STUDENT NAME : KACHALA SHIVA RAMA KRISHNA

MAIL ID : kachalashivaram016@gmail.com

COLLEGE NAME : VISAKHA INSTITUTE OF ENGINEERING AND TECHNOLOGY

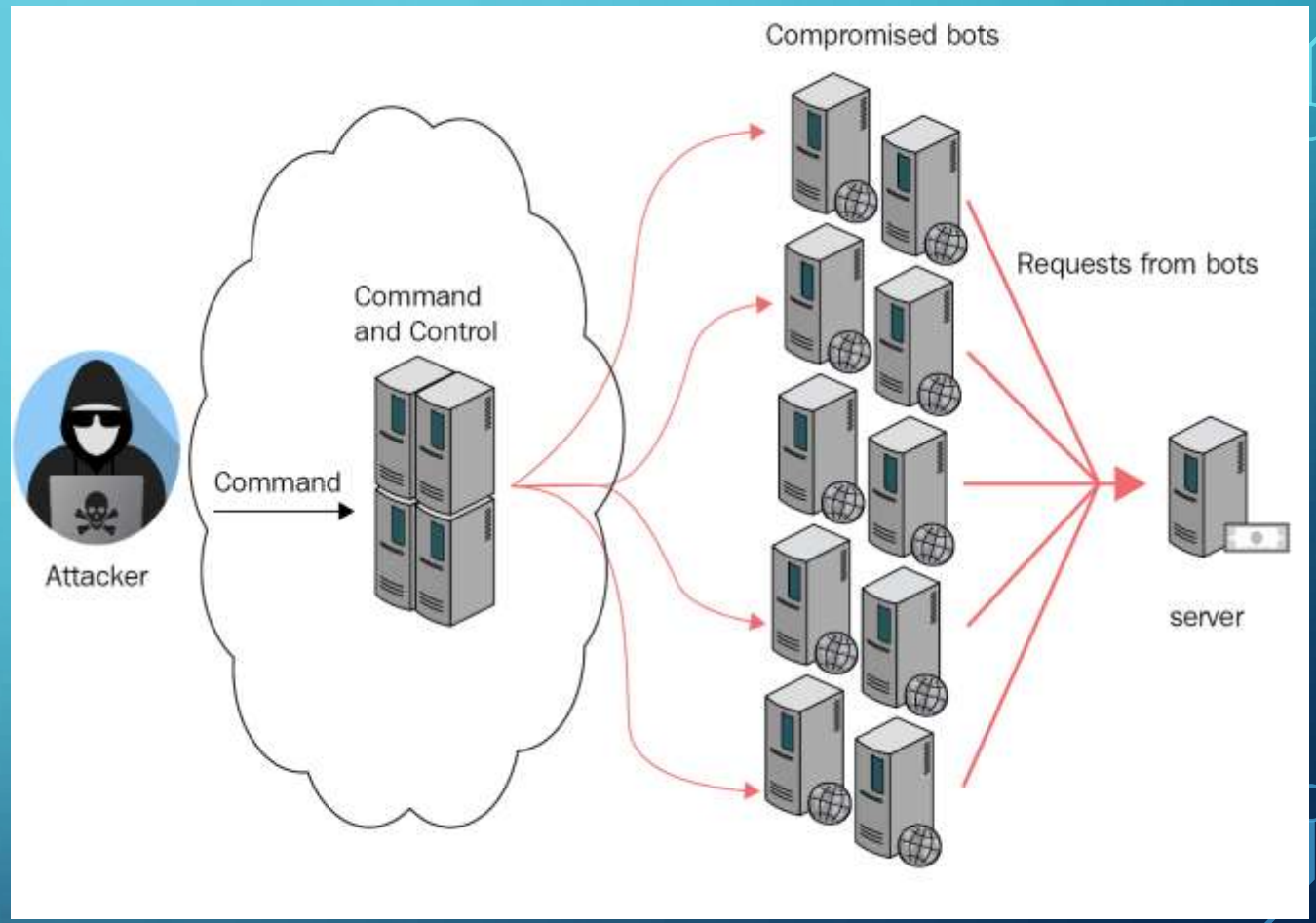
COLLEGE STATE : ANDHRA PRADESH

START AND END DATE : 05/06/2023 TO 05/07/2023

PROJECT TITLE : DOS ATTACK USING NS2

PROJECT TITLE

DOS ATTACK USING NS2



INTRODUCTION - DOS ATTACK USING NS2

- The topology in the wired network is set-up using the node and link creation apis. The tcl script in DDOS_attack. Tcl creates the DDOS attack with the aim of denying normal service or degrading of the quality of services.
- In distributed denial-of-service (DDOS) attacks huge amount of requests are generated to victims through compromised computers (zombies).
- Data transmission is carried out between the genuine client and also from attacker to victim using the UDP connection and CBR application.

AGENDA

- **Introduction to dos attacks:** Explanation of what dos attacks are and their impact on network performance.
- **Overview of ns2:** Brief introduction to ns2 (network simulator 2) and its usage for simulating network scenarios.
- **Implementation of dos attack scenario:** Discussion on different techniques to simulate dos attacks in ns2 (Traffic generation, configuration settings). - Selection of dos attack type to be considered for the simulation.
