DHCP Starvation Attack

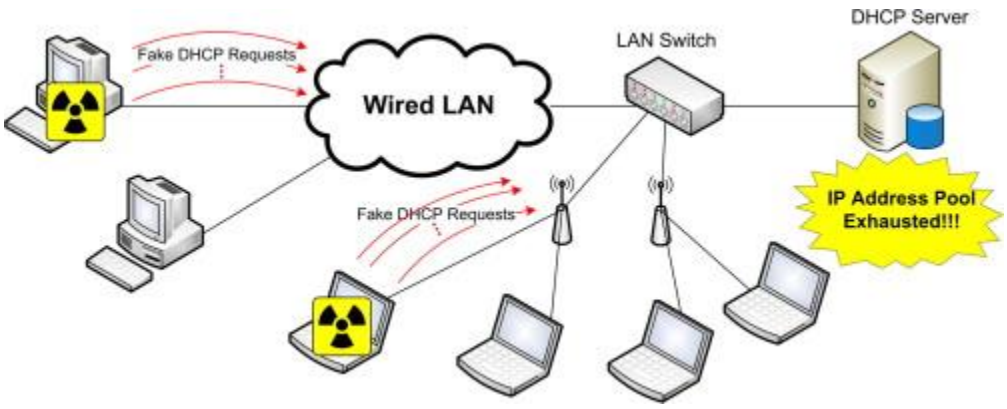
Najrin Sultana

Student ID : 1605042

Definition :

DHCP starvation attack is an attack that targets DHCP servers whereby forged DHCP requests are crafted by an attacker with the intent of exhausting all available IP addresses that can be allocated by the DHCP server. Once that happens, the attacker can deny legitimate network users service, or even supply an alternate DHCP connection that leads to a Man-in-the-Middle (MITM) attack.

Topology Diagram :



DHCP Protocol :

A Dynamic Host Configuration Protocol (DHCP) server is responsible for issuing IP addresses and other communication parameters (i.e subnet mask, default gateway, DNS servers) to devices on its network. This is done through a series of packet exchanges between individual DHCP clients and DHCP servers.

A DHCP IP address allocation transaction depends on four types of packets: DISCOVER, OFFER, REQUEST, and ACKNOWLEDGEMENT. The details about each packet are discussed below :

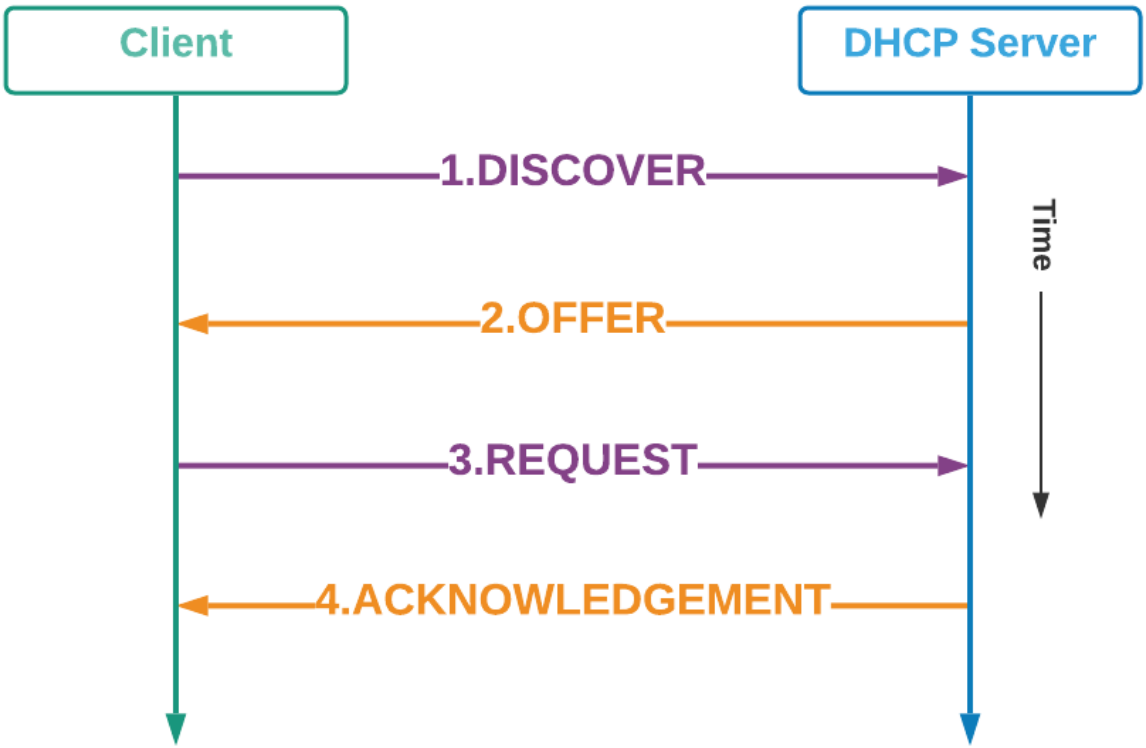
DISCOVER : When a host boots up on the network, if it's a DHCP client, it's going to broadcast a DHCP DISCOVER packet to all hosts in Layer 2 segment (destination address is FF:FF:FF:FF:FF:FF). Frame with this DISCOVER message hits the DHCP Server.

