Programming Assignment 2

Middle East Technical University, Computer Engineering 04/12/2018

Overview

In this assignment, you are going to practice in DoS attacks. For grading, you are going to be assigned to demo-session-slots and you are going to make a demo about your work in the deadline date with your computers. For details, please look at the submission section and Piazza course page for the following announcements. For this homework, you are going to use mininet environment which is really useful tool not only for network enthusiasts but also security analysists. We strongly recommend you to learn it thoughtly; for more, you can visit the their official web page.

Prank

Here is the story. Assume that your friends are talking to each other and you just want to disturb them. Since they are not normal guys, they prefer telnet for communication. Since you are a bad guy in this story and take Ceng489 course, Introduction to Computer Security, you take a seat and start to think. Of course, the first thing that came to your mind is TCP Syn attack.(innocent guess here) You know that using TCP Syn attack you can fill the receiver's buffer and can cut the communication. To do that, you create fake and unused(preferred, why it is preferred can be googled) IPs as a source and pick one of your friends IP(the server one) as a destination.When you are done with writing your code, you will run your program and sit back and start to smile. For this assignment, you are going to use Mininet nodes for representing people in the story.To give a general idea about Mininet, the tool is going to be examined in the following sections.

Mininet in a nutshell

Mininet creates a realistic virtual network, running real kernel, switch and application code, on a single machine (VM, cloud or native), in seconds.Mininet is actively developed and supported, and is released under a permissive BSD Open Source license.

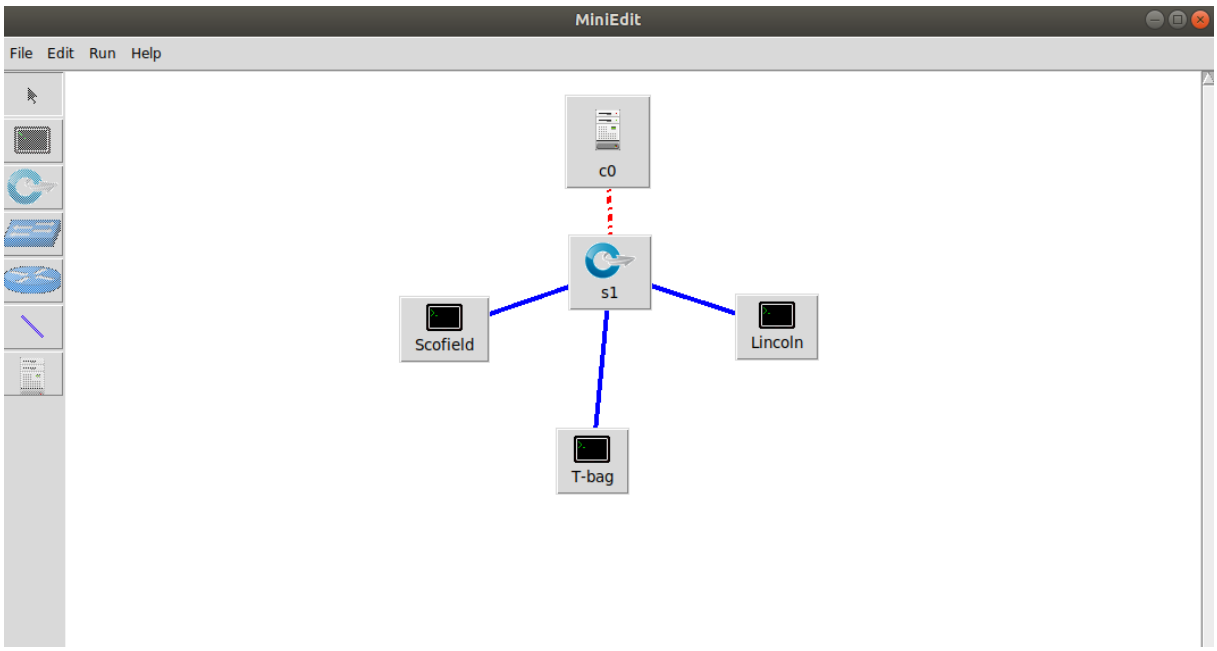

Figure 1: A demo for mininet environment.

You can follow the instructions from Mininet website to install the mininet.

Listing 1: Get Mininet command.

```
1 sudo apt-get install mininet
2 git clone git://github.com/mininet/mininet
3 cd mininet/examples
4 sudo ./miniedit.py
```

For cleaning the environment:(or another ways you find)

Listing 2: Clean the Mininet Environment command.

```
1 sudo apt-get install mininet
2 sudo mn -c
```

Demo Attack

When the server receives the initial SYN packet, it uses a special data structure called Transmission Control Block (TCB) to store the information about this connection. At this step, the connection is not fully established yet; it is called a half-open connection. Before the three-way handshake protocol is finished, the server stores all the half-open connections in a queue, and the queue does have a limited capacity. If attackers can fill up this queue quickly, there will be no space to store the TCB for any new half-open connection; basically, the server will not be

