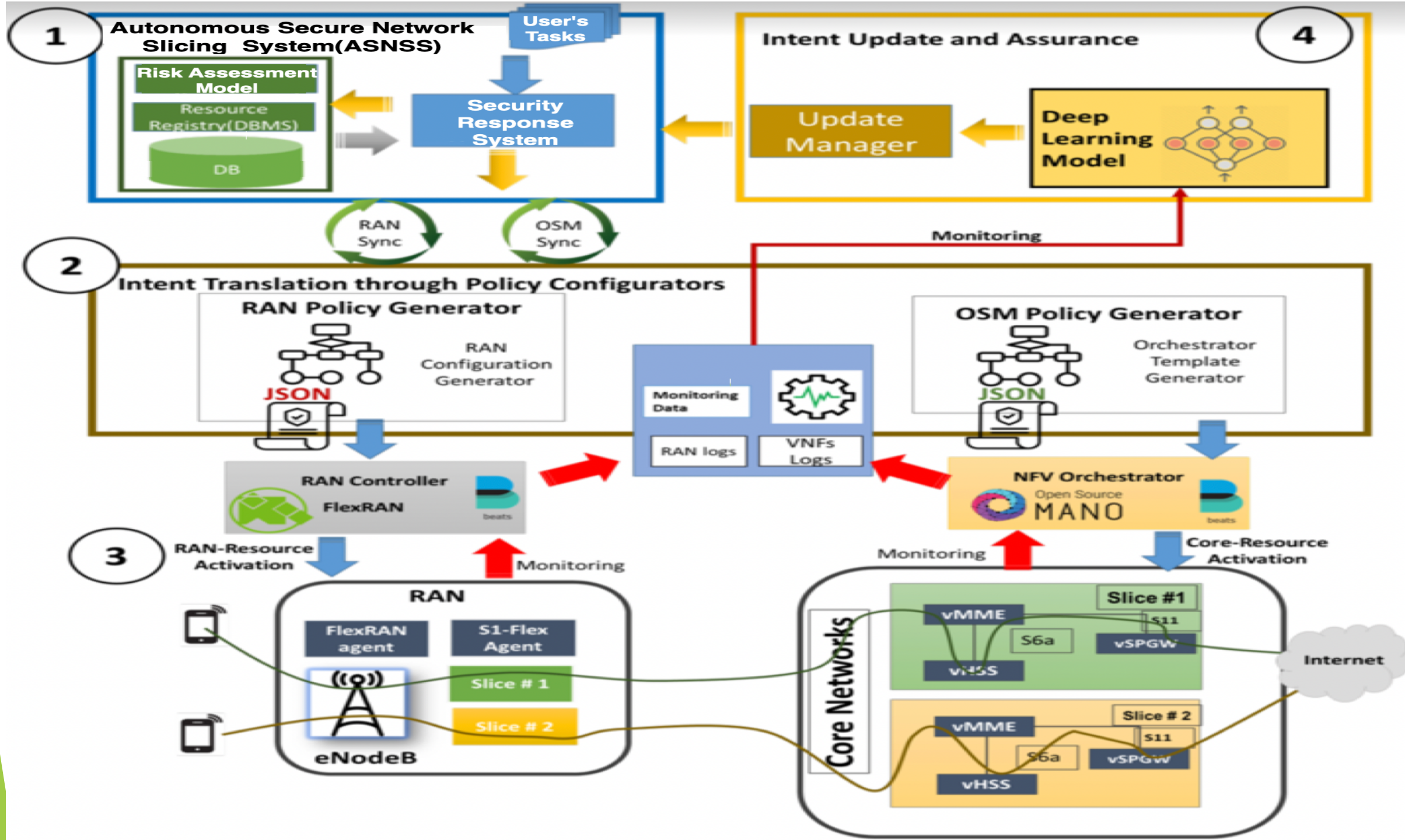
Ksniff as a Kubernetes-integrated packet sniffer