OFFER : The DHCP server has a pool of addresses it can select from. When it receives a DISCOVER packet, the DHCP server chooses one of its remaining IP addresses from its pool, reserves it for the new client and offers it to the new client by unicast via OFFER message.

REQUEST : After the client receives the OFFER message, it requests the exclusive rights on that offered IP by sending a REQUEST message to the server by unicast.

ACKNOWLEDGEMENT : Server sends ACKNOWLEDGE message to the client and anyone else listening confirming the DHCP lease to client. Now the client is allowed to use new IP settings.

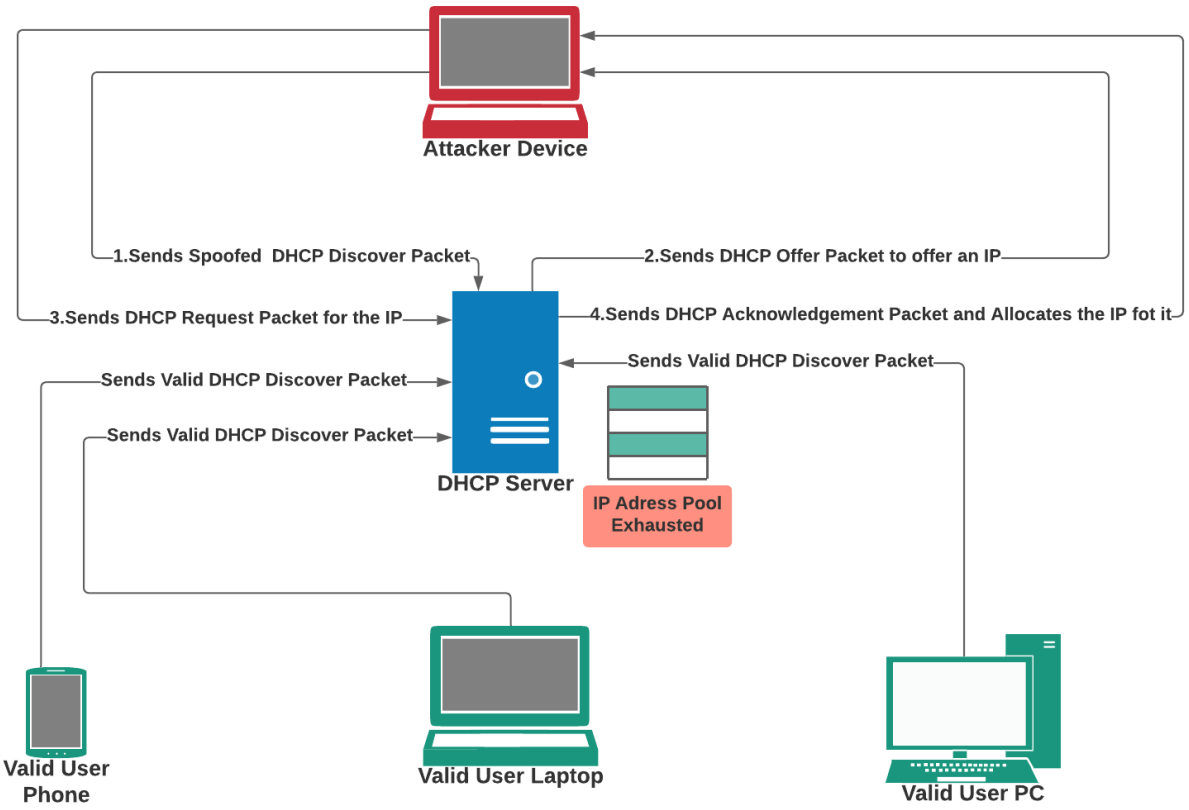
Timing Diagram of DHCP Protocol :