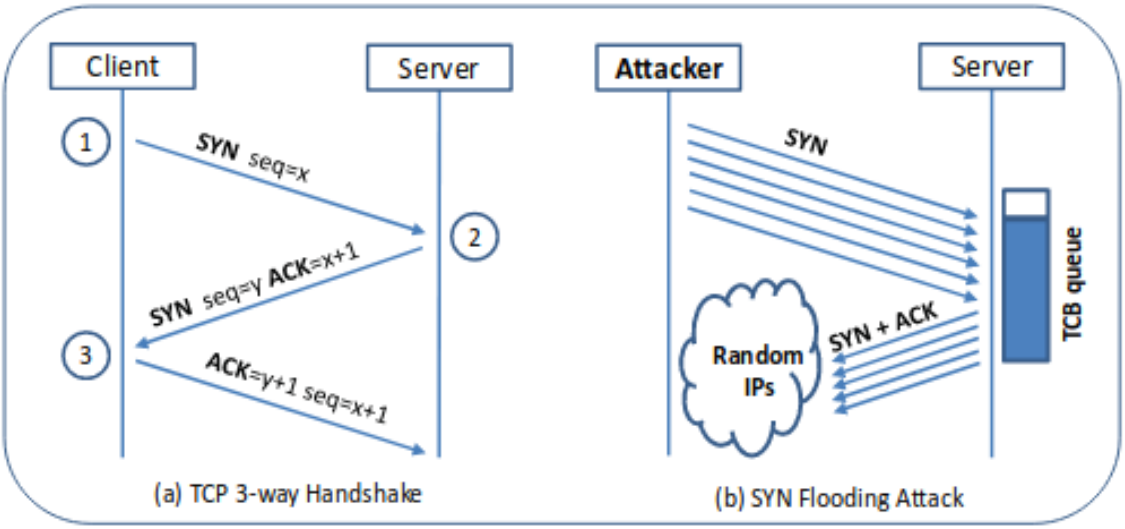

Figure 2: TCP Three Way Handshake and Syn Flooding

able to accept new SYN packets. To launch a SYN flooding attack, we need to send out a large number of SYN packets. Even though the server's CPU and bandwidth have not reached their capacity yet, nobody can connect to it any more.It is shown in Figure 2.

On server, we need to turn off a countermeasure called SYN cookies, which is enabled by default in Ubuntu. This countermeasure is effective against SYN flooding attacks. We can turn it off using the following command:

Listing 3: Turn off Syn Cookies command.

```
1 sudo sysctl -w net.ipv4.tcp_syncookies=0
```

The size of the queue has a system-wide setting. In Linux, we can check the system queue size setting using the following command:

Listing 4: Queue size command.

```
1 sysctl -q net.ipv4.tcp_max_syn_backlog
```

We can use command "netstat -na" to check the usage of the queue, i.e., the number of half-opened connection associated with a listening port. The state for such connections is SYN-RECV. If the 3-way handshake is finished, the state of the connections will be ESTABLISHED. While the attack is ongoing, run the "netstat -na" command on the victim machine, and observe the result with that before the attack.

In this section, attack is demonstrated by using Netwox tool.For more information about Net-

wox, you can visit their official website. The tool is called Synflood, which is Tool 76 in the Netwox tools.

For demonstration:

- Scofield -> client
- Lincoln -> server
- T-bag -> attacker

There are 3 nodes in the network as depicted in Figure 1. Since there are 3 different nodes in the environment, there are 3 different roles in the system. Node-Lincoln represents server, he waits escape plans from Node-Scofield so he listens incoming messages. In his terminal, it is basically run:

Listing 5: Lincoln's command.

```
1 nc -l 8080
2 netstat -lntu
```

- First command: just listens port 8080(nc represents netcat)
- Second command: gives the open ports in Linux.

Node-Scofied will send the secret message to Node-Lincoln in order to start the execution of escape plan.So he is the client in the story and the following command is run in his terminal:

Listing 6: Scofield's command.

```
1 telnet 10.0.0.2 8080
```

connects to Lincoln's machine by using Lincoln's IP and port.(you can learn Lincoln's IP by writing "ifconfig" in Lincoln's terminal.)

T-bag(we are in this story) will be the attacker and cut the communication between Scofield and Lincoln. There is a clever tool named Netwox. Its option is going to be used in our demo attack.Netwox has so many options. For TCP Syn Attack, Netwox 76 is going to be employed. In T-bag's terminal, if following command is run, the communication is broken due to the overloading of Lincoln's buffer:

Listing 7: T-bag's command.

```
1 sudo netwox 76 -i 10.0.0.2 -p 8080 -s raw
```

In our attack, we target Server's telnet server, which is listening to TCP port 8080; Server's IP address is 10.0.0.2. Therefore, our command is the following (this command needs to be executed using the root privilege; the choice of raw for the -s option means to spoof at the IP4/IP6 level, as opposed to the link level).

After this, when Scofield tries to open a new connection, the connection will not be established due to the capacity of TCB. To see the results, you can setup the environment and run the mentioned commands in your Mininet environment.

Your Task

Your task is going to be what is done in attacker's(T-bag's) terminal.Instead of using netwox 76, you are going to write your own code and run it in T-bag's terminal in order to cut the communication. When Scofield tries to open a new connection, the connection should not be established as a result of our purpose.

After Q-A Session

Question1: Should the port number be 8080?
Answer1: No, port can be any number.

Question2: Is the port number preset?
Answer2: Yes, it is preset.Client and Server set this number and somehow the attacker(T-bag node) also heard it, so all three know this number.

Question3: What can be seen after we try to make a new communication to server?
Answer3: Basically, server cannot accept any new connection. So try of connection can be resulted as: "Trying 10.0.0.2..." and some "no route to server error". You can also try to use command "netstat -tna" in the server node to see if the syn-recv packets come from attacker.

Submission and Regulations

- Due date: 16 December 2018, Sunday, 23:59.

- For programming languages, you are not forced to use any specific programming language. But we recommend you to use C/C++.
- Cheating: We have a zero tolerance policy for cheating. All work must be your own work and you must work alone.
- Newsgroup: Please follow Piazza for announcements and possible updates.