Name: Arka Ghosh

ID: B00911033

Assignment: 06 (Exercise 2)

Brute Force Attack: In the IKE protocol of IPSec, there happens two Diffie Hellman exchanges that generates a master key in Phase 1 and another secret key in Phase 2. The secret key in the Phase 2 is refreshed every few minutes which generates a new secret key for data transmission. Even if a secret key is compromised, a new secret key will generate after few moment which makes it harder for the attacker to brute force it.

Replay Attack: To establish a secure connection between the source and destination nodes in the network, IPSec utilizes a unidirectional security association which checks if a message received has been replayed [1]. It operates by assigning each encrypted packet with a monotonically increasing Sequence Number and keeping track of the sequence numbers as the packets arrive at their destination. This mechanism of IPSec helps in preventing Replay Attacks.

Man-in-the-middle attack: Data funneled through an IPSec tunnel is encrypted that makes it harder for the attacker to decode it even if intercepted [2]. Additionally, Authentication Header is used in IPSec to place a digital signature on the contents of each packet. Because IPSec adds signatures to each packet, no component of a packet can be modified without being noticed [3].

IP Spoofing: Mutual authentication between the nodes, which is a technique to establish the identity of the entity behind the IP address, is required while negotiating an IPSec connection. The authentication headers used by IPSec allow each end of a connection to verify the other's identity. An attacker can spoof an IP address, but they won't be able to persuade the other party to believe it unless they compromise the credentials used.

SYN Flooding: Since the adoption of IKEv2, DDoS attacks like TCP SYN flooding have been largely eliminated through IPSec [4]. In such kind of attack, the attacker sends a high number of IKE_SA_INIT messages but no IKE_Auth, resulting in the creation of half-open IKE_SA structures [5]. A half-open IKE SA timer begins when an IKE_SA_INIT request is received. The half-open IKEv2 IKE SA is cleared if no IKE_AUTH message is received before the timer ends which prevents the SYN flooding.

References

[1] "Troubleshoot IPsec Anti-Replay Check Failures", *Cisco*. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/internet-key-exchange-ike/116858-problem-replay-00.html.

[2] "VPN can prevent a man-in-the-middle attack", *Professional Security*, 2019. [Online]. Available: https://www.professionalsecurity.co.uk/news/press-releases/vpn-can-prevent-a-man-in-the-middle-attack/.

[3] "IPSec - Internet Protocol Security", *Firewall.cx*. [Online]. Available: https://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html.

[4] "What is an IPSec Flood DDoS Attack?", *NETSCOUT*. [Online]. Available: https://www.netscout.com/what-is-ddos/ipsec-flood. [Accessed: 14- Apr- 2022].

[5] "IPSec Reference, StarOS Release 21.18 - IKEv2 - Protection Against Distributed Denial of Service [Cisco ASR 5000 Series]", *Cisco*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-18_6-12/IPSec-Reference/21-18-ipsec-reference/21-17-IPSec-Reference_chapter_010011.html.