**ASSIGNMENT7**

**Zheng (Rio) yin----a1691850**

**2019/5/6—My birthday, still working on assignment.**

**Q1.**

**1).**

**DHCP discovery: Broadcast**

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 whether the server is set up as authoritative or not. An authoritative server denies the request, causing the client to issue a new request. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to expire the request and ask for a new IP address.

**DHCP offer: Unicast**

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. The DHCP server may also take notice of the hardware-level MAC address in the underlying transport layer: according to current RFCs the transport layer MAC address may be used if no client ID is provided in the DHCP packet.

The DHCP server determines the configuration based on the client's hardware address as specified in the CHADDR (client hardware address) field. Here the server, 192.168.1.1, specifies the client's IP address in the YIADDR (your IP address) field.

**DHCP request: Broadcast**

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 required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.[12]:Section 3.1, Item 3 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.

**DHCP acknowledgement: Unicast**

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. after the client obtains an IP address, it should probe the newly received address

**2).**

Without doing active man-in-the-middle, malicious sniffer can only see broadcast messages. Thus,

Its **DHCP Acknowledgement** and **DHCP discovery**.

**3).**

SIADDR (Server IP address), YIADDR (Your IP address), SIADDR (Server IP address), CHADDR (Client hardware address).

**4).**

After a DHCP starvation attack and setting up a rogue DHCP server, the attacker can start **distributing IP addresses and other TCP/IP configuration settings to the network DHCP clients**. TCP/IP configuration settings include Default Gateway and DNS Server IP addresses. Network attackers can now **replace the original legitimate Default Gateway IP Address and DNS Server IP Address with their own IP Address**. Once the Default Gateway IP Address of the network devices are is changed, the network clients start sending the traffic destined to outside networks to the attacker's computer. The **attacker can now capture sensitive user data and launch a man-in-the-middle attack**. This is called as DHCP spoofing attack. Attacker can also set up a rogue DNS server and deviate the end user traffic to fake web sites and launch phishing attacks.

**5).**

the only thing he need to do is:

1.View initial ARP cache on the Victim PC

2.View initial ARP cache on the Attacker PC

3.View initial MAC Address-Table on the Cisco Catalyst (switch)

**4.broadcast fake messages.**

Only need one message.

**6).**

**True,**

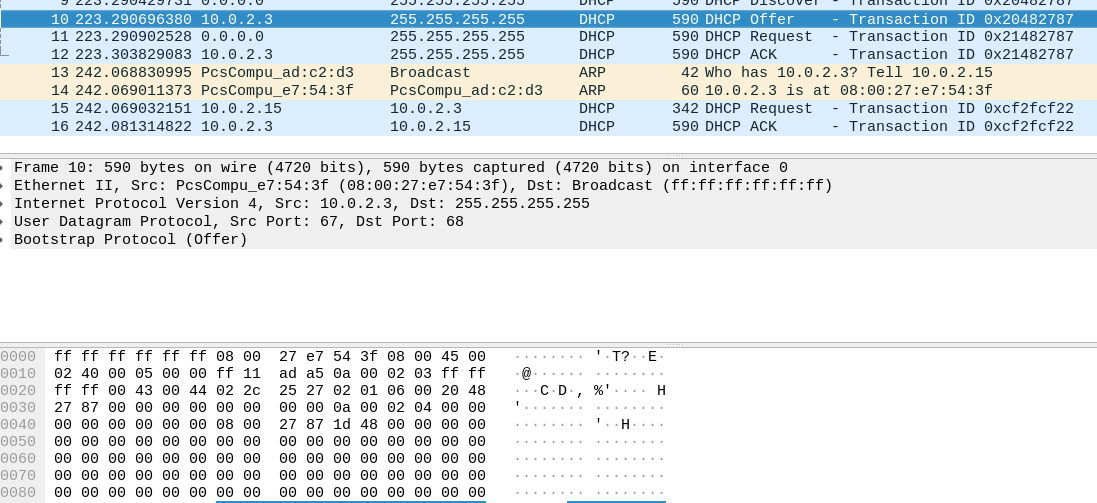
A rogue DHCP server is a DHCP server on a network which is not under the administrative control of the network staff. It is a network device such as a **modem or a router** connected to the network by a user who may be either **unaware of the consequences of their actions** or may be knowingly **using it for network attacks** such as man in the middle. Some kind of computer viruses or malicious software have been found to set up a rogue DHCP, especially for those classified in the category.

