DHCP Starvation Attack

Zahin Wahab

St ID: 1505031

Introduction:

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.

Detailed Description of Attack Implementation:

1. **Creating a raw socket:** A raw socket is created using socket () system call in Linux. Parameters passed are: AF_INET (for IPV4 protocols),SOCK_DGRAM (connectionless, unreliable messages of fixed length),IPPROTO_UDP (DHCP uses UDP in underlying transport layer).
2. **Random MAC Address is created:** Random address are generated for spoofing the chadrr (Client Hardware Address) field in DHCP Discover packets.
3. **Making DHCP discover packets:** Raw DHCP Discover packets are used for this attack. Parameters used in this packet are:

   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. Set to a random number of uint32_t. Using random() function.

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

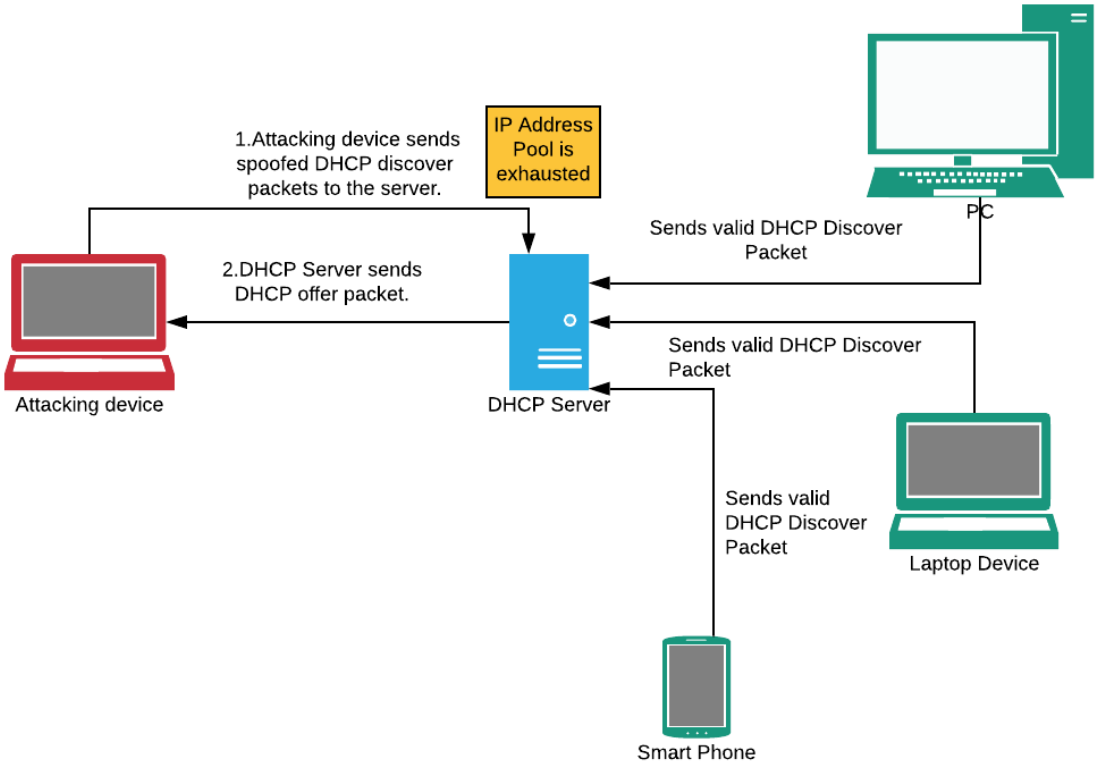
giaddr : Relay agent (gateway) IP address; filled in by the relay agent with the address of the interface through which Dynamic Host Configuration Protocol (DHCP) message was received. So we need to set this to 0

chaddr: Client's hardware address (Layer 2 address). Set to the spoofed MAC address.

