51. What is the man-in-the-middle attack?

This is a type of cyber-attack in which the attacker stays between the two to carry out their mission. The type of function it can perform is to modify the communication between two parties so that both parties feel like they are communicating over a secure network.

52. What is a traceroute? Why is it used?

Traceroute is a widely used command-line tool available on almost all operating systems. A complete route to the destination address is displayed. It also shows the time (or delay) between intermediate routers.

Uses of traceroute:

It enables us to locate where the data was unable to be sent along

Traceroute helps provide a map of data on the Internet from source to destination

It works by sending ICMP (Internet Control Message Protocol) packets.

You can do a visual traceroute to get a visual representation of each hop.

Please refer to the article: Traceroute in Network Layer to know more about it.

53. What is the difference between HIDS and NIDS?

HIDS: This intrusion detection system sees the host itself as a whole world. It can be a computer (PC) or a server that can act as a standalone system and analyze and monitor its own internals. It works by looking at the files/data coming in and out of the host you're working on. It works by taking existing file system snapshots from a previously taken file system and comparing them to each other. If they are the same, it means the host is safe and not under attack, but a change could indicate a potential attack.

NIDS: This system is responsible for installation points across the network and can operate in mixed and hybrid environments. Alerts are triggered when something malicious or anomalous is detected in your network, cloud, or other mixed environments.

54. What is the difference between VA (Vulnerability Assessment) and PT (Penetration Testing)?

Penetration testing: This is performed to find vulnerabilities, malicious content, bugs, and risks. Used to set up an organization's security system to protect its IT infrastructure. Penetration testing is also known as penetration testing. This is an official procedure that can be considered helpful, not a harmful attempt. This is part of an ethical hacking process that focuses solely on breaking into information systems.

Vulnerability assessment: It is the technique of finding and measuring (scanning) security vulnerabilities in a particular environment. This is a location-comprehensive evaluation (result analysis) of information security. It is used to identify potential vulnerabilities and provide appropriate mitigations to eliminate them or reduce them below the risk level.

Please refer to the article: Differences between Penetration Testing and Vulnerability Assessments to know more.

55. What is RSA?

The RSA algorithm is an asymmetric encryption algorithm. Asymmetric means that it actually works with two different keys. H. Public and Private Keys. As the name suggests, the public key is shared with everyone and the private key remains secret.

56. What is the Blowfish algorithm?

Blowfish is an encryption technique developed by Bruce Schneier in 1993 as an alternative to the DES encryption technique. It is considerably faster than DES and provides excellent encryption speed even though no effective cryptanalysis techniques have been discovered so far. It was one of the first secure block ciphers to be patent-free and therefore freely available to everyone.

Block size: 64 bits

keys: variable size from 32-bit to 448-bit

Number of subkeys: 18 [P array]

Number of rounds: 16

Number of replacement boxes: 4 [each with 512 entries of 32 bits]

57. What is the difference between a vulnerability and an exploit?

Vulnerability: A vulnerability is an error in the design or implementation of a system that can be exploited to cause unexpected or undesirable behaviour. There are many ways a computer can become vulnerable to security threats. A common vulnerability is for attackers to exploit system security vulnerabilities to gain access to systems without proper authentication.

Exploit: Exploits are tools that can be used to exploit vulnerabilities. They are created using vulnerabilities. Exploits are often patched by software vendors as soon as they are released. They take the form of software or code that helps control computers and steal network data.

Please refer to the article: Difference Between Vulnerability and Exploit to know more about it.

58. What do you understand by Risk, Vulnerability and threat in a network?

Cyber threats are malicious acts aimed at stealing or corrupting data or destroying digital networks and systems. A threat can also be defined as the possibility of a successful cyberattack to gain unethical access to sensitive data on a system.

Vulnerabilities in cybersecurity are deficiencies in system designs, security procedures, internal controls, etc. that can be exploited by cybercriminals. In very rare cases, cyber vulnerabilities are the result of cyberattacks rather than network misconfigurations.

Cyber ​​risk is the potential result of loss or damage to assets or data caused by cyber threats. You can't eliminate risk, but you can manage it to a level that meets your organization's risk tolerance. Therefore, our goal is not to build a system without risk but to keep the risk as low as possible.

59. Explain Phishing and how to prevent it.

Phishing is a type of cyber-attack. The name phishing comes from the word 'phish', which means fish. Placing bait to catch fish is a common phenomenon. Phishing works similarly. Tricking users or victims into clicking on malicious websites is an unethical practice.

Here's how to protect your users from phishing attacks.

* Download software only from authorized sources
* Do not share personal information on unknown links.
* Always check website URLs to prevent such attacks.
* If you receive an email from a known source, but the email seems suspicious, contact the sender with a new email instead of using the reply option.
* Avoid posting personal information such as phone numbers, addresses, etc. on social media.
* Monitor compromised websites with malicious content using phishing detection tools. Try to avoid free Wi-Fi.

60. What do you mean by Forward Secrecy, and how does it work?

Forward secrecy is a feature of some key agreement protocols that guarantees that the session keys will remain secure even if the server's private key is compromised. Perfect forward secrecy, also known as PFS, is the term used to describe this. The "Diffie-Hellman key exchange" algorithm is employed to achieve this.