Picus Cyber Talent Academy- Second Week Assignment

Question 1

Denial of Service (DoS attack) is a cyber attack that aims to temporarily or indefinitely disrupt the services of an internet-connected host, making a machine or network resources inaccessible to actual users. It is usually performed in the form of making the target system unable to respond to incoming requests due to overload due to overloading the target machine or resource with unnecessary requests.

The attackers can use amplification techniques for attacks with higher bandwidth than they have and the DNS Protocol statistically has been used/exploited much more than the other protocols.

a. Why is this type of attack preferred, especially in the DNS protocol? Please explain briefly.

b. In DNS Amplification Attacks, are there any technical limitations or disadvantages for the attacker?

c. Please find a suitable IP address for amplification attacks in DNS protocol and explain step by step how to find such servers easily.

Question 2

The source files of a sample application are attached as a .zip file. Please unzip the zip file in a directory.

The code in the app.py file in the unzipped directory contains several OWASP Top 10:2021 vulnerabilities. Please review the code, identify contained vulnerabilities, and suggest possible mitigations to resolve the identified vulnerabilities. Each area has to include:

- What is the vulnerability?
- Why does the vulnerability arise (what is the reason for the vulnerability)?
- What is your mitigation suggestion to close the vulnerability?

Note 1: 10 areas are given below to write your answers. However, the application may or may not include 10 vulnerabilities.

Note 2: Applicants can run the sample application using docker with the “docker-compose up” command if necessary.

Vulnerability 1 & Mitigation:

Vulnerability 2 & Mitigation:

Vulnerability 3 & Mitigation:

Vulnerability 4 & Mitigation:

Vulnerability 5 & Mitigation:

Vulnerability 6 & Mitigation:

Vulnerability 7 & Mitigation:

Vulnerability 8 & Mitigation:

Vulnerability 9 & Mitigation:

Vulnerability 10 & Mitigation: