NETWORKING & DATA SECURITY- (COMP8677)

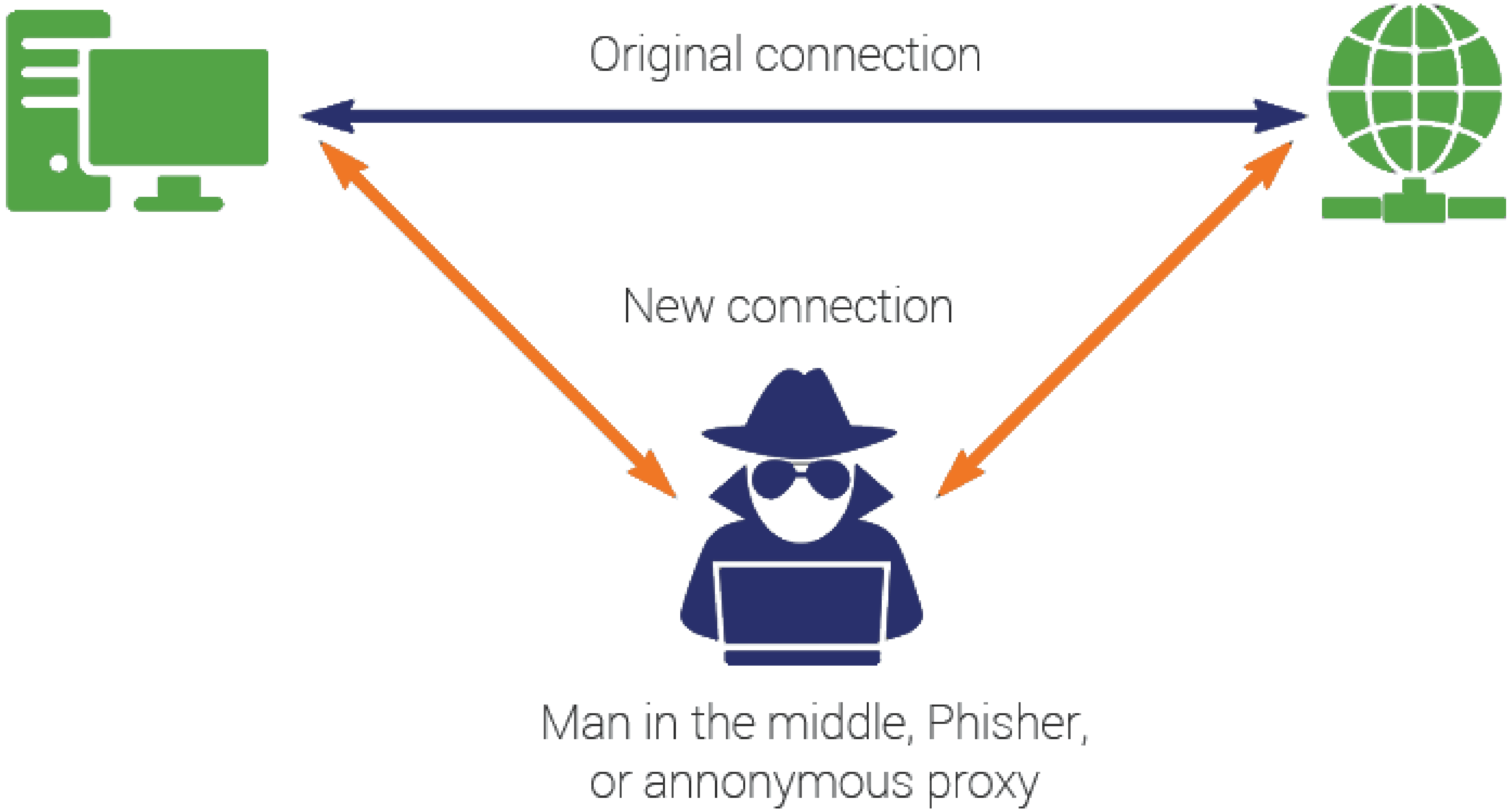
FINAL PROJECT PRESENTATION

Modified Mitnick Attack with CAM Overflow

- Rahul Banerjee
- Tanya Agarwal
- Avinash Gupta

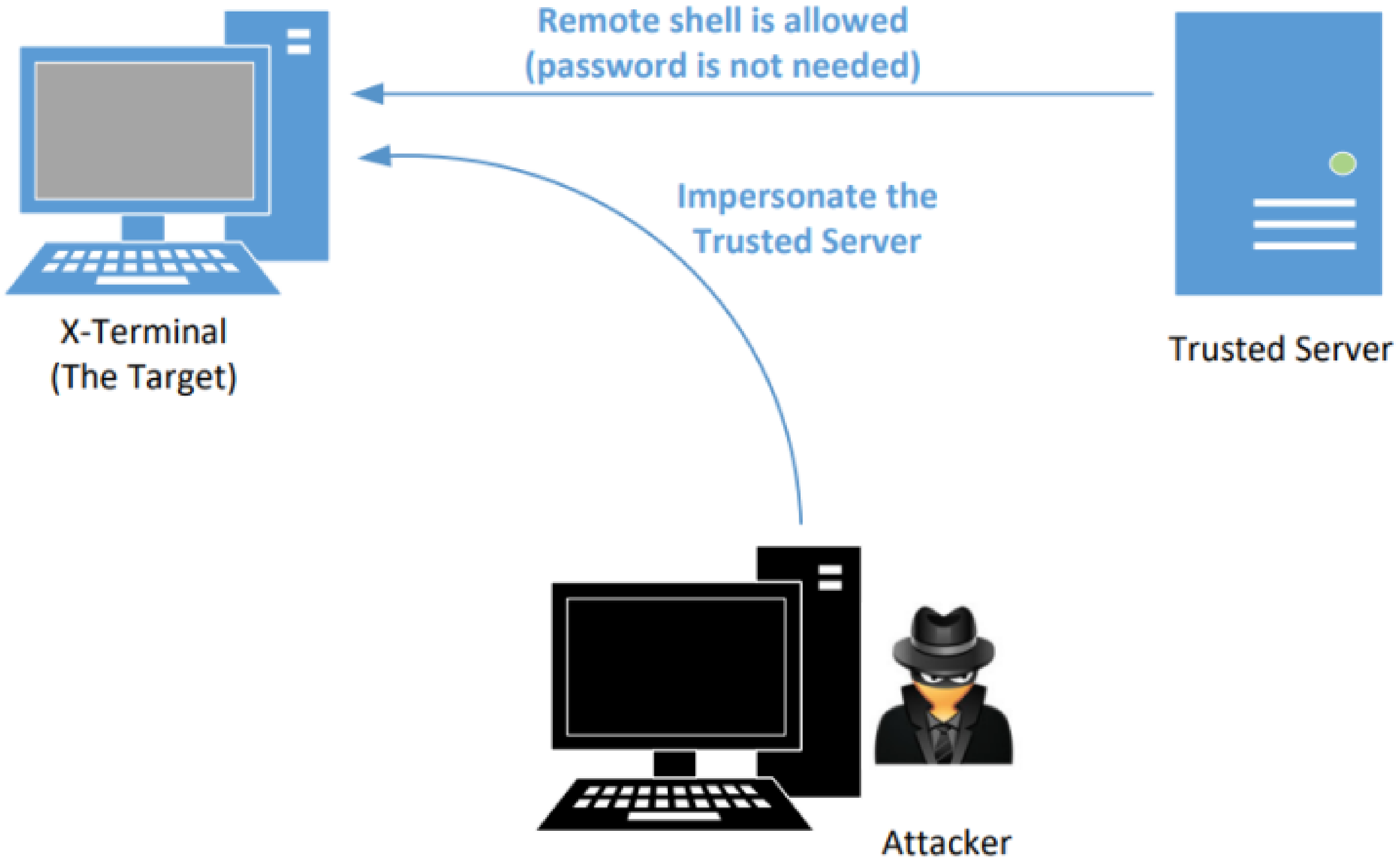
Man in The Middle Attack

A man-in-the-middle (MitM) attack is a type of cyberattack in which communications between two parties is intercepted, often to steal login credentials or personal information, spy on victims, sabotage communications, or corrupt data.



What is Mitnick Attack?

The Mitnick attack is a special case of TCP session hijacking attacks, where Instead of hijacking an existing TCP connection between victims A and B, the Mitnick attack creates a TCP connection between A and B first on their behalf, and then naturally hijacks the connection.



Features Implemented

Overview:

