Experiment 2

Chinmay Parikh A059

Questions and Answers

1. What is the purpose of DHCP server in a network?

   Ans: Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e. a scope) configured for a given network.

2. Explain the working of DHCP?

   Ans-

   1. DHCPDISCOVER It is a DHCP message that marks the beginning of a DHCP interaction between client and server. This message is sent by a client (host or device connected to a network) that is connected to a local subnet. It's a broadcast message that uses 255.255.255.255 as destination IP address while the source IP address is 0.0.0.0
   2. DHCPOFFER It is DHCP message that is sent in response to DHCPDISCOVER by a DHCP server to DHCP client. This message contains the network configuration settings for the client that sent the DHCPDISCOVER message.
   3. DHCPREQUEST This DHCP message is sent in response to DHCPOFFER indicating that the client has accepted the network configuration sent in DHCPOFFER message from the server.
   4. DHCPACK This message is sent by the DHCP server in response to DHCPREQUEST received from the client. This message marks the end of the process that started with DHCPDISCOVER. The DHCPACK message is nothing but an acknowledgement by the DHCP server that authorizes the DHCP client to start using the network configuration it received from the DHCP server earlier.
   5. DHCPNAK This message is the exact opposite to DHCPACK described above. This message is sent by the DHCP server when it is not able to satisfy the DHCPREQUEST message from the client.
   6. DHCPDECLINE This message is sent from the DHCP client to the server in case the client finds that the IP address assigned by DHCP server is already in use.
   7. DHCPINFORM This message is sent from the DHCP client in case the IP address is statically configured on the client and only other network settings or configurations are desired to be dynamically acquired from DHCP server.

8. DHCPRELEASE This message is sent by the DHCP client in case it wants to terminate the lease of network address it has been provided by DHCP server.

Here are the steps:

Step 1: When the client computer (or device) boots up or is connected to a network, a DHCPDISCOVER message is sent from the client to the server. As there is no network configuration information on the client so the message is sent with 0.0.0.0 as source address and 255.255.255.255 as destination address. If the DHCP server is on local subnet then it directly receives the message or in case it is on different subnet then a relay agent connected on client's subnet is used to pass on the request to DHCP server. The transport protocol used for this message is UDP and the port number used is 67. The client enters the initializing stage during this step.

Step 2: When the DHCP server receives the DHCPDISCOVER request message then it replies with a DHCPOFFER message. As already explained, this message contains all the network configuration settings required by the client.For example, the yaddr field of the message will contain the IP address to be assigned to client. Similarly the subnet mask and gateway information is filled in the options field. Also, the server fills in the client MAC address in the chaddr field. This message is sent as a broadcast (255.255.255.255) message for the client to receive it directly or if DHCP server is in different subnet then this message is sent to the relay agent that takes care of whether the message is to be passed as unicast or broadcast. In this case also, UDP protocol is used at the transport layer with destination port as 68. The client enters selecting stage during this step.

Step 3: The client forms a DHCPREQUEST message in reply to DHCPOFFER message and sends it to the server indicating it wants to accept the network configuration sent in the DHCPOFFER message. If there were multiple DHCP servers that received DHCPDISCOVER then client could receive multiple DHCPOFFER messages. But, the client replies to only one of the messages by populating the server identification field with the IP address of a particular DHCP server. All the messages from other DHCP servers are implicitly declined. The DHCPREQUEST message will still contain the source address as 0.0.0.0 as the client is still not allowed to use the IP address passed to it through DHCPOFFER message. The client enters requesting stage during this step.

Step 4: Once the server receives DHCPREQUEST from the client, it sends the DHCPACK message indicating that now the client is allowed to use the IP address assigned to it. The client enters the bound state during this step.