- **Running and analysing the simulation:** Demonstration of how to run the simulation in ns2. Collection and analysis of network performance metrics during the attack..
- **Prevention and mitigation techniques:** Discussion on possible techniques to prevent or mitigate against DoS attacks.

OVERVIEW

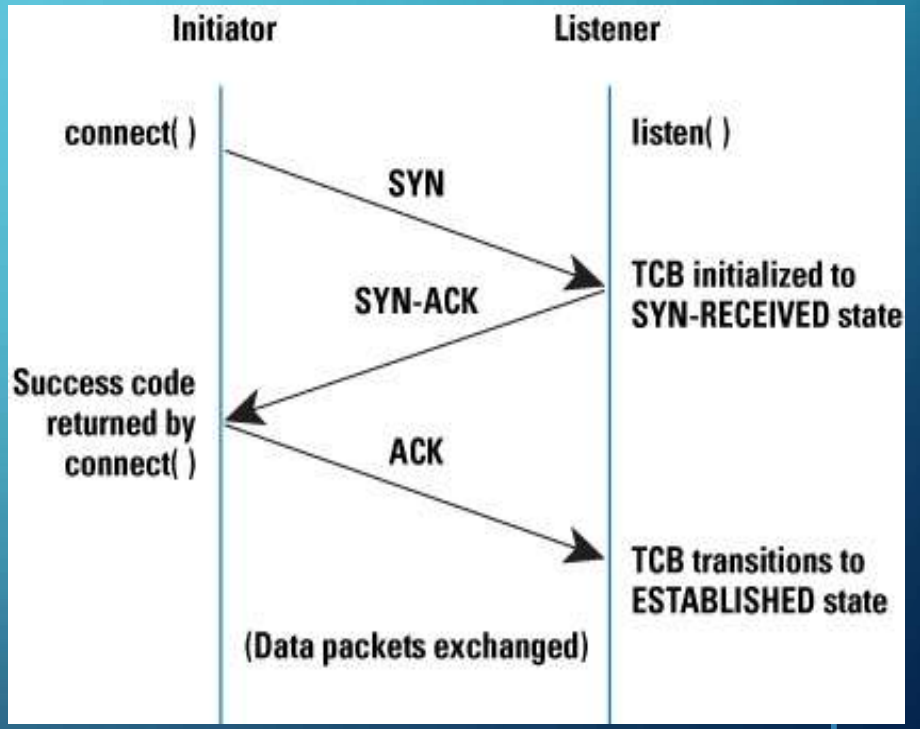
- **Network Topology**: Set up the network topology by defining the nodes, links, and their connections. You can create a network with different types of nodes, such as routers, switches, or hosts, and establish appropriate links between them.
- **Traffic Generation**: Determine the traffic pattern and characteristics for the DoS attack. This involves the number of attacking nodes, their locations, and the type of traffic they generate.
- **Implement Attack Mechanism**: Develop a mechanism to initiate the DoS attack. This can involve scripting in NS2 using Tcl (Tool Command Language) or using existing modules and protocols provided by NS2.
- **Run the Simulation**: Execute the NS2 simulation with the specified network topology, traffic pattern, and attack mechanism.
- **Analyze Results**: Analyze the simulation results to understand the impact of the DoS attack on the network.

