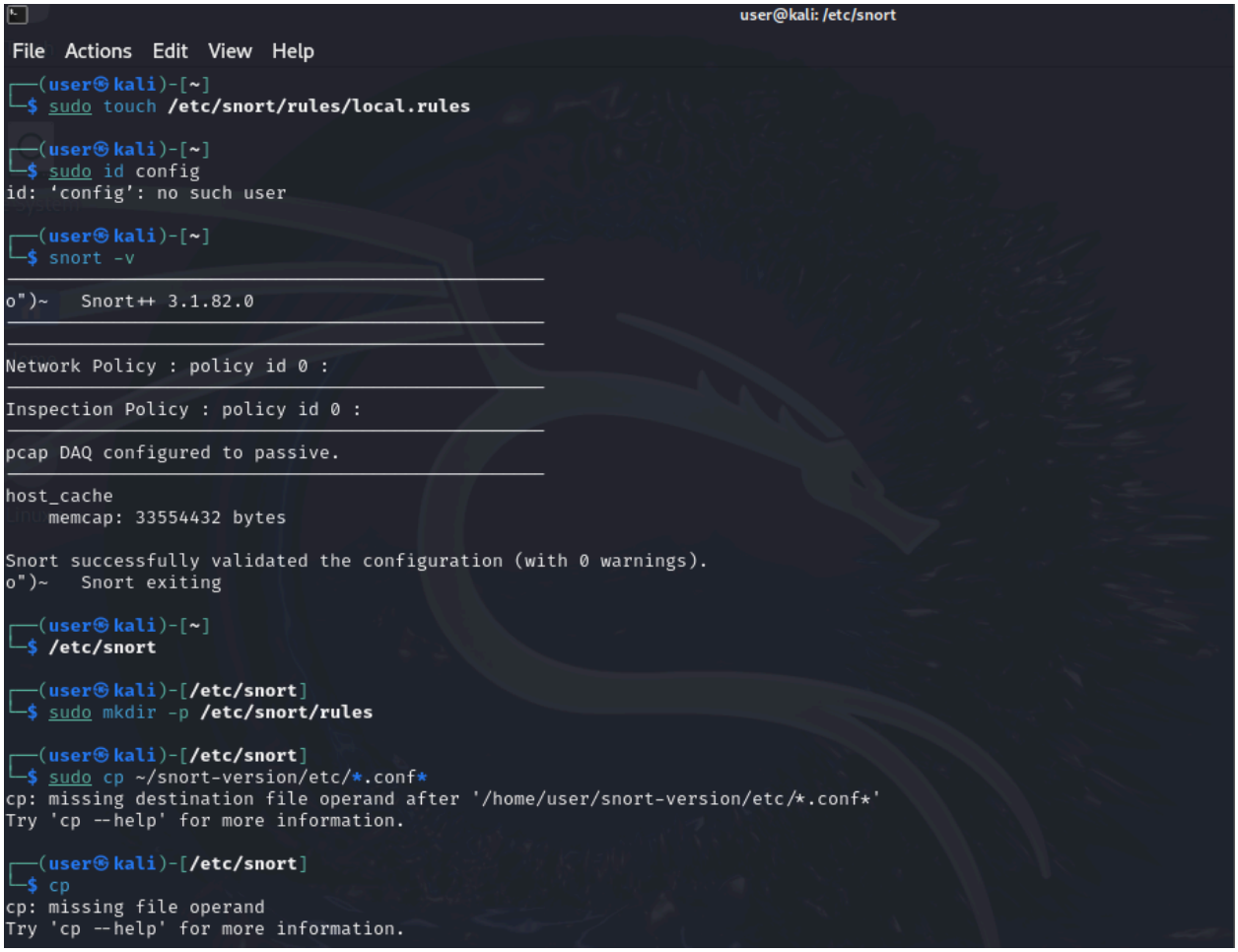
4.)

