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,

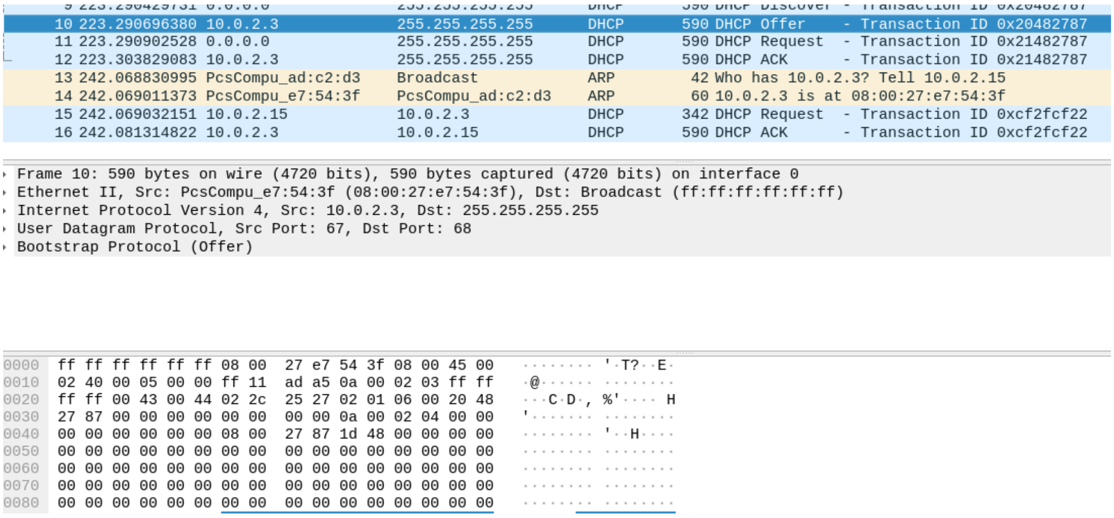
A rogue DHCP server is a DHCP server on a network which is not under the administrative control of the network staff. It is a network device such as a **modem or a router** connected to the network by a user who may be either **unaware of the consequences of their actions** or may be knowingly **using 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:

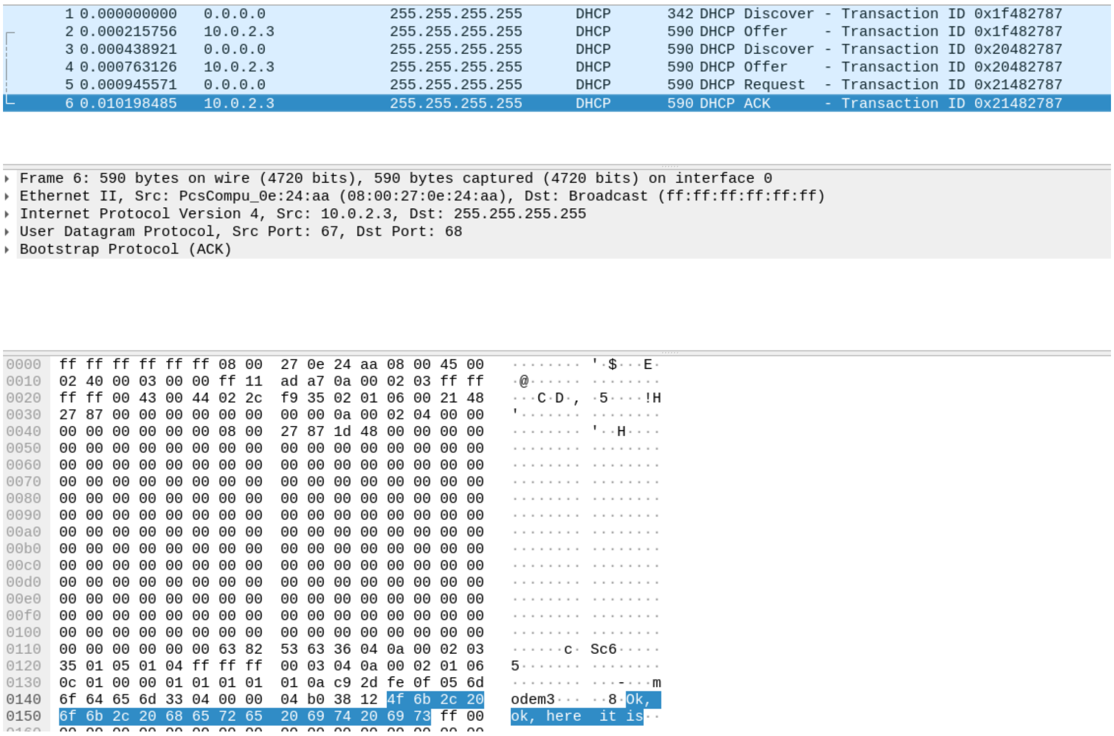


```
   9 223.290429731 0.0.0.0            255.255.255.255      DHCP     590 DHCP Discover  - Transaction ID 0x20482787
  10 223.290696380 10.0.2.3           255.255.255.255      DHCP     590 DHCP Offer     - Transaction ID 0x20482787
  11 223.290902528 0.0.0.0            255.255.255.255      DHCP     590 DHCP Request   - Transaction ID 0x21482787
  12 223.303829083 10.0.2.3           255.255.255.255      DHCP     590 DHCP ACK       - Transaction ID 0x21482787
  13 242.068830995 PcsCompu_ad:c2:d3  Broadcast            ARP       42 Who has 10.0.2.3? Tell 10.0.2.15
  14 242.069011373 PcsCompu_e7:54:3f  PcsCompu_ad:c2:d3    ARP       60 10.0.2.3 is at 08:00:27:e7:54:3f
  15 242.069032151 10.0.2.15          10.0.2.3             DHCP     342 DHCP Request   - Transaction ID 0xcf2fcf22
