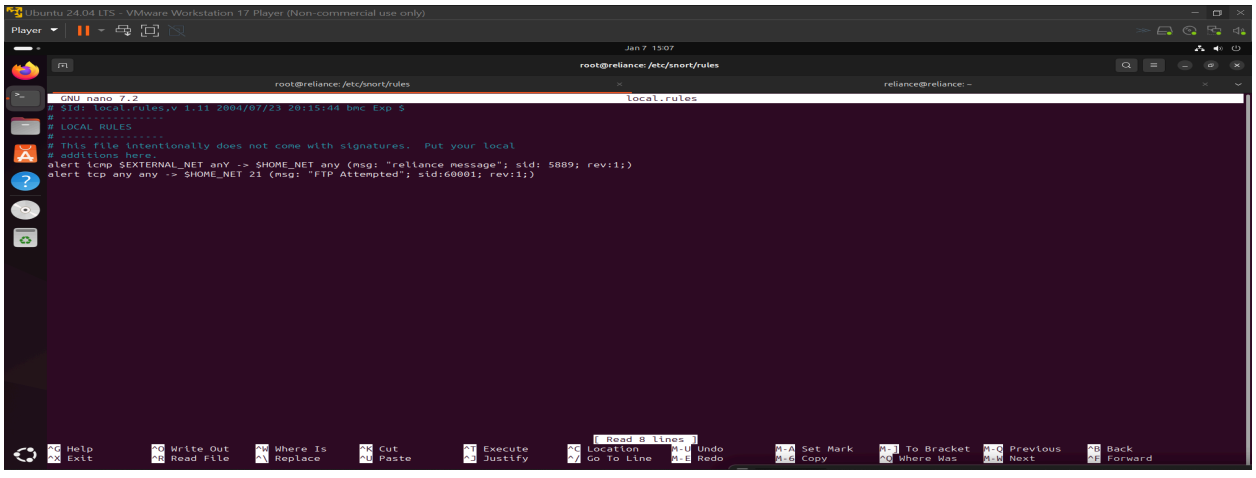



Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 7 14:27
root@reliance: /etc/snort/rules
root@reliance: /etc/snort/rules
reliance@reliance: ~
| 2 byte states : 13.96
| 4 byte states : 0.00
+----------
[Number of patterns truncated to 20 bytes: 1038]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x75f99b8006c0 (4553)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 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 3.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Commencing packet processing (pid=4543)
Snipping Tool
New


Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 7 14:36
root@reliance: /etc/snort/rules
root@reliance: /etc/snort/rules
reliance@reliance: ~
+----------
[Number of patterns truncated to 20 bytes: 1038]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x75f99b8006c0 (4553)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 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 3.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Commencing packet processing (pid=4543)
01/07-14:30:33.063603 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.140.28:63855 -> 192.168.140.13:705
01/07-14:30:33.073460 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.140.28:63855 -> 192.168.140.13:161