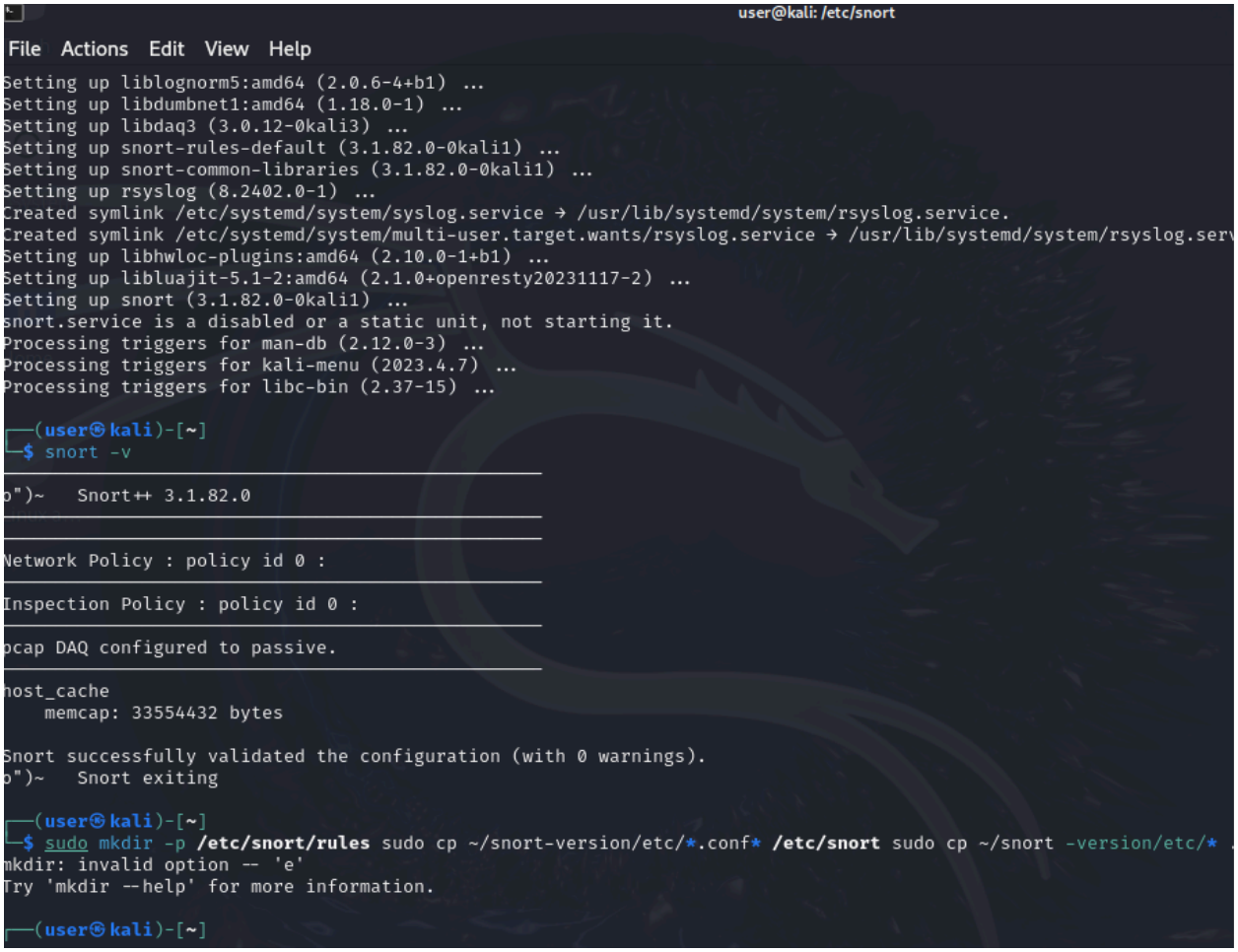
```
┌──(user㉿kali)-[/etc/snort]
└─$ alert icmp any any -> $HOME_NET any (msg:"ICMP Test"; sid:100001;)
zsh: parse error near `)'

┌──(user㉿kali)-[/etc/snort]
└─$ icmp test
Command 'icmp' not found, did you mean:
  command 'cmp' from deb diffutils
  command 'icmp6' from deb ipv6toolkit
  command 'icp' from deb renameutils
  command 'zcmp' from deb gzip
  command 'zcmp' from deb zutils
  command 'icmd' from deb renameutils
  command 'icmd' from deb ipmiutil
Try: sudo apt install <deb name>

┌──(user㉿kali)-[/etc/snort]
└─$ sudo snort -q -A console -i YOUR_INTERFACE -C /etc/snort/snort.conf -l/var/log/snort
[sudo] password for user:
ERROR: can't set -C /etc/snort/snort.conf
ERROR: usage: -C print out payloads with character data only (no hex)
FATAL: see prior 2 errors
Fatal Error, Quitting..

┌──(user㉿kali)-[/etc/snort]
└─$ sudo snort -q

┌──(user㉿kali)-[/etc/snort]
└─$
```

```
┌──(user㉿kali)-[/etc/snort]
└─$ icmp test
Command 'icmp' not found, did you mean:
  command 'icmd' from deb renameutils
  command 'icmd' from deb ipmiutil
  command 'cmp' from deb diffutils
  command 'icmp6' from deb ipv6toolkit
  command 'icp' from deb renameutils
  command 'zcmp' from deb gzip
  command 'zcmp' from deb zutils
Try: sudo apt install <deb name>
```

