CAP6135: Malware and Software vulnerability analysis **Sudip Prasai**
Programming Assignment 3: Internet worm propagation simulation March 23, 2020.

1 Design

In this assignment , we have implemented the simulation of simple worm propagation in a medium-scale network by using discrete-time simulation method. We assume an isolated network with omega(Ω = 100,000) IP address space which means the IP range in our network ranges from 1 to 100,000. It is assumed that there are N = 1,000 computers that are vulnerable to the worm in this isolated network. The IP addresses of the vulnerable computer has the following pattern of IP addresses:

1, 2, 3,. . . , 10,

1001, 1002, ..., 1010,

2001, 2002, . . . , 2010,

....

From this we can see that, each cluster of 10 computers with the consecutive IPs are vulnerable to the worm, and in every 1000 consecutive IP addresses there will be one cluster of 10 vulnerable computers (so there are 100 clusters of vulnerable computers overall).

We further assume that worm starts to propagate infection within the network initially from 1 machine which has IP address of 1001. The scan rate(n) of infected machine is 3.This implies that a worm-infected computer can scan to 3 other IP addresses in the network at each time step. A vulnerable computer is immediately infected if a scan finds it and this newly infected computer can also begin infection other 3 IP addresses from the next time step. In this way the worm propagates and infect the whole computer in a network.

2 Implementation

We need to find the number of infected computers at each time step t(t=1,2,3...) which is represented as I(t). We simulate the worm propagation 3 times to get the three vector of the number of infected IP, I(t). The simulation ends when all the vulnerable machines are infected. At initial point, I(0) = 1. We have implemented simulation of two kinds of scanning:

2.1 Random Scanning

In this method, an infected computer x randomly selects another 3 IP addresses with in the entire IP address space in a time unit.

2.2 Local preference Scanning

In this method, an infected computer at each time step with IP value x picks the target IP address value y by the following rule:

1. With probability p = 0.8, it picks a random value y such that y $\in$ [x-10, x+10]
2. With the remaining probability 0.2, it picks a random value y between 1 to 100,000.

3 Results and Analysis:

We performed three simulation runs for both random scanning and local-preference scanning method. As an output, we plotted a curve that shows the number of infected computers at each time step as shown in the figure1 and 2. The plot of worm propagation across the network follows a sigmoid curve (S-curve) in both the methods. It can be seen that the infected computers at the beginning increases slowly and rapidly increases with the time as the number of infected computers increases and finally reach the maximum point.