CAM Overflow Attack

- Rahul Banerjee

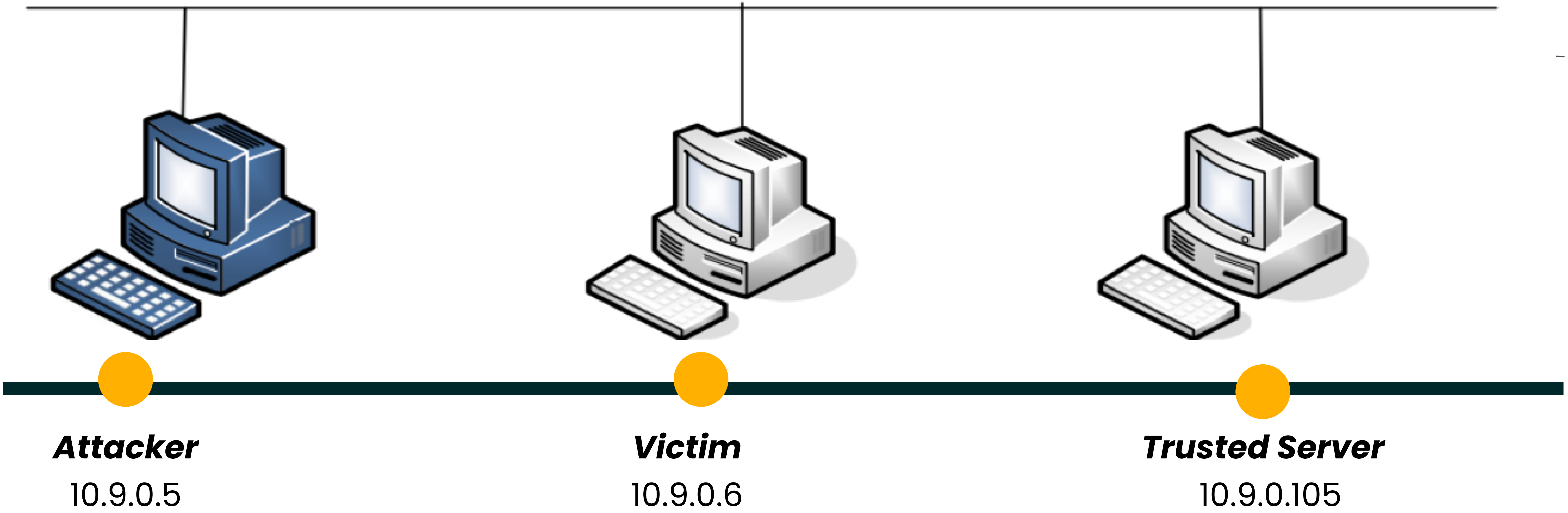
Syn Flooding

- Tanya Agarwal

Three way handshake

- Avinash Gupta

Network Setup



CAM Attack

01

The switch knows which port to forward the frames to based on the destination MAC address. This table is called the context-addressable memory (CAM) table.

02

The switch can hold only a specific number of MAC addresses in this table.

03

A CAM overflow attack occurs when an attacker connects to a single or multiple switch ports and then runs a tool that mimics the existence of thousands of random MAC addresses on those switch ports.

04

The switch enters these into the CAM table, and eventually the CAM table fills to capacity. A CAM overflow attack turns a switch into a hub, which enables the attacker to eavesdrop on a conversation

Syn Flooding

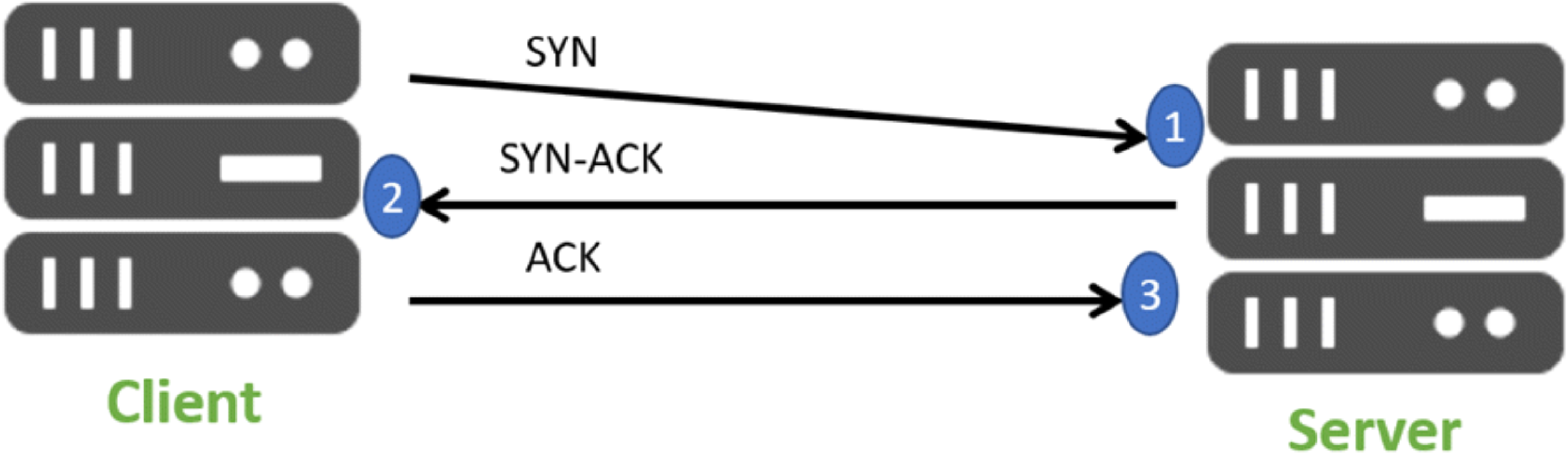
TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

Three Way handshake

TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps—SYN, SYN-ACK, and ACK

- **Step 1:** In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.
- **Step 2:** In this step **s**erver responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
- **Step 3:** In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.



The Team

Rahul Banerjee

110035198

Tanya Agarwal

110060426

Avinash Gupta

110060197

Thank you!