LAB EXERCISE

5

COMP3134

Introduction to Cyber Security

Week: 9

Objective(s):
Generate custom network activity and demonstrating various network attacking techniques

Learning Outcome(s):
Implement various tactics to attack a network or application
Critique and execute mitigation techniques

Table of Contents

Contents

Summary

Goal: Generate custom network activity and demonstrating various network attacking techniques

In Effort To: Implement various tactics to attack a network or application, as well as to critique and execute mitigation techniques

A. Clone GitHub Repo

Clone course GitHub repo to any location on your local machine
Navigate to the location above and create a folder named **wk9**
Use this local folder created above to create all the files necessary for this Lab Exercise

B. DoS Attack Overview

Definition
A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Techniques
Send requests to host at rate in which it cannot perform its normal functions

C. Connect to your Droplet Server

Using GitBash (on Windows) or the Terminal (on Mac), connect to your droplet server by executing the following command

```
ssh droplet_username@droplet_ip_address
```

When prompted, user your droplet password

Start listening to all incoming and outgoing traffic on your droplet. Write the output of to a file name **all_traffic_YYYYMMDD_HHMM** (instead of to standard output)

Write in a text file named **all_triffic.txt** the command needed to complete the above step.

D. DoS Attack Using Localhost Command Line

Connect to your Localhost Command Line

On a Windows machine, open the Command Prompt application
On a Mac machine, open the Terminal application

Ping

A ping is a signal sent to a host that requests a response. It serves two primary purposes: 1) to check if the host is available and 2) to measure how long the response takes.
A ping request can be performed using a ping command, which is a standard command in most command line interfaces.

Ping Manual

The manual for the ping command can be found here:
https://linux.die.net/man/8/ping

Using Ping Command

On your localhost machine, execute the following commands

- Send ping to your droplet server with packet size of 3200 bytes for 2 minutes
    - Take a screenshot of the Localhost command line/terminal application
    - Name the **screenshot ping_1.png**
    - View droplet server terminal application to verify packets are being delivered
        - Open a new droplet terminal window if needed
    - Take a screenshot of your droplet server terminal application to confirm the traffic
        - Name the screenshot **all_traffic_during_ping_1.png**

- Send ping to your droplet server with packet size of 65500 continuously until either
    - the command fails
    - 5 minutes have elapsed

  Take a screenshot of the Localhost command line/terminal application AND the system clock right after initializing the command
  Name the screenshot **ping_2_start.png**

  View droplet server terminal application to verify packets are being delivered.
  You may have to run or re-run a command
  Take a screenshot of your droplet server terminal application
  Name the screenshot **all_traffic_during_ping_2.png**

  Take a screenshot of the Localhost command line/terminal application AND the system clock after either the command failed of the time has elapsed
  Name the screenshot **ping_2_end.png**

If necessary, restart the apache server on your droplet

E. DoS Attack Using Packet Sender

Open the Packet Sender application
Navigate to the url below and generate a string of 30,000 characters:
https://www.random.org/strings/

Using the Intense Traffic Generator tool, continuous send this string of data to your droplet server with a delay between 3/4 and 3/2 of a second. Do this for a minimum run time of 5 minutes.

Take a screenshot of the Packet Sender application after 5 minutes have elapsed
Name the screenshot **intense_traffic.png**

View droplet server terminal application to verify packets are being delivered.
You may have to run or re-run a command
Take a screenshot of your droplet server terminal application
Name the screenshot **all_traffic_during_ping_3.png**

F. Commit and Upload Changes to GitHub repo

Commit the changes to your repo by:

1. Opening a GitBash window and ensure that it is connected to your local machine
2. Navigate to local repository directory location
3. Add all the files completed in this Lab Exercise
4. Commit the changes
5. Push the changes to your GitHub course repo

Please refer to the instructions in the last section of Lab Exercise 1