CSEC 1310: DDOS Attacks Lab

V2.0

William Cox
Rebecca Passmore
March 2024

Cybersecurity
UA LITTLE ROCK | Department of Computer Science

Contents

Introduction

Welcome to your team's workout where you will learn about the Denial of Service 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 web server 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.

Objectives

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.

Phase 1: Conducting a DoS Attack

1. On the CyberArena, click the `Connect` to connect to the Attacker host.
2. Once connected, open a terminal by clicking the icon at the bottom of the screen.
3. SSH into the target server. Accept the ssh key warning and then type in the password `Let's workout!` (no quotes)

   ```
   ssh cybergym@10.1.1.33
   ```

4. Once connected to the target server, 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
   ```

5. On the Attacker host's Desktop, click the `LOIC` icon to open the Low Orbit Ion Cannon.

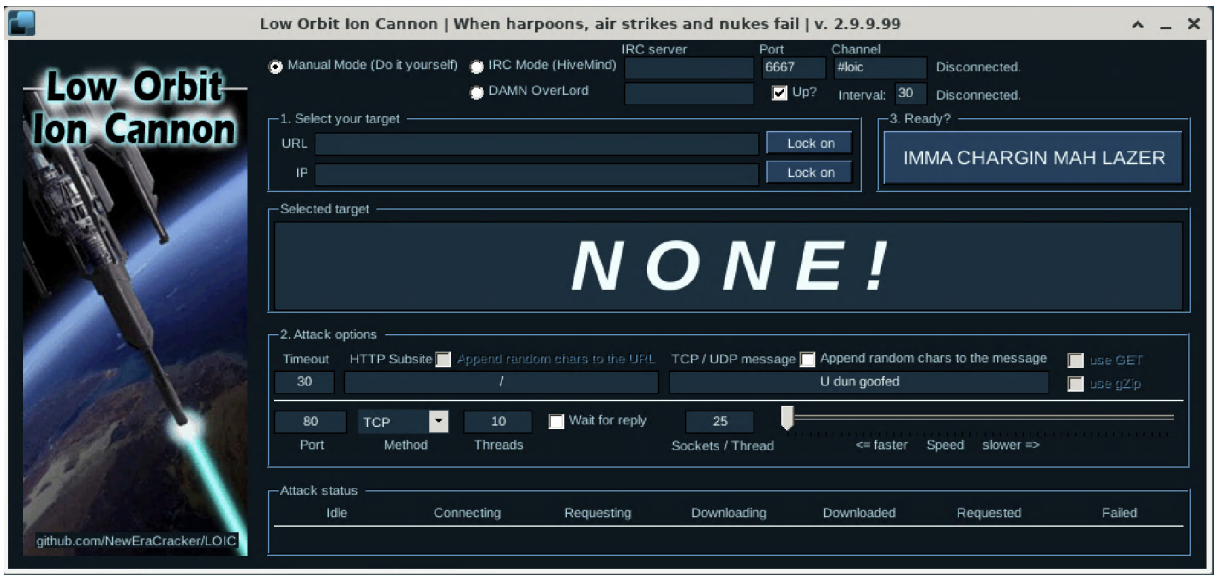

Figure 1: Image of Low Orbit Ion Cannon Application

6. In the `Select Your Target` Section, type in the IP address of the target server: `10.1.1.33`. Click the `Lock On` Button.

Figure 2: Image of Section 1: Select Your Target

7. in section 2, 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 web server.

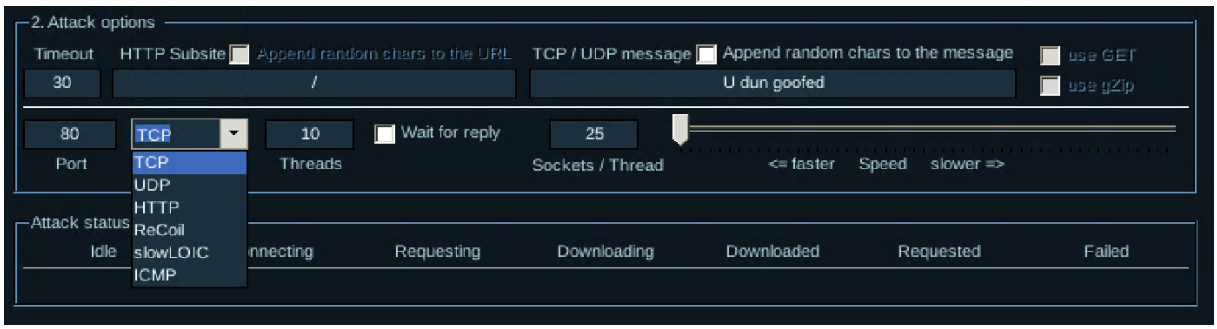

Figure 3: Image of Section 2: Attack options

8. Go back to the terminal and observe the change in CPU usage. Keep the attack running for at least 3 to 5 minutes.

Phase 2: Protecting the Server

If you have completed the assessment, try protecting the server from this attack. Using the built in Firewall, you will be able to block the IP address of the attacker.

Note: If you have competed Phase 1 and stopped your workout. You can skip step 1.

1. Go back to the Terminal window where the CPU usage is displaying. Stop the output running from `sar` by pressing `Ctrl-c`.
2. On the web server terminal, type the command: `sudo ufw enable`
3. To add a Firewall rule to block incoming HTTP from 10.1.1.9, type the command: `sudo ufw deny from 10.1.1.9 to any port 80`
4. Rerun the CPU usage command listed from before to see the CPU usage again. `sar -u 1 10000`
5. On the Attacker host, start the Low Orbit Ion Cannon again and observe the CPU usage on the web server terminal.

Lab Assessment

Below are the questions you will need to answer in your lab assessment. You will need to submit your answers to your your professor/instructor. Write a short essay (minimum 350 words) for each question. Your essay should be well-structured, grammatically sound, and demonstrate critical thinking. You should also provide a clear argument supported by evidence and examples. Review the rubric for each question to understand the criteria for evaluation.x

Rubric for Question 1 - LOIC as a DDOS Tool and its Ethical Implications

Criteria	Excellent (21-25)	Good (16-20)	Satisfactory (11-15)	Needs Improvement (0-10)