3.)


user@kali: /etc/snort
File Actions Edit View Help
┌──(user㉿kali)-[~]
└─$ sudo touch /etc/snort/rules/local.rules
┌──(user㉿kali)-[~]
└─$ sudo id config
id: ‘config’: no such user
┌──(user㉿kali)-[~]
└─$ snort -v
o")~ Snort++ 3.1.82.0
Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.
host_cache
memcap: 33554432 bytes
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting
┌──(user㉿kali)-[~]
└─$ /etc/snort
┌──(user㉿kali)-[/etc/snort]
└─$ sudo mkdir -p /etc/snort/rules
┌──(user㉿kali)-[/etc/snort]
└─$ sudo cp ~/snort-version/etc/*.conf*
cp: missing destination file operand after '/home/user/snort-version/etc/*.conf*'
Try 'cp --help' for more information.
┌──(user㉿kali)-[/etc/snort]
└─$ cp
cp: missing file operand
Try 'cp --help' for more information.

2.)

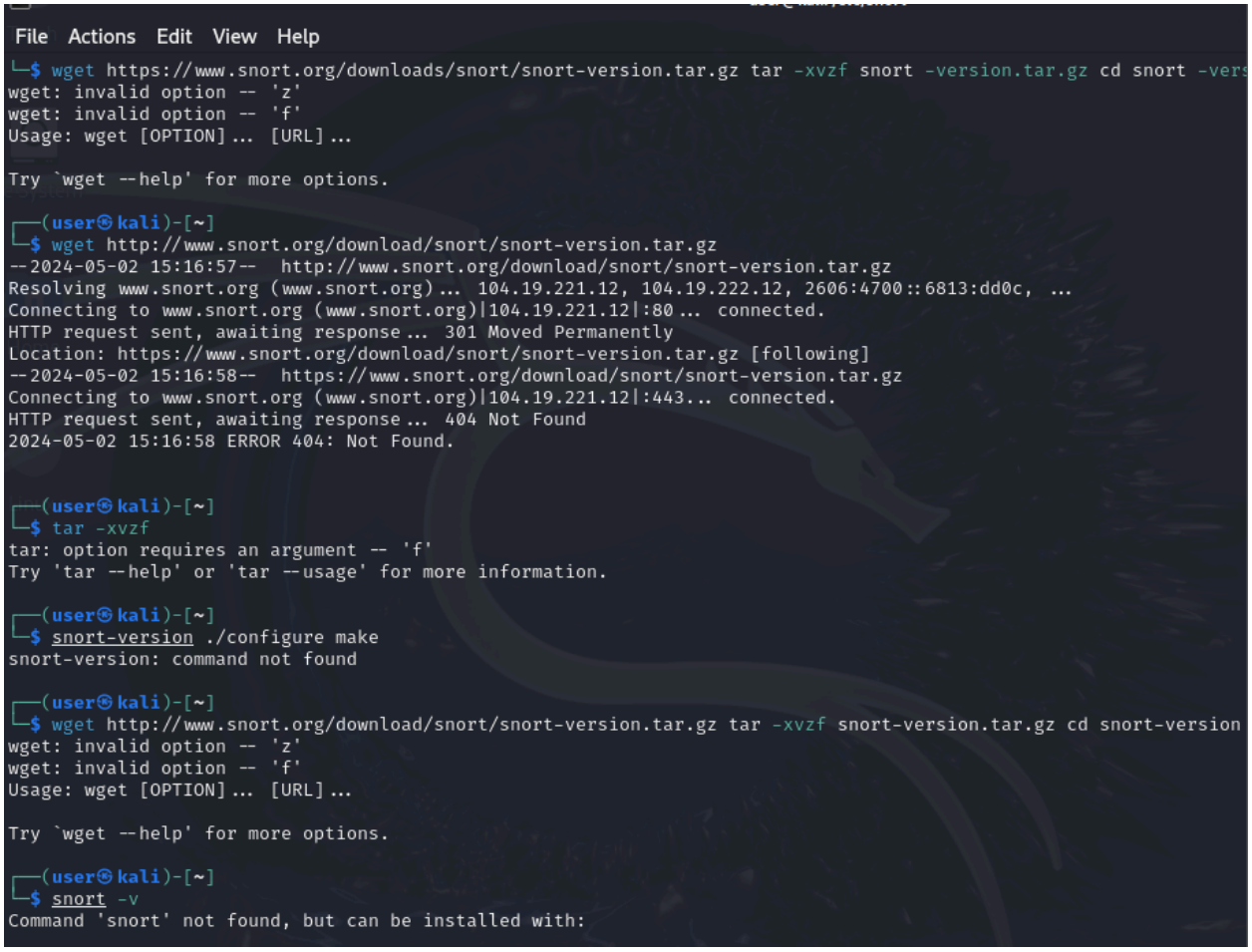

user@kali: /etc/snort
File Actions Edit View Help
Setting up liblognorm5:amd64 (2.0.6-4+b1) ...
Setting up libdumbnet1:amd64 (1.18.0-1) ...
Setting up libdaq3 (3.0.12-0kali3) ...
Setting up snort-rules-default (3.1.82.0-0kali1) ...
Setting up snort-common-libraries (3.1.82.0-0kali1) ...
Setting up rsyslog (8.2402.0-1) ...
Created symlink /etc/systemd/system/syslog.service → /usr/lib/systemd/system/rsyslog.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service → /usr/lib/systemd/system/rsyslog.serv
Setting up libhwloc-plugins:amd64 (2.10.0-1+b1) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+openresty20231117-2) ...
Setting up snort (3.1.82.0-0kali1) ...
snort.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for libc-bin (2.37-15) ...
┌──(user㉿kali)-[~]
└─$ snort -v
o")~ Snort++ 3.1.82.0
Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.
host_cache
memcap: 33554432 bytes
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting
┌──(user㉿kali)-[~]
└─$ sudo mkdir -p /etc/snort/rules sudo cp ~/snort-version/etc/*.conf* /etc/snort sudo cp ~/snort -version/etc/*
mkdir: invalid option -- 'e'
Try 'mkdir --help' for more information.
┌──(user㉿kali)-[~]

1.)