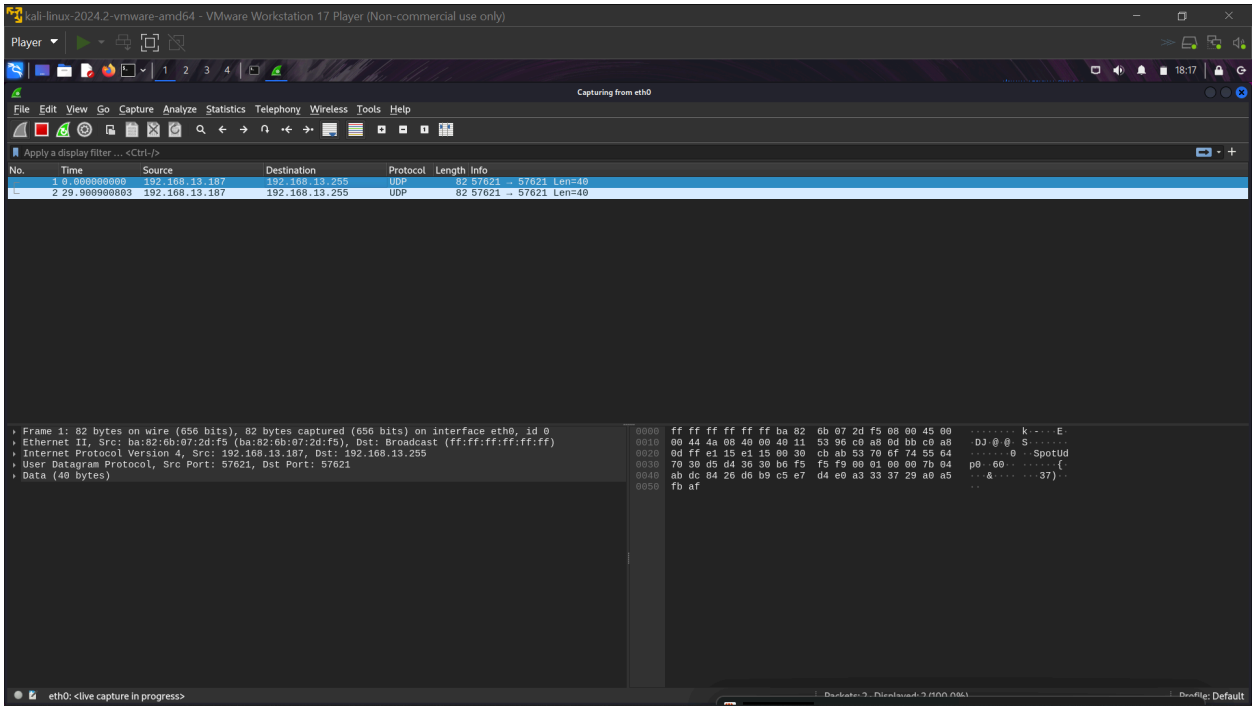

Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 7 15:03
root@reliance: /etc/snort/rules
root@reliance: /etc/snort/rules
reliance@reliance: ~
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Commencing packet processing (pid=4777)
01/07-15:02:10.839596 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificatio
01/07-15:03:11.492332 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificatio
01/07-15:03:17.001749 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:17.002116 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:18.018190 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:18.018226 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:19.019821 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:19.019861 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:20.021151 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:20.021206 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:21.025726 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:21.025762 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:22.027462 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:22.027509 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:23.029391 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:23.029520 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:24.031788 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:24.031833 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:25.033173 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:03:25.033195 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
(root㉿kali)-[/home/kali]
ping 192.168.140.13
PING 192.168.140.13 (192.168.140.13) 56(84) bytes of data.
64 bytes from 192.168.140.13: icmp_seq=1 ttl=64 time=0.788 ms
64 bytes from 192.168.140.13: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.140.13: icmp_seq=3 ttl=64 time=1.06 ms
64 bytes from 192.168.140.13: icmp_seq=4 ttl=64 time=0.706 ms
64 bytes from 192.168.140.13: icmp_seq=5 ttl=64 time=1.01 ms
64 bytes from 192.168.140.13: icmp_seq=6 ttl=64 time=1.13 ms
64 bytes from 192.168.140.13: icmp_seq=7 ttl=64 time=1.39 ms
64 bytes from 192.168.140.13: icmp_seq=8 ttl=64 time=1.40 ms
64 bytes from 192.168.140.13: icmp_seq=9 ttl=64 time=0.616 ms
^C
— 192.168.140.13 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8032ms
rtt min/avg/max/mdev = 0.616/1.020/1.395/0.261 ms
(root㉿kali)-[/home/kali]
#