1
Autonomous Secure Network Slicing System(ASNSS)
User's Tasks
Risk Assessment Model
Resource Registry(DBMS)
DB
Security Response System
RAN Sync
OSM Sync
4
Intent Update and Assurance
Update Manager
Deep Learning Model
Monitoring
2
Intent Translation through Policy Configurators
RAN Policy Generator
JSON
RAN Configuration Generator
Monitoring Data
RAN logs
VNFs Logs
OSM Policy Generator
JSON
Orchestrator Template Generator
RAN Controller
FlexRAN
NFV Orchestrator
Open Source MANO
3
RAN-Resource Activation
Monitoring
Monitoring
Core-Resource Activation
RAN
FlexRAN agent
S1-Flex Agent
Slice # 1
Slice # 2
eNodeB
Core Networks
Slice #1
vMME
S11
S6a
vSPGW
vHSS
Slice # 2
vMME
S11
S6a
vSPGW
vHSS
Internet

Ksniff as a Kubernetes-integrated packet sniffer

- Troubleshooting containers in Kubernetes is a recurring topic.
- The current traditional tools are not enough.
- So, in those cases, how do we get to inspect this traffic? So this is the question that this work answers.

Ksniff as a Kubernetes-integrated packet sniffer

- Ksniff is shipped as a kubectl plugin that allows using tcpdump and Wireshark to capture traffic on a specific pod within a cluster.
- Ksniff uses kubectl to upload a tcpdump binary (packet sniffer) to the target container, and redirects the output to the Wireshark instance running in my machine.
- Well, Ksniff has specific flag (*-p*) for that. This approach can be also used to sniff traffic in distroless containers.

Installation process

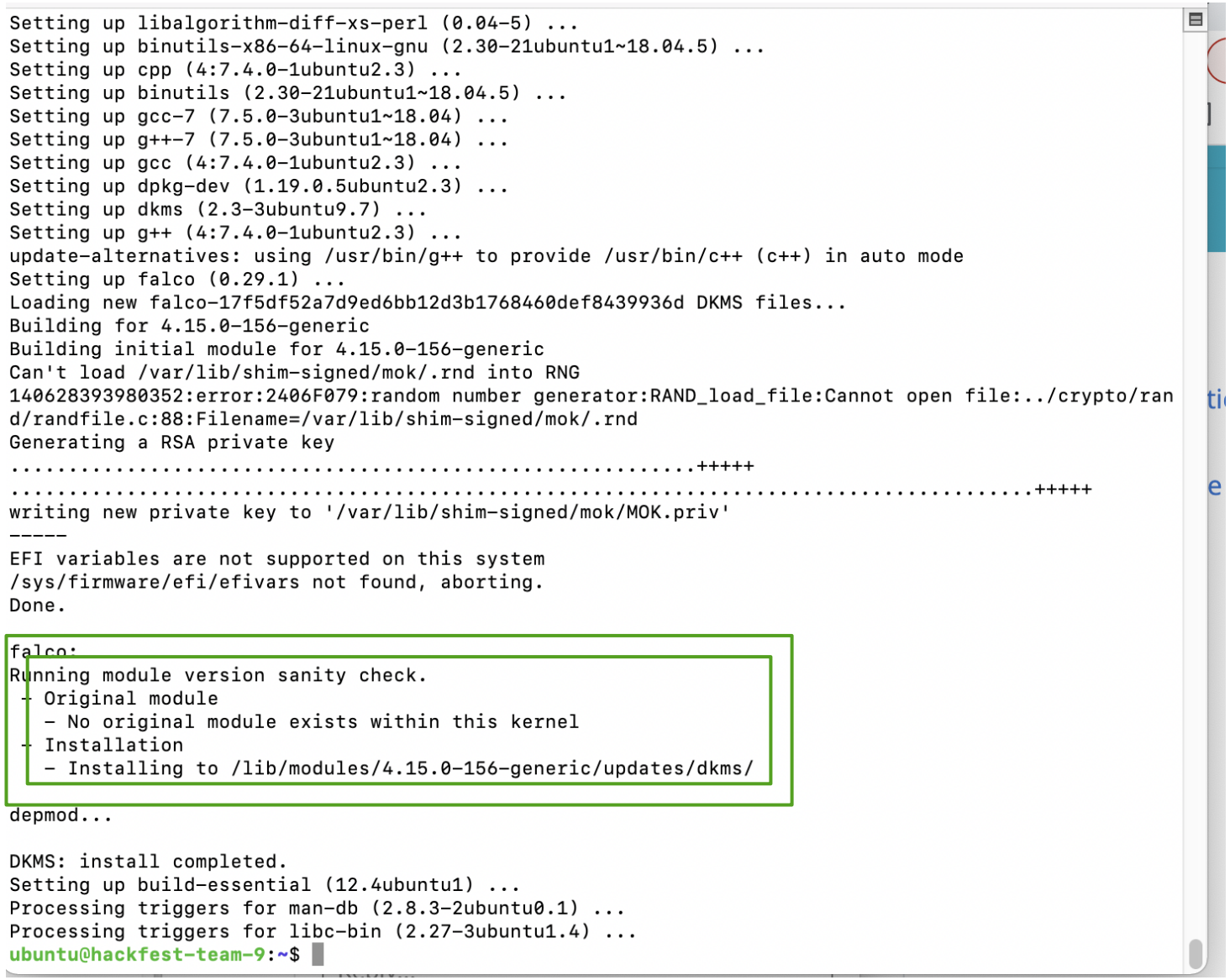
- 1- Install Falco. Open Source run time security tool.
  - Parsing the Linux system calls from the kernel at runtime.
  - Asserting the stream against a powerful rules engine.
  - Alerting when a rule is violated.
- 2. Install Krew.
  - Krew is a tool that makes it easy to use kubectl plugins. Krew helps you discover plugins, install and manage them on your machine. It is similar to tools like apt, dnf or brew.
- 3. Installing sniff/Ksniff.
  - capture traffic on a specific pod within a cluster. Ksniff uses kubectl to upload a tcpdump binary (packet sniffer) to the target container, and redirects the output to the Wireshark instance running in your machine
- 4. Installing libpcap-dev for tcpdump compilation (generate the binary file).
- 5. Install LOIC
- 6. Install Wireshark
- Falco→ Krew-->Ksnif→LOIC→ libpcap-dev→ Wireshark