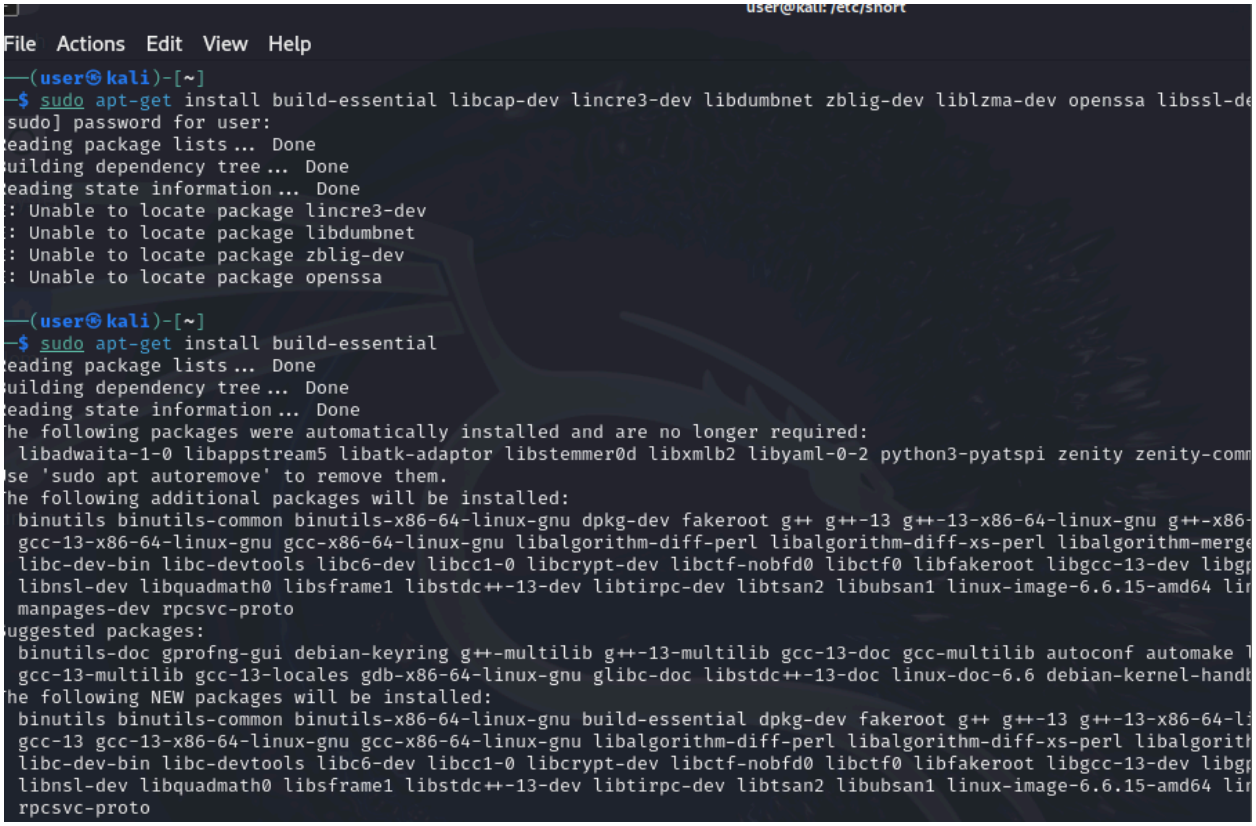
d.)


┌──(user㉿kali)-[~]
└─$ snort -v
o")~ Snort++ 3.1.82.0
Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.
