Mitigating a DoS Attack

Dr Rob Hegarty

Overview

In the previous lab session, you developed an understanding of how port scans and DoS attacks work, and carried out a port scan and DoS attack on a virtual webserver in your virtual network. The effects of a DoS scan should have been very obvious, with the webserver being unreachable by the host machine. In order to mitigate against a DoS attack you must first be able to determine its source before carrying out remedial action. In this lab session you will learn how to identify the source of a DoS attack and mitigate it.

When DDoS attacks are carried out, it is possible to filter traffic, but obviously the task is much larger, and often infeasible for a single human operative. In these circumstances an upstream filtering provider such as CloudFlare can carry out filtering of network traffic on your behalf before it reaches your network.

Learning Outcomes

- Distinguish between legitimate and malicious network traffic
- Identify malicious actors though log analysis
- Evaluate various mitigation strategies
- Employ appropriate techniques to mitigate the effects of a DoS attack

Analysing Network Connections

https://www.loggly.com/blog/how-to-detect-and-analyze-ddos-attacks-using-log-analysis/

Netstat is a powerful command line utility available on most operating systems. It displays information about network interfaces and TCP connections.

1. Start the Ubuntu VM, open the terminal, and access the man page for the Netstat command by typing the following command:
   a. `man netstat`
2. Skim read the documentation for netstat, and identify the flags needed to display all the interfaces using a numeric format.
3. Run the command you identified in the previous step followed by `| less` and view the output of the command, it should look similar to that shown below:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
udp        0      0 0.0.0.0:60241           0.0.0.0:*
udp        0      0 0.0.0.0:36746           0.0.0.0:*
udp        0      0 0.0.0.0:26590           0.0.0.0:*
udp        0      0 0.0.0.0:3065            0.0.0.0:*
udp        0      0 127.0.1.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:24631           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 127.0.0.1:35294         127.0.1.1:53            ESTABLISHED
udp        0      0 0.0.0.0:57960           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::37321                :::*
raw6       0      0 :::58                   :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     20534    @/tmp/.ICE-unix/1564
unix  2      [ ]         DGRAM                    18889    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     18890    /run/user/1000/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     10944    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     18921    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     19179    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     19183    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     10939    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     10943    /run/systemd/fsck.progress
```

The active Internet connections are important as they display the local and foreign address for each of the connections.

4. Access the webserver on the Ubuntu VM via the browser of your host machine, then reissue the command from step 3, notice how a connection from the host now shows, in the example below the last line shows the IP address of the host machine and connect being made to port 80 on the webserver:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 192.168.145.128:80      192.168.145.1:51254     FIN_WAIT2
```

5. Make a note of the IP addresses and port numbers used to connect the host machine to the webserver and explain their purpose, you will need to carry out online research in order to complete this task.

Detecting DoS Attacks

For this task you will need to refer to the notes you made when carrying out the DoS attack lab session.

Ensure both your Ubuntu and Kali VMs are configured to use **the Nat network you created in previous lab session.**

1. Recap on the nping command using either the man page or an online resource
2. Start the Kali VM and carry out TCP connect DoS attack by issuing the following command (substitute TARGET_IP_ADDRESS with the IP address of the webserver VM):
   a. `nping --tcp-connect -rate=9000 -c 900000 -q TARGET_IP_ADDRESS`

3. While DoS attack is running, rerun the netstat command on the Ubuntu/Webserver VM, the output should now look similar to that below:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 192.168.145.128:80      192.168.145.129:38447   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:32791   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:40347   ESTABLISHED
tcp6       1      0 192.168.145.128:80      192.168.145.129:41903   CLOSE_WAIT
tcp6       0      0 192.168.145.128:80      192.168.145.129:42531   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:46072   SYN_RECV
tcp6       0      0 192.168.145.128:80      192.168.145.129:37161   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:33462   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:41453   SYN_RECV
tcp6       0      0 192.168.145.128:80      192.168.145.129:38464   SYN_RECV
tcp6       0      0 192.168.145.128:80      192.168.145.129:44261   SYN_RECV
tcp6       0      0 192.168.145.128:80      192.168.145.129:43585   ESTABLISHED
tcp6       0      0 192.168.145.128:80      192.168.145.129:46762   ESTABLISHED
```

   Note the numerous connections from the Kali machine (check the IP address by running ifconfig on the Kali machine) The TCP-CONNECT attack is attempting to create many connections to the webserver and exhaust all the available resources, thus preventing legitimate users from connecting.

Mitigating a DoS Attack

Network firewalls get there name from the firewalls built into buildings to prevent the spread of fire. They can be either software or hardware, software firewalls are applications or part of the operating system used to restrict connections on a computer. Hardware firewalls are devices which connect to the network and filter all traffic to provide protection to the other devices connected to the network.

In the virtual network you have created we will be employing a software firewall using UFW. UFW is a very well established software firewall bundled with most Linux distributions.

1. Review the man page for UFW at the link below:
   a. https://help.ubuntu.com/community/UFW
2. Create a rule to drop traffic from the IP address associated with the Kali VM.
3. Ping the Ubuntu/Webserver VM from the Kali VM to confirm that the rule is working, you should not be able to ping the webserver.
4. Repeat the DoS Attack and observe the output of the netstat command, you should not see any connections from the Kali VM.
5. Research how to remove the UFW rule and ensure that the webserver is reachable from the Kali VM.

Extended Task

Research and implement an UFW rule to block traffic on a specific port number. Research and document a recent high-profile DoS attack include the follow;

- What was the cost?
- Who was responsible?
- How was it mitigated?
- How would your organisation cope with such an attack?