Magic cookie : Set to 0x63825363

4. **Sending out DHCP discover packets:** DHCP Discover packets are broadcasted using sendto() sytem call of Linux using the raw socket opened in the previous step.
5. **Keep sending DHCP Discover Packets until all IP addresses are used up:** Packets are continually sent out.

Timing diagram of attack:



Steps of Attack:

Using Terminal:

For compilation:

gcc <*file-name*> -o <*object-file-name*>

For running:

sudo ./<*object-file-name*> <*interface-name*>

or,

echo <*user-password*> | sudo –S ./<*object-file-name*> <*interface-name*>

Special Note: Interface can be found out by typing ifconfig command in terminal.

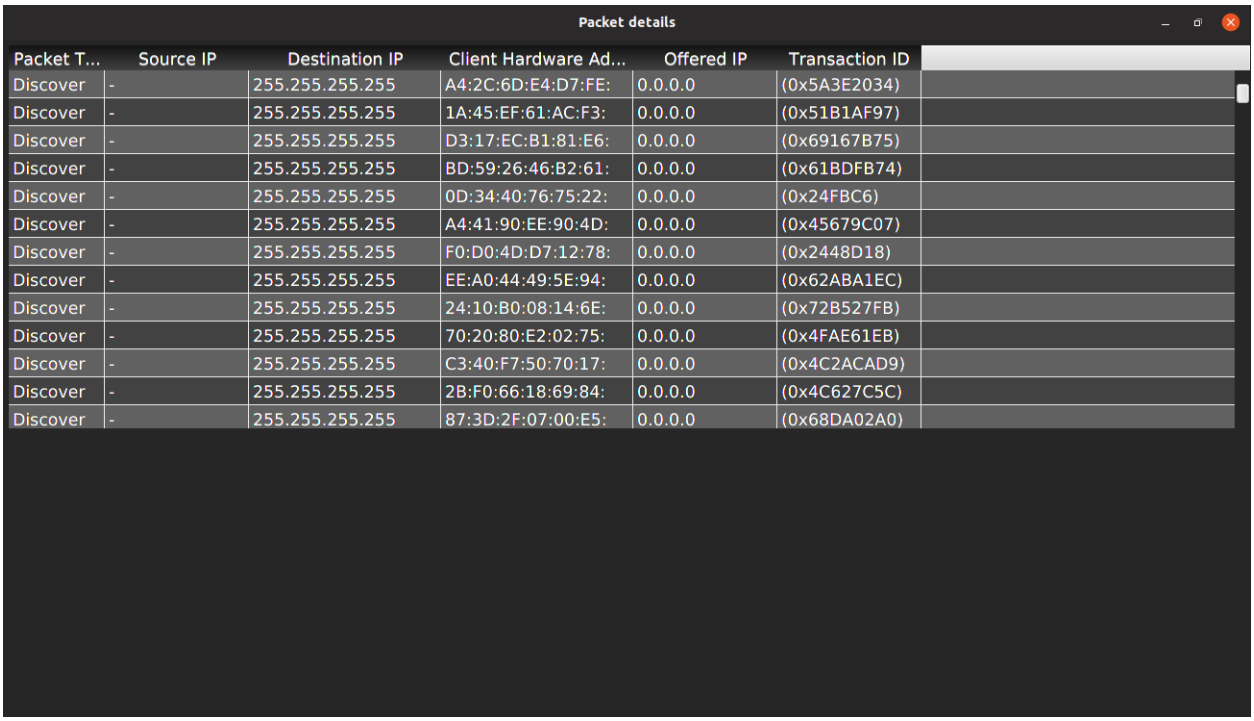
Observed output in terminal:

```
DHCP Stravation is starting
File descriptor for new socket: 3
Random address generated: f6:38:8d:0e:a6:b7
Hardware address: f6388dea6b7
Random address generated: eb:7b:9a:35:0b:2b
Hardware address: eb7b9a35b2b
Random address generated: 45:25:a2:bd:a3:ab
Hardware address: 4525a2bda3ab
Random address generated: 41:db:ab:71:60:ca
Hardware address: 41dbab7160ca
Random address generated: c5:88:ad:dd:27:fd
Hardware address: c588addd27fd
Random address generated: 91:e4:22:5f:e0:a5
Hardware address: 91e4225fe0a5
Random address generated: 15:db:ba:04:2a:1f
Hardware address: 15dbba42a1f
Random address generated: 37:60:b0:1a:44:ca
```