host_cache
memcap: 33554432 bytes
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting

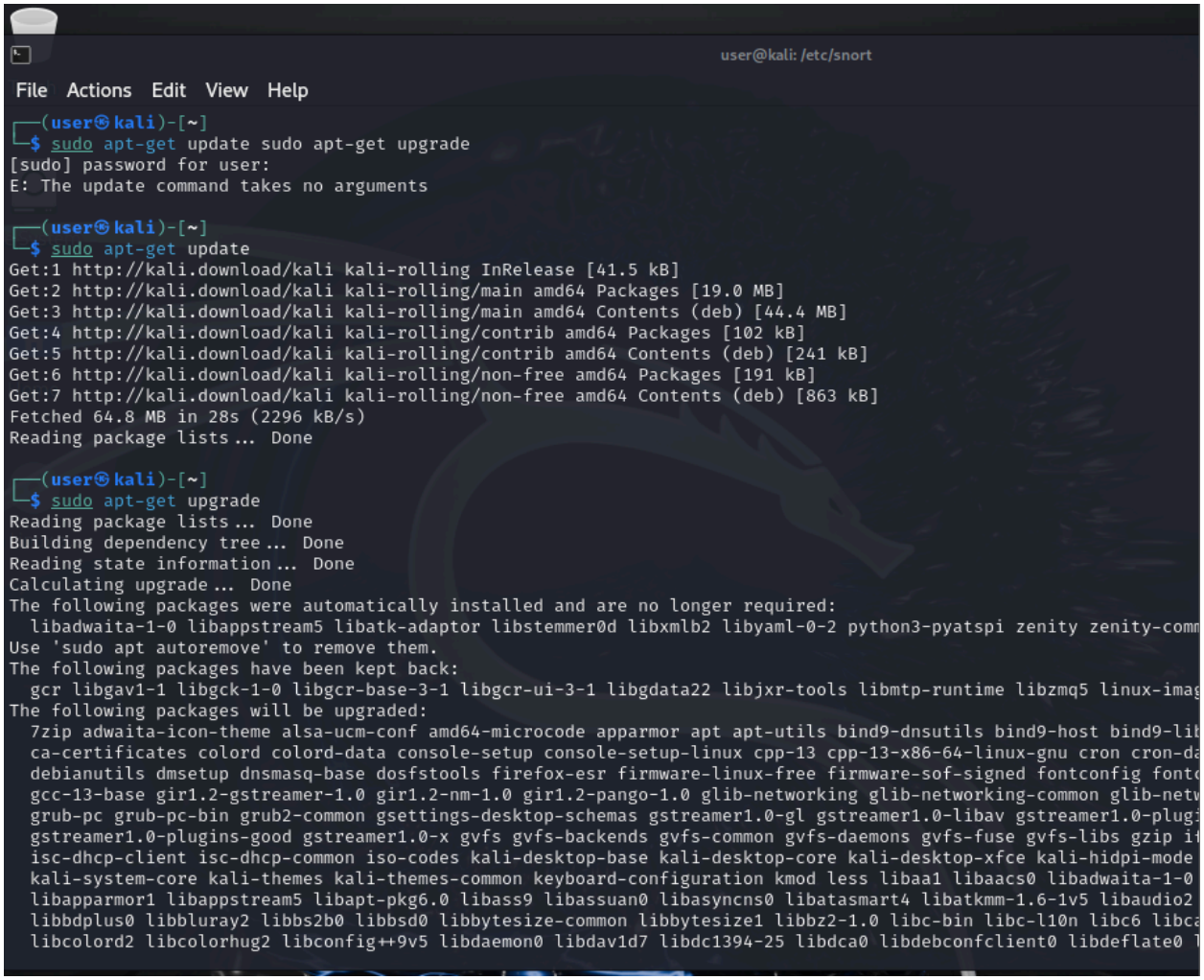
c.)

