# Assignment: Network Security

Answer the following questions succinctly and clearly by providing your answers below each question. When applicable, show your work to earn full credit. Provide your name below:

**Name**: Sai Jyothsna Pulivarthi-811255910

1. How is the sender authentication carried out in PGP?

**Answer**

Pretty Good Privacy (PGP) is an encryption program which uses symmetric, asymmetric encryption in order to provide authentication for data communication. Sender uses digital signature to maintain authentication. The signature is a generated by encrypting the private key of the sender with the hash value of the message. The signature is appended with the message and sent to the receiver.

The receiver will check the authentication by decrypting the signature with sender’s public key and comparing it to the hash value of the received message. If the signature is valid then we can say that the message is unaltered and sent from the sender. In this way PGP provides authentication in data communication.

1. How is IPSec grafted onto IPv4? The protocol field of the IPv4 header plays a critical role in this. How?  
   **Answer**

The IPv4 header contains the protocol field which will help us to know if it the packet is a IPsec packet or not. If it is set to (50,51) then it confirms that it contains IPSec protected information which is then decrypted to verify data. The receiver uses the protocol field of IPv4 to identify that the IP datagram contains IPSec protected packets and provide authentication by verifying the data.

The protocol field specifies

1. What is the difference between the server-only authentication and server-client authentical in SSL/TLS?

**Answer**:

Server-only authentication and server-client authentical are two authentication modes of SSL/TLS.

In server-only validation, the client does not have to verify itself to the server; instead, the server uniquely identifies itself to the client. The server's digital identity is often checked by the client to ensure that perhaps the website is who it says it is. This method is appropriate for programs when just the server must be verified, such as blogs where clients must enter a login detail to access.

On the other hand, mutual authorization demands that simultaneously the sender and the recipient authenticate themselves to one another. In this mode, in addition to validating the server's certificate mostly during SSL/TLS handshake, the client simultaneously submits its own digital identity to the server. After that, the server checks the client's credentials and only permits the session if it is legitimate. This mode is appropriate for applications where server and client authentication are required, like online financial services and e-commerce transactions.

In conclusion mutual authentication demands both a server and the client to verify themselves to each other and offers a better level of security, server-only authentication with SSL/TLS only requires the server to be authenticated.

1. We say that SSL/TLS is not really a single protocol, but a stack of protocols. Explain. What are the different protocols in the SSL/TLS stack?

**Answer**:

SSL/TLS is a combination of protocols to provide a secure internet connection. The stack of protocols includes Record protocol, Handshake Protocol, Change Cipher Spec protocol, Alert protocol.

* Record protocol is responsible for fragmenting, reducing size, encrypting, and verifying data transmission between the sender and receiver.
* The handshake protocol is used for both initial connection establishment and renegotiating cryptographic settings.
* Change Cipher Spec protocol helps to change the connection from being insecure to secure.
* Errors, alert notifications among sender and secure connections are managed using Alert Protocol.

By using all these protocols SSL/TLS helps to establish secure connection among the sender and receiver by maintaining confidentiality and integrity.

1. What is the role of the SSL Record Protocol in SSL/TLS?

**Answer**:

SSL Record Protocol is one among the stack of SSL/TLS. The application data packets across the uppermost levels in the SSL/TLS protocol stack are divided into smaller parts which are called records. The records are then compressed in to smaller size and applies a message authentication code for every record and performs encryption. These encrypted data is then passed to the third party to decrypt and verify with the original data which will provide the authentication feature over the network.

1. What is the role of the Heartbeat Extension Protocol in SSL/TLS?

**Answer**:

Heartbeat Extension protocol in SSL/TLS will help to maintain the connection alive and obtain its status continuously from the endpoints. In this process the user will send the heartbeat message to the server which contains some information regarding the connection such as payload. The server will respond with the same payload specifying that it is maintaining the connection alive. If the heartbeat is not received for specified amount of time the connection will be considered as lost and the tries to reconnect. In this way the heartbeat protocol helps to maintain the connection alive.

1. What is the relationship between the svchost.exe program and the  
   DLLs in your Windows machine? What is the role of the svchost process at the system boot time?

**Answer**:

The svchost.exe program’s job is to maintain multiple windows services. Each svchost.exe instance can host one or more services, each of which is represented by a dynamic-link library (DLL) file. svchost.exe loads the required DDL into its platform and executes the necessary operations which results in enhancing the performance by sharing the single instance.

During the system boot time svchost.exe will run first among all and collects the configurations from the window registry and identify the services dependencies that are required. Then, it starts each of these services in a different instance in the svchost.exe process, categorizing them according to their shared needs as well as traits.