Using Graphical User Interface (GUI):

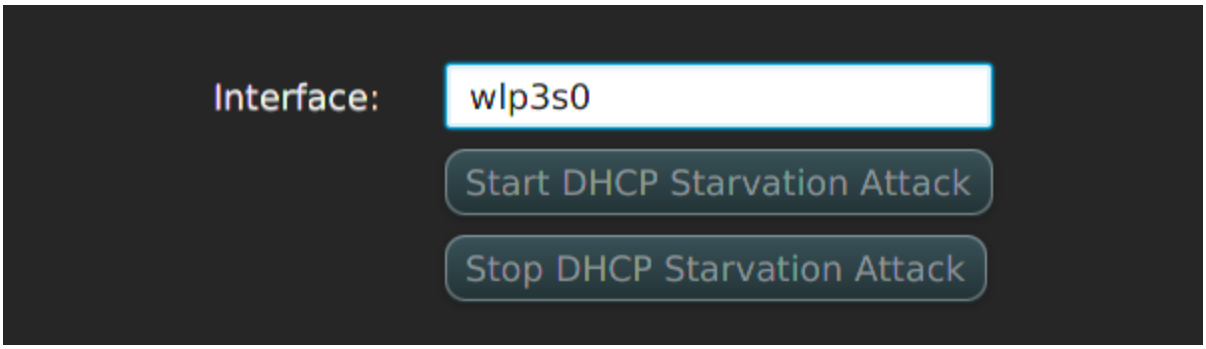
Step 1: Type in Interface in the text field.

Step 2: Press the button “Start DHCP Starvation Attack” to start attacking on DHCP Server. Following button will pop up which will show the burst of spoofed DHCP Discover Packets that we are sending.

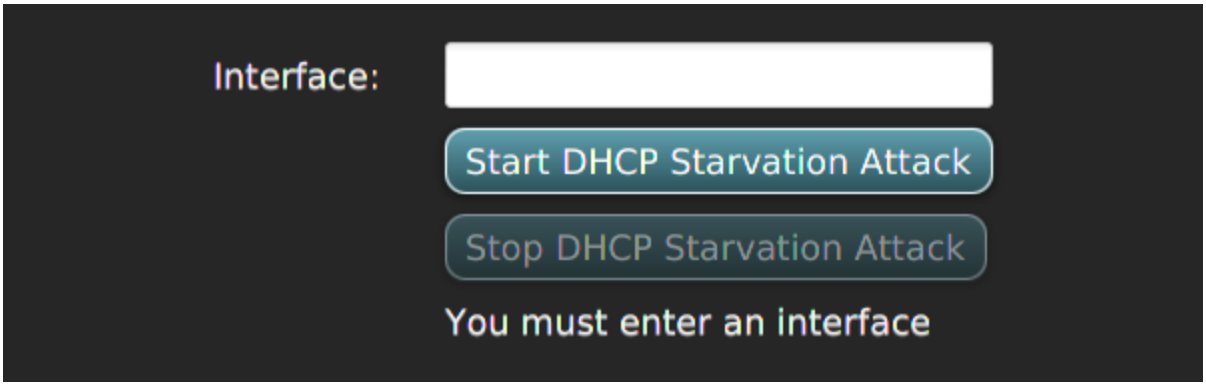


Packet T...	Source IP	Destination IP	Client Hardware Ad...	Offered IP	Transaction ID
Discover	-	255.255.255.255	A4:2C:6D:E4:D7:FE:	0.0.0.0	(0x5A3E2034)
Discover	-	255.255.255.255	1A:45:EF:61:AC:F3:	0.0.0.0	(0x51B1AF97)
Discover	-	255.255.255.255	D3:17:EC:B1:81:E6:	0.0.0.0	(0x69167B75)
Discover	-	255.255.255.255	BD:59:26:46:B2:61:	0.0.0.0	(0x61BDFB74)
Discover	-	255.255.255.255	0D:34:40:76:75:22:	0.0.0.0	(0x24FBC6)
Discover	-	255.255.255.255	A4:41:90:EE:90:4D:	0.0.0.0	(0x45679C07)
Discover	-	255.255.255.255	F0:D0:4D:D7:12:78:	0.0.0.0	(0x2448D18)
Discover	-	255.255.255.255	EE:A0:44:49:5E:94:	0.0.0.0	(0x62ABA1EC)
Discover	-	255.255.255.255	24:10:B0:08:14:6E:	0.0.0.0	(0x72B527FB)
Discover	-	255.255.255.255	70:20:80:E2:02:75:	0.0.0.0	(0x4FAE61EB)
Discover	-	255.255.255.255	C3:40:F7:50:70:17:	0.0.0.0	(0x4C2ACAD9)
Discover	-	255.255.255.255	2B:F0:66:18:69:84:	0.0.0.0	(0x4C627C5C)
Discover	-	255.255.255.255	87:3D:2F:07:00:E5:	0.0.0.0	(0x68DA02A0)

Step 3: Press the button “Stop DHCP Starvation Attack” to stop attacking on DHCP Server.



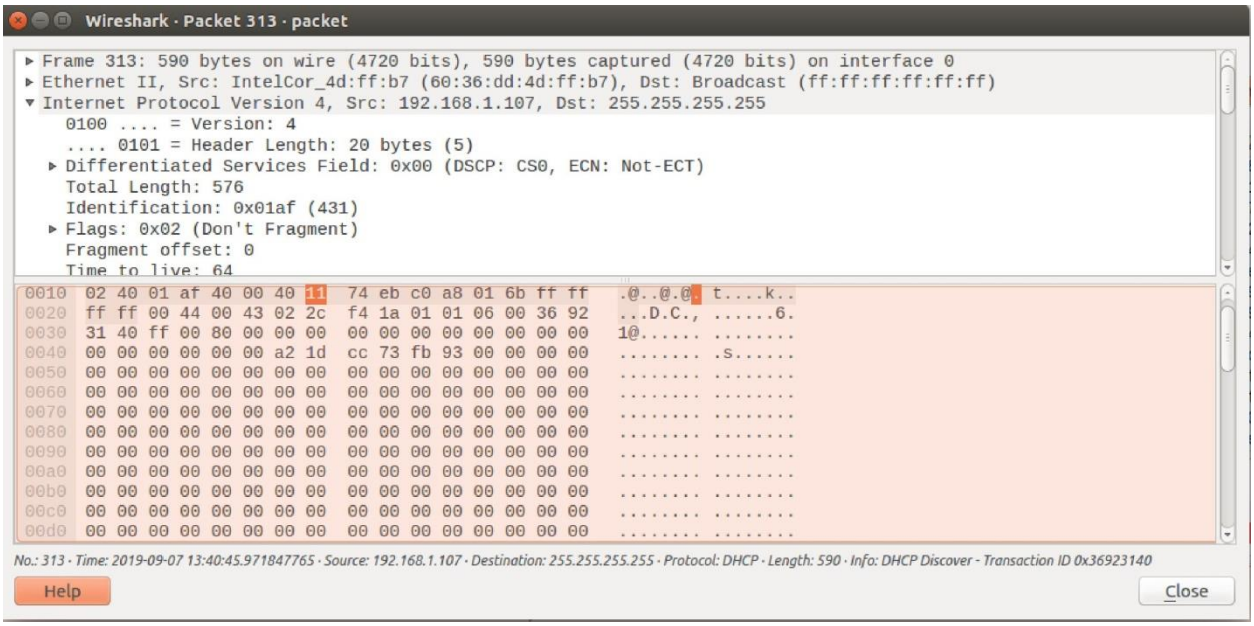
In case attacker forgets to type in the interface name, following alert shows up.