  16 242.081314822 10.0.2.3           10.0.2.15            DHCP     590 DHCP ACK       - Transaction ID 0xcf2fcf22
```

```
▸ Frame 10: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_e7:54:3f (08:00:27:e7:54:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Bootstrap Protocol (Offer)
```

```
0000  ff ff ff ff ff ff 08 00  27 e7 54 3f 08 00 45 00   ········ '·T?··E·
0010  02 40 00 05 00 00 ff 11  ad a5 0a 00 02 03 ff ff   ·@······ ········
0020  ff ff 00 43 00 44 02 2c  25 27 02 01 06 00 20 48   ···C·D·, %'····· H
0030  27 87 00 00 00 00 00 00  00 00 0a 00 02 04 00 00   '······· ········
0040  00 00 00 00 00 00 08 00  27 87 1d 48 00 00 00 00   ········ '··H····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Mode = Deny:

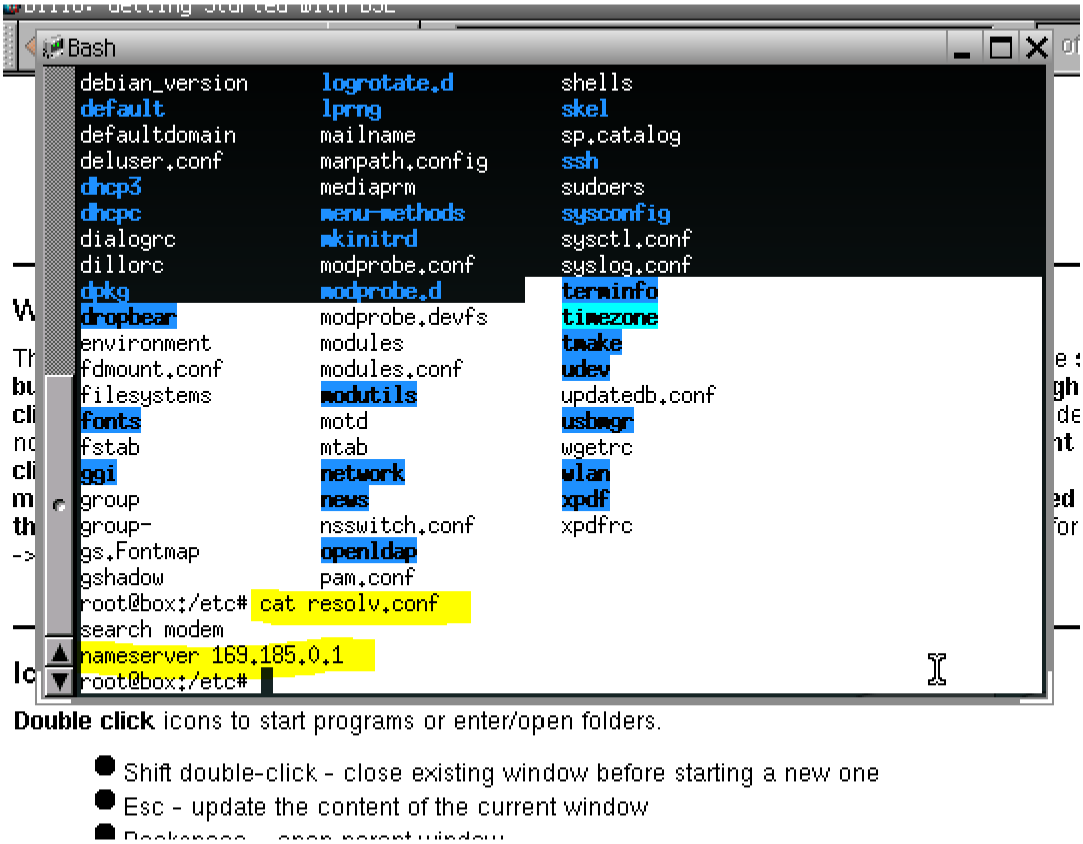