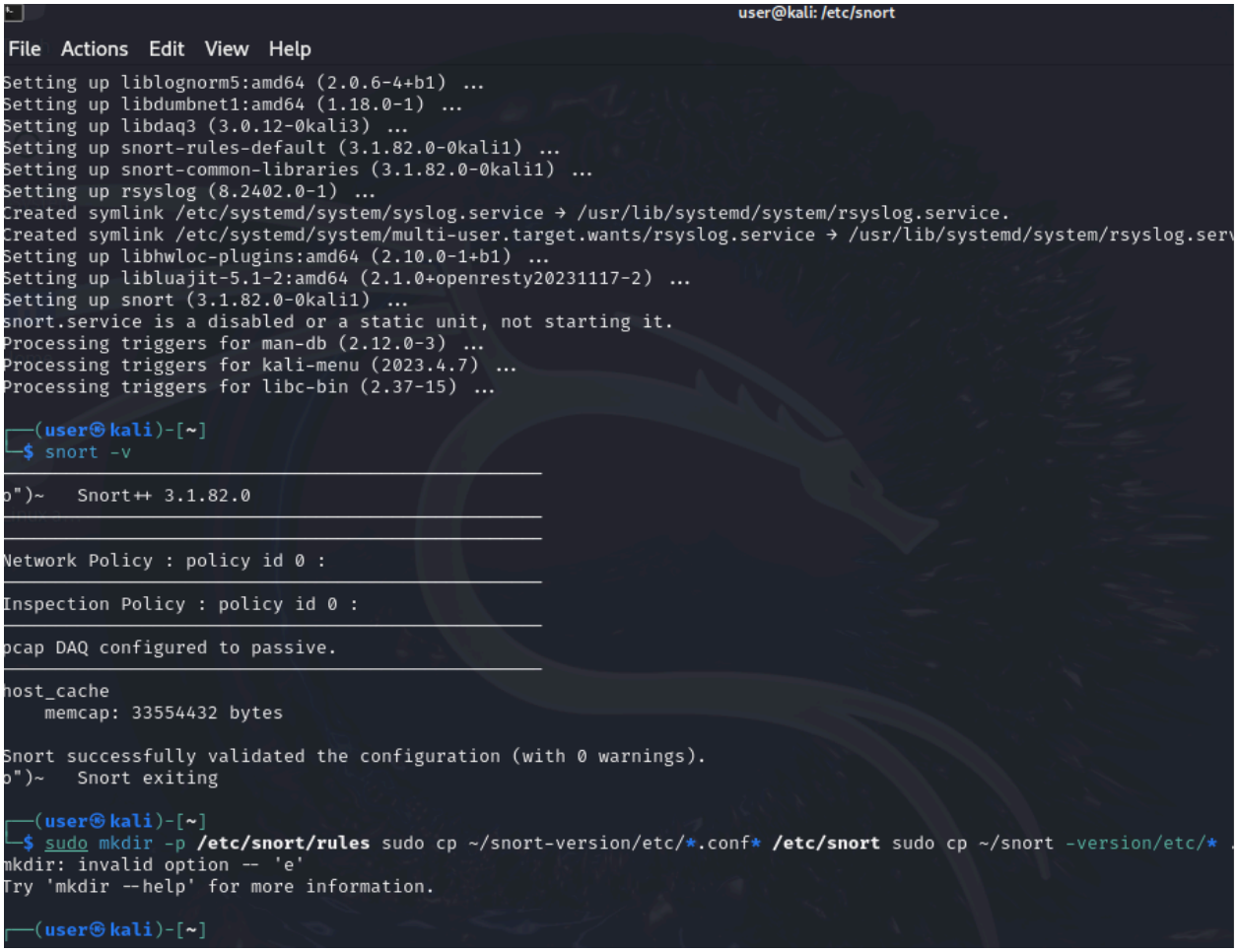

File Actions Edit View Help
└─$ wget https://www.snort.org/downloads/snort/snort-version.tar.gz tar -xvzf snort -version.tar.gz cd snort -vers
wget: invalid option -- 'z'
wget: invalid option -- 'f'
Usage: wget [OPTION]... [URL]...
Try `wget --help' for more options.
┌──(user㉿kali)-[~]
└─$ wget http://www.snort.org/download/snort/snort-version.tar.gz
--2024-05-02 15:16:57-- http://www.snort.org/download/snort/snort-version.tar.gz
Resolving www.snort.org (www.snort.org)... 104.19.221.12, 104.19.222.12, 2606:4700::6813:dd0c, ...
Connecting to www.snort.org (www.snort.org)|104.19.221.12|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.snort.org/download/snort/snort-version.tar.gz [following]
--2024-05-02 15:16:58-- https://www.snort.org/download/snort/snort-version.tar.gz
Connecting to www.snort.org (www.snort.org)|104.19.221.12|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-05-02 15:16:58 ERROR 404: Not Found.
┌──(user㉿kali)-[~]
└─$ tar -xvzf
tar: option requires an argument -- 'f'
Try 'tar --help' or 'tar --usage' for more information.
┌──(user㉿kali)-[~]
└─$ snort-version ./configure make
snort-version: command not found
┌──(user㉿kali)-[~]
└─$ wget http://www.snort.org/download/snort/snort-version.tar.gz tar -xvzf snort-version.tar.gz cd snort-version
wget: invalid option -- 'z'
wget: invalid option -- 'f'
Usage: wget [OPTION]... [URL]...
Try `wget --help' for more options.
┌──(user㉿kali)-[~]
└─$ snort -v
Command 'snort' not found, but can be installed with:

b.)


user@kali: /etc/short
File Actions Edit View Help
┌──(user㉿kali)-[~]
└─$ sudo apt-get install build-essential libcap-dev lincre3-dev libdumbnet zblig-dev liblzma-dev openssa libssl-de
sudo] password for user:
