UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Engineering, Built Environment and Information Technology

School of Information Technology
Department of Computer Science

COS330 Computer Security and Ethics:
Practical 6 2024

Release Date: 20 September 2024

Submission Date: 10 October 2024 @ 23:59

Lecturers: Prof H.S Venter & Mr S.M Makura

Total: 50 Marks

Objectives

1. To understand the concept of Denial of Service (DoS) attacks.
2. To simulate a simple DoS attack in a controlled environment.
3. To analyse the impact of the attack and discuss mitigation strategies.
4. To effectively demonstrate and present practical setup and execution in a video format.

Instructions:

You will work in a controlled environment (e.g., VirtualBox or VMWare). The goal is to simulate a basic DoS attack, understand its impact on the target system, and propose mitigation strategies. You must record a 5-minute video demonstrating the setup, execution, and results of your practical.

Ensure you follow ethical guidelines and only use provided tools and networks.

Software Requirements

1. **Virtual Machines (VMs):** One as the attacker (Kali Linux) and another as the victim (Ubuntu with an Apache web server running). You can download Kali Linux from here: https://www.kali.org/get-kali/#kali-platforms . Then you can download Ubuntu 24.04 LTS from here: https://ubuntu.com/download/desktop
2. **Wireshark** for traffic analysis. Can be downloaded from here: https://www.wireshark.org/download.html
3. **LOIC (Low Orbit Ion Cannon)** or **hping3** (available in Kali Linux) for DoS simulation. You can download LOIC from here: https://sourceforge.net/projects/loic/

Submission Procedure:

When you are done:

1. You must submit a 5-minute video demonstrating the setup, execution, and results of your practical. The video file must be named **uXXXXXXXX-Initials and Surname.mp4**
   Where **XXXXXXXX** is your student number.

NO LATE submissions will be accepted after the submission date and time has lapsed. Do not wait till the last minute to submit and start giving excuses that you faced technical challenges when you tried to submit.

Task 1: Setting Up the Environment (10 Marks):

- Install Kali Linux (attacker) and Ubuntu (victim) using a virtualization software like VirtualBox or VMware.
- Ensure both VMs are connected to the same virtual network for communication (important).
- Install and configure Apache on the victim VM to serve a simple webpage.

Marking Criteria:

- *Successful setup of both VMs.*
- *Apache server is running on the victim machine.*
- ***Video Recording Requirement:*** *In your video, demonstrate how you set up the attacker and victim VMs, and how you configured the Apache web server.*

Task 2: Simulating a DoS Attack (25 marks)

- Use LOIC from the attacker VM to simulate a DoS attack on the Apache server.
- Monitor the victim server and record its response (e.g., server slowdown or crash).
- Use Wireshark to capture network traffic during the attack.

Marking Criteria:

- *Correct usage of LOIC to generate a flood attack.*
- *Wireshark capture includes attack traffic (e.g., TCP or HTTP flood).*
- *Explanation of the impact of the attack on the victim server.*
- *Video Recording Requirement: Demonstrate the attack using LOIC and the results observed on the victim server in your video. Show the Wireshark traffic capture as well. You do not need to show the entire attack & packet capturing (as this will make the video lengthy), but snippets of the progression.*

Task 3: Mitigation Strategies (15 marks)

- Research and suggest three mitigation strategies to defend against DoS attacks.
- Implement basic rate limiting or firewall rules on the victim machine to mitigate the attack.

Marking Criteria:

- *Clear explanation of at least three DoS mitigation strategies.*
- *Correct implementation of one basic mitigation technique (e.g., rate limiting using iptables).*
- ***Video Recording Requirement:*** *If possible, demonstrate the implementation of at least one mitigation strategy in your video, such as configuring firewall rules or rate limiting on the victim server.*

[**Total Marks: 50**]