Installing Falco

```
update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in auto mo
de
Setting up libgcc-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...
Setting up cpp-7 (7.5.0-3ubuntu1~18.04) ...
Setting up libstdc++-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...
Setting up libalgorithm-merge-perl (0.08-3) ...
Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up binutils-x86-64-linux-gnu (2.30-21ubuntu1~18.04.5) ...
Setting up cpp (4:7.4.0-1ubuntu2.3) ...
Setting up binutils (2.30-21ubuntu1~18.04.5) ...
Setting up gcc-7 (7.5.0-3ubuntu1~18.04) ...
Setting up g++-7 (7.5.0-3ubuntu1~18.04) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up dpkg-dev (1.19.0.5ubuntu2.3) ...
Setting up dkms (2.3-3ubuntu9.7) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up falco (0.29.1) ...
Loading new falco-17f5df52a7d9ed6bb12d3b1768460def8439936d DKMS files...
Building for 4.15.0-156-generic
Building initial module for 4.15.0-156-generic
Can't load /var/lib/shim-signed/mok/.rnd into RNG
140628393980352:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/ran
d/randfile.c:88:Filename=/var/lib/shim-signed/mok/.rnd
Generating a RSA private key
.....................................................+++++
.....................................................................................+++++
writing new private key to '/var/lib/shim-signed/mok/MOK.priv'
-----
EFI variables are not supported on this system
/sys/firmware/efi/efivars not found, aborting.
Done.

falco:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/4.15.0-156-generic/updates/dkms/

depmod
```


Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up binutils-x86-64-linux-gnu (2.30-21ubuntu1~18.04.5) ...
Setting up cpp (4:7.4.0-1ubuntu2.3) ...
Setting up binutils (2.30-21ubuntu1~18.04.5) ...
Setting up gcc-7 (7.5.0-3ubuntu1~18.04) ...
Setting up g++-7 (7.5.0-3ubuntu1~18.04) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up dpkg-dev (1.19.0.5ubuntu2.3) ...
Setting up dkms (2.3-3ubuntu9.7) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up falco (0.29.1) ...
Loading new falco-17f5df52a7d9ed6bb12d3b1768460def8439936d DKMS files...
Building for 4.15.0-156-generic
Building initial module for 4.15.0-156-generic
Can't load /var/lib/shim-signed/mok/.rnd into RNG
140628393980352:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/var/lib/shim-signed/mok/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/var/lib/shim-signed/mok/MOK.priv'

EFI variables are not supported on this system
/sys/firmware/efi/efivars not found, aborting.
Done.
falco:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/4.15.0-156-generic/updates/dkms/
depmod...
DKMS: install completed.
Setting up build-essential (12.4ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...
ubuntu@hackfest-team-9:~$

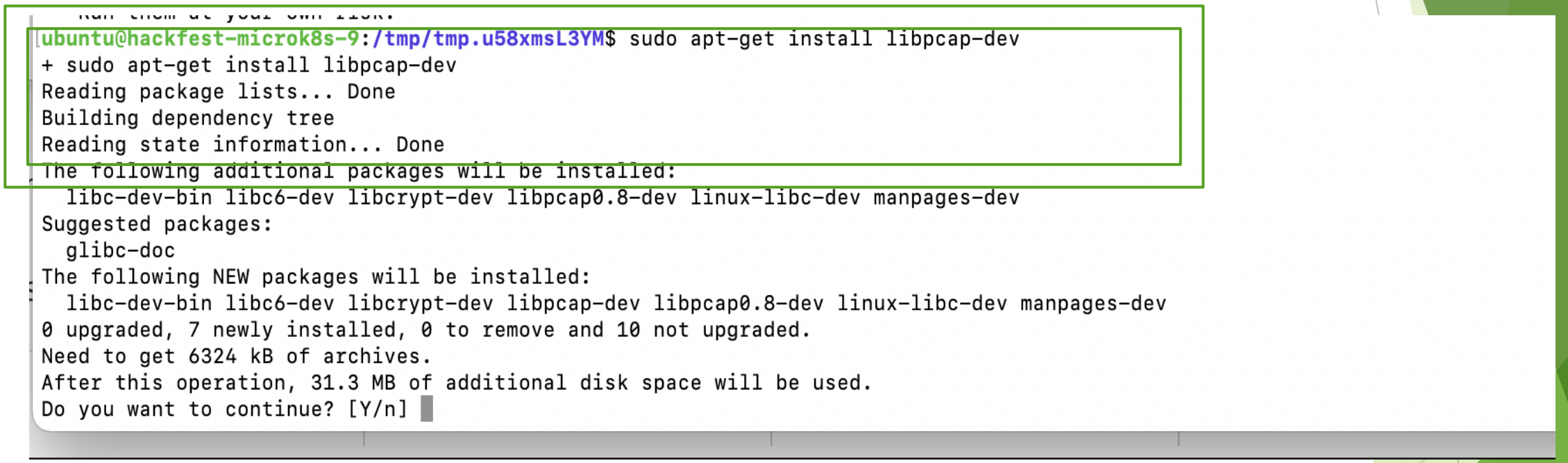
Installing Krew

```
ubuntu@hackfest-microk8s-9:~$ git (
  set -x; cd "$(mktemp -d)" &&
  OS="$(uname | tr '[:upper:]' '[:lower:]')" &&
  ARCH="$(uname -m | sed -e 's/x86_64/amd64/' -e 's/\(arm\)\(64\)\?.*/\1\2/' -e 's/aarch64$/arm64/')" &&
  curl -fsSLO "https://github.com/kubernetes-sigs/krew/releases/latest/download/krew.tar.gz" &&
  tar zxvf krew.tar.gz &&
  KREW=./krew-"${OS}_${ARCH}" &&
  "$KREW" install krew
)
-bash: syntax error near unexpected token `newline'
++ mktemp -d
+ cd /tmp/tmp.u58xmsL3YM
++ uname
++ tr '[:upper:]' '[:lower:]'
+ OS=linux
++ uname -m
++ sed -e s/x86_64/amd64/ -e 's/\(arm\)\(64\)\?.*/\1\2/' -e 's/aarch64$/arm64/'
+ ARCH=amd64
+ curl -fsSLO https://github.com/kubernetes-sigs/krew/releases/latest/download/krew.tar.gz
+ tar zxvf krew.tar.gz
./LICENSE
./krew-darwin_amd64
./krew-darwin_arm64
./krew-linux_amd64
./krew-linux_arm
./krew-linux_arm64
./krew-windows_amd64.exe
+ KREW=./krew-linux_amd64
+ ./krew-linux_amd64 install krew
Adding "default" plugin index from https://github.com/kubernetes-sigs/krew-index.git.
Updated the local copy of plugin index.
Installing plugin: krew
Installed plugin: krew
```