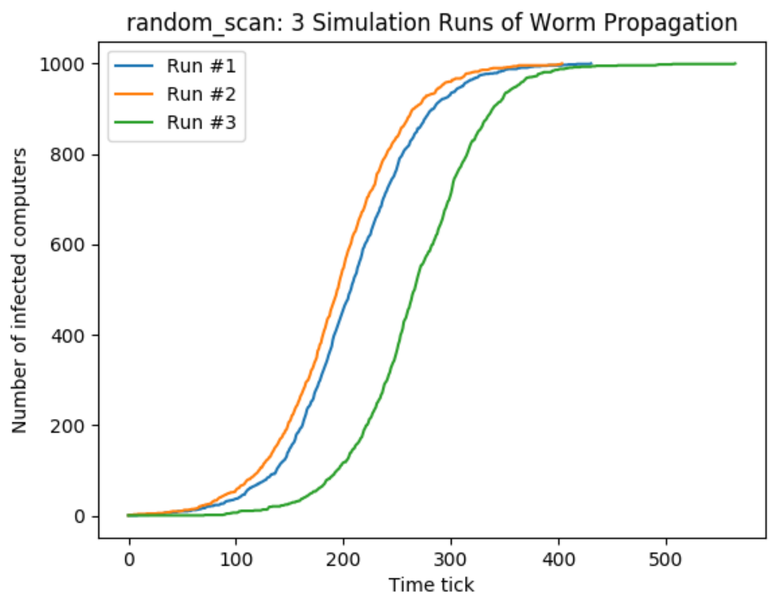


Figure 1: Three simulation run on worm propagation using random scanning method

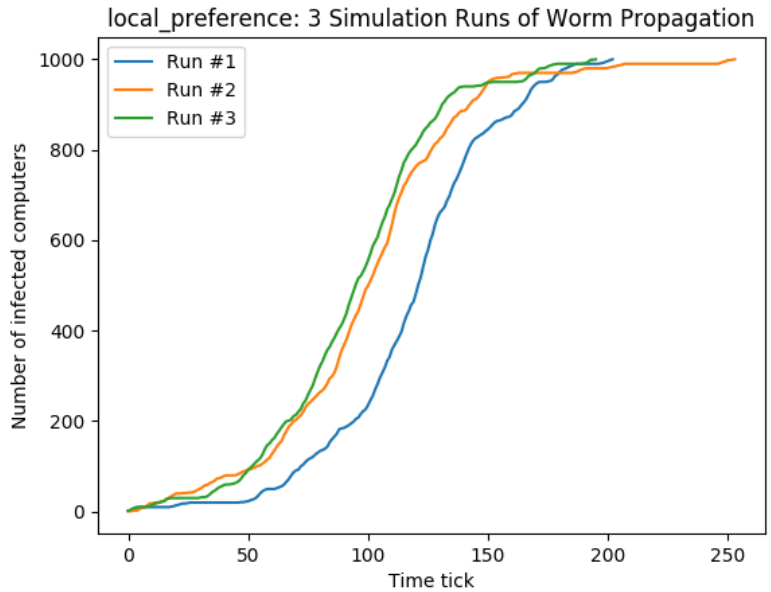


Figure 2: Three simulation run on worm propagation using local preference scanning method

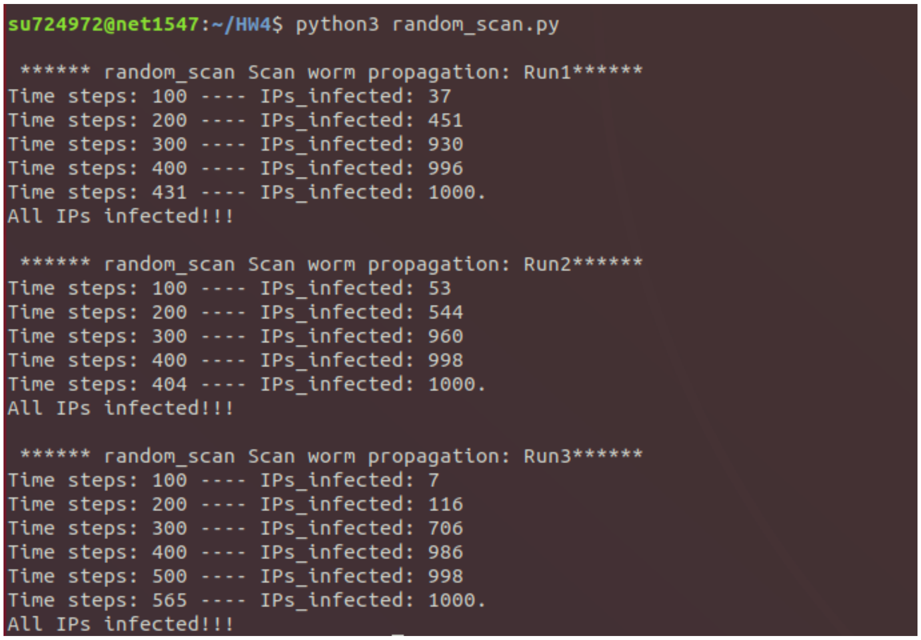
Also, we observed the number of time steps required by each method to infect all of the 1000 vulnerable computers in the network which is shown in the table 1. It took 431, 404 and 565 time steps in case of random scanning when simulating for three runs, and it took 169, 267 and 183 in case of local preference scanning. From this data, we can conclude that local preference scanning spread worms faster in the network than the random scanning method.