1. What is it about the svchost.exe program in a Windows machine that makes its vulnerabilities particularly deadly?

**Answer**:

Svchost.exe program is targeted by malware and cyber attackers to get access to the system which makes the vulnerabilities hazardous by allowing the intruders to execute code. This will allow them to steal data, install malware etc.

Another factor that makes svchost.exe vulnerabilities so dangerous is that they might be challenging to find and fix. Any effort to delete or alter svchost.exe might result in system instability and issues because it is a crucial system process. Furthermore, it may be challenging to isolate and patch a single vulnerability without impacting other services since svchost.exe hosts several services.

1. Describe briefly the three principal propagation mechanisms for the Conficker worm?

**Answer:** Conficker worm infected millions of machines. It spread by combining the three main distribution mechanisms:

* Exploiting system flaws: Conficker was created to take use of Windows operating system flaws, particularly the MS08-067 vulnerability in the Windows Server service, which allowed it to infect machines without the need for human involvement. The worm would try to infect further computers on a shared network after discovering a susceptible system by searching for additional weak points and taking advantage of the same weakness.
* Guessing Password: In this method the conficker worm will try attack by predicting the passwords that are poor on sharing networks and administrator credentials. It is done using a dictionary attack to guess and create a new password.
* USB autorun: Due to the windows autorun function the worm will be propagated through USB flash devices. The infected computer will contain an autorun.inf file that runs the worm’s code whenever the drive was plugged into another machine. It will also spread over network and infects a lot of machines.

Through these propagation mechanisms enable conficker spread the worms across the machines.

1. How does the Conficker worm drop a copy of itself in the hard disks of the other computers that are mapped in your computer?

**Answer**:

The conficker worm copy is dropped in other computers which are connected or mapped to the infected machine. It will duplicate itself in the system and place it in a common folder and look for the other machines connected in the same network and targets a vulnerable machine. It is difficult to identify, remove it as the worm uses techniques like creating hidden folders, randomly generating the file names that the user cannot predict. By using different techniques, it will spread its effect to the whole network and cause destruction without user knowing it.

1. What is a honeypot in network security research? What is a honeynet?

**Answer**:

A honeypot is a security tool used for network safety research to intimate weak systems and services in order to identify and prevent attempts at unwanted network access. A honeypot's aim is to draw in and divert attackers while giving researchers useful information about their strategies, tactics, and processes.

Honeypots appear as a virtual machine or any physical hardware which appears as an easy target for the attackers. The professionals will attack the honeypot using their own techniques, the researchers will observe these and prepare the reports and collects the data. The researchers will analyze the data and create new security methods. Honeypots are only handled by the professionals by following the network security policies. Sometimes we use honeypots to provide evidence for a cybercrime.

Honeynet is an extended version of honeypot. It is a combination of honeypots, used to find the unauthorized access. it will provide a real time environment for the researchers to study the origin of the attacks. Honeynets require high maintenance to handle as it may also cause risk for security for themselves.

1. Carefully read the paper: [Amazon Web Services Best Practices for DDoS Resiliency](https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf) and answer the following questions:
   1. How does AWS classify DDoS attacks in general?

**Answer:**

Amazon web services classified the DDoS attacks into three categories based on type of attack, methods used by intruders. They are volumetric attacks, protocol attacks, application layer attacks.

* In Volumetric attacks, the bandwidth of the attacker will be consumed by the attacker by flooding it with very high volume of traffic which will lead to depletion of the performance of legitimate traffic.
* Protocol attacks take use of flaws in network protocols to prevent the target system from communicating with its clients.
* Application layer attack: The purpose of these assaults is to take advantage of holes in the target system's installed programs. Attackers can flood the computer system with tasks that need a lot of processing power by aiming at the application layer, which can cause the system to sluggishly or even crash.
  1. How does AWS classify Infrastructure Layer Attacks and Application Layer Attacks?

**Answer**:  
 The infrastructure layer attacks will interrupt the normal operations of the devices connected to the network and its infrastructure components. Some of the infrastructure attacks are Volumetric, Protocol, Fragmentation, Spoofing.

The application layer attacks will be targeted on the top layer of OSI model which effects the network infrastructure. The common application attacks are HTTP floods, slow attacks, Zero-day attack, DNS amplification attacks.

* 1. How is AWS classification mapped into the OSI model?

**Answer:**

* 1. What unique aspects of AWS DDoS mitigation makes it unique for web services?  
     **Answer**:

Aws DDoS mitigation has several distinctive features that makes it best for the internet-based services such as scalability, cost-effective, multi-layered protection, Granular control, Automated Detection, and mitigation.

* The AWS services like Amazon cloudFront, AWS Shield etc will automatically scale up the traffic automatically whenever there is a demand for it without anyone intervention. This will help to handle the traffic situation.
* As AWS is a pay-as-you-go we do not have to pay for the extra resources and can buy the exact resources needed. This will reduce the cost.