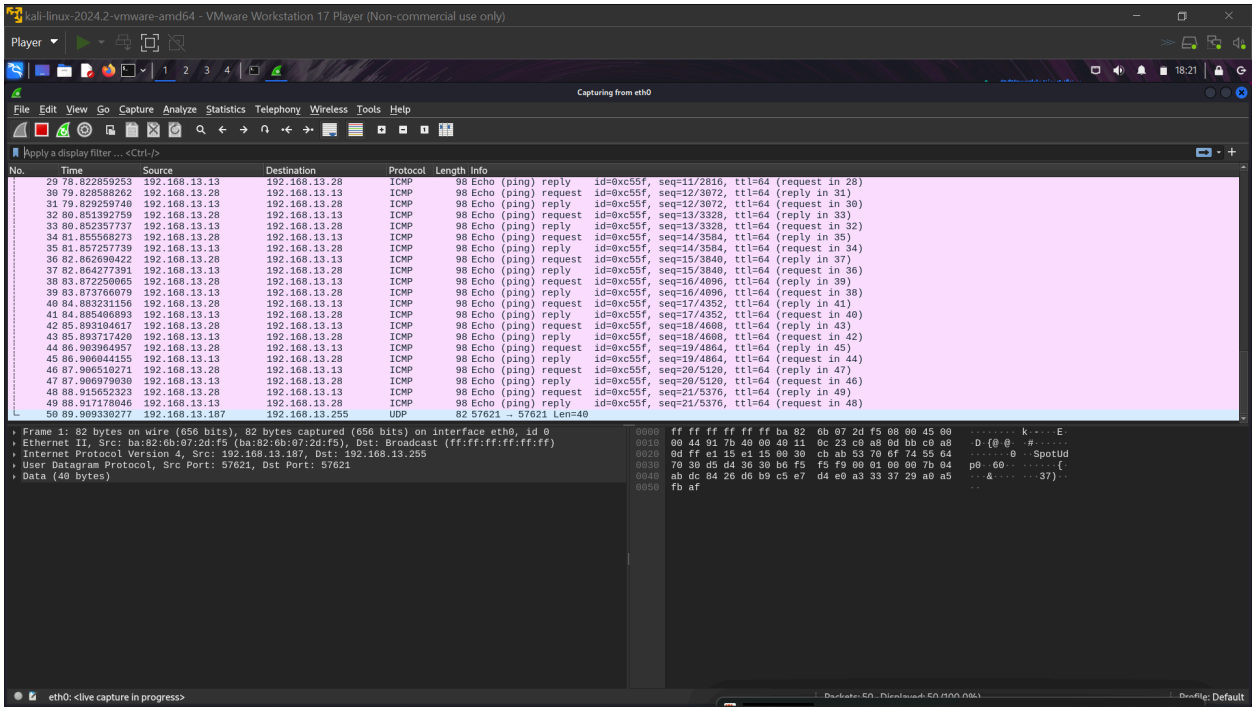

Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 7 15:14
root@reliance: /etc/snort/rules
root@reliance: /etc/snort/rules
reliance@reliance: ~
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
01/07-15:12:12.780919 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:13.782083 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:13.782105 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:14.786857 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:14.786878 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:15.810914 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:15.810935 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:16.835207 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:16.835226 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:17.859578 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:17.859613 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:18.862196 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:18.862222 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:19.864026 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:19.864047 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:20.865713 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:20.865771 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:21.868184 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:21.868208 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:22.869895 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:22.869938 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:23.872182 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:23.872227 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:24.874082 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:24.874104 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:25.891578 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:25.891612 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:26.893028 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:26.893049 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:27.908320 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:27.908469 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:28.909879 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:28.909922 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:29.911911 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:29.911952 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:30.913944 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:12:30.913989 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP}
01/07-15:13:44.092200 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192
64 bytes from 192.168.140.13: icmp_seq=6 ttl=64 time=1.13 ms
64 bytes from 192.168.140.13: icmp_seq=7 ttl=64 time=1.39 ms
64 bytes from 192.168.140.13: icmp_seq=8 ttl=64 time=1.40 ms
64 bytes from 192.168.140.13: icmp_seq=9 ttl=64 time=0.616 ms
^C
— 192.168.140.13 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8032ms
rtt min/avg/max/mdev = 0.616/1.020/1.395/0.261 ms
(root㉿kali)-[/home/kali]
ping 192.168.140.13
PING 192.168.140.13 (192.168.140.13) 56(84) bytes of data.
64 bytes from 192.168.140.13: icmp_seq=1 ttl=64 time=0.764 ms
64 bytes from 192.168.140.13: icmp_seq=2 ttl=64 time=0.917 ms
64 bytes from 192.168.140.13: icmp_seq=3 ttl=64 time=1.85 ms
64 bytes from 192.168.140.13: icmp_seq=4 ttl=64 time=0.554 ms
64 bytes from 192.168.140.13: icmp_seq=5 ttl=64 time=0.359 ms
64 bytes from 192.168.140.13: icmp_seq=6 ttl=64 time=0.562 ms
64 bytes from 192.168.140.13: icmp_seq=7 ttl=64 time=0.549 ms
64 bytes from 192.168.140.13: icmp_seq=8 ttl=64 time=0.940 ms
64 bytes from 192.168.140.13: icmp_seq=9 ttl=64 time=1.19 ms
64 bytes from 192.168.140.13: icmp_seq=10 ttl=64 time=1.01 ms
64 bytes from 192.168.140.13: icmp_seq=11 ttl=64 time=0.937 ms
64 bytes from 192.168.140.13: icmp_seq=12 ttl=64 time=1.52 ms
64 bytes from 192.168.140.13: icmp_seq=13 ttl=64 time=1.17 ms
64 bytes from 192.168.140.13: icmp_seq=14 ttl=64 time=1.22 ms
64 bytes from 192.168.140.13: icmp_seq=15 ttl=64 time=0.650 ms
64 bytes from 192.168.140.13: icmp_seq=16 ttl=64 time=0.995 ms
64 bytes from 192.168.140.13: icmp_seq=17 ttl=64 time=0.735 ms
64 bytes from 192.168.140.13: icmp_seq=18 ttl=64 time=1.93 ms
^X64 bytes from 192.168.140.13: icmp_seq=19 ttl=64 time=1.21 ms
64 bytes from 192.168.140.13: icmp_seq=20 ttl=64 time=1.13 ms
64 bytes from 192.168.140.13: icmp_seq=21 ttl=64 time=1.33 ms
^C
— 192.168.140.13 ping statistics —
21 packets transmitted, 21 received, 0% packet loss, time 20155ms
rtt min/avg/max/mdev = 0.359/0.987/1.933/0.358 ms
(root㉿kali)-[/home/kali]
ftp 192.168.140.13
ftp: Can't connect to `192.168.140.13:21': Connection refused
ftp: Can't connect to `192.168.140.13:ftp'
ftp>

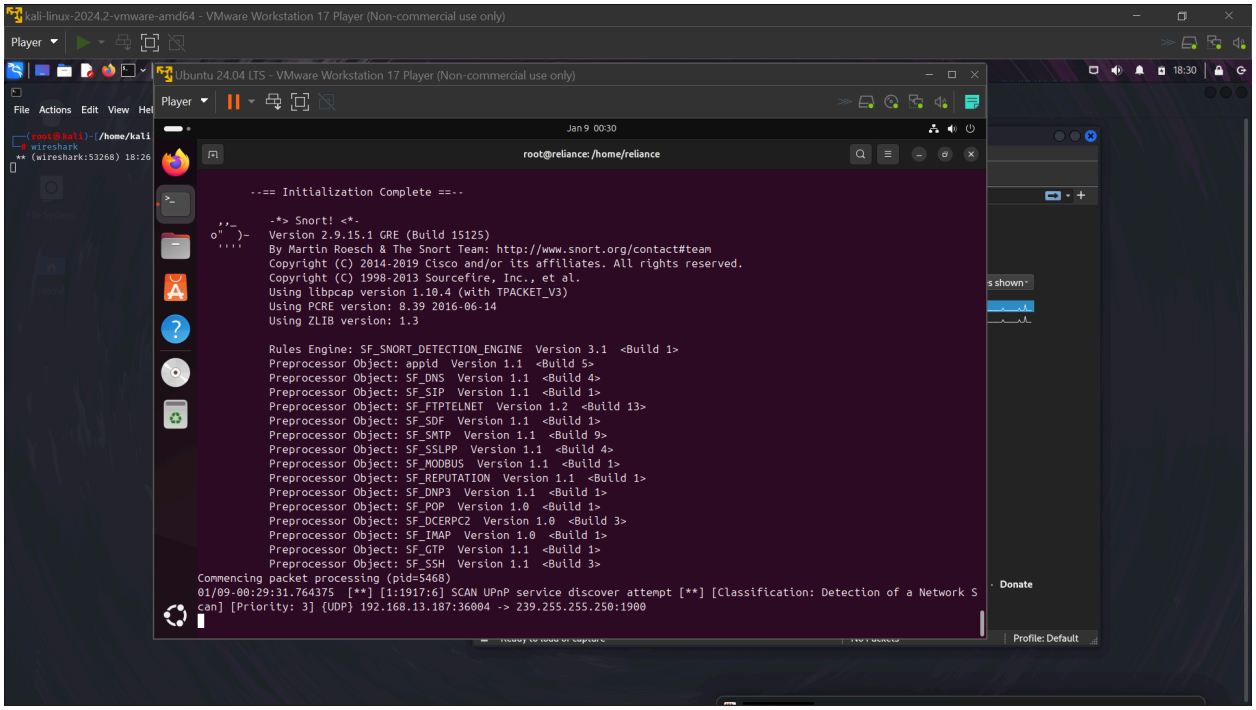

Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 7 15:07
root@reliance: /etc/snort/rules
root@reliance: /etc/snort/rules
reliance@reliance: ~
GNU nano 7.2
local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

