## **Activity File: Networking Review**

### **Part One: HTTP**

Open reviewpackets.pcap.

* Filter for HTTP traffic.
* Make sure Name Resolution for Resolving Network Addresses is enabled.
* There should be four HTTP packets.

A. Answer the following questions on HTTP:

1. What does HTTP stand for?
   1. Hyper Text Transfer Protocol
2. What is the port number for HTTP?
   1. Port 80
3. What types of services does HTTP provide?
   1. Communicating and accessing resources on the internet
4. Which OSI layer does HTTP exist in?
   1. Layer 7: Application
5. What website is being accessed?
   1. example.com
6. What is the source port being used?
   1. 58424
7. What is the the port number range that this port is part of?
   1. This is a private port

B. Use a filter to find the count of ARP responses, and answer the following questions:

* What is the IP of the device that is responding? **10.0.0.32, which can be seen in the packet details, ARP reply.**
* To what IP is the device responding to? **10.0.0.31.**
* Write out in simple terms what has taken place, describing the request and response. **In this packet, 10.0.0.32 is telling 10.0.0.31 that its MAC address is a0:a4:c5:10:ac:c0.**

### **Part Three: DHCP**

Continue viewing the same PCAP.

* Filter for DHCP traffic.
* There should be four DHCP packets.

A. Answer the following questions on DHCP:

1. What does DHCP Stand for? **Dynamic Host Configuration Protocol**.
2. What service does DHCP provide? **DHCP dynamically assigns out IP addresses to devices on its network.**
3. What OSI Layer does DHCP exist in? **Layer 7: Application.**
4. What are the four steps of DHCP? **DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK.**

B. Use a filter to view the DHCP Discover, and answer the following questions on that packet:

1. What is the original source IP? **0.0.0.0.**
2. Why does it have that value? **Because the device does not have an IP address and is requesting one.**
3. What is the original destination IP **255.255.255.255.**
4. What does that value signify? **This IP signifies a broadcast request, broadcasting the request across the local network.**

C. Use a filter to view the DHCP ACK, and answer the following questions on that packet.

1. Explain in simple terms what is happening in this packet: **This is the final confirmation from the DHCP server that the IP and DHCP lease have been provided.**
2. Define the term "DHCP lease." **The period of time for which the DHCP server issues out an IP address.**
3. What is the DHCP lease time provided in this packet? **Under IP address lease time, it displays seven days.**

### **Part Four: TCP and UDP**

Continue viewing the same PCAP.

* Filter for the following IP address: 185.42.236.155.
* There should be five packets.

A. Answer the following questions on TCP:

1. What does TCP stand for? **Transmission Control Protocol**.
2. Is TCP connection-oriented or connection-less? **Connection-oriented**.
3. What OSI Layer does tcp exist in? **Layer 4: Transport**.
4. What are the steps in a TCP connection? **SYN > SYN/ACK > ACK**
5. What are the steps in a TCP termination? **FIN > ACK > FIN > ACK.**
6. What steps do you see in the packets displayed? **SYN > SYN/ACK > ACK.**
7. What type of activity/protocol is TCP establishing a connection for? **HTTP**.
8. What is the website name that is being accessed after the TCP connection? **sportingnews.com**.

B. Answer the following questions on UDP:

1. What does UDP stand for? **User Datagram Protocol**.
2. Is UDP connection-oriented or connection-less? **Connection-less.**
3. What type of services is UDP good for? **UDP can be beneficial when some data loss is okay, such as in video streaming.**

### **Part Five: Network Devices, Topologies, and Routing**

Open reviewdoc.pdf and answer the following questions:

* **Topologies**
  1. What are the Topologies for A, B, C?
  2. **A: Tree**
  3. **B:Hybrid**
  4. **C: Ring**
  5. What the advantages and disadvantages for each?
  6. **Tree**:  
     + Advantages: Easy to expand the network.
     + Disadvantages: If the top node is impacted, all devices below it are be impacted.
  7. **Hybrid**:  
     + The advantages and disadvantages depend on the types of networks combined.
  8. **Ring**:  
     + Advantages:  
       - Simple to build.
       - Does not require a central node to manage data transmission.
       - Adding devices to the network is easy.
     + Disadvantages:  
       - If any one device goes down, the entire network is affected. In other words, every device is a point of failure.
       - Latency is variable between devices on the network. For example, devices near one another will trade data quickly, but devices far away will experience high communication delay.
* **Network Devices**
  1. In the network devices illustration, what are numbers one through four?
  2. 1: Internet
  3. 2: Firewall
  4. 3: Router
  5. 4: Switch
  6. What does the dashed line represent in number five? **The separation from the WAN on the left, to the LAN on the right.**
  7. What is a load balancer? **A load balancer is an intelligent network security device that distributes incoming network traffic across multiple servers.**
  8. Where would you place a load balancer? **Load balancers are typically placed after a firewall, between #2 and #3 in the diagram.**