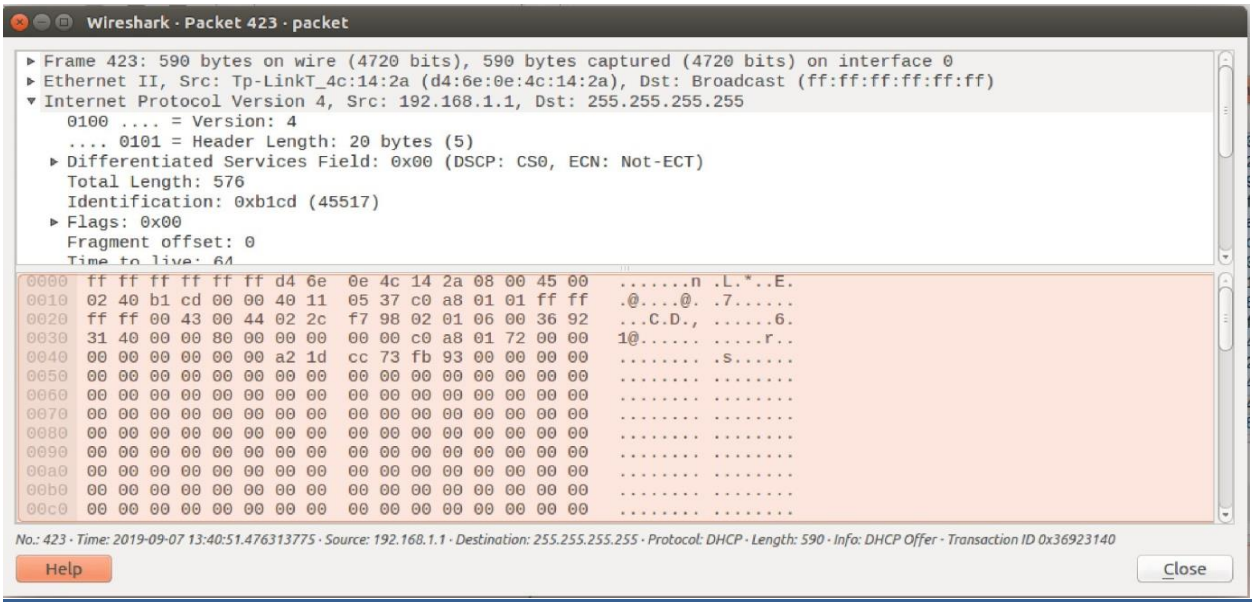
Observed output in victim's screen:

Although password was typed in correctly, this user could not access the wi-fi router.

Captured packet using packet sniffer tool (Wireshark):



DHCP Discover Packet (Transaction ID: 0x36923140)



DHCP Offer Packet (Transaction ID: 0x36923140)

Assessment of the attack:

This attack was successful because as all the IP Addresses were offered to the attacker unknowingly, no new user could be assigned an IP address. Although victim machine tried to join the network and typed in the required credential (password), it was denied service repeatedly. Victim could join the network only if the attack was stopped. In many cases, routers needed to be restarted in order to function properly.

Possible Countermeasure of this attack:

If wired connection was used, then by limiting number of DHCP Discover Packets through a single port, DHCP starvation attack could be prevented. This countermeasure is called port security. It cannot be used in case of wireless connection.