Experiment 9: To demonstrate IPsec using Packet Tracer

Bhuvi Ghosh
60009210191

Aim:

The aim of this experiment is to demonstrate the implementation of IPsec (Internet Protocol Security) using Packet Tracer. IPsec provides a framework for securing communication over an IP network through the use of cryptographic protocols. The goal is to showcase the setup, configuration, and functionality of IPsec in a simulated network environment.

Requirements:

1. Packet Tracer software.

2. A network topology with at least two routers and two

hosts. 3. Basic understanding of IP addressing and routing.

4. Knowledge of IPsec concepts, including Phase 1 and Phase 2 parameters.

Procedure:

1. Topology Setup:

- Open Packet Tracer and create a network topology with routers and hosts.
- Connect the devices appropriately to form a functional network.

2. IP Address Assignment:

- Assign IP addresses to the interfaces of routers and hosts. Ensure devices are in the correct subnets for communication.

3. Routing Configuration:

- Configure routing on the routers using static routes or a routing protocol of choice. Verify basic connectivity between devices.

4. Basic Communication Test:

- Confirm basic communication by pinging between hosts to ensure the initial network setup is functional.

5. IPsec Configuration:

- Access the command-line interface of each router.
- Configure Phase 1 (ISAKMP) parameters, specifying authentication and encryption settings.
- Configure Phase 2 (IPsec) parameters, defining the transform set and security associations.

6. Security Policy Definition:

- Create access control lists (ACLs) to identify the interesting traffic that should be protected by IPsec.

7. Application of IPsec Policies:

- Apply IPsec policies to the appropriate interfaces on the routers.

8. IPsec Communication Test:

- Test communication between hosts again. Confirm that IPsec is active and protecting the specified traffic.

9. Monitoring and Verification:

- Use monitoring tools or commands on routers to verify that IPsec is encrypting and decrypting traffic.
- Check logs for any errors or issues.

10. Troubleshooting (if necessary):

- Address any issues that arise during the testing phase. Review configurations and logs for potential errors.

11. Documentation:

- Document the IPsec configuration, including Phase 1 and Phase 2 parameters, security policies, and applied configurations.

12. Conclusion:

- Summarize the key findings of the experiment. Highlight the successful implementation of IPsec and its impact on securing communication within the simulated network.

Conclusion:

This experiment demonstrated the successful implementation of IPsec using Packet Tracer. By configuring Phase 1 and Phase 2 parameters, defining security policies, and applying IPsec to specific traffic, the communication between hosts was secured through encryption. The experiment highlighted the importance of IPsec in enhancing network security and confidentiality.