LOIC Mechanics	Detailed and accurate understanding of LOIC.	Clear understanding with minor gaps.	Basic understanding with significant gaps	Limited or incorrect understanding.
Ethical/Legal Analysis	In-depth analysis of ethical/legal aspects.	Adequate analysis with some depth.	Basic and superficial analysis.	Minimal or no analysis.
Critical Thinking	Well-structured, insightful argument.	Clear argument with some depth.	Basic argument, lacks depth.	Poorly structured or no argument.
Writing & Organization	Clear, well-organized, grammatically sound.	Mostly clear and well-organized.	Some disorganization and errors.	Poorly organized, hard to understand.

Question 1 - Understanding the Mechanics and Ethical Implications of LOIC as a DDOS Tool
Discuss in detail how the Low Orbit Ion Cannon (LOIC) functions as a tool for Distributed Denial of Service (DDoS) attacks.

1. Your answer should explore the technical mechanisms through which LOIC enables users to overwhelm target systems with traffic.
2. Additionally, critically evaluate the ethical and legal implications of using LOIC in various contexts, including cyber activism and cyber warfare.
3. Reflect on the potential consequences for both attackers and victims, and provide a reasoned argument about the ethical considerations of using such tools in the digital age.

Rubric for Question 2 - Essay on Defending Against LOIC-Based DDoS Attacks

Criteria	Excellent (21-25)	Good (16-20)	Satisfactory (11-15)	Needs Improvement (0-10)
Defense Strategies	Comprehensive understanding of strategies.	Clear understanding with minor gaps.	Basic understanding with major gaps.	Limited or incorrect understanding.
Strategy Effectiveness	In-depth evaluation of effectiveness.	Adequate evaluation with some insight.	Basic evaluation, lacks depth.	Minimal or no evaluation.
Broader Security Implications	Thorough understanding of broader implications	Adequate understanding, some connection.	Basic and superficial understanding.	Fails to connect to broader implications.
Writing & Organization	Clear, well-organized, grammatically sound.	Mostly clear and well-organized.	Some disorganization and errors.	Poorly organized, hard to understand.

Question 2 - Strategies for Defending Against LOIC-Based DDoS Attacks Examine the challenges and methodologies in defending against DDoS attacks, specifically those executed using tools like the Low Orbit Ion Cannon (LOIC).

1. Your Answer should provide an in-depth analysis of the various defense strategies and technologies that can be employed to mitigate the effects of such attacks.
2. Discuss the roles of network architecture, firewall configurations, traffic filtering, and response planning in defending against DDoS attacks.
3. Evaluate the effectiveness of these strategies and consider any potential drawbacks or limitations they may present.
4. Additionally, explore the broader implications of DDoS attacks on internet security and the measures that organizations and individuals can take to enhance their resilience against such threats.