END USERS OF THE PROJECT

- A denial-of-service (DoS) attack is an attempt to make a network, service, or website unavailable to its intended users by overwhelming it with a flood of illegitimate requests or by exploiting vulnerabilities in its infrastructure. The end users of a DoS attack are typically not the ones launching the attack but rather the victims who are affected by it. The end users can be individuals, organizations, or even entire networks that rely on the targeted service or website.
- In a DoS attack, the end users may experience degraded or complete loss of service, rendering the targeted resource inaccessible.
- The end users are not responsible for the attack itself. The attack is typically carried out by malicious individuals or groups with the intent to disrupt services, cause financial losses, or create chaos.

SOLUTION AND ITS VALUE PREPOSITION

- A denial-of-service (DoS) attack is a cyberattack that attempts to keep the authorized users of a device or network from using that device or network. DoS attacks use two primary strategies to accomplish that goal.
- The first and most popular strategy is flooding: overwhelming a device or network with traffic.
- The second strategy is crashing services: exploiting weaknesses in the device or network's security in order to cause it to shut down.
- One of the most challenging DoS attacks to prevent and recover from is a distributed denial-of-service attack (DDoS). In a DDoS attack, numerous malicious external systems work in tandem to execute the attack.



CUSTOMIZING THE PROJECT DONE BY ME

- Define the project goals to clearly understand the objectives and requirements of the project.
- Familiarize yourself with the software to gain a good understanding of NS2 and its capabilities.
- Identify the areas for customization to determine which parts of the project we want to modify. It could be the network topology, traffic patterns, protocols, algorithms, or simulation parameters.
- Modify the code or configuration to depending on the desired customization, you may need to modify the code/scripts or configuration files of the project.
- Test and validate after making changes, run the modified project and evaluate its behaviour. Verify that the customizations meet your objectives and requirements.

MODELLING

- **Network topology:** set up the network topology in NS2 by defining nodes, links, and connections.
- **Attack mechanism:** implement the attack mechanism in NS2. This involves scripting the behaviour of the attacking nodes and their interaction with the target node.
- **Attack Parameters:** Configure the attack parameters, such as the attack duration, attack intensity (number of attacking nodes, packet rate.
- **Simulation Execution:** Run the NS2 simulation with the defined network topology, traffic generation, and attack mechanism.
- **Performance Analysis:** Analyze the simulation results to evaluate the impact of the DoS attack on the network. Measure performance metrics such as packet loss, throughput, latency.

RESULTS

- Impact on target node: you can analyse the behaviour of the target node under the dos attack.
- Network performance: evaluate the impact of the dos attack on the overall network performance.
- Attack detection and mitigation: if you have implemented attack detection or mitigation techniques Simulation time: evaluate the time it takes to simulate the dos attack scenario using NS2.
- The results of a simulation in NS2 represent a simulated environment and may not directly reflect real-world scenarios.

REFERENCES

- https://skillsbuild.edunetworld.com/courses/cs/dos-attack-using-ns2/
- https://www.researchgate.net/publication/283550534_Impact_Evaluation_of_Distributed_Denial_of_Service_Attacks_using_NS2
- https://networksimulator2.com/ns2-ddos-attack/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6982801/
- https://slogix.in/source-code/ns2-sample-for-wired-networks/how-to-create-ddos-attack-in-wired-network-in-ns2/


THANK
YOU