CSCI 530 - Lab-9

Rishit Saiya (rsaiya@usc.edu)

1. a.

The node4 tunnel endpoint is appropriate for the current network configuration. The clients are on node 4, which is the cause of the issue. The client and server's encrypted communication takes place over the node4 tunnel endpoint. The data will need to be sent through node3 and node4 if another endpoint, such as node3, is utilized as the endpoint, which could put the data at risk because it could become susceptible.

1. b.

Node1 and node3 must contain the tunnel endpoint. This is due to the fact that the scenario is connected to remote-access VPNs. VPNs link various hosts to various networks. Having VPNs on each of the 100 to 200 nodes in this system wastes resources, so it is not the best course of action. To conserve resources, it is therefore preferable to configure VPN at a distant node (endpoints node1 and node3).

2.

The three products that have been implemented do not consistently employ the same cipher algorithm. Yes, one product may be more secure than another due to the usage of various implementation strategies that give products varying levels of security. Key sizes, encryption techniques, and HMACS are also taken into account.

SSH: For logging into and running commands on a distant machine, it is a secure shell. Over insecure networks, it enables secure communication. SSH is available in several versions. Versions 1 and 2 utilize 3DES-CBC, AES128-CBC, and Blowfish-CBC, respectively, while version 1 uses DES, 3DES, and Blowfish encryption algorithms. If SSH is not configured correctly, an attack is feasible over it. In the event that the private key is compromised, an attack could occur.

SSHD: The SSH daemon application is used to connect to several clients on the server side. It controls data exchange, encryption, key exchange, and authentication. The client selects the encryption algorithm and uses 128-bit AES, Blowfish, etc. to encrypt data.

Stunnel: As a tunneling service, Stunnel is employed. Furthermore, it serves as an SSL wrapper between distant clients and servers. The algorithms used for encryption are DES-CBC3-SHA and IDEA-CBC-MD5. If the private key is compromised, there could be an attack because it functions like SSL. HMACs are not utilized since the tunnel lacks an integrity check. Instead, RSA keys with adjustable sizes are employed.

OpenVPN: It is an open source daemon for VPNs. OpenVPN employs encryption techniques including Blowfish-CBC-448 bits, BC, CFB, and OFB. TCP/UDP tunneling that is not encrypted is also supported. The OpenSSL library is utilized. HMAC is used to verify integrity rather than a stunnel.

3.

Only the ping command would have been successful if further tests for the ping and echo commands had been added. In the transport layer, the ping command employs the ICMP protocol for message routing while the echo command uses the TCP protocol. The echo command would not have been successful because stunnel uses the TCP protocol, but the ping command would have.

Yes, we can set up a VPN connection using OpenVPN to cover any communication attempting to travel between node4 and node0. We can configure it to establish an encrypted channel between each node.