Simulation method of worm propagation	Time steps to infect all 1000 computers		
	Run 1	Run 2	Run 3
Random scan	431	404	565
Local preference scan	169	267	183

Table 1: Table to show the time steps required to infect all the vulnerable computers in the network.

4 Output

The screenshot of the output of the program is shown in the figure 3 and 4.



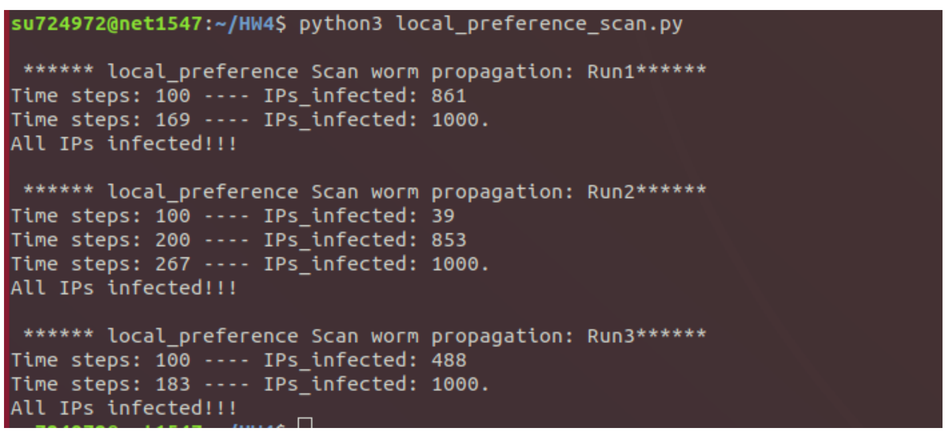
```
su724972@net1547:~/HW4$ python3 random_scan.py

 ****** random_scan Scan worm propagation: Run1******
Time steps: 100 ---- IPs_infected: 37
Time steps: 200 ---- IPs_infected: 451
Time steps: 300 ---- IPs_infected: 930
Time steps: 400 ---- IPs_infected: 996
Time steps: 431 ---- IPs_infected: 1000.
All IPs infected!!!

 ****** random_scan Scan worm propagation: Run2******
Time steps: 100 ---- IPs_infected: 53
Time steps: 200 ---- IPs_infected: 544
Time steps: 300 ---- IPs_infected: 960
Time steps: 400 ---- IPs_infected: 998
Time steps: 404 ---- IPs_infected: 1000.
All IPs infected!!!

 ****** random_scan Scan worm propagation: Run3******
Time steps: 100 ---- IPs_infected: 7
Time steps: 200 ---- IPs_infected: 116
Time steps: 300 ---- IPs_infected: 706
Time steps: 400 ---- IPs_infected: 986
Time steps: 500 ---- IPs_infected: 998
Time steps: 565 ---- IPs_infected: 1000.
All IPs infected!!!
```

Figure 3: Output of random scanning method



```
su724972@net1547:~/HW4$ python3 local_preference_scan.py

 ****** local_preference Scan worm propagation: Run1******
Time steps: 100 ---- IPs_infected: 861
Time steps: 169 ---- IPs_infected: 1000.
All IPs infected!!!

 ****** local_preference Scan worm propagation: Run2******
Time steps: 100 ---- IPs_infected: 39
Time steps: 200 ---- IPs_infected: 853
Time steps: 267 ---- IPs_infected: 1000.
All IPs infected!!!

 ****** local_preference Scan worm propagation: Run3******
Time steps: 100 ---- IPs_infected: 488
Time steps: 183 ---- IPs_infected: 1000.
All IPs infected!!!
```

Figure 4: Output of local preference scanning method

5 Instruction to run the code

I have submitted file called "*WormPropagation.zip*" with this report. To run the code, follow the following instructions.

- Unzip 'WormPropagation.zip' and change directory to 'WormPropagation'.
  - $ unzip WormPropagation.zip
  - $ cd WormPropagation

- Install prerequisite libraries.
  - $ pip3 install numpy
  - $ pips install matplotlib
- Run the code
  - $ python3 random_scan.py
  - $ python3 local_ preference_scan.py