eading package lists ... Done
uilding dependency tree ... Done
eading state information ... Done
: Unable to locate package lincre3-dev
: Unable to locate package libdumbnet
: Unable to locate package zblig-dev
: Unable to locate package openssa
┌──(user㉿kali)-[~]
└─$ sudo apt-get install build-essential
eading package lists ... Done
uilding dependency tree ... Done
eading state information ... Done
he following packages were automatically installed and are no longer required:
libadwaita-1-0 libappstream5 libatk-adaptor libstemmer0d libxmlb2 libyaml-0-2 python3-pyatspi zenity zenity-comm
se 'sudo apt autoremove' to remove them.
he following additional packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu dpkg-dev fakeroot g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-
gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge
libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libfakeroot libgcc-13-dev libgp
libnsl-dev libquadmath0 libsframe1 libstdc++-13-dev libtirpc-dev libtsan2 libubsan1 linux-image-6.6.15-amd64 lin
manpages-dev rpcsvc-proto
uggested packages:
binutils-doc gprofng-gui debian-keyring g++-multilib g++-13-multilib gcc-13-doc gcc-multilib autoconf automake l
gcc-13-multilib gcc-13-locales gdb-x86-64-linux-gnu glibc-doc libstdc++-13-doc linux-doc-6.6 debian-kernel-handb
he following NEW packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu build-essential dpkg-dev fakeroot g++ g++-13 g++-13-x86-64-li
gcc-13 gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorith
libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libfakeroot libgcc-13-dev libgp
libnsl-dev libquadmath0 libsframe1 libstdc++-13-dev libtirpc-dev libtsan2 libubsan1 linux-image-6.6.15-amd64 lin
rpcsvc-proto

a.)