Installing sniff

```
ubuntu@hackfest-microk8s-9:/tmp/tmp.u58xmsL3YM$ kubectl krew install sniff
+ kubectl krew install sniff
Updated the local copy of plugin index.
Installing plugin: sniff
Installed plugin: sniff
\
 | Use this plugin:
 |      kubectl sniff
 | Documentation:
 |      https://github.com/eldadru/ksniff
 | Caveats:
 | \
 |  | This plugin needs the following programs:
 |  | * wireshark (optional, used for live capture)
 | /
/
WARNING: You installed plugin "sniff" from the krew-index plugin repository.
   These plugins are not audited for security by the Krew maintainers.
   Run them at your own risk.
ubuntu@hackfest-microk8s-9:/tmp/tmp.u58xmsL3YM$
```

Installing libpcap-dev for tcpdump complilation



Installing libpcap-dev For Tcpdump Compilation

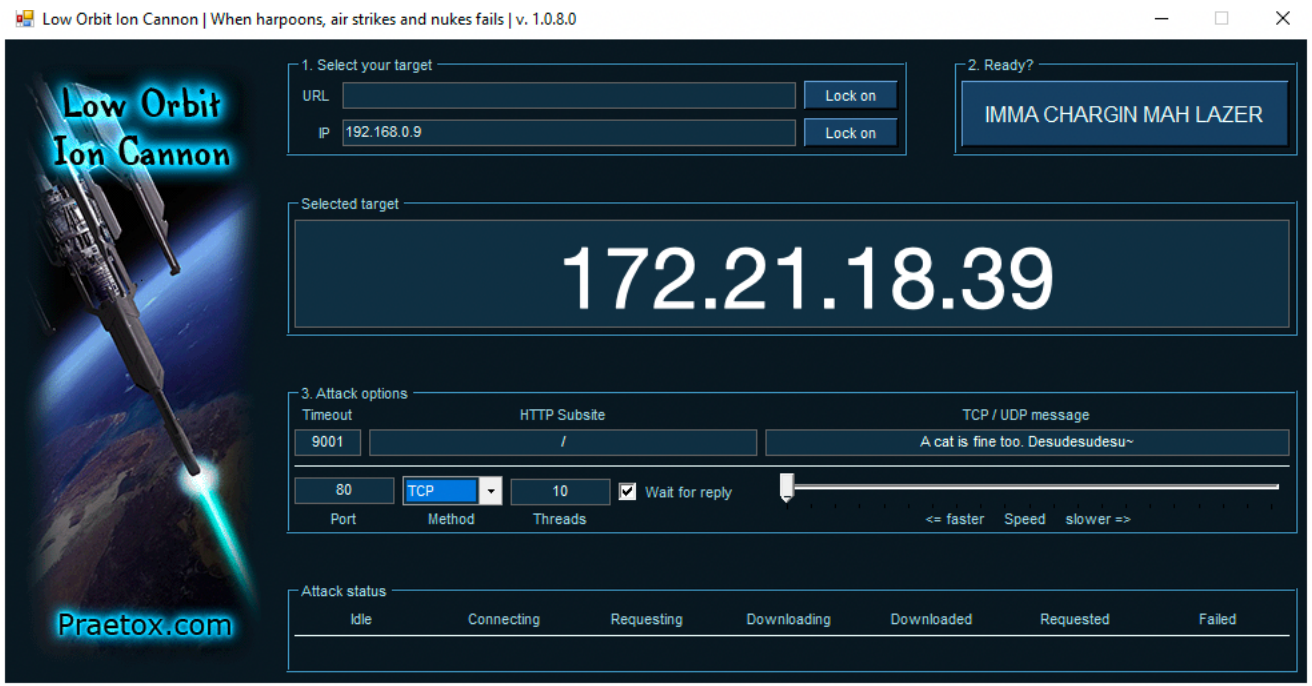
```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-dev-bin libc6-dev libcrypt-dev libpcap0.8-dev linux-libc-dev manpages-dev
Suggested packages:
  glibc-doc
The following NEW packages will be installed:
  libc-dev-bin libc6-dev libcrypt-dev libpcap-dev libpcap0.8-dev linux-libc-dev manpages-dev
0 upgraded, 7 newly installed, 0 to remove and 10 not upgraded.
Need to get 6324 kB of archives.
After this operation, 31.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libc-dev-bin amd64 2.31-0ubuntu9.2 [71.8 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 linux-libc-dev amd64 5.4.0-84.94 [1115 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libcrypt-dev amd64 1:4.4.10-10ubuntu4 [104 kB]
Get:4 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libc6-dev amd64 2.31-0ubuntu9.2 [2520 kB]
Get:5 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libpcap0.8-dev amd64 1.9.1-3 [244 kB]
Get:6 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1.9.1-3 [3484 B]