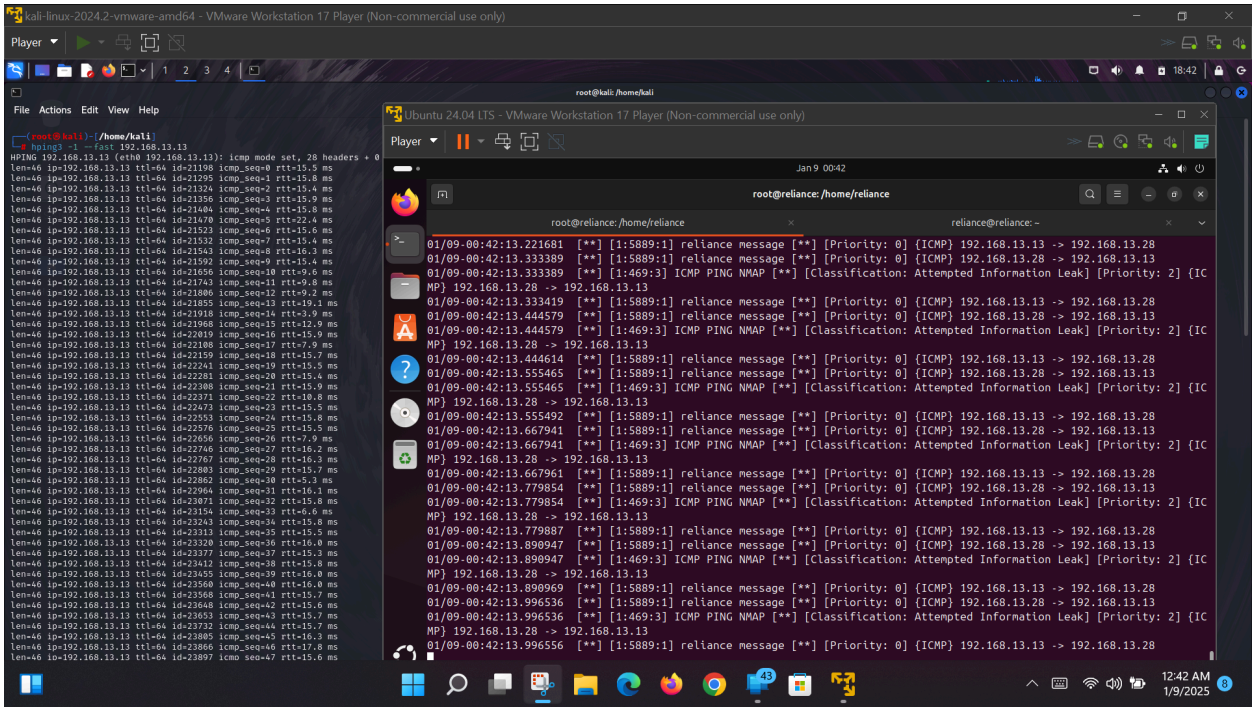
LOCAL RULES

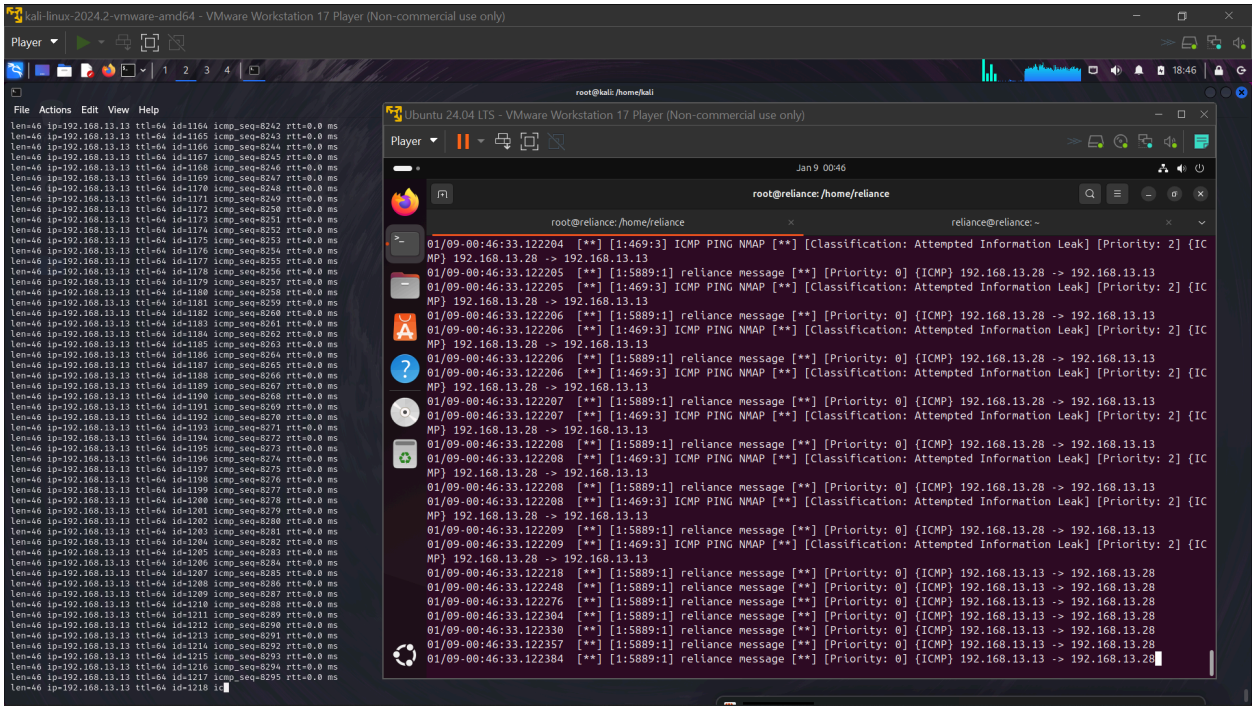
This file intentionally does not come with signatures. Put your local
additions here.
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "reliance message"; sid: 5889; rev:1;)
alert tcp any any -> $HOME_NET 21 (msg: "FTP Attempted"; sid:60001; rev:1;)
[Read 8 lines]
^G Help
^O Write Out
^W Where Is
^K Cut
^T Execute
^C Location
M-U Undo
M-A Set Mark
M-] To Bracket
M-Q Previous
^B Back
^X Exit
^R Read File
^\ Replace
^U Paste
^J Justify
^/ Go To Line
M-E Redo
M-6 Copy
^Q Where Was
M-W Next
^F Forward

