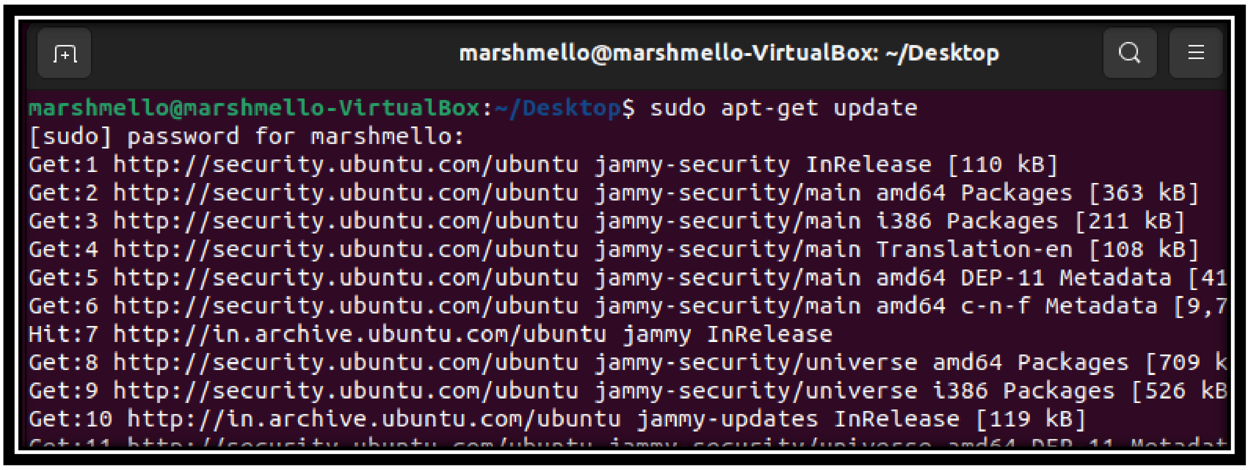
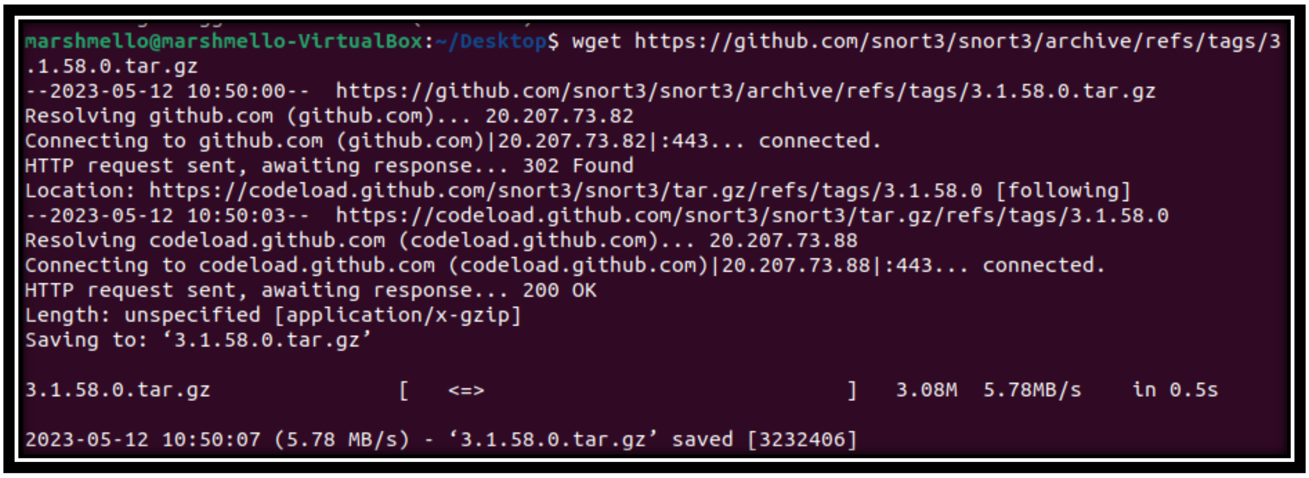
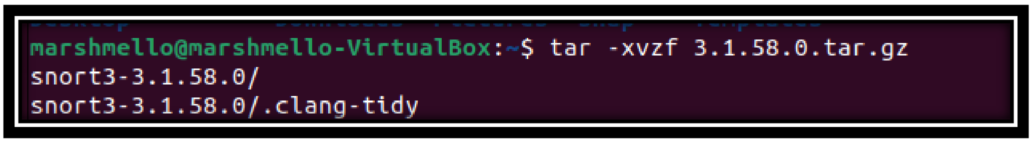
Snort Installations:



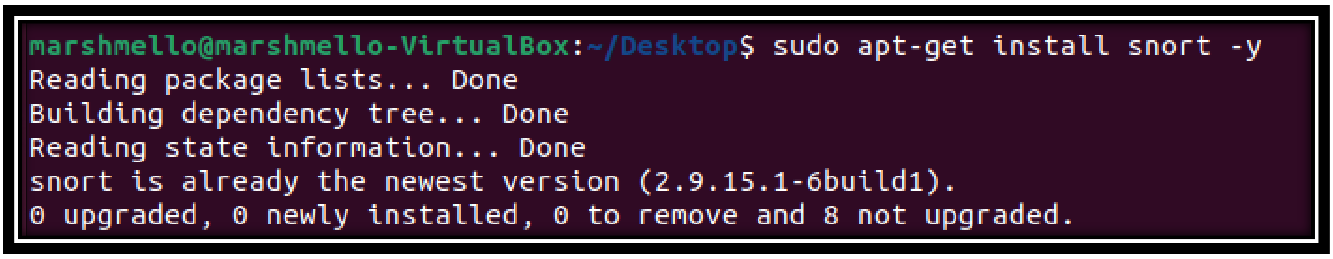
```
marshmello@marshmello-VirtualBox:~/Desktop$ sudo apt-get update
[sudo] password for marshmello:
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [363 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [211 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [108 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [9,7
Hit:7 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:8 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [709 k
Get:9 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [526 kB
Get:10 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadat
```



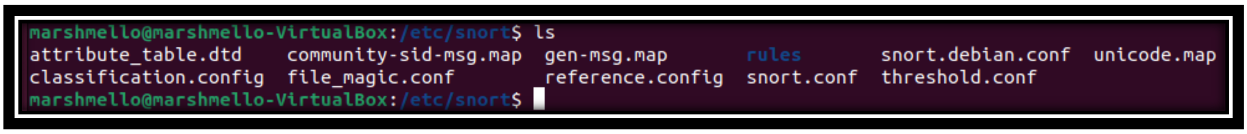
```
marshmello@marshmello-VirtualBox:~/Desktop$ wget https://github.com/snort3/snort3/archive/refs/tags/3
.1.58.0.tar.gz
--2023-05-12 10:50:00--  https://github.com/snort3/snort3/archive/refs/tags/3.1.58.0.tar.gz
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/snort3/snort3/tar.gz/refs/tags/3.1.58.0 [following]
--2023-05-12 10:50:03--  https://codeload.github.com/snort3/snort3/tar.gz/refs/tags/3.1.58.0
Resolving codeload.github.com (codeload.github.com)... 20.207.73.88
Connecting to codeload.github.com (codeload.github.com)|20.207.73.88|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: ‘3.1.58.0.tar.gz’

3.1.58.0.tar.gz             [   <=>                            ]   3.08M  5.78MB/s    in 0.5s

2023-05-12 10:50:07 (5.78 MB/s) - ‘3.1.58.0.tar.gz’ saved [3232406]
```



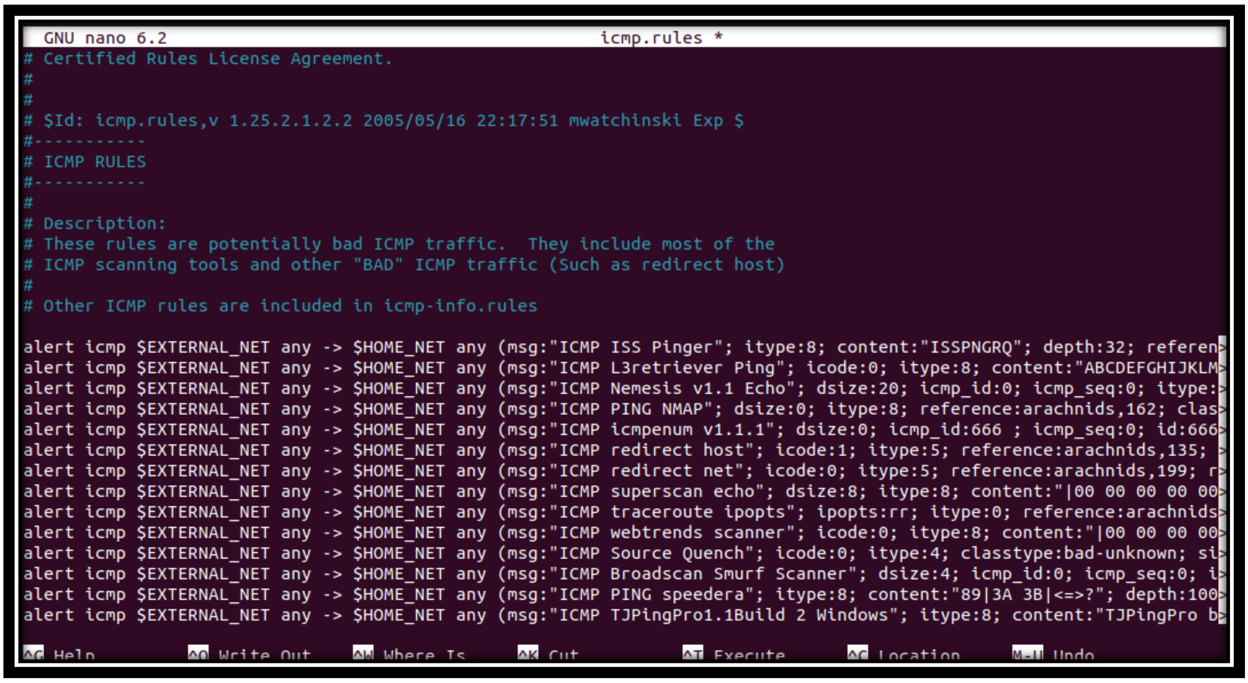
```
marshmello@marshmello-VirtualBox:~$ tar -xvzf 3.1.58.0.tar.gz
snort3-3.1.58.0/
snort3-3.1.58.0/.clang-tidy
```