**7).**

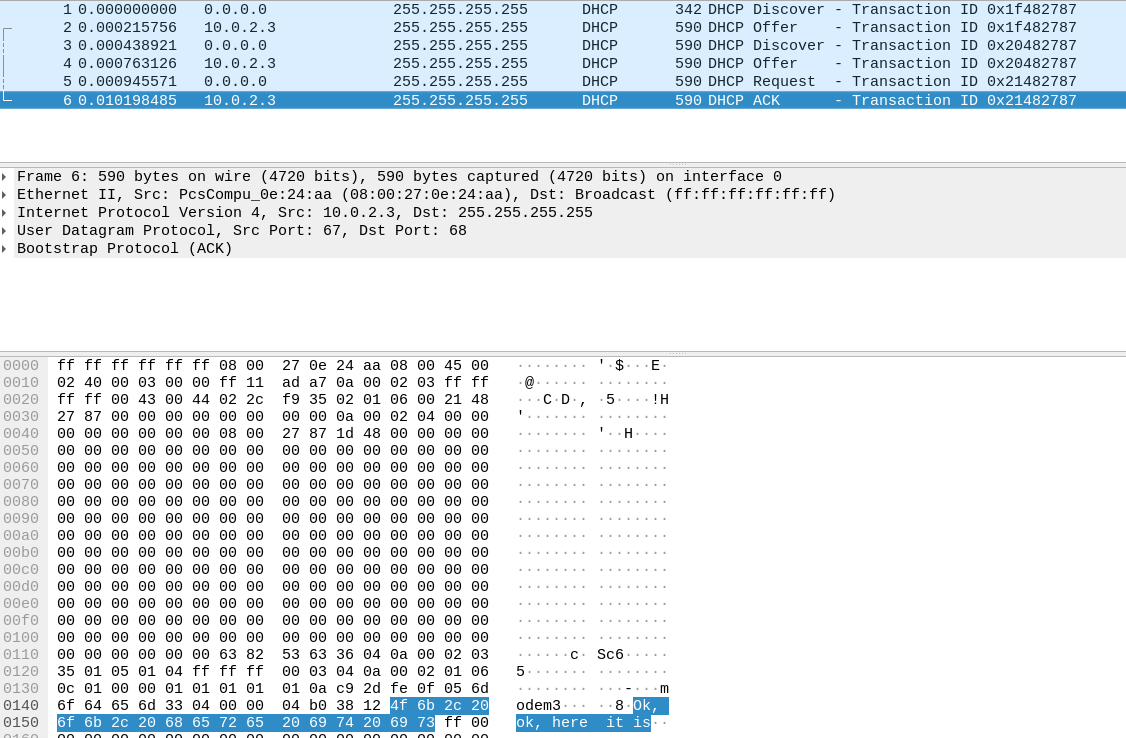
DHCP snooping is built on the switch by creating a bindings table block legitimate DHCP servers to mitigate issues with rogue DHCP servers.