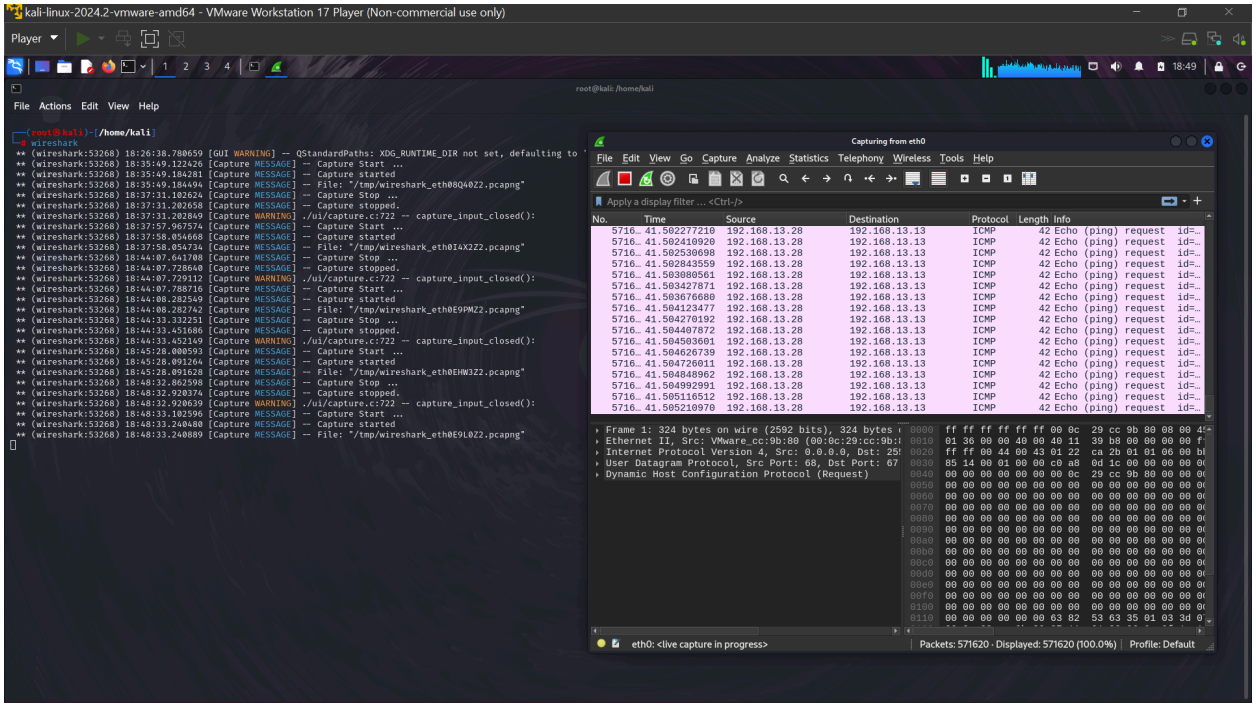

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.13.187 192.168.13.255 UDP 82 57621 → 57621 Len=40
2 29.900900803 192.168.13.187 192.168.13.255 UDP 82 57621 → 57621 Len=40
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface eth0, id 0
Ethernet II, Src: ba:82:6b:07:2d:f5 (ba:82:6b:07:2d:f5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.13.187, Dst: 192.168.13.255
User Datagram Protocol, Src Port: 57621, Dst Port: 57621
Data (40 bytes)
0000 ff ff ff ff ff ff ba 82 6b 07 2d f5 08 00 45 00
0010 00 44 4a 08 40 00 40 11 53 96 c0 a8 0d bb c0 a8
0020 0d ff e1 15 e1 15 00 30 cb ab 53 70 6f 74 55 64
0030 70 30 d5 d4 36 30 b6 f5 f5 f9 00 01 00 00 7b 04
0040 ab dc 84 26 d6 b9 c5 e7 d4 e0 a3 33 37 29 a0 a5
0050 fb af
eth0: <live capture in progress>

