1 :: What is File Transfer Protocol (FTP)?

FTP (File Transfer Protocol) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications, which solves the problem of different end host configurations (i.e., Operating System, file names). File Transfer Protocol is used with user-based password authentication or with anonymous user access.

2 :: Explain security concerns of FTP?

The original FTP specification has many security concerns. In May 1999, the following flaws were addressed:

- ► Bounce Attacks
- ► Spoof Attacks
- ► Brute Force Attacks
- ► Sniffing
- ► Username Protection
- ► Port Stealing

3 :: Explain Anonymous FTP?

A host that provides an FTP service may additionally provide anonymous FTP access. Users typically log into the service with an anonymous account when prompted for user name. Although users are commonly asked to send their email address in lieu of a password, no verification is actually performed on the supplied data, examples of anonymous FTP servers can be found here.

4 :: Explain Remote FTP or FTPmail?

Where FTP access is restricted, a remote FTP or FTPmail service can be used to circumvent the problem. An email containing the FTP commands to be performed is sent to a remote FTP server, which is a mail server that parses the incoming email, executes the FTP commands, and sends back an email with any downloaded files as an attachment. Obviously this is less flexible than an FTP client, as it is not possible to view directories interactively or to modify commands, and there can also be problems with large file attachments in the response not getting through mail servers. As most internet users these days have ready access to FTP, this procedure is no longer in everyday use.

5 :: What is NAT traversal?

The representation of the IP addresses and port numbers in the PORT command and PASV reply poses a challenge to FTP in traversing Network address translators (NAT). The NAT device must alter these values, so that they contain the IP address of the NAT ed client, and a port chosen by the NAT device for the data connection. The new address

and port will probably differ in length in their decimal representation from the original address and port. Such translation is not usually performed in most NAT devices, but special application layer gateways exist for this purpose.

6 :: Explain FTP bounce attack?

FTP bounce attack is an exploit of the FTP protocol whereby an attacker is able to use the PORT command to request access to ports indirectly through the use of the victim machine as a middle man for the request.

This technique can be used to port scan hosts discreetly, and to access specific ports that the attacker cannot access through a direct connection.

nmap is a port scanner that can utilize an FTP bounce attack to scan other servers.

7 :: Explain FTP Spoofing attack?

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

8 :: What is Brute force attack?

In cryptography, a brute force attack is a strategy used to break the encryption of data. It involves traversing the search space of possible keys until the correct key is found.

The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack. By obfuscating the data to be encoded, brute force attacks are made less effective as it is more difficult to determine when one has succeeded in breaking the code.