**Q2.**

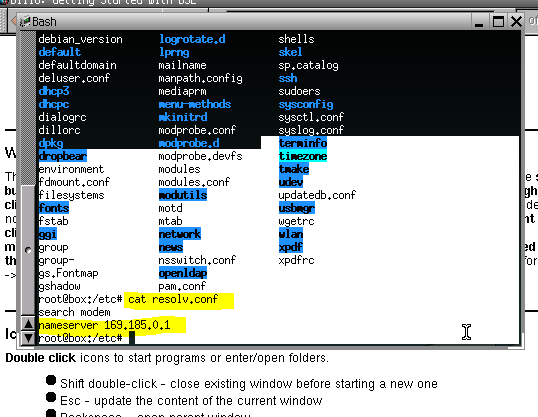
**Mode = Allow Any:**



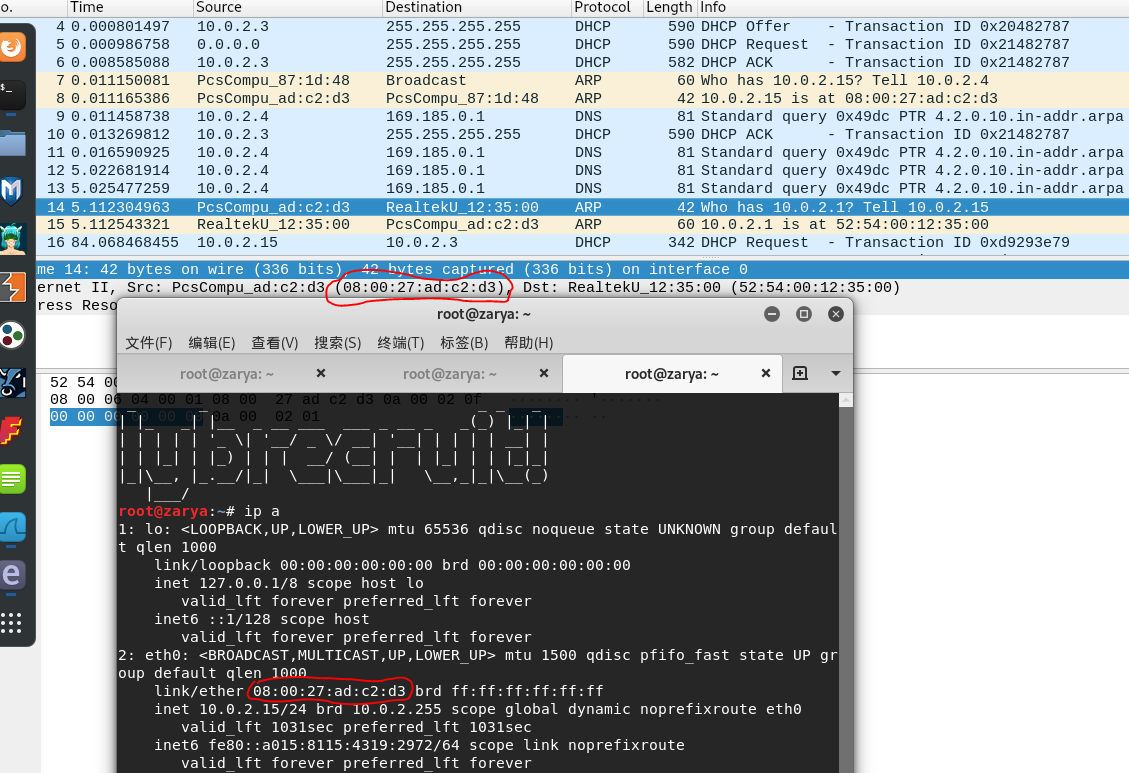
**Mode = Deny:**



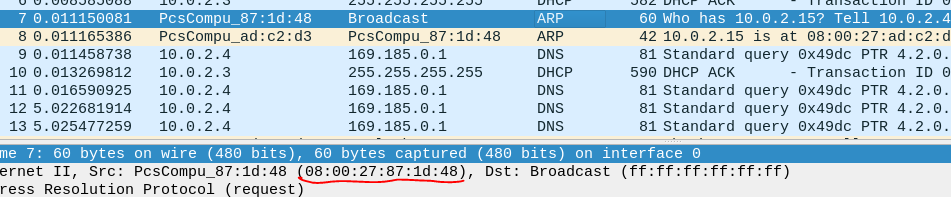
**Q3.**



**Fake:**



**REAL:**



**Q4.**

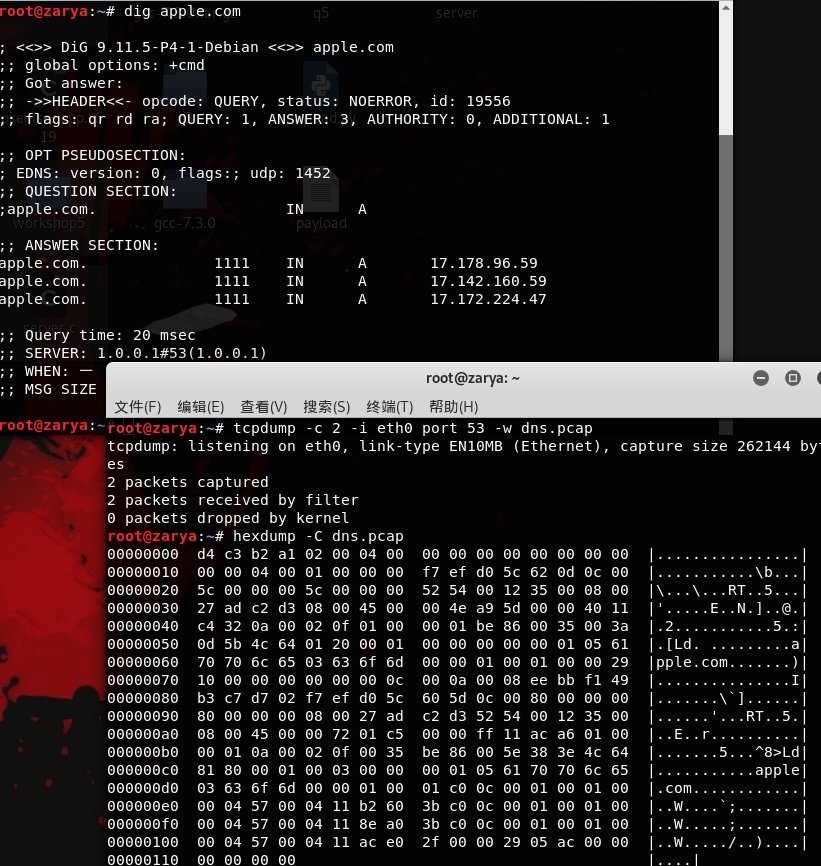
**Exit after capturing 2 packets: -c 2**

**Capture on eth0 interface: -i eth0**

**Only UDP packets with port 53: port 53**

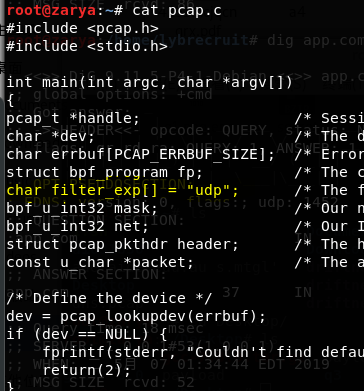
**Save captured packets to dns.pcap: -w dns.pcap**

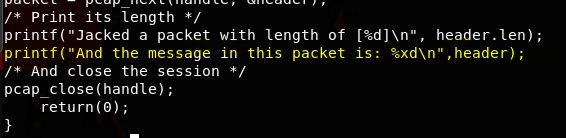
**arbitrary DNS lookups: dig examples.com**



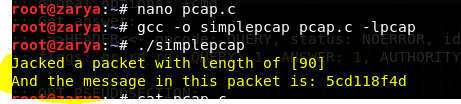
**Q5.**

**Code:**





**Sample output:**



**Reference:**

<http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>

<https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html>

<http://www.pearsonitcertification.com/articles/article.aspx?p=2474170>