Nirbhay Sharma (B19CSE114)

CyberSecurity Lab - Protocols

1. **IPSec**

- **working:-** IpSec is a protocol which is used to setup encrypted and secure connection between devices, IP stands for Internet protocol and Sec stands for security so IPSec stands for Internet protocol security and it helps to keep data secure over public channels. So basically it uses key exchange techniques for encryption purposes apart from that it uses authentication, encryption etc to make the network secure.
- **application:-** it is used to setup VPN connection and it works by encrypting IP packets along with authentication. it can also encrypt encryption layer data. Ipsec protocol works in network layer.
- **strength and weaknesses:-** the strength of ipsec is that it can provide network layer security, confidentiality, it has zero dependency on application. but apart from that it has some weaknesses as well which includes, compatibility issues, cpu overhead (since it encrypt and decrypt so it demands CPU and hence it has some overhead on CPU)

2. **VPNs**

- **working:-** VPN refers to (Virtual Private Network) It is an encryption connection between two or more computers, the VPN connection is done over public channel but the data exchange is still private and secure due to encryption that it uses. so we can say that it gives online privacy and anonimity by creating a private network from a public internet connection,
- **application:-** vpn has found various application in accessing region-restricted websites and also it provides security so it has application in ethical hacking as well, while using public wifi VPN is recommended. the vpn also works in network layer.
- **strength and weaknesses:-** vpn has various strengths such as it provides safety, secure remote connection, cost effective, can bypass firewalls. Apart from that it has various weaknesses such as vpn may decrease the internet speed, it is not legal in all countries since it can also take us to restricted websites, compatibility issues.

3. **SSL**

- **working:-** SSL stands for Secure Socket Layer, it is an encryption based internet security protocol, it is basically for securing communication that take place on internet, so it is for securing communication between client and server. the basic working is SSL encrypt data and transmit it and so SSL initiates an authentication process called handshake between server and client, ssl also provides data integrity by verifying the data change.
- **application:-** SSL is used in secure credit card transactions, data transfer between client and server and also in login systems. SSL sits between application layer and transport layer
- **strength and weaknesses:-** the strength of ssl are authentication, security, relaibility, data integrity the weakness includes performance, cost issues etc.

4. **TLS**

- **working:-** TLS stands for Transport layer security, TLS also uses encryption techniques to secure the communication between client and server and also TLS can protect web applications from data breaches and other attacks. The working of TLS is as follows so TLS ensures three components i.e. encryption, authentication, integrity, TLS also uses TLS handshake to establish secure connection between client and server.
- **application:-** TLS finds application in web browser and websites etc, and it operates between application and transport layer.
- **strength and weaknesses:-** the advantages of TLS are integrity, trust, security and also it can prevent malware prevention but it has some weakness as well as it is vulnerable to MiM attack and it has high implementation cost, it fails as network complexity increases.

it looks like that TLS and SSL are more or less same so here are some of the points of difference

- ssl uses message digest to create master secret while tls uses pseudo-random function to create master secret
- ssl uses MAC (message authentication code) while tsl used Hashed Message authentication code protocol
- ssl is more complex to implement while tls is simple
- ssl is less secured while tls is more secured as it uses secure cryptographic hash functions.

5. **PGP**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

6. **HTTPS/SHTTP**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

7. **SET**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

8. **PEM**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

9. **Kerberos**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

10. **S/MIME**

- **working:-**
- **application:-**
- **strength and weaknesses:-**

protocol	Vulnerability in the protocol
IPSec	it may allow authenticated remote attacker to affect the system, the vulnerability lies in improper parsing of malformed IPsec packets
VPNs	vpn's are vulnerable as they are exposed to public internet and might work as entry point for any attacker
SSL	heartbleed bug is a vulnerabiliy in open ssl, this vulnerability allows the attacker to steal private keys attached to ssl certificates
TLS	it can be vulnerable to attack like poodle due to outdated cyrptographic method used which is CBC (Cipher Block Chaining)
PGP	vulnerability is that modern e-mail programs allow for embedded html objects so an attacker can interrupt and modify a message intransit
HTTPS/SHTTP	attacker can use DDos attack to create a denial of service from server side since http is a client server protocol
SET	
PEM	
Kerberos	vulnerability lies in the fact that any unauthenticated remote attacker can impersonate the kerberos key distribution center (KDC) and bypass authentication
S/MIME	attacker can modify the message intransit and sends updated message