ARP Protocol: Address Resolution Protocol Works at Network Layer

Mac address is the physical address of the device; it is a global unique number which is assigned to every network interface card. The ARP protocol is used to resolve IP address to MAC address.

To communicate with system over LAN IP address alone is not sufficient to make the communication here MAC(media access control) address is also required as it is unique for each device. This Protocol is used to acquire the MAC address of the device.

Let's take an example : Let say Four computers A, B, C, D are connected . A want to communicate with System B. Each computer knows the IP of other computers connected.A knows IP of B but mac address is still unknown. To find mac address of B, The computer A will look into its internal list called ARP cache to see mac address of matching IP address of B computer. If no entries are found in ARP cache then it returns ARP cache free. So now Computer A will send Broadcast message over a network. In the Broadcast message A is asking who is (IP of B)? And asks for MAC address and B will respond with it's mac address. Once the mac address is received it will store it in ARP cache table. ARP cache table contains Internet Address ,Physical Address ,Type. ARP cache is created to make the Network communication more efficient. There are basically two types of entries in Type column of the table a. Static b. Dynamic

Static: In this type of entry someone has to manually enter the mac address association with respect to ip address.

Arp -s ip mac address ---> command for manual entry

Dynamic: Entries received from broadcast message. They are not permanent. They are flushed out Periodically.

ARP Spoofing:

It is MiTM Attack which allows the attacker to intercept any communication between the devices over the network.

Attack process flow :

1. Attacker need to get connected to a target network. Now they scan the network and obtain at least 2 IP address
2. With the help of spoofing tools they send out forged ARP responses. (Tools: Drifnet)
3. Forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
4. Both the device update their apr cache and communicate via attacker instead of direct communication.

DNS : Domain Name System- Application Layer Protocol

Application layer protocols are divided into categories a, Protocols which are used by the users (email)b. Protocols which supports the protocols used by the user.(DNS)

DNS works on client server model. It is an internet service that translate domain name into IP address. Ex. www.gmail.com it is a domain name this is converted into IP address

DNS Spoofing

There are two types of DNS Spoofing 1, DNS cache poisoning 2. DNS ID spoofing
In DNS cache poisoning the attacker places the compromised DNS server containing forged entries of genuine website names with the IP of the attacker. When the request is sent to Local DNS then it replied with a forged entry resulting in redirection to a false website planted by the attacker.
DNS ID spoofing he packet ID and IP information generated for the resolve request sent by the client is duplicated with false information inside it

FTP/S File Transfer Protocol over Secure Socket Layer Port 21

It is used to exchange files overt the Internet. To enable the data transfer FTP uses TCP/IP Protocol. FTP is the most common protocol used over the internet to upload and download files. FTP can be invoked from command prompt or GUI . The files transfer also allows you to add, remove, delete, update, move from the server. It used the reserved port no 21. To transfer a file 2 connection are established in parallel

1. Control connection
2. Data Connection

Control connection: It is initiated on port no 21. FTP uses this connection to send out control information like user identification , passwords , to retrive or store files.

Data Connection: To send out actual file it used data connection. It is initiated over port 20. FTP sends the control information out-of-band as it uses a separate control connection.
FTP Session:
When the FTP connection is created between client and server The control tcp connection is initiated by client to the server side. The control information is sent out during this and when the server receives it the data connection is initiated from server side. 1 data connection 1 file can be sent out. The control connection is valid/active throughout the session.

FTP/S runs over port 990.When the clients connect over port 990 then SSL handshake is performed implicitly without any extra command because port implies security ! When the client is connected over port 21 then user need to explicitly give instruction for SS handshake using **AUTH SSL** or **AUTH TLS** commands.

FTP exploits :
1. Anonymous Authentication
2. Directory Traversal Attack
3.Dridex based malware attack

HTTP/S Hyper text transfer protocol secured | Port 80,443

Primary protocol used to send data between website and web browser. To add on security feature HTTPs is introduced which means the data will be transmitted in the encrypted form to avoid any man in the middle attack It used TLS(Transport layer security) or SSL (Secure socket layer) . Communication is secured by asymmetric public key infrastructure
Private Key: owned by owner of the website
Public Key: owned by the users who want to interact with that website.