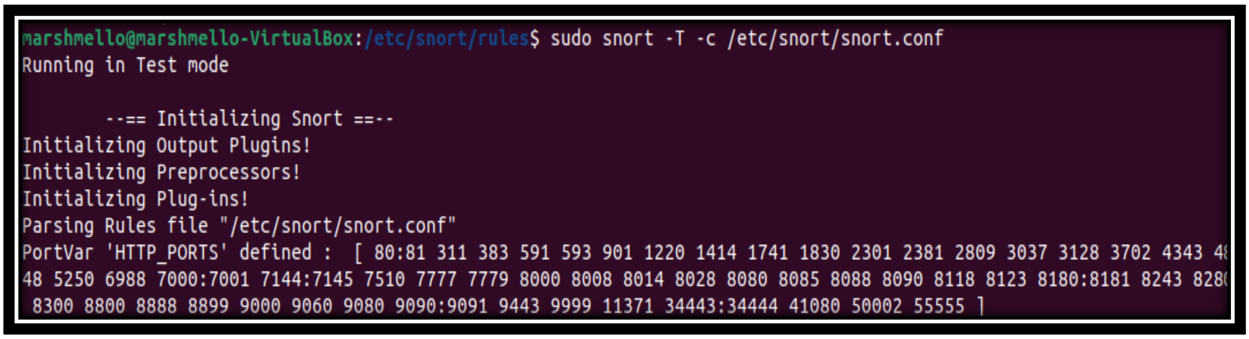
```
marshmello@marshmello-VirtualBox:~/Desktop$ sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.15.1-6build1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```



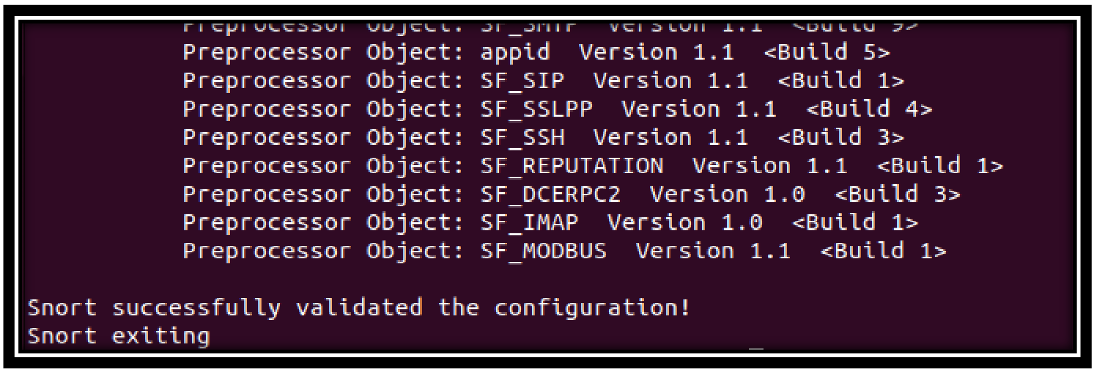
```
marshmello@marshmello-VirtualBox:/etc/snort$ ls
attribute_table.dtd    community-sid-msg.map  gen-msg.map       rules      snort.debian.conf  unicode.map
classification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
marshmello@marshmello-VirtualBox:/etc/snort$ 
```



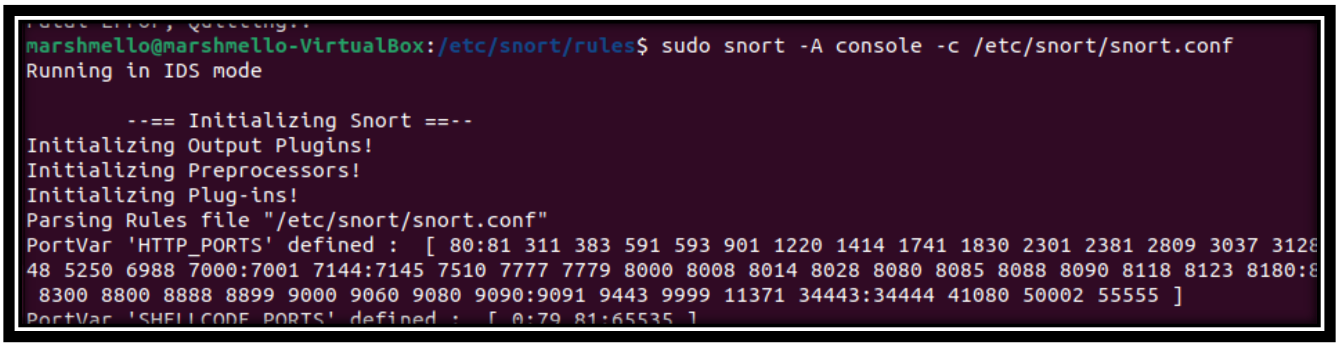
```
  GNU nano 6.2                                 icmp.rules *
# Certified Rules License Agreement.
#
#
# $Id: icmp.rules,v 1.25.2.1.2.2 2005/05/16 22:17:51 mwatchinski Exp $
#-----------
# ICMP RULES
#-----------
#
# Description:
# These rules are potentially bad ICMP traffic.  They include most of the
# ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
#
# Other ICMP rules are included in icmp-info.rules

