Denial of Service (DoS) Student Workout Instructions

Introduction

Welcome to your team's *Denial of Service* workout where you will learn about the loss of availability effects of a denial of service attack. A Denial of Service (DoS) attack occurs when an adversary prevents access to a system, device, or network resource, and this often occurs through a flood of network traffic directed at a target computer. That network traffic can be thousands of data packets per second directed at a network service. It can cause a delay in response to the user or prevent them from accessing the service altogether. In this workout, you will conduct a DoS attack on a webserver and witness its effect on CPU usage.

> ⚠ WARNING: The tools used in this workout should only be used for learning purposes in this controlled environment. Using these tools on other computers outside of the Cyber Gym is considered a cyber attack and may result in criminal penalties.

Your Mission

There are two phases to your mission. The first phase can be completed by consistently maintaining a CPU usage of over 40% for the target server. The next following these instructions. The next phase requires some additional configuration and requires consistently maintaining a CPU usage of over 70% for the target server.

- A terminal should be up when you initially login. Type in ssh cybergym@10.1.1.33. Accept the ssh key warning and then type in the password ‘Let’s workout!' (no quotes)
- Type in the following command to output CPU usage every second for a 1000 seconds and view the current CPU usage: `sar -u 1 10000`
- Open a new tab in the terminal by clicking File New Tab. In the new tab, change your directory to LOIC/: `cd LOIC`
- Run the following shell script by typing in

```
./loic-net4.5.sh run
```

- In the Low Orbital Ion Cannon Tool, target the webserver at the IP address 10.1.1.33 by typing it in the *Select Your Target IP* field. Then click *Lock On.*
- In the attack options, change the Method drop-down from TCP to HTTP and hit the ready button (i.e. IMMA CHARGIN MAH LAZER) to begin the flood of HTTP packets to the webserver.
- Go back to the previous terminal and observe the change in CPU usage. Keep the attack running for at least 3 to 5 minutes. An assessment script will set your workout to complete when you have finished the attack.
- Now, stop the attack, and observe the CPU usage goes back to normal.

If you have completed the assessment, try protecting the server from this attack. Stop the output running from `sar` by pressing Ctrl-c while in the terminal window where the CPU percentage is displaying. Then, type the command:

```
sudo ufw deny html from 10.1.1.9
```

- Re-run the CPU usage command listed from before to see the CPU usage again.
- Re-activate the Low Orbital Ion Cannon without changing any of the settings from before.
- Observe the Low Orbital Ion Cannon’s feedback regarding failed packets.
- Observe the CPU usage on the webserver terminal.