**Homework 4**

**sdh140430 Swapnil Hasabe**

Answer:

1. IPSec Protocol provides security at Network Protocol.

2. IPsec provides authentication and Confidentiality services for Data

3. My laptop is host at 192.168.0.8 initiates IPSec Processing to server (204.12.196.42)

4. IPSec Protocol works as follows:

IKE's two phases:

Phase 1: To create ISAKMP SA : It establishes Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange provide authenticated keying material for use with ISAKMP. So, Secure channel is set up in this phase

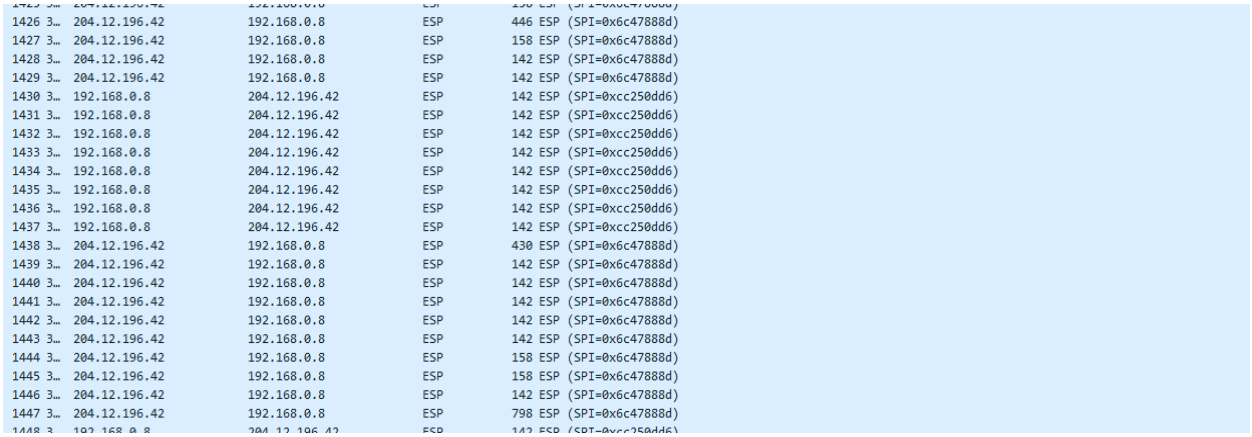
| | | | | | |
|---|---|---|---|---|---|
| 188 8… | 208.87.151.22 | 192.168.0.8 | DNS | 89 | Standard query response 0x7552 Server failure A www.system-maintenancepro.com |
| 189 8… | 192.168.0.8 | 208.87.151.23 | DNS | 89 | Standard query 0xca2e A www.system-maintenancepro.com |
| 190 8… | 208.87.151.23 | 192.168.0.8 | DNS | 89 | Standard query response 0xca2e Server failure A www.system-maintenancepro.com |
| 191 8… | 192.168.0.8 | 208.87.151.22 | DNS | 89 | Standard query 0xca2e A www.system-maintenancepro.com |
| 192 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 270 | Identity Protection (Main Mode) |
| 193 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 242 | Identity Protection (Main Mode) |
| 194 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 242 | Identity Protection (Main Mode) |
| 195 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 242 | Identity Protection (Main Mode) |
| 196 8… | 192.168.0.8 | 204.12.196.42 | ISAKMP | 114 | Identity Protection (Main Mode) |
| 197 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 114 | Identity Protection (Main Mode) |
| 198 8… | 192.168.0.8 | 204.12.196.42 | ISAKMP | 378 | Quick Mode |
| 199 8… | 208.87.151.22 | 192.168.0.8 | DNS | 89 | Standard query response 0xca2e Server failure A www.system-maintenancepro.com |
| 200 8… | 192.168.0.8 | 208.87.151.23 | DNS | 89 | Standard query 0xf98d A www.system-maintenancepro.com |
| 201 8… | 204.12.196.42 | 192.168.0.8 | ISAKMP | 234 | Quick Mode |
| 202 8… | 192.168.0.8 | 204.12.196.42 | ISAKMP | 106 | Quick Mode |
| 203 8… | 192.168.0.8 | 204.12.196.42 | ESP | 206 | ESP (SPI=0xcc250dd6) |
| 204 8… | 208.87.151.23 | 192.168.0.8 | DNS | 89 | Standard query response 0xf98d Server failure A www.system-maintenancepro.com |
| 205 8… | 192.168.0.8 | 208.87.151.22 | DNS | 89 | Standard query 0xf98d A www.system-maintenancepro.com |

Main mode: IPSec Parameters and Policy

Quick Mode: Negotiate the SA for Data

**Phase 2:** To create IPSec SA : Use the secure channel established in Phase 1 to protect message exchanges.
Security Association: An SA is a one-way relationship between sender and receiver
– Specifies cryptographic processing to be applied to this datagram from this sender to this receiver

**Layer 4 ESP protocol Protects data**. It provides Confidentiality and authentication for Payload
ESP specifies a header and trailing fields to be added to IP datagrams
• Fields in header include:
– SPI: Identifies which algorithms and keys are to be used for IPSec processing (more later)
– Sequence number



| | | | | |
|---|---|---|---|---|
| 1426 3… | 204.12.196.42 | 192.168.0.8 | ESP | 446 ESP (SPI=0x6c47888d) |
| 1427 3… | 204.12.196.42 | 192.168.0.8 | ESP | 158 ESP (SPI=0x6c47888d) |
| 1428 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1429 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1430 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1431 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1432 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1433 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1434 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1435 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1436 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1437 3… | 192.168.0.8 | 204.12.196.42 | ESP | 142 ESP (SPI=0xcc250dd6) |
| 1438 3… | 204.12.196.42 | 192.168.0.8 | ESP | 430 ESP (SPI=0x6c47888d) |
| 1439 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1440 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1441 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1442 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1443 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1444 3… | 204.12.196.42 | 192.168.0.8 | ESP | 158 ESP (SPI=0x6c47888d) |
| 1445 3… | 204.12.196.42 | 192.168.0.8 | ESP | 158 ESP (SPI=0x6c47888d) |
| 1446 3… | 204.12.196.42 | 192.168.0.8 | ESP | 142 ESP (SPI=0x6c47888d) |
| 1447 3… | 204.12.196.42 | 192.168.0.8 | ESP | 798 ESP (SPI=0x6c47888d) |

**Important Note**: **Secure channel between Host and Server starts when IKE phase2 starts protecting massages exchanges over secure channel.**

**Phase 2 uses a secure channel to perform further SA negotiation**

**ESP Provides Host (192.168.0.8) to Host Security (204.12.196.42) in Transport Mode.**

**How ESP protects information flowing through secure channel:**

Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.