Attacking Strategies :

1. A raw socket will be opened.
2. A random MAC address will be created.
3. DHCP Discover packet will be broadcasted.
4. After receiving the DHCP offer packet, the DHCP request packet will be sent.
5. If the steps from 2-4 are done repeatedly, the IP addresses will get used up in no time.
6. Sending DHCP discover packets will be stopped when no more DHCP offer packets are received in a fixed time interval.

Timing Diagram of Attack :



UDP Header :

Source port is 68 as the attacker is the DHCP client. Destination port is 67 as the DHCP server listens on this port.

Ethernet Header :

DA [Destination MAC Address](6 bytes) : 0xFFFFFF
SA [Source MAC Address](6 bytes) : Spoofed MAC address

DHCP DISCOVER Packet Details :

Operation Code	**Set to 0x01** (As client i.e. attacker is sending discover packets)
Hardware Type	**Set to 0x01** (Ethernet)
Hardware Address Length	Length of Mac Address. **Set to 0x06**
Hops	**Set to 0x00** so that packet reaches the router of the LAN the attacker is in
Transaction Identifier (XID)	A 32-bit identification field generated by the client, to allow it to match up the request with replies received from DHCP servers. **Set to a random number of uint32_t**
Seconds	Elapsed Time. **Set to 0x0000**
Flags	**Set to 0x8000** (Broadcast bit is set to 1 as everyone gets the broadcast message)
CIADDR	Client's IP address; set by the client when the client has confirmed that its IP address is valid. So we need to **set this to 0x00000000**
YIADDR	Client's IP address; set by the server to inform the client of the client's IP Address. So we need to **set this to 0x00000000**
SIADDR	IP Address of the next server for the client to use in the configuration process. So we need to **set this to 0x00000000**
GIADDR	Gateway IP address; filled in by the relay agent with the address of the interface through which Dynamic Host Configuration Protocol (DHCP) message was received. We need to **set this to 0x00000000**
CHADDR	Client's hardware address (Layer 2 address). **Set to the spoofed MAC address.**
Magic Cookie	**Set to 0x63825363**

DHCP REQUEST Packet Details :

Operation Code	**Set to 0x03** (As client i.e. attacker is sending request packets)
Hardware Type	**Set to 1** (Ethernet)
Hardware Address Length	Length of Mac Address. **Set to 6**
Hops	**Set to 0** so that packet reaches the router of the LAN the attacker is in
Transaction Identifier(XID)	A 32-bit identification field generated by the client, to allow it to match up the request with replies received from DHCP servers. **Set to a random number of uint32_t**
Seconds	Elapsed Time. **Set to 0x0000**
Flags	**Set to 0x0000** (unicast)
CIADDR	**Set to the offered IP address received via OFFER Packet** to request for the exclusive rights on that offered IP.
YIADDR	Client's IP address; set by the server to inform the client of the client's IP Address. So we need to **set this to 0x00000000**
SIADDR	**Set to the IP Address of the DHCP server** known from the OFFER Packet.
GIADDR	Gateway IP address; filled in by the relay agent with the address of the interface through which Dynamic Host Configuration Protocol (DHCP) message was received. So we need to **set this to 0x00000000**
CHADDR	Client's hardware address (Layer 2 address). **Set to the same spoofed MAC address** of the DISCOVER Packet.
Magic Cookie	**Set to 0x63825363**

IP Header:

Version	IPV4 is used. **Set to 4**
Header Length	**5**
Priority and Type of Service	
Total Length	
Identification	
Flags	
Fragmented Offset	
Time to live(TTL)	**Set to 255**
Protocol	UDP protocol. **Set to 17**
Header Checksum	Calculated and set.
Source IP Address	**Set to 0.0.0.0**
Destination IP Address	Broadcast Address. **Set to 255.255.255.255**

Justification :

As spoofed DHCP requests are sent to the victim DHCP server repeatedly until no new offer packet is received from the server, the IP address pool of the server gets exhausted quickly. So any valid client trying to get attached to the attacked LAN cannot get any new IP address.