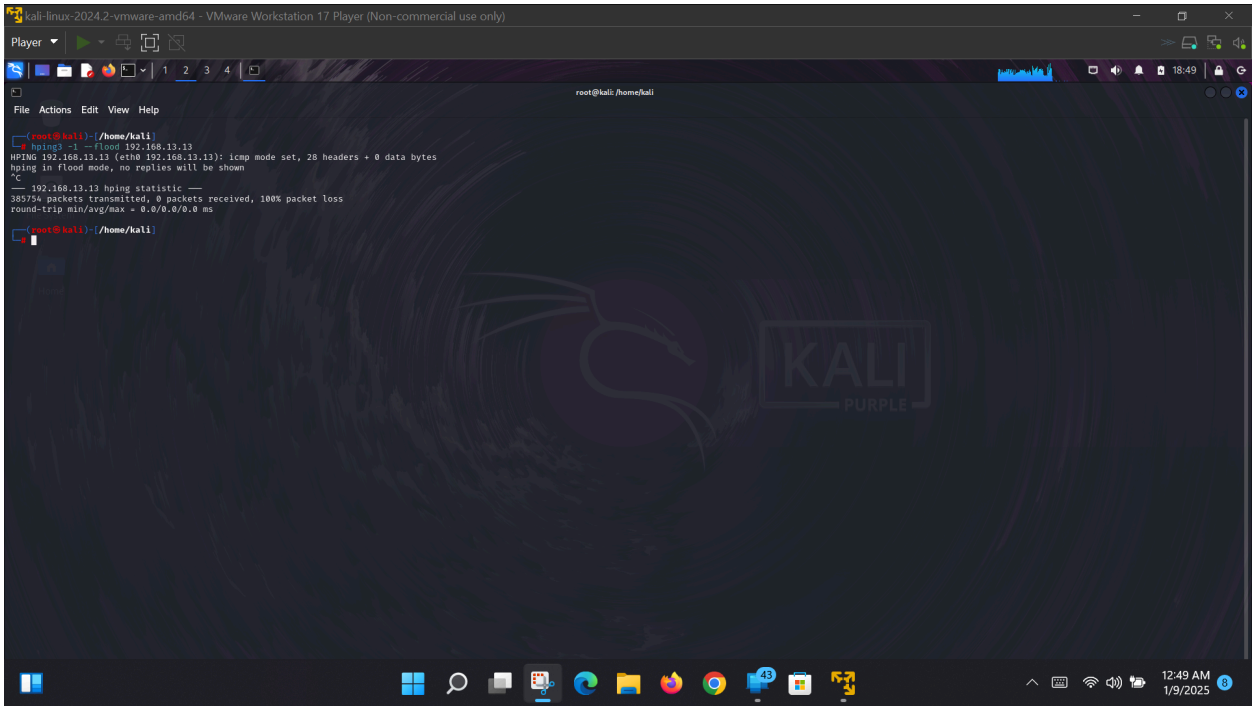

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
29 78.822859253 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=11/2816, ttl=64 (request in 28)
30 79.828588262 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=12/3072, ttl=64 (reply in 31)
31 79.829259740 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=12/3072, ttl=64 (request in 30)
32 80.851392759 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=13/3328, ttl=64 (reply in 33)
33 80.852357737 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=13/3328, ttl=64 (request in 32)
34 81.855568273 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=14/3584, ttl=64 (reply in 35)
35 81.857257739 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=14/3584, ttl=64 (request in 34)
36 82.862690422 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=15/3840, ttl=64 (reply in 37)
37 82.864277391 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=15/3840, ttl=64 (request in 36)
38 83.872250065 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=16/4096, ttl=64 (reply in 39)
39 83.873766079 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=16/4096, ttl=64 (request in 38)
40 84.883231156 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=17/4352, ttl=64 (reply in 41)
41 84.885406893 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=17/4352, ttl=64 (request in 40)
42 85.893104617 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=18/4608, ttl=64 (reply in 43)
43 85.893717420 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=18/4608, ttl=64 (request in 42)
44 86.903964957 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=19/4864, ttl=64 (reply in 45)
45 86.906844155 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=19/4864, ttl=64 (request in 44)
46 87.906510271 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=20/5120, ttl=64 (reply in 47)
47 87.906979030 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=20/5120, ttl=64 (request in 46)
48 88.915652323 192.168.13.28 192.168.13.13 ICMP 98 Echo (ping) request id=0xc55f, seq=21/5376, ttl=64 (reply in 49)
49 88.917178046 192.168.13.13 192.168.13.28 ICMP 98 Echo (ping) reply id=0xc55f, seq=21/5376, ttl=64 (request in 48)
50 89.909330277 192.168.13.187 192.168.13.255 UDP 82 57621 → 57621 Len=40
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface eth0, id 0
Ethernet II, Src: ba:82:6b:07:2d:f5 (ba:82:6b:07:2d:f5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.13.187, Dst: 192.168.13.255
User Datagram Protocol, Src Port: 57621, Dst Port: 57621
Data (40 bytes)
0000 ff ff ff ff ff ff ba 82 6b 07 2d f5 08 00 45 00
0010 00 44 91 7b 40 00 40 11 0c 23 c0 a8 0d bb c0 a8
0020 0d ff e1 15 e1 15 00 30 cb ab 53 70 6f 74 55 64
0030 70 30 d5 d4 36 30 b6 f5 f5 f9 00 01 00 00 7b 04
0040 ab dc 84 26 d6 b9 c5 e7 d4 e0 a3 33 37 29 a0 a5
0050 fb af
eth0: <live capture in progress>

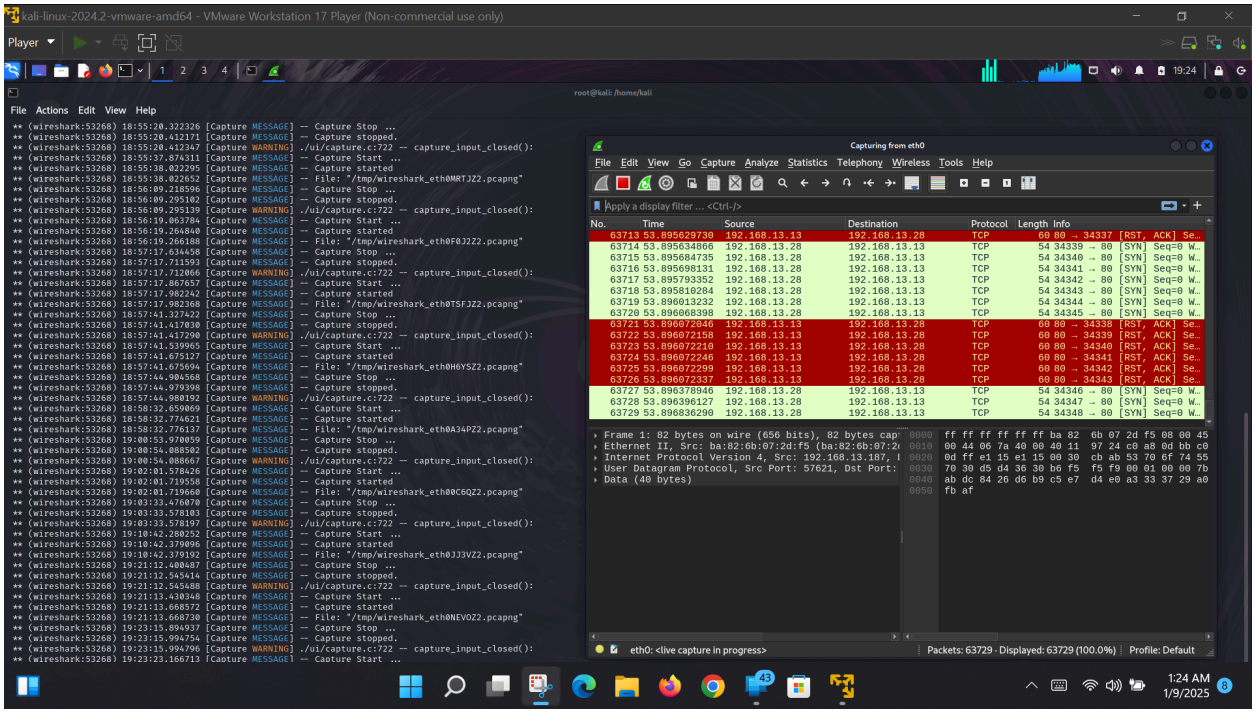

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 9 00:30
root@reliance: /home/reliance
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 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 3.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Commencing packet processing (pid=5468)
01/09-00:29:31.764375 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.13.187:36004 -> 239.255.255.250:1900
Donate
Profile: Default

