DHCP Starvation Attack

Zahin Wahab

St ID: 1505031

Definition:

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack just like a synchronization (SYN) flood attack. Network attackers can then set up a rogue DHCP server on their system and respond to new DHCP requests from clients on the network.

DHCP:

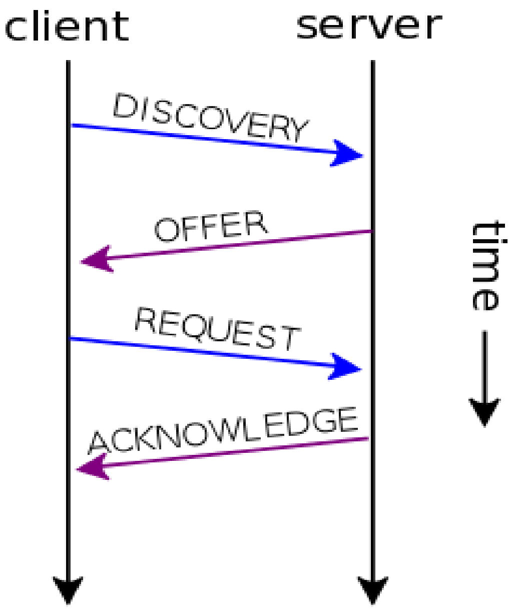
DHCP (Dynamic Host Configuration Protocol) is a protocol that is commonly used in networks for dynamic IP addressing configuration. Every user's device needs at least IP address to join the network and connect to services. When computer first connects to local network with cable or WiFi SSID, first thing is to look for IP address, netmask, default gateway and DNS servers.

How does DHCP work?

1. Host connecting to network (cable or wireless) sends DHCP discover message 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.
2. After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast.

3. Now after the client receives the offer it requests the information officially sending **REQUEST** message to server this time by unicast.
4. Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.

Timing Diagram of original protocol:



Attacking Strategies:

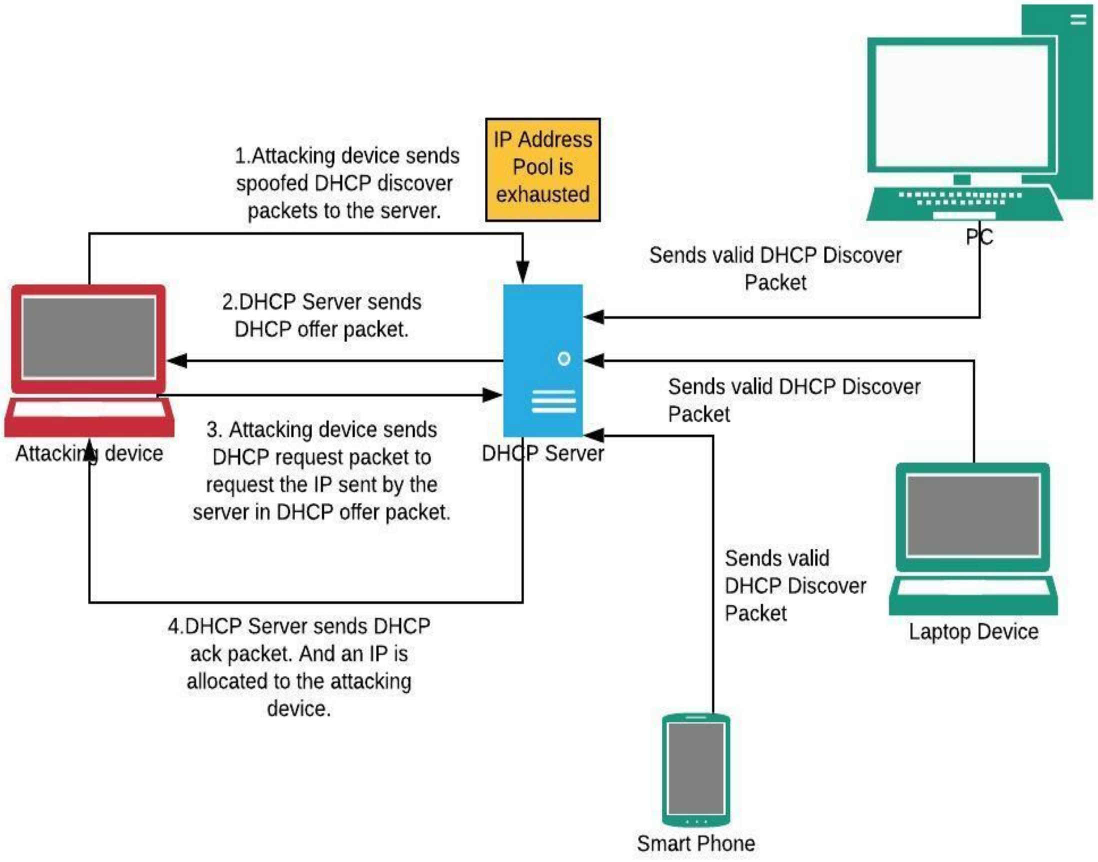
1. A raw socket is opened.
2. A random MAC address is created.
3. DHCP Discover packet is broadcasted.
4. After receiving DHCP offer packet, DHCP request packet is sent.
5. If the steps from 2-4 is done repeatedly, the IP addresses get used up in no time.

6. Sending DHCP discover packets are stopped when no more DHCP offer packets are received in a fixed time interval.

Justification:

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

Topology and timing diagram of attack:



1.Attacking device sends spoofed DHCP discover packets to the server.
IP Address Pool is exhausted
PC
Sends valid DHCP Discover Packet
2.DHCP Server sends DHCP offer packet.
Sends valid DHCP Discover Packet
Attacking device
3. Attacking device sends DHCP request packet to request the IP sent by the server in DHCP offer packet.
DHCP Server
Sends valid DHCP Discover Packet
Laptop Device
4.DHCP Server sends DHCP ack packet. And an IP is allocated to the attacking device.
Smart Phone

Packet Details: DHCP Discover Packet:

Operation Code	**Set to 1 (As client i.e. attacker is sending discover 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	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 0**
Flags	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 0**
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 0**
siaddr	IP Address of the next server for the client to use in the configuration process (for example, the server to contact for TFTP download of an operating system kernel) **. So we need to set this to 0**
giaddr	Relay agent (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 0**
chaddr	Client's **hardware address (Layer 2 address)**. **Set to the spoofed MAC address.**
Magic cookie	**Set to 0x63825363**

DHCP Request Packet:

Since DHCP request, first option is set to 3. The next option is the requested IP. Final option is the IP for the DHCP Server.

Ethernet header:

DA [Destination MAC Address](**6 bytes)** : 0xFFFFFF

SA [Source MAC Address](**6 bytes)** : Spoofed MAC address

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	
Source IP Address	**0.0.0.0**
Destination IP Address	Broadcast Address**. 255.255.255.255**

UDP Header:

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