Get:7 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 manpages-dev all 5.05-1 [2266 kB]
Fetched 6324 kB in 3s (2188 kB/s)
Selecting previously unselected package libc-dev-bin.
(Reading database ... 94545 files and directories currently installed.)
Preparing to unpack .../0-libc-dev-bin_2.31-0ubuntu9.2_amd64.deb ...
Unpacking libc-dev-bin (2.31-0ubuntu9.2) ...
Selecting previously unselected package linux-libc-dev:amd64.
Preparing to unpack .../1-linux-libc-dev_5.4.0-84.94_amd64.deb ...
Unpacking linux-libc-dev:amd64 (5.4.0-84.94) ...
Selecting previously unselected package libcrypt-dev:amd64.
Preparing to unpack .../2-libcrypt-dev_1%3a4.4.10-10ubuntu4_amd64.deb ...
Unpacking libcrypt-dev:amd64 (1:4.4.10-10ubuntu4) ...
Selecting previously unselected package libc6-dev:amd64.
Preparing to unpack .../3-libc6-dev_2.31-0ubuntu9.2_amd64.deb ...
Unpacking libc6-dev:amd64 (2.31-0ubuntu9.2) ...
Selecting previously unselected package libpcap0.8-dev:amd64.
Preparing to unpack .../4-libpcap0.8-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap0.8-dev:amd64 (1.9.1-3) ...
Selecting previously unselected package libpcap-dev:amd64.
Preparing to unpack .../5-libpcap-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap-dev:amd64 (1.9.1-3) ...
Selecting previously unselected package manpages-dev.
Preparing to unpack .../6-manpages-dev_5.05-1_all.deb ...
Unpacking manpages-dev (5.05-1) ...
Setting up manpages-dev (5.05-1) ...
Setting up linux-libc-dev:amd64 (5.4.0-84.94) ...
Setting up libcrypt-dev:amd64 (1:4.4.10-10ubuntu4) ...
Setting up libc-dev-bin (2.31-0ubuntu9.2) ...
Setting up libc6-dev:amd64 (2.31-0ubuntu9.2) ...
Setting up libpcap0.8-dev:amd64 (1.9.1-3) ...
Setting up libpcap-dev:amd64 (1.9.1-3) ...
Processing triggers for man-db (2.9.1-1) ...
```

The name of the pod to collect the TCPDUMP:
Pod/Kubernetes-bootcamp-57978f5f5d-vbzb4