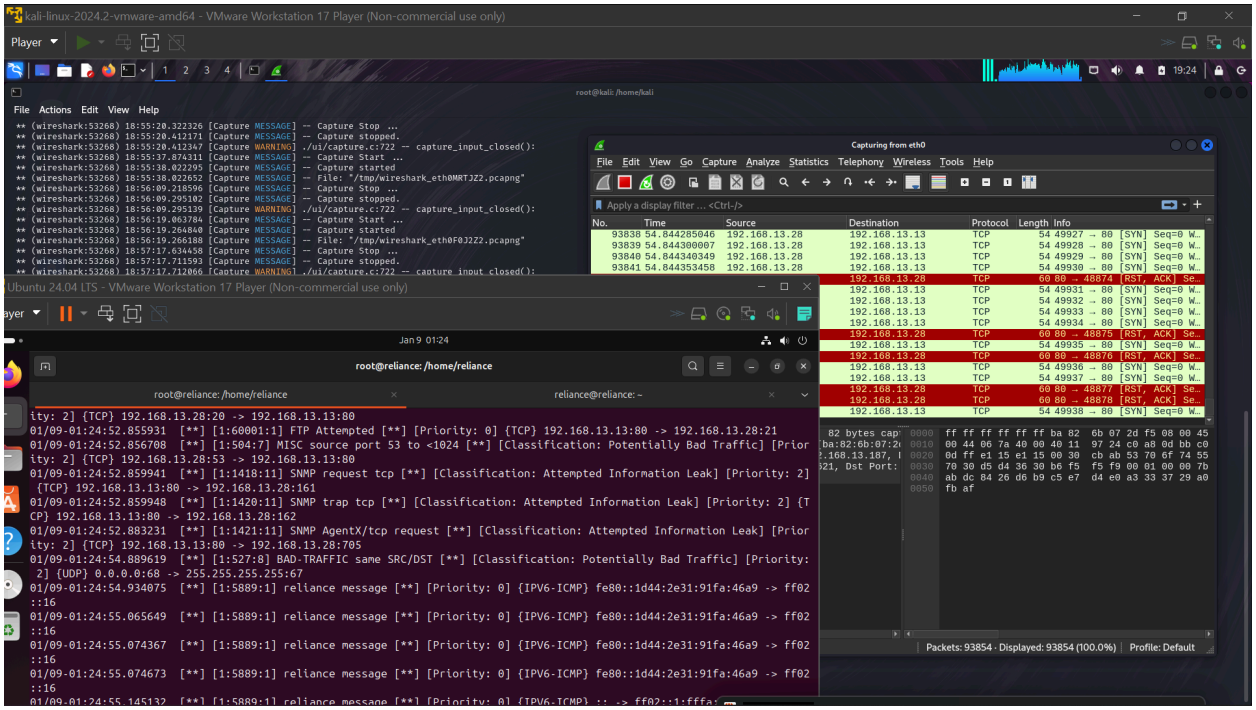

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
hping3 -1 --fast 192.168.13.13
HPING 192.168.13.13 (eth0 192.168.13.13): icmp mode set, 28 headers + 0
Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
Player
Jan 9 00:42
root@reliance: /home/reliance
root@reliance: /home/reliance
reliance@reliance: ~
01/09-00:42:13.221681 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.333389 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.333389 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.333419 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.444579 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.444579 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.444614 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.555465 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.555465 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.555492 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.667941 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.667941 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.667961 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.779854 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.779854 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.779887 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.890947 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.890947 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.890969 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:42:13.996536 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.996536 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:42:13.996556 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
12:42 AM
1/9/2025


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
Ubuntu 24.04 LTS - VMware Workstation 17 Player (Non-commercial use only)
root@reliance: /home/reliance
01/09-00:46:33.122204 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122205 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122205 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122206 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122206 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122206 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122206 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122207 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122207 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122208 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122208 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122208 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122208 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122209 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122209 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.13.28 -> 192.168.13.13
01/09-00:46:33.122218 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122248 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122276 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122304 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122330 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122357 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28
01/09-00:46:33.122384 [**] [1:5889:1] reliance message [**] [Priority: 0] {ICMP} 192.168.13.13 -> 192.168.13.28


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5716… 41.502277210 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.502410920 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.502530698 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.502843559 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.503080561 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.503427871 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.503676680 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504123477 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504270192 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504407872 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504503601 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504626739 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504726011 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504848962 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.504992991 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.505116512 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
5716… 41.505210970 192.168.13.28 192.168.13.13 ICMP 42 Echo (ping) request id=…
Frame 1: 324 bytes on wire (2592 bits), 324 bytes
Ethernet II, Src: VMware_cc:9b:80 (00:0c:29:cc:9b:
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 25
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
eth0: <live capture in progress>
Packets: 571620 · Displayed: 571620 (100.0%)
Profile: Default


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
hping3 -1 --flood 192.168.13.13
HPING 192.168.13.13 (eth0 192.168.13.13): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.13.13 hping statistic ---
385754 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(root@kali)-[/home/kali]
#
12:49 AM
1/9/2025