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; content:"ISSPNGRQ"; depth:32; referen>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; content:"ABCDEFGHIJKLM>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp_id:0; icmp_seq:0; itype:>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; reference:arachnids,162; clas>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsize:0; icmp_id:666 ; icmp_seq:0; id:666>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:1; itype:5; reference:arachnids,135; >
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0; itype:5; reference:arachnids,199; r>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize:8; itype:8; content:"|00 00 00 00 00>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ipopts:rr; itype:0; reference:arachnids>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; icode:0; itype:8; content:"|00 00 00 00>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode:0; itype:4; classtype:bad-unknown; si>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scanner"; dsize:4; icmp_id:0; icmp_seq:0; i>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING speedera"; itype:8; content:"89|3A 3B|<=>?"; depth:100>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP TJPingPro1.1Build 2 Windows"; itype:8; content:"TJPingPro b>

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
```



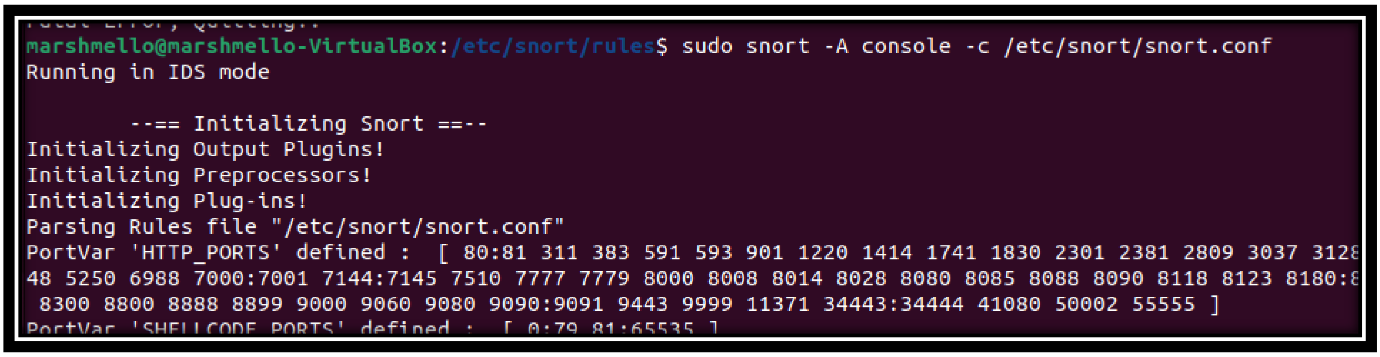
```
marshmello@marshmello-VirtualBox:/etc/snort/rules$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4
48 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 828
 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
```



```
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
```



```
Fatal Error, Quitting!!
marshmello@marshmello-VirtualBox:/etc/snort/rules$ sudo snort -A console -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128
48 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8
 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 ]
```



```
Fatal Error, Quitting!!
marshmello@marshmello-VirtualBox:/etc/snort/rules$ sudo snort -A console -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128
48 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8
 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 ]
```