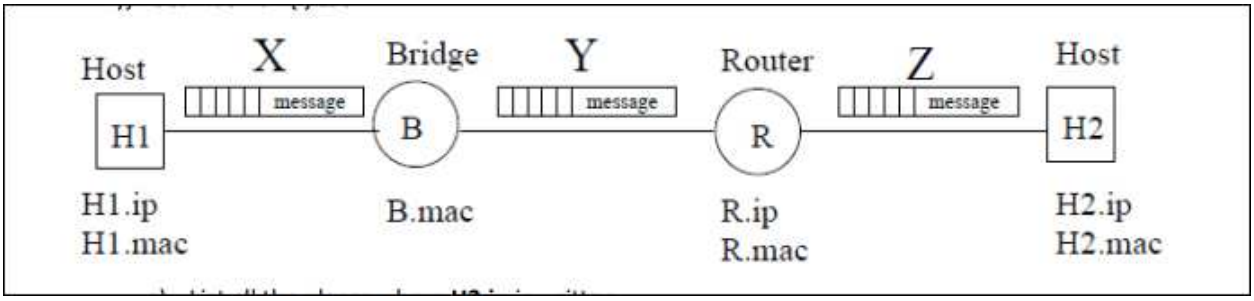
Activity 2: – TCP/IP Concepts and Protocols (Ethical Hacking)

Md. Anisur Rahman

Exercise 1: Review Layering Concepts

OSI Layers	TCP Layers	Why used (main functions)	PDU Names	Example Protocols	Connection with security
Application	Application	Data show	Data	TELNET, FTP , SMTP, TFTP	DDos, SQL injections Security.
Presentation		Data rearrangement	Data Rearrange	SSL, HTTP, FTP	SSL, HTTPS
Session		Data format , Time Stream	Data Format	ASP, PPTP	OpSec
Transport	Transport	Fragmentation	Segments	TCP, SPX	TLS
Network	Network	Next Hop Packet Transfer	Packets	IP, ICMP	IPsec
Data link	Network Interface	Frame header to Packet	Frames	Ethernet	VPN
Physical		Bit to make frame	Bits, signal, Symbols		

Exercise 2: Understanding Packet Headers



a) **H2.ip** is written in Router (R) and Host (H1)
Header: PDU is packet
Header's format: specified
Protocol: Internet protocol (IP), UDP, TCP, ICMP
Bytes: 20 bytes
Layers: Layer 3 and Layer 2, {}

b) **R1.ip** is written in Host (H1)
Header: PDU is data
Header's format: specified
Layers: Layer 3

c) **B.mac** is written in R, H1
Header: PDU is packet
Header's format: specified
Protocol: Internet protocol (IP), ARP
Layers: Layer 3 and Layer 2

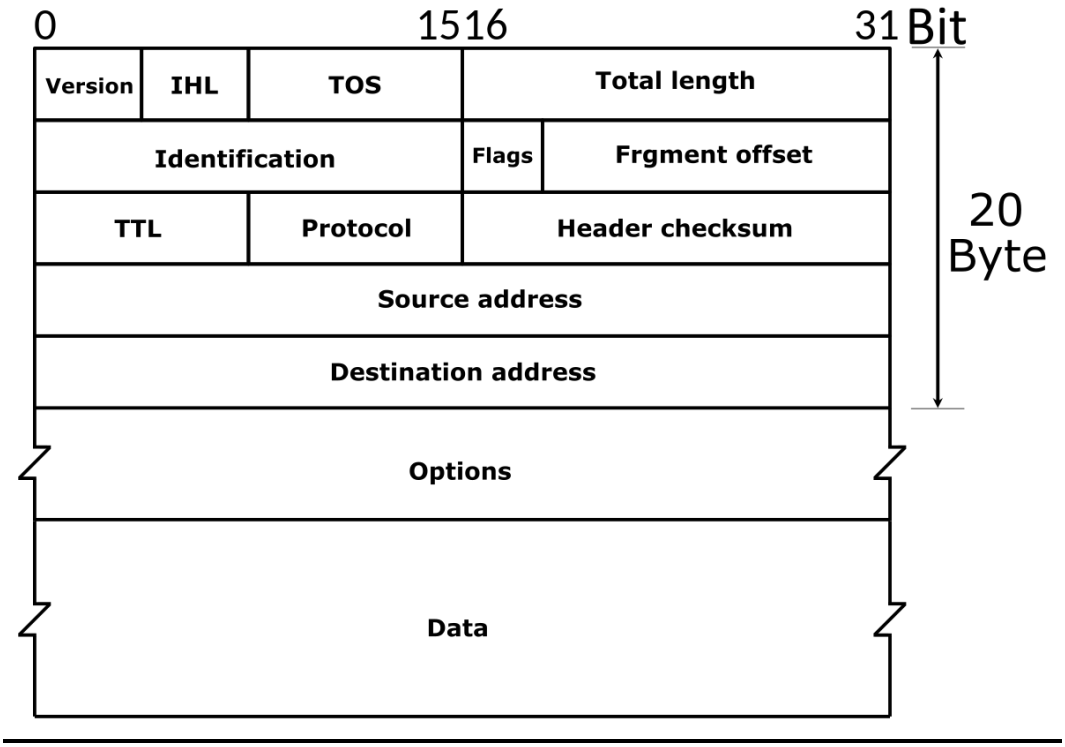
d) **R1.mac** is written in H1 and B
Header's format: specified
Protocol: Internet protocol (IP), ARP
Layers: Layer 3 and Layer 2

e) **H2.mac** is written in R1
Header's format: specified
Layers: Layer 3 and Layer 2

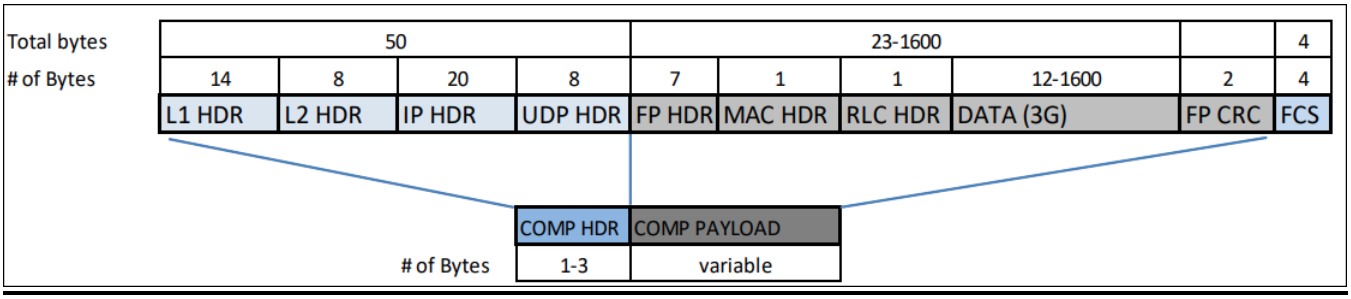
f) 8888 port is written in H1
g) 9999 port is written in H2

Exercise 3: Header vs. Payload:

Header:



Payload:



Assume that no optional fields of the IP header are in use (i.e. IP header is 20 bytes)

The original datagram was 1000 bytes, subtracting 20 bytes for header,

That leaves 1000 - 20 = 980 bytes of data.

Assume the ID of the original packet is 'x' with an Maximum of only of 500 bytes,

500 - 20 = 480 bytes of data may be transmitted in each packet.

Therefore, ceiling (1000 / 480) = 2 packets are needed to carry the data.

The packets will have the following characteristics (NOTE: offset is measured in 8 byte blocks, you don't need to specify Total_len)

Packet 1: ID=x, Total_len=500, MF=1, Frag_offset=0

Packet2: ID=x,Total_len=500,MF=1,Frag_offset=60

Packets Sizes: 480 bytes Transmitted.

Exercise 4: DNS Record Structure

Name Server Variable	Resource Record
A_{root}	{com, a.gtld-servers.net, NS, IN}
A_{root}	{a.gtld-servers.net, 192.5.6.30, A, IN}
A_{com}	{google.com, ns1.google.com, NS, IN}
A_{com}	{ns1.google.com, 216.239.32.10, A, IN}
$A_{google.com}$	{www.google.com, 66.102.7.104, A, IN}
$A_{google.com}$	{mail.google.com, 66.102.7.83, A, IN}

a)

Acom: hostname=a.gtld-servers.net,

IP address=192.5.6.30

Agoogle.com: hostname=ns1.google.com,

IP address=216.239.32.10

b)

- C queries L to resolve www.google.com
- L queries Aroot at 198.41.0.4 to resolve www.google.com.
- Aroot returns {com, a.gtld-servers.net, NS, IN} and {a.gtld-servers.net, 192.5.6.30, A, IN}.
- L queries Acom at 192.5.6.30 to resolve www.google.com
- Acom returns {google.com, ns1.google.com, NS, IN} and {ns1.google.com, 216.239.32.10, A, IN}
- L queries Agoogle.com at 216.239.32.10 to resolve www.google.com
- Agoogle.com returns {www.google.com, 66.102.7.83, A, IN}
- L returns 66.102.7.83 to C

Exercise 5: DNS Record Structure

a)

Need to provide registrar with names and IP addresses of your authoritative name server. So the company needs to provide two RR records:

- flashBd.com, dns.flashBD.com
- dns.flashBD.com, 128.119.12.40

b)

- flashBD.com, 128.119.12.55
- flashBD.com, 128.119.12.56
- www.flashBD.com, flashBD.com
- flashBD.com, mail.flashBD.com
- mail.flashBD.com, 128.119.12.60

Exercise 6: IP Fragmentation

Assume that no optional fields of the IP header are in use (i.e. IP header is 20 bytes)

The original datagram was 5000 bytes, subtracting 20 bytes for header, that leaves 4980 bytes of data.

Assume the ID of the original packet is 'x'

With an MTU of 1500 bytes, 1500 - 20 = 1480 bytes of data may be transmitted in each packet

Therefore, ceiling (4980 / 1480) = 3 packets are needed to carry the data.

The packets will have the following characteristics

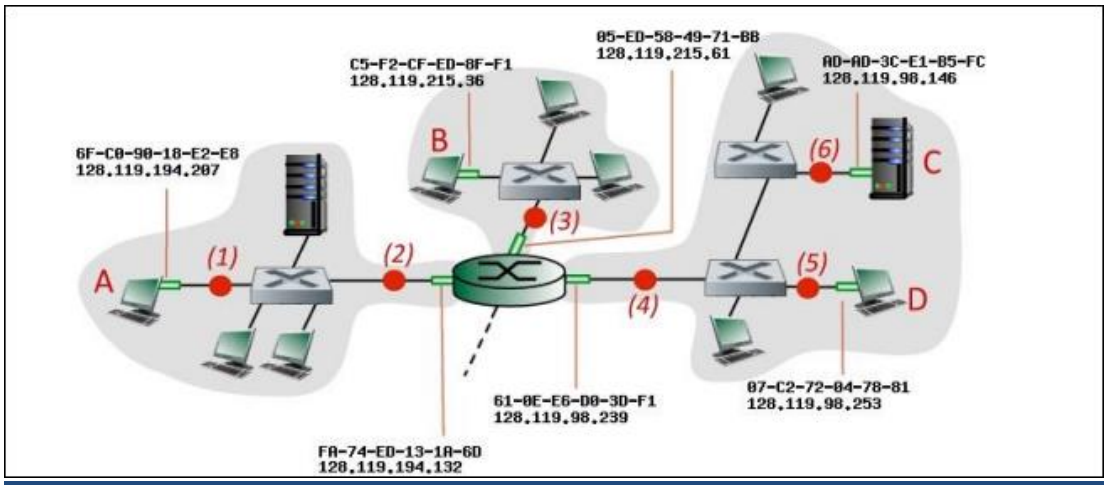
(NOTE: offset is measured in 8 byte blocks; you don't need to specify Total_len)

Packet 1: ID=x, Total_len=500, MF=1, Frag_offset=0

Packet 2: ID=x, Total_len=500, MF=1, Frag_offset=60

Packet 3: ID=x, Total_len=500, MF=1, Frag_offset=120

Exercise 7: ARP & MAC Table



i) **IP address** is 128.119.194.132 (interface 2)

ii) **Mac Source**: 6F-C8-18-E2-E8

Destination Address: 128.119.98.146

Points 6:

IP Source: 128.119.98.146

Destination Address: 128.119.215.61 (3), 128.119.194.132 (2), 128.119.194.287 (1).

Points 4:

IP Source: 128.119.98.239

Destination Address: 128.119.215.61 (3), 128.119.194.132 (2), 128.119.194.287 (1).

Points 2:

IP Source: 128.119.194.132

Destination Address: 128.119.215.61 (3), 128.119.98.239 (4), 128.119.98.253 (5), 128.119.98.146 (6).

Points 1:

IP Source: 128.119.194.287

Destination Address: 128.119.215.61 (3), 128.119.98.239 (4), 128.119.98.253 (5), 128.119.98.146 (6).

Exercise 8: Short Questions

a) Netstat command. Port No. 110
b) Pop3 on port 110 is the older of the two popular protocols used to retrieve eMail from remote mail servers. (The newer protocol, imap, the Internet message access protocol, uses port 143.
c) The answer is DNS is mostly UDP Port 53.
d) TCP 3-Way Handshake (SYN, SYN-ACK, ACK). 1 and 2
e) Type 8
f) Type 3
g) ACK - The acknowledgment flag is used to acknowledge the successful receipt of a packet. As we can see from the diagram above, the receiver sends an ACK as well as a SYN in the second step of the three way handshake process to tell the sender that it received its initial packet.
h) An ICMPv6 Time Exceeded message is sent by a router when the Hop Limit field of the IPv6 header reaches 0 (ICMPv6 Code = 0) or when the receiver's fragment reassembly timeout (senders can still fragment under IPv6) has expired (ICMPv6 Code = 1).
The format is the same as for the ICMPv6 Destination Unreachable message, except that the Type is 3.
i) ARP poisoning occurs at the Data Link layer.
j) HTTP GET Flood An HTTP GET Flood is a layer 7
application layer DDoS attack method in which attackers send a huge flood of requests to the server to overwhelm its resources. As a result, the server cannot respond to legitimate requests from the server.
k) Source routing was designed to enable individuals to specify the route that a packet should take through a network or to allow users to bypass network problems or congestion.

l) **Private IP Range:**

Range from 10.0.0.0 to 10.255.255.255 - a 10.0.0.0 network with a 255.0.0.0

Range from 172.16.0.0 to 172.31.255.255 - a 172.16.0.0 network with a 255.240.0.0

Range from 192.168.0.0 to 192.168.255.255 range, which is a 192.168.0.0 network masked by 255.255.0.0.