user@kali: /etc/snort
File Actions Edit View Help
┌──(user㉿kali)-[~]
└─$ sudo apt-get update sudo apt-get upgrade
[sudo] password for user:
E: The update command takes no arguments
┌──(user㉿kali)-[~]
└─$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [102 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [241 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [191 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [863 kB]
Fetched 64.8 MB in 28s (2296 kB/s)
Reading package lists ... Done
┌──(user㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
libadwaita-1-0 libappstream5 libatk-adaptor libstemmer0d libxmlb2 libyaml-0-2 python3-pyatspi zenity zenity-comm
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
gcr libgav1-1 libgck-1-0 libgcr-base-3-1 libgcr-ui-3-1 libgdata22 libjxr-tools libmtp-runtime libzmq5 linux-imag
The following packages will be upgraded:
7zip adwaita-icon-theme alsa-ucm-conf amd64-microcode apparmor apt apt-utils bind9-dnsutils bind9-host bind9-lib
ca-certificates colord colord-data console-setup console-setup-linux cpp-13 cpp-13-x86-64-linux-gnu cron cron-da
debianutils dmsetup dnsmasq-base dosfstools firefox-esr firmware-linux-free firmware-sof-signed fontconfig fontc
gcc-13-base gir1.2-gstreamer-1.0 gir1.2-nm-1.0 gir1.2-pango-1.0 glib-networking glib-networking-common glib-netw
grub-pc grub-pc-bin grub2-common gsettings-desktop-schemas gstreamer1.0-gl gstreamer1.0-libav gstreamer1.0-plugi
gstreamer1.0-plugins-good gstreamer1.0-x gvfs gvfs-backends gvfs-common gvfs-daemons gvfs-fuse gvfs-libs gzip if
isc-dhcp-client isc-dhcp-common iso-codes kali-desktop-base kali-desktop-core kali-desktop-xfce kali-hidpi-mode
kali-system-core kali-themes kali-themes-common keyboard-configuration kmod less libaa1 libaacs0 libadwaita-1-0
libapparmor1 libappstream5 libapt-pkg6.0 libass9 libassuan0 libasyncns0 libatasmart4 libatkmm-1.6-1v5 libaudio2
libbdplus0 libbluray2 libbs2b0 libbsd0 libbytesize-common libbytesize1 libbz2-1.0 libc-bin libc-l10n libc6 libca
libcolord2 libcolorhug2 libconfig++9v5 libdaemon0 libdav1d7 libdc1394-25 libdca0 libdebconfclient0 libdeflate0 l


user@kali: /etc/snort
File Actions Edit View Help
Setting up liblognorm5:amd64 (2.0.6-4+b1) ...
Setting up libdumbnet1:amd64 (1.18.0-1) ...
Setting up libdaq3 (3.0.12-0kali3) ...
Setting up snort-rules-default (3.1.82.0-0kali1) ...
Setting up snort-common-libraries (3.1.82.0-0kali1) ...
Setting up rsyslog (8.2402.0-1) ...
Created symlink /etc/systemd/system/syslog.service → /usr/lib/systemd/system/rsyslog.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service → /usr/lib/systemd/system/rsyslog.serv
Setting up libhwloc-plugins:amd64 (2.10.0-1+b1) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+openresty20231117-2) ...
Setting up snort (3.1.82.0-0kali1) ...
snort.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for libc-bin (2.37-15) ...
┌──(user㉿kali)-[~]
└─$ snort -v
o")~ Snort++ 3.1.82.0
Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.
host_cache
memcap: 33554432 bytes
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting
┌──(user㉿kali)-[~]
└─$ sudo mkdir -p /etc/snort/rules sudo cp ~/snort-version/etc/*.conf* /etc/snort sudo cp ~/snort -version/etc/*
mkdir: invalid option -- 'e'
Try 'mkdir --help' for more information.
┌──(user㉿kali)-[~]