```
      1 0.000000000   0.0.0.0             255.255.255.255     DHCP      342 DHCP Discover - Transaction ID 0x1f482787
      2 0.000215756   10.0.2.3            255.255.255.255     DHCP      590 DHCP Offer    - Transaction ID 0x1f482787
      3 0.000438921   0.0.0.0             255.255.255.255     DHCP      590 DHCP Discover - Transaction ID 0x20482787
      4 0.000763126   10.0.2.3            255.255.255.255     DHCP      590 DHCP Offer    - Transaction ID 0x20482787
      5 0.000945571   0.0.0.0             255.255.255.255     DHCP      590 DHCP Request  - Transaction ID 0x21482787
      6 0.010198485   10.0.2.3            255.255.255.255     DHCP      590 DHCP ACK      - Transaction ID 0x21482787
```

```
▸ Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_0e:24:aa (08:00:27:0e:24:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Bootstrap Protocol (ACK)
```

```
0000  ff ff ff ff ff ff 08 00  27 0e 24 aa 08 00 45 00   ········ '·$···E·
0010  02 40 00 03 00 00 ff 11  ad a7 0a 00 02 03 ff ff   ·@······ ········
0020  ff ff 00 43 00 44 02 2c  f9 35 02 01 06 00 21 48   ···C·D·, ·5····!H
0030  27 87 00 00 00 00 00 00  00 00 0a 00 02 04 00 00   '······· ········
0040  00 00 00 00 00 00 08 00  27 87 1d 48 00 00 00 00   ········ '··H····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 36 04 0a 00 02 03   ······c· Sc6·····
0120  35 01 05 01 04 ff ff ff  00 03 04 0a 00 02 01 06   5······· ········
0130  0c 01 00 00 01 01 01 01  01 0a c9 2d fe 0f 05 6d   ········ ···-···m
0140  6f 64 65 6d 33 04 00 00  04 b0 38 12 4f 6b 2c 20   odem3··· ··8·Ok, 
0150  6f 6b 2c 20 68 65 72 65  20 69 74 20 69 73 ff 00   ok, here  it is··
```

Q3.

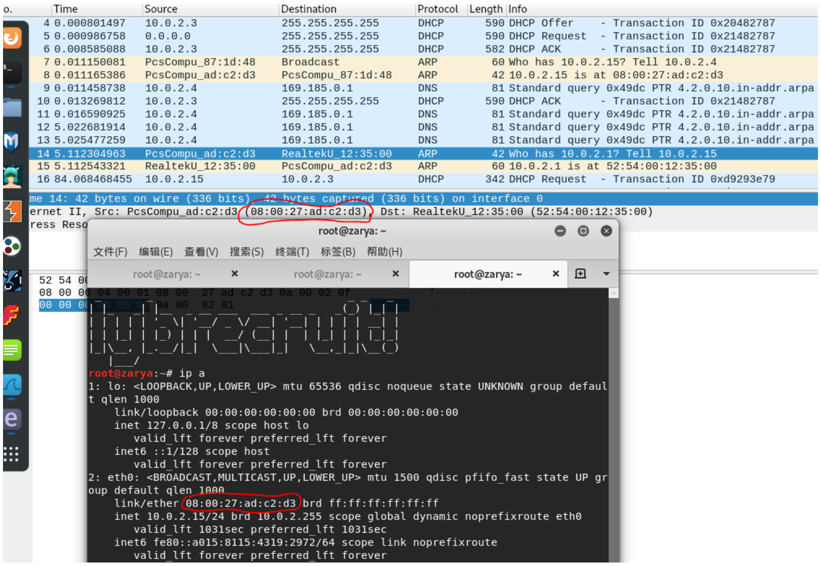


```
debian_version      logrotate.d         shells
default             lprng               skel
defaultdomain       mailname            sp.catalog
deluser.conf        manpath.config      ssh
dhcp3               mediaprm            sudoers
dhcpc               menu-methods        sysconfig
dialogrc            mkinitrd            sysctl.conf
dillorc             modprobe.conf       syslog.conf
dpkg                modprobe.d          terminfo
dropbear            modprobe.devfs      timezone
environment         modules             tmake
fdmount.conf        modules.conf        udev
filesystems         modutils            updatedb.conf
fonts               motd                usbmgr
fstab               mtab                wgetrc
ggi                 network             wlan
group               news                xpdf
group-              nsswitch.conf       xpdfrc
gs.Fontmap          openldap
gshadow             pam.conf
root@box:/etc# cat resolv.conf
search modem
nameserver 169.185.0.1
root@box:/etc# 
```

Double click icons to start programs or enter/open folders.

- Shift double-click - close existing window before starting a new one
- Esc - update the content of the current window

Fake:

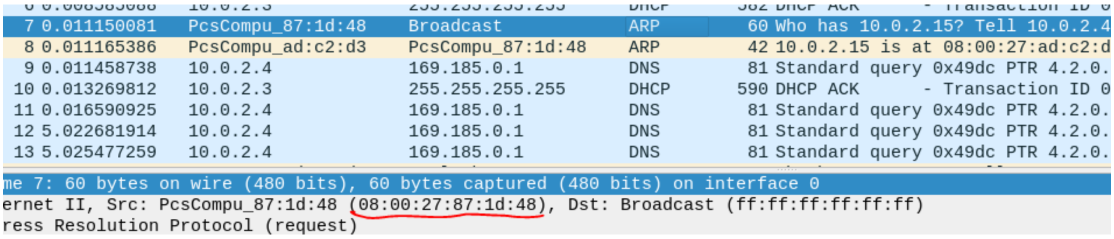


```
o.      Time            Source              Destination         Protocol  Length Info
      4 0.000801497     10.0.2.3            255.255.255.255     DHCP         590 DHCP Offer    - Transaction ID 0x20482787
      5 0.000986758     0.0.0.0             255.255.255.255     DHCP         590 DHCP Request  - Transaction ID 0x21482787
      6 0.008585088     10.0.2.3            255.255.255.255     DHCP         582 DHCP ACK      - Transaction ID 0x21482787
      7 0.011150081     PcsCompu_87:1d:48   Broadcast           ARP           60 Who has 10.0.2.15? Tell 10.0.2.4
      8 0.011165386     PcsCompu_ad:c2:d3   PcsCompu_87:1d:48   ARP           42 10.0.2.15 is at 08:00:27:ad:c2:d3
      9 0.011458738     10.0.2.4            169.185.0.1         DNS           81 Standard query 0x49dc PTR 4.2.0.10.in-addr.arpa
     10 0.013269812     10.0.2.3            255.255.255.255     DHCP         590 DHCP ACK      - Transaction ID 0x21482787
     11 0.016590925     10.0.2.4            169.185.0.1         DNS           81 Standard query 0x49dc PTR 4.2.0.10.in-addr.arpa
     12 5.022681914     10.0.2.4            169.185.0.1         DNS           81 Standard query 0x49dc PTR 4.2.0.10.in-addr.arpa
     13 5.025477259     10.0.2.4            169.185.0.1         DNS           81 Standard query 0x49dc PTR 4.2.0.10.in-addr.arpa
     14 5.112304963     PcsCompu_ad:c2:d3   RealtekU_12:35:00   ARP           42 Who has 10.0.2.1? Tell 10.0.2.15
     15 5.112543321     RealtekU_12:35:00   PcsCompu_ad:c2:d3   ARP           60 10.0.2.1 is at 52:54:00:12:35:00
     16 84.068468455    10.0.2.15           10.0.2.3            DHCP         342 DHCP Request  - Transaction ID 0xd9293e79
me 14: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
ernet II, Src: PcsCompu_ad:c2:d3 (08:00:27:ad:c2:d3), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
ress Reso
```

root@zarya: ~

```
52 54 00
08 00 06 04 00 01 08 00  27 ad c2 d3 0a 00 02 0f
00 00 00          0a 00  02 01
root@zarya:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:ad:c2:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 1031sec preferred_lft 1031sec
    inet6 fe80::a015:8115:4319:2972/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

REAL:



```
  6 0.008585088   10.0.2.3            255.255.255.255    DHCP      582 DHCP ACK       - Transaction ID 0
  7 0.011150081   PcsCompu_87:1d:48   Broadcast          ARP        60 Who has 10.0.2.15? Tell 10.0.2.4
  8 0.011165386   PcsCompu_ad:c2:d3   PcsCompu_87:1d:48  ARP        42 10.0.2.15 is at 08:00:27:ad:c2:d
  9 0.011458738   10.0.2.4            169.185.0.1        DNS        81 Standard query 0x49dc PTR 4.2.0.
 10 0.013269812   10.0.2.3            255.255.255.255    DHCP      590 DHCP ACK       - Transaction ID 0
 11 0.016590925   10.0.2.4            169.185.0.1        DNS        81 Standard query 0x49dc PTR 4.2.0.
 12 5.022681914   10.0.2.4            169.185.0.1        DNS        81 Standard query 0x49dc PTR 4.2.0.
 13 5.025477259   10.0.2.4            169.185.0.1        DNS        81 Standard query 0x49dc PTR 4.2.0.
me 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
ernet II, Src: PcsCompu_87:1d:48 (08:00:27:87:1d:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
ress Resolution Protocol (request)
```

Q4.

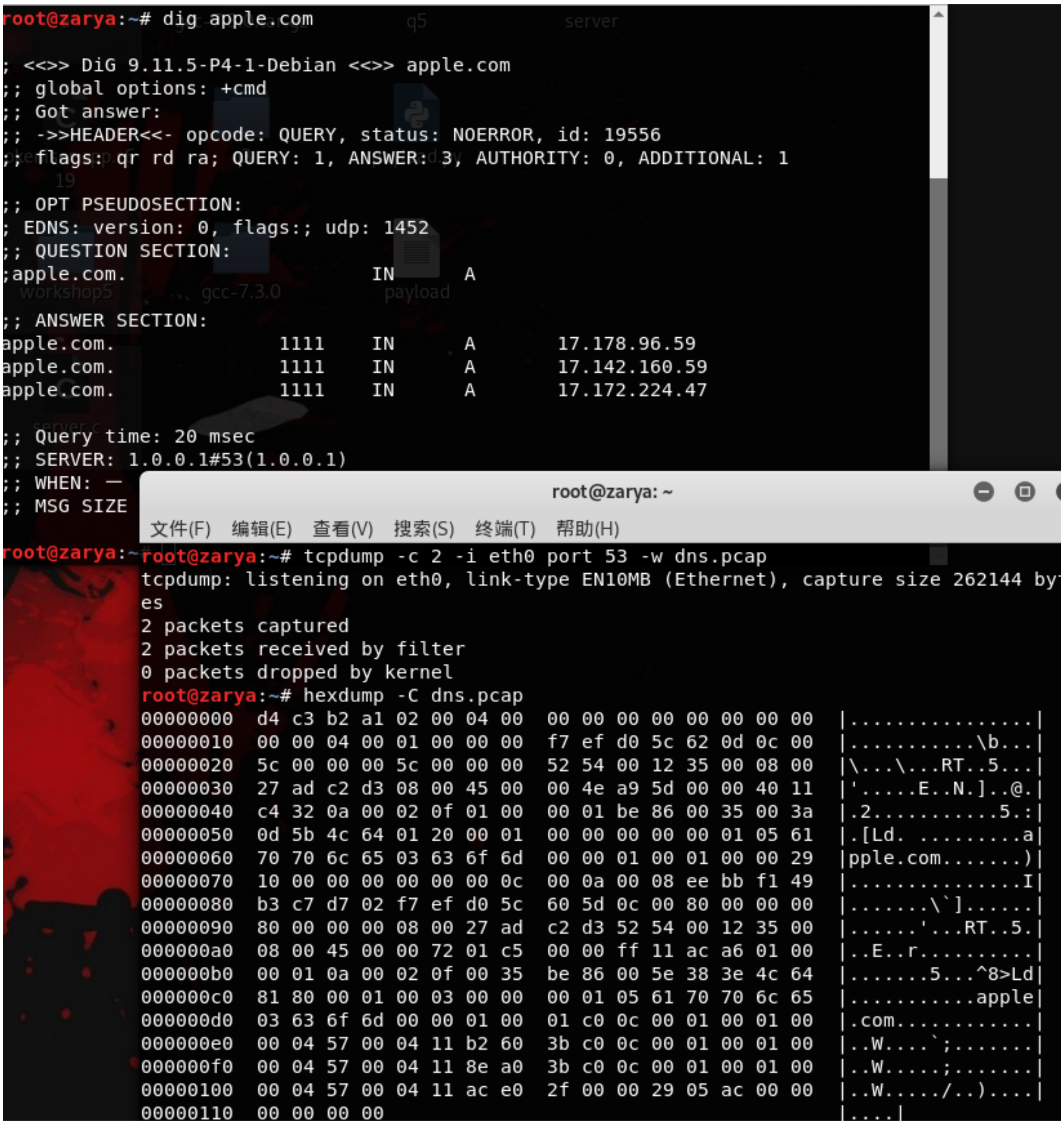
Exit after capturing 2 packets: -c 2

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

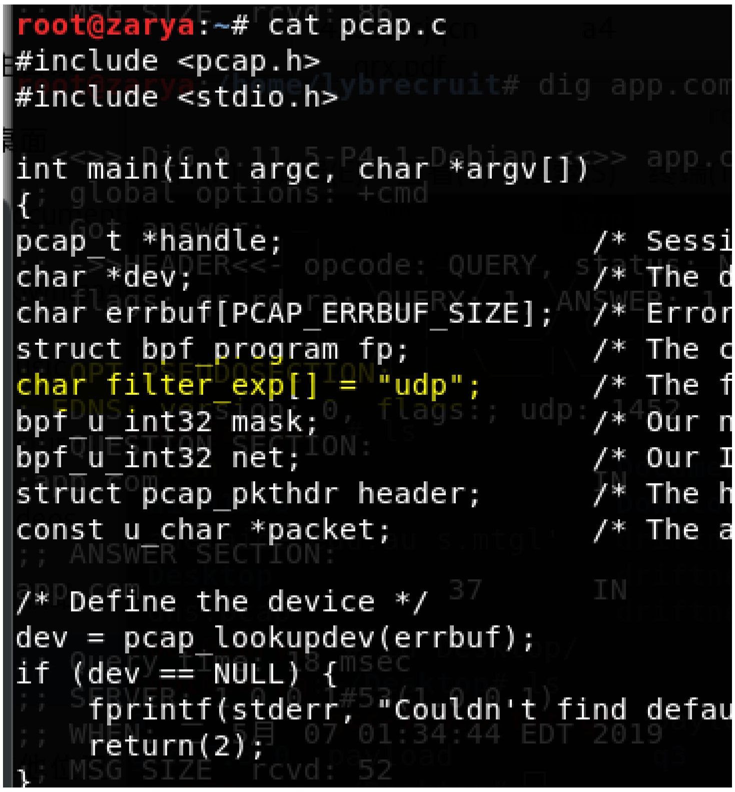


```
root@zarya:~# dig apple.com

; <<>> DiG 9.11.5-P4-1-Debian <<>> apple.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19556
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;apple.com.                     IN      A

;; ANSWER SECTION:
apple.com.              1111    IN      A       17.178.96.59
apple.com.              1111    IN      A       17.142.160.59
apple.com.              1111    IN      A       17.172.224.47

;; Query time: 20 msec
;; SERVER: 1.0.0.1#53(1.0.0.1)
;; WHEN: —
;; MSG SIZE

root@zarya:~
```

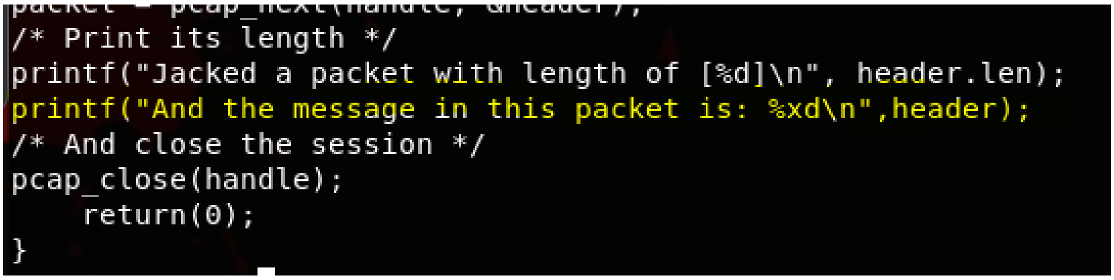
```
root@zarya:~# tcpdump -c 2 -i eth0 port 53 -w dns.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 by
es
2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@zarya:~# hexdump -C dns.pcap
00000000  d4 c3 b2 a1 02 00 04 00  00 00 00 00 00 00 00 00  |................|
00000010  00 00 04 00 01 00 00 00  f7 ef d0 5c 62 0d 0c 00  |...........\b...|
00000020  5c 00 00 00 5c 00 00 00  52 54 00 12 35 00 08 00  |\...\...RT..5...|
00000030  27 ad c2 d3 08 00 45 00  00 4e a9 5d 00 00 40 11  |'.....E..N.]..@.|
00000040  c4 32 0a 00 02 0f 01 00  00 01 be 86 00 35 00 3a  |.2...........5.:|
00000050  0d 5b 4c 64 01 20 00 01  00 00 00 00 00 01 05 61  |.[Ld. .........a|
00000060  70 70 6c 65 03 63 6f 6d  00 00 01 00 01 00 00 29  |pple.com.......)|
00000070  10 00 00 00 00 00 00 0c  00 0a 00 08 ee bb f1 49  |...............I|
00000080  b3 c7 d7 02 f7 ef d0 5c  60 5d 0c 00 80 00 00 00  |.......\`]......|
00000090  80 00 00 00 08 00 27 ad  c2 d3 52 54 00 12 35 00  |......'...RT..5.|
000000a0  08 00 45 00 00 72 01 c5  00 00 ff 11 ac a6 01 00  |..E..r..........|
000000b0  00 01 0a 00 02 0f 00 35  be 86 00 5e 38 3e 4c 64  |.......5...^8>Ld|
000000c0  81 80 00 01 00 03 00 00  00 01 05 61 70 70 6c 65  |...........apple|
000000d0  03 63 6f 6d 00 00 01 00  01 c0 0c 00 01 00 01 00  |.com............|
000000e0  00 04 57 00 04 11 b2 60  3b c0 0c 00 01 00 01 00  |..W....`;.......|
000000f0  00 04 57 00 04 11 8e a0  3b c0 0c 00 01 00 01 00  |..W.....;.......|
00000100  00 04 57 00 04 11 ac e0  2f 00 00 29 05 ac 00 00  |..W...../..)....|
00000110  00 00 00 00                                       |....|
```

Q5.

Code:

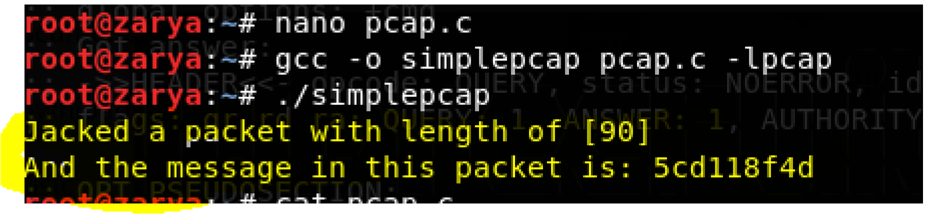


```
root@zarya:~# cat pcap.c
#include <pcap.h>
#include <stdio.h>

int main(int argc, char *argv[])
{
pcap_t *handle;                 /* Sessi
char *dev;                      /* The d
char errbuf[PCAP_ERRBUF_SIZE];  /* Error
struct bpf_program fp;          /* The c
char filter_exp[] = "udp";      /* The f
bpf_u_int32 mask;               /* Our n
bpf_u_int32 net;                /* Our I
struct pcap_pkthdr header;      /* The h
const u_char *packet;           /* The a

/* Define the device */
dev = pcap_lookupdev(errbuf);
if (dev == NULL) {
    fprintf(stderr, "Couldn't find defau
    return(2);
}
```



```
packet = pcap_next(handle, &header);
/* Print its length */
printf("Jacked a packet with length of [%d]\n", header.len);
printf("And the message in this packet is: %xd\n",header);
/* And close the session */
pcap_close(handle);
    return(0);
}
```

Sample output:



```
root@zarya:~# nano pcap.c
root@zarya:~# gcc -o simplepcap pcap.c -lpcap
root@zarya:~# ./simplepcap
Jacked a packet with length of [90]
And the message in this packet is: 5cd118f4d
root@zarya:~# cat pcap.c
```

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