# lab no. 5

# Analysis of DOS ATTACK Techniques

## Lab Purpose

A DoS (Denial of Service) attack is a type of cyber attack in which a malicious actor aims to render a service unavailable to its intended users. These attacks can be performed on every layer of a communication system and most of them are very easy to execute. DoS attacks typically exploit security vulnerabilities present in network protocols or software design.

This lab is designed for students to experience some common DoS attack techniques. After completing this lab, students will hopefully gain knowledge and skill about this type of attack.

## Lab Environment

* Operating System: Ubuntu
* Tools: Docker, Wireshark, Python, hping3, Saddam, iftop and top

## Lab Preparation Tasks

* Review lectures and documents on DoS attack
* Read the lab handout
* Be familiar with aforementioned tools:
  + hping3: <https://techradix.in/hping-3-tutorials/>
  + Saddam: <https://github.com/S4kur4/Saddam-new>
  + top: <https://www.howtogeek.com/668986/how-to-use-the-linux-top-command-and-understand-its-output/>
  + iftop: <https://linoxide.com/monitoring-2/iftop-network-traffic/>

## Lab Instructions

In this lab, each student is provided with a virtual machine (VM) running Ubuntu 20.04 on VirtualBox virtualization software. This VM acts as the host for Docker containers. Attack scenarios are carried out on the virtualized network using Docker,

## Lab content

### Attack scenario 1 (3 points)

Network diagram:

A computer and monitor with a blue background

Description automatically generated with medium confidence

* **Step 1:** [Victim] Open Terminalwindow no.1 and execute the command below. Wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
  + **Command: sudo top**
* **Step 2:** [Victim] Open Terminalwindow no.2 and execute the command below. Capture the screen and put it in the report.
  + **Command: sudo iftop -i Name\_of\_victim\_interface**
* **Step 3:** [Victim] Launch Wiresharkand capture packets on relevant network interface
* **Step 4:** [Attack] Open Terminalwindow and execute the command below to attack victim’s device.
  + **Command: sudo hping3 --icmp Victim\_IP -d 65000 –-flood --rand-source**
* **Step 5:** [User] Open Terminalwindow and try to communicate with the victim’s device using the Telnet service. The response time may be longer than usual.
  + **Command: telnet Victim\_IP**
* **Step 6:** [Victim] Open Terminalwindow in step 1 (**top** command) and wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
* **Step 7:** [Attack] Stop **hping3** tool.
* **Step 8:** [Victim] Open Terminal window in step 2 (**iftop** command) and stop executing **iftop.** Capture the screen and put it in the report.
* **Step 9:** [Victim] Stop capturing packets in Wireshark and analyze network traffic.

|  |
| --- |
| **Question 1.**   * Analyze result from executing **top** and indicate the victim CPU and RAM usage before and during the attack. * Analyze result from executing **iftop** and indicate the traffic the victim received before and during the attack. * Analyze network traffic in Wireshark and identify the attack technique used against the victim. What is the result of this attack on the victim’s device? |

### Attack scenario 2 (3 points)

Network diagram:

A computer and monitor with a blue background

Description automatically generated with medium confidence

* **Step 1:** [Victim] Open Terminalwindow no.1 and execute the command below. Wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
  + **Command: sudo top**
* **Step 2:** [Victim] Open Terminalwindow no.2 and execute the command below. Capture the screen and put it in the report.
  + **Command: sudo iftop -i Name\_of\_victim\_interface**
* **Step 3:** [Victim] Launch Wiresharkand capture packets on relevant network interface
* **Step 4:** [Attack] Open Terminalwindow and execute the command below to attack victim’s device.
  + Command: **sudo hping3 -S -p 23 Victim\_IP –-flood --rand-source**
* **Step 5:** [User] Open Terminalwindow and try to communicate with the victim’s device using the Telnet service. The response time may be longer than usual.
  + Command: **telnet Victim\_IP**
* **Step 6:** [Victim] Open Terminalwindow in step 1 (**top** command) and wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
* **Step 7:** [Attack] Stop **hping3** tool.
* **Step 8:** [Victim] Open Terminal window in step 2 (**iftop** command) and stop executing **iftop.** Capture the screen and put it in the report.
* **Step 9:** [Victim] Stop capturing packets in Wireshark and analyze network traffic.

|  |
| --- |
| **Question 2.**   * Analyze result from executing **top** and indicate the victim CPU and RAM usage before and during the attack. * Analyze result from executing **iftop** and indicate the traffic the victim received before and during the attack. * Analyze network traffic in Wireshark and identify the attack technique used against the victim. What is the result of this attack on the victim’s device? * Describe briefly how to defense against this attack technique |

### Attack scenario 3 (4 points)

Network diagram:

A computer and a computer monitor

Description automatically generated with medium confidence

* **Step 1:** [Victim] Open Terminalwindow no.1 and execute the command below. Wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
  + **Command: sudo top**
* **Step 2:** [Victim] Open Terminalwindow no.2 and execute the command below. Capture the screen and put it in the report.
  + **Command: sudo iftop -i Name\_of\_victim\_interface**
* **Step 3:** [Victim] Launch Wiresharkand capture packets on relevant network interface
* **Step 4:** [Attack] Open Terminalwindow. Open *dns.txt* file and write IP address of DNS Server
  + **Command: cd ~**
  + **Command: sudo gedit dns.txt**

Save the content of *dns.txt* file.

* **Step 5:** [Attack] Open Terminalwindow and execute the command below to attack victim’s device.
  + **Command: sudo python saddam.py Victim\_IP -d dns.txt:www.test.com**
* **Step 6:** [User] Open Terminalwindow and try to communicate with the victim’s device using the Telnet service. The response time may be longer than usual.
  + **Command: telnet Victim\_IP**
* **Step 7:** [Victim] Open Terminalwindow in step 1 (**top** command) and wait about 30 seconds for the figures to stabilize. Capture the screen and put it in the report.
* **Step 7:** [Attack] Stop **Saddam.py** tool.
* **Step 8:** [Victim] Open Terminal window in step 2 (**iftop** command) and stop executing **iftop.** Capture the screen and put it in the report.
* **Step 9:** [Victim] Stop capturing packets in Wireshark and analyze network traffic.

|  |
| --- |
| **Question 3.**   * Analyze result from executing **top** and indicate the victim CPU and RAM usage before and during the attack. * Analyze result from executing **iftop** and indicate the traffic the victim received before and during the attack. * Analyze network traffic in Wireshark and identify the attack technique used against the victim. What is the result of this attack on the victim’s device? * Describe briefly how to defense against this attack technique |