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
63713 53.895629730 192.168.13.13 192.168.13.28 TCP 60 80 → 34337 [RST, ACK] Se…
63714 53.895634866 192.168.13.28 192.168.13.13 TCP 54 34339 → 80 [SYN] Seq=0 W…
63715 53.895684735 192.168.13.28 192.168.13.13 TCP 54 34340 → 80 [SYN] Seq=0 W…
63716 53.895698131 192.168.13.28 192.168.13.13 TCP 54 34341 → 80 [SYN] Seq=0 W…
63717 53.895793352 192.168.13.28 192.168.13.13 TCP 54 34342 → 80 [SYN] Seq=0 W…
63718 53.895810284 192.168.13.28 192.168.13.13 TCP 54 34343 → 80 [SYN] Seq=0 W…
63719 53.896013232 192.168.13.28 192.168.13.13 TCP 54 34344 → 80 [SYN] Seq=0 W…
63720 53.896068398 192.168.13.28 192.168.13.13 TCP 54 34345 → 80 [SYN] Seq=0 W…
63721 53.896072046 192.168.13.13 192.168.13.28 TCP 60 80 → 34338 [RST, ACK] Se…
63722 53.896072158 192.168.13.13 192.168.13.28 TCP 60 80 → 34339 [RST, ACK] Se…
63723 53.896072210 192.168.13.13 192.168.13.28 TCP 60 80 → 34340 [RST, ACK] Se…
63724 53.896072246 192.168.13.13 192.168.13.28 TCP 60 80 → 34341 [RST, ACK] Se…
63725 53.896072299 192.168.13.13 192.168.13.28 TCP 60 80 → 34342 [RST, ACK] Se…
63726 53.896072337 192.168.13.13 192.168.13.28 TCP 60 80 → 34343 [RST, ACK] Se…
63727 53.896378946 192.168.13.28 192.168.13.13 TCP 54 34346 → 80 [SYN] Seq=0 W…
63728 53.896396127 192.168.13.28 192.168.13.13 TCP 54 34347 → 80 [SYN] Seq=0 W…
63729 53.896836290 192.168.13.28 192.168.13.13 TCP 54 34348 → 80 [SYN] Seq=0 W…
Frame 1: 82 bytes on wire (656 bits), 82 bytes cap
Ethernet II, Src: ba:82:6b:07:2d:f5 (ba:82:6b:07:2
Internet Protocol Version 4, Src: 192.168.13.187, I
User Datagram Protocol, Src Port: 57621, Dst Port:
Data (40 bytes)
0000 ff ff ff ff ff ff ba 82 6b 07 2d f5 08 00 45
0010 00 44 06 7a 40 00 40 11 97 24 c0 a8 0d bb c0
0020 0d ff e1 15 e1 15 00 30 cb ab 53 70 6f 74 55
0030 70 30 d5 d4 36 30 b6 f5 f5 f9 00 01 00 00 7b
0040 ab dc 84 26 d6 b9 c5 e7 d4 e0 a3 33 37 29 a0
0050 fb af
eth0: <live capture in progress>
Packets: 63729 · Displayed: 63729 (100.0%)
Profile: Default
1:24 AM
1/9/2025



Here we went through the process of configuring a network intrusion detection system and we used it to detect traffic.

Please do note that this video is for educational purposes only and it's not intended to cause any harm or promote cybercrime. Thank you.

Demonstration of SNORT as a Network Intrusion Detection System

This demonstration highlights how SNORT functions as a network intrusion detection system (NIDS). We'll use **Ubuntu** as the victim machine and **Kali Linux** as the threat actor. SNORT will be installed on Ubuntu, and Kali will be used to simulate attacks. We'll observe how SNORT detects and logs packets sent from Kali.

Installing and Configuring SNORT

1. **Install SNORT on Ubuntu:**

Open the terminal on Ubuntu and run:
`sudo apt-get install snort -y`

Navigate to the SNORT configuration directory:
`cd /etc/snort`

List the contents of the directory and open the configuration file:
`nano snort.conf`

    - The configuration file, `snort.conf`, defines the servers and ports to monitor. SNORT uses this file to scan network traffic for potential threats.
2. **Custom Rules Setup:**

Navigate to the rules directory:
`cd rules`

    -

Open the `local.rules` file for editing:
`nano local.rules`
Custom rules can be created here. For instance, you can write a rule to detect FTP attempts on port 21 with a custom alert message:
```
alert tcp any any -> $HOME_NET 21 (msg: "FTP
ATTEMPTED"; sid:60001; rev:1;)
```

    - Similarly, rules can be written for other protocols like SSH.

Testing Configuration: After adding rules, always test the configuration to ensure it's valid:
`snort -T -c /etc/snort/snort.conf`

If successful, you'll see a message like:
Copy code
`Successfully validated the configuration.`

3. Errors in rules can prevent SNORT from starting, so testing is critical.

Starting SNORT: Begin intrusion detection with:
`snort -A console -c /etc/snort/snort.conf`

4. SNORT will now listen for incoming packets.

Simulating and Detecting Attacks

1. **Packet Detection:**
    - From Kali Linux, run a network scanning tool like `nmap` targeting Ubuntu.
    - On the Ubuntu terminal, observe SNORT capturing packets in real-time.
2. **Custom Rule Detection:**

Add a rule in `local.rules` to detect ICMP requests:
`alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "ICMP DETECTED"; sid:5889; rev:1;)`

    -
    - Test the configuration, then restart SNORT.
    - From Kali, ping the Ubuntu machine. SNORT will display the custom message "ICMP DETECTED" whenever packets are received.
3. **FTP and SSH Detection:**

Add similar rules for FTP (port 21) and SSH (port 22):
`alert tcp any any -> $HOME_NET 22 (msg: "SSH ATTEMPTED"; sid:60002; rev:1;)`

    -

- Restart SNORT and test by attempting to establish FTP or SSH connections from Kali. SNORT will log these attempts.

Advanced Attack Simulations

1. **Ping Flood (DoS) Attack:**

Use tools like `hping3` to send ICMP echo requests at varying intervals:
`hping3 -1 -c 6 -i 5 <target-IP>`
This sends 6 packets, each 5 seconds apart. For faster attacks:
`hping3 -1 --flood <target-IP>`

   - SNORT and tools like Wireshark will detect and log the flood of packets.
2. **IP Spoofing:**

Spoof the source IP address of ICMP packets:
`hping3 -1 -a <spoofed-IP> -c 1 <target-IP>`

   - This conceals the attacker's IP.
3. **SYN Flood Attack:**

Send a large number of SYN packets to overwhelm a server:
`hping3 -S --flood -p 80 <target-IP>`

   - This simulates a denial-of-service (DoS) attack.
4. **Distributed Denial of Service (DDoS):**
   - A DDoS attack involves multiple systems flooding a server with requests. Hackers often use botnets—malicious scripts that take control of multiple systems to orchestrate such attacks.

Mitigation Strategies for DoS and DDoS Attacks

- **Intrusion Prevention Systems (IPS):** Combine firewalls, VPNs, anti-spam filters, and DDoS protection.

- **Traffic Filtering:** Identify and block malicious patterns while allowing legitimate traffic.
- **Traffic Diversion:** Redirect malicious traffic away from critical systems.
- **Load Balancing:** Distribute traffic across multiple servers to prevent overload.

Other things we can do with SNORT IS :

1. Signature-Based Detection: Snort uses rule sets to match traffic patterns against known attack signatures.

2. Real-Time Alerts: Provides alerts for suspicious activities, including port scans, buffer overflows, and SQL injection attacks.

3. Customizability: Users can write custom rules to tailor detection to specific environments.
4. Open-Source Flexibility: Frequent updates and community-driven contributions.