2.5 DHCP attacks

DHCP attacks

The DHCP protocol replaced RARP as we learned. Here's a brief overview of how the DHCP protocol operates. Compare it to your diagram and explanation from the 'Study the DHCP protocol' activity.

DHCP protocol

View description

A diagram showing the DHCP protocol exchange between client and server: words 'client' and 'server' are placed each at the top of two parallel, vertical lines ending with arrows pointing down. A third arrow pointing down on the right represents 'time'. Starting from the top of the parallel lines, an arrow labelled 'discovery' connects the client to the server; then, moving down, a second arrow labelled 'offer' connects the server to the client; a third arrow labelled 'request' connects again the client to the server; lastly an arrow labelled 'acknowledge' connects the server to the client.

The DHCP client broadcasts a DHCPDISCOVER message on the network subnet using the destination address 255.255.255.255 (limited broadcast) or the specific subnet broadcast address (directed broadcast). A DHCP client may also request its last known IP address. If the client remains connected to the same network, the server may grant the request. Otherwise, it depends on whether the server is set up.

When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the DHCP server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client. This message contains the client's client id (traditionally a MAC address), the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

In response to the DHCP offer, the client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on the required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they have made to the client and return the offered IP address to the pool of available addresses.

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed. The protocol expects the DHCP client to configure its network interface with the negotiated parameters.

DHCP starvation

Now let's look at an attack aimed at the DHCP protocol.

DHCP starvation is a situation where the DHCP server, which is in charge of distributing IP addresses and their configuration, is not able to fulfil its job as it is receiving too many requests. In a DHCP starvation attack, an attacker needs to broadcast a large number of DHCP_REQUEST messages using spoofed source MAC addresses. The ultimate goal of the attacker is to make the DHCP server unable to answer legit requests:

1. This can be considered as an attack on the availability of the DHCP Server.
2. This can be seen as the first step to perform a DHCP spoofing attack.

Once the available number of IP addresses in the DHCP server is depleted, network attackers could **set up a rogue DHCP server** and respond to new DHCP requests from network DHCP clients. The rogue server starts distributing IP addresses and other TCP/IP configuration settings including default Gateway and DNS server IP addresses, which can now point to an IP address controller by the attacker. This can facilitate MITM and sniffing attacks.