Attack SSL Stripping attack

SMTP (Simple Mail Transfer Protocol)| Port 25 | Application layer

A TCP connection is open to SMTP server when the user initiates the mail process. The SMTP server is always on listen mode. After successfully establishing the TCP connection the client process sends the mail instantly. The SMTP protocol can be broadly divided into two types a) End to end method b) Store and forward method.
End to End is used between different organizations while store and forward is used within an organization. The client who is willing to send out mail will contact destination host SMTP to send mail to it. The SMTP server will keep the mail until and unless the mail has been successfully copied to receivers SMTP.

POP3(Post office Protocol Version 3) | Port 110 , 995 (secured) | Application Layer

This protocol is used to receive the email from remote server to local client server. It allows you to download the email on the local system and then you can access it. This protocol is good option when you want to access the email from a single system. If you want to access it from multiple machines then you should not use this server. The default Port is 110 which is unencrypted.
If the client wants to use a secure connection then Port 995 should be used as communication is encrypted .

IMAP Internet Message Access Protocol | Port 143, 993(secured) | Application Layer

This protocol is used to receive the email from remote server to local client server. It allows you to download the email on the local system and then you can access it. This protocol is good option when you want to access the email from multiple machines . IMAP allows simultaneous access by multiple clients The default Port is 143 which is unencrypted.
If the client wants to use a secure connection then Port 993 should be used as communication is encrypted .

RDP(Remote Desktop Protocol) | Port 3389 | Runs over TCP/IP

It allows to gain access to machine situated at another location. It allows to used that machine like we are sitting next to it. Poking holes into firewalls is not good options to get access that machine as attackers can use automated tools and scripts to gain access.RDP works by providing users with a graphical interface, that allows them to connect to another computer remotely. RDP works with multiple different types of network technologies.

SIP (Signalling Protocol) | Application Layer

SIP protocol works on Application layer. It is network signalling protocol for creation and terminating sessions with 1 or more participants . It is designed designed to be independent of underlying transport protocol. This allows SIP applications to run on TCP, UDP, and other protocols It is most common protocol used in VoIP.

SMB (Server Message Block)

SMB (Server Message Block) is a protocol for file sharing , printer , serial ports, and communications abstractions such as named pipes among computers.
It is an application layer protocol and and it communicated using TCP over port 445.
It is more flexible over protocols like FTP and other.

SNMP(Simple Network Management Protocol)| 161 Port | Application Layer

It is an application layer protocol which used UDP port number 161/162. It is used to monitor, detect, network and flaws in the network. It is often used to configure remote devices . It has three agent

1. SNMB Manager : It is a centralised system used to monitor network.It is also known as Network Management Station
2. SNMP Agent: software module installed on a managed device. Managed devices can be network devices like PC
3. Management Information Base (MIB): MIB consists of information of resources that are to be managed.

SSH (Secure Shell)

It is a cryptographic network protocol that is used for transferring encrypted data over network. It enables us to connect to a server/ servers, without having you to remember or enter your password for each system that is to login remotely from one system into an other.

It always comes in key pair:

1. **For encryption function Public key is used and it is visible to everyone**
2. **For decryption function private key is used which stays in computer**

Telent

Telnet is the joint abbreviation of Telecommunications and Networks and it is a networking protocol best known for UNIX platform. Telnet uses the port 23 and it was designed specifically for local area networks.

Telnet is **not a secure communication protocol** because it does not use any security mechanism and transfers the data over network/internet in a plain-text form including the passwords and so any one can sniff the packets to get that important information.

VNC

Virtual network computing facilitates remote desktop sharing, a form of remote access on computer networks. VNC shows the visual work area show of another PC and control that PC over a system association. Far off work area innovation like VNC stumbles into home PC systems to get to a PC from another piece of the house or while voyaging. It is additionally helpful for organize overseers in business situations, for example, data innovation divisions who need to distantly investigate frameworks.