3. What is DoS attack? Is DHCP starvation attack a kind of DoS attack?

   Ans: DoS Attack -

- Consuming the IP address space allocated by a DHCP server
- An attacker broadcasts a large number of DHCP requests using spoofed MAC addresses
- The DHCP server will lease its IP addresses one by one to the attacker until it runs out of available IPs for new, normal clients Leads to DoS
- Can easily be achieved with tools such as gobbler If enough requests flooded onto the network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time. Clients of the victim network are then starved of the DHCP resource(s), thus DHCP Starvation can be classified as a Denial of Service attack.The network attacker can then set up a Rogue DHCP on the network and perform man in the middle attacks, or simply set their machine as the default gateway and sniff packets.

4. What are counter measures available to prevent DHCP starvation attack?

   Ans: Prevention - Do not allow more than certain number of requests per port.

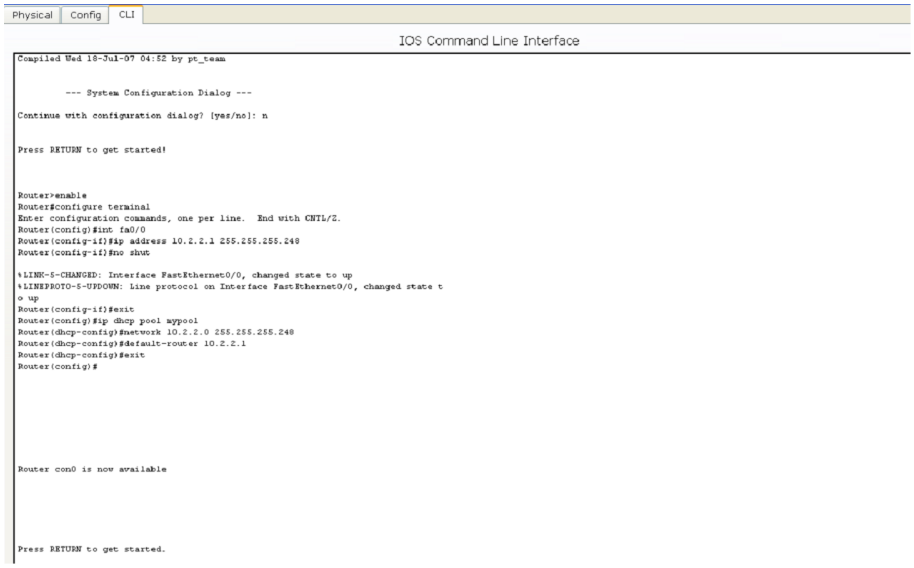
5. What is Rogue DHCP Server attack?

   Ans: Setting up a Rogue DHCP Server is one technique that an attacker can use to gain access to network traffic. This is achieved by spoofing responses that would normally be sent by an authorized DHCP server. The authorized DHCP server will also reply to the client DHCP requests, but if the rogue device is closer (less hops) to the client, its reply to the client may arrive first.

6. What are counter measures available for Rogue DHCP server attack?

   Ans: Counter Measures to prevent Rogue DHCP server attack can be done by using DHCP Snooping. When DHCP servers are allocating IP addresses to the clients on the LAN, DHCP snooping can be configured on LAN switches to harden the security on the LAN to only allow clients with specific IP/MAC addresses to have access to the network.

Output




```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#no ip address
Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.248
Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
Router(config-if)#exit
Router(config)#ip dhcp pool mypool
Router(dhcp-config)#network 10.1.1.0 255.255.255.248
Router(dhcp-config)#dns-server 10.1.1.2
Router(dhcp-config)#default-router 10.1.1.1
Router(dhcp-config)#exit
Router(config)#sh ip dhcp binding
               ^
% Invalid input detected at '^' marker.

Router(config)#ip dhcp binding
                  ^
% Invalid input detected at '^' marker.

Router(config)#sh ip dhcp binding
               ^
% Invalid input detected at '^' marker.

Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
Router#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.1.1.2         0000.0C79.4823           --                     Automatic
10.1.1.3         0000.0C77.3323           --                     Automatic
10.1.1.4         0060.3E56.6C67           --                     Automatic
Router#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
```