DDOS ATTACKS

COMPUTER NETWORKING

Time: 60 mins

Introduction

In this class, the student/s will learn how DOS and DDOS attacks are made and perform it.

New Commands Introduced

● socket.gethostbyname(host)	Returns the IP address of a given host name
● socket.AF_INET	Specifies the internet address family for IPv4
● socket.SOCK_STREAM	Specifies protocol that will be used to transport messages in the network
● ddos.connect()	Establishes a connection between host and a port
● get_random_url()	Gets a random URL
● json.dumps(random_url).encode()	Encodes the URL and stores it on JSON format
● .ddos.send(message.encode())	Encodes the message
● ddos.sendto(message.encode(), (ip, port))	Encodes the message using IP and port addresses

Vocabulary

- **Virtual Machine (VM)** is a compute resource that uses software instead of a physical computer to run programs and deploy apps.
- **Kali Linux** is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.
- When multiple malicious systems send multiple requests to the server affecting the server resources like CPU and storage, and network bandwidth, it in turn slows down the server, leading to denial of service to the users. This kind of attack is known as **DDOS(Distributed Denial of Service) attack**.

- **DOS** stands for Denial of Service where a server is unable to give services to the request.

Learning Objectives

Student/s should be able to:

- ***Recall*** the use of socket programming to make multiple connections to the server.
- ***Demonstrate*** the installation and setup of Kali Linux and the VMware software.
- ***Explain*** how to perform the DOS and DDoS attacks.

Activities

Class Narrative: *(3 mins)*

- Brief the student/s that the webpage isn't loading and the reason may be a cyber attack.

Concept Introduction Activity: *(4 mins)*

- Let the student/s observe that the high number of connection requests cause the website to load slowly.
- Explain that flooding the target network's infrastructure with a large volume of requests saturates the available bandwidth, causing the targeted network to become slow or unresponsive.
- Explain the DOS and DDoS attack.
- Using the slides, explain that the student/s will learn:
    - to download, install and setup the virtual machine
    - to perform the DOS attack
    - to perform the DDOS attack

Activity 1: Download, Install and Setup the Virtual Machine *(16 mins)*

Teacher Activity: *(8 mins)*

- Explain about the virtual machine.
- Demonstrate how to download, install, and set up the Kali Linux and VMware machine.

Student Activity: *(8 mins)*

- Guide the student/s to download, install, and set up the Kali Linux and VMware machine.

Activity 2: Perform the DOS Attack *(10 mins)*

- Explain how we will connect to the host server using TCP protocol in socket programming.
- Explain how we will perform the denial of service attack on a website server by connecting the host to the port and sending the messages.

  Student Activity: *(10 mins)*

- Guide the student/s to perform a DOS attack.

Activity 3: Perform the DDOS Attack *(12 mins)*

- Introduce how the DOS attack can be easily prevented and hence a DDoS attack needs to be performed where multiple systems attack simultaneously.
- Explain how multiprocessing can be used to attack from multiple connections using socket programming and perform DDOS attacks.

  Student Activity: *(6 mins)*

- Guide the students to perform a DDoS attack.

Introduce the Post class project: *(2 min)*

- Install Ubuntu on the VMware with similar setup and test if the DDoS attacks can be performed.

Test and Summarize the class learnings: *(5 mins)*

- Check for understanding through quizzes and summarize learning after respective activities.
- Summarize the overall class learning towards the end of the class.

Additional activities:

- Encourage the student/s to create a clone of your virtual Machine and perform DDoS.
- Encourage the student/s to debug the code to perform the DDoS attack.

State the Next Class Objective: *(1 min)*

- In the next class, student/s will learn how phishing attacks are performed.

U.S. Standards:

CSTA: 2-AP-11, 2-AP-12, 2-AP-13, 2-AP-14, 2-AP-19

Links Table

Activity	Activity Name	Link
Class Presentation	DDOS ATTACKS	https://s3-whjr-curriculum-uploads.whjr.online/81a3a727-f29c-4dbb-85f7-b52ff99a2650.html
Explore Activity	DDOS ATTACKS	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP
Student Activity 1	Download, Install and Setup the Virtual Machine	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP
Teacher Reference: Student Activity 1 Solution	Download, Install and Setup the Virtual Machine	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS
Teacher Activity 2	Perform the DOS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-TAS-BP
Teacher Reference: Teacher Activity 2 Solution	Perform the DOS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-TAS
Student Activity 2	Perform the DOS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP
Teacher Reference: Student Activity 2 Solution	Perform the DOS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS
Teacher Activity 3	Perform the DDoS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-TAS-BP
Teacher Reference: Teacher Activity 3 Solution	Perform the DDoS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-TAS
Student Activity 3	Perform the DDoS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP
Teacher Reference: Student Activity 3 Solution	Perform the DDoS Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS
Student's Additional Activity 1	Perform DDOS on a Clone	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP
Teacher Reference: Student's Additional Activity 1 Solution	Perform DDOS on a Clone	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS
Student's Additional Activity 2	Debug the Code	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS-BP

Teacher Reference: Student's Additional Activity 2 Solution	Debug the Code	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-SAS
Post Class Project	Install Ubuntu on Virtual Machine	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-PCP-BP
Teacher Reference: Post Class Project Solution	Install Ubuntu on Virtual Machine	https://github.com/Tynker-Computer-Networks/TNK-M16-C122-PCP