Nodes deployed in the cluster

```
Last login: Fri Sep 17 02:19:56 2021 from 172.21.18.1
ubuntu@hackfest-microk8s-9:~$ microk8s kubectl get nodes
NAME                STATUS   ROLES    AGE     VERSION
hackfest-microk8s-9   Ready    <none>   6d11h   v1.21.4-3+e5758f73ed2a04
ubuntu@hackfest-microk8s-9:~$ microk8s kubectl get deployments
NAME                READY   UP-TO-DATE   AVAILABLE   AGE
kubernetes-bootcamp   1/1     1            1           71m
ubuntu@hackfest-microk8s-9:~$
```

The LOIC


Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0
Low Orbit Ion Cannon
Praetox.com
1. Select your target
URL
Lock on
IP
192.168.0.9
Lock on
2. Ready?
IMMA CHARGIN MAH LAZER
Selected target
172.21.18.39
3. Attack options
Timeout
HTTP Subsite
TCP / UDP message
9001
/
A cat is fine too. Desudesudesu~
80
TCP
10
Wait for reply
Port
Method
Threads
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed

The Wireshark analysis

22432	135.319408	192.168.51.61	192.168.51.189	TCP	60 52881 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22433	135.319511	192.168.51.61	192.168.51.189	TCP	60 52885 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22434	135.319529	192.168.51.189	192.168.51.61	TCP	54 80 → 52890 [FIN, ACK] Seq=498 Ack=65 Win=29312 Len=0
22435	135.319540	192.168.51.189	192.168.51.61	TCP	54 80 → 52897 [FIN, ACK] Seq=498 Ack=65 Win=29312 Len=0
22436	135.319561	192.168.51.61	192.168.51.189	TCP	60 52886 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22437	135.319584	192.168.51.189	192.168.51.61	TCP	54 80 → 52894 [FIN, ACK] Seq=498 Ack=65 Win=29312 Len=0
22438	135.319591	192.168.51.189	192.168.51.61	TCP	54 80 → 52887 [FIN, ACK] Seq=498 Ack=65 Win=29312 Len=0
22439	135.319592	192.168.51.61	192.168.51.189	TCP	60 52890 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22440	135.319601	192.168.51.189	192.168.51.61	TCP	54 80 → 52889 [FIN, ACK] Seq=498 Ack=65 Win=29312 Len=0
22441	135.319622	192.168.51.61	192.168.51.189	TCP	60 52882 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22442	135.319671	192.168.51.61	192.168.51.189	TCP	60 52895 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22443	135.319695	192.168.51.61	192.168.51.189	TCP	60 52894 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22444	135.319718	192.168.51.61	192.168.51.189	TCP	60 52883 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22445	135.319756	192.168.51.61	192.168.51.189	TCP	60 52887 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22446	135.319781	192.168.51.61	192.168.51.189	TCP	60 52884 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22447	135.319818	192.168.51.61	192.168.51.189	TCP	60 52893 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22448	135.319846	192.168.51.62	192.168.51.189	TCP	60 63684 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
22449	135.319877	192.168.51.61	192.168.51.189	TCP	60 52892 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22450	135.319898	192.168.51.61	192.168.51.189	TCP	60 52896 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22451	135.319920	192.168.51.61	192.168.51.189	TCP	60 52897 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22452	135.319957	192.168.51.61	192.168.51.189	TCP	60 52889 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22453	135.319984	192.168.51.62	192.168.51.189	TCP	117 [TCP segment of a reassembled PDU]
22454	135.320023	192.168.51.189	192.168.51.62	TCP	54 80 → 63684 [ACK] Seq=1 Ack=64 Win=29312 Len=0
22455	135.320063	192.168.51.61	192.168.51.189	TCP	60 52891 → 80 [RST, ACK] Seq=65 Ack=498 Win=0 Len=0
22456	135.322965	192.168.51.61	192.168.51.189	TCP	60 52942 → 80 [FIN, ACK] Seq=64 Ack=1 Win=65536 Len=0
22457	135.323099	192.168.51.61	192.168.51.189	TCP	60 52900 → 80 [FIN, ACK] Seq=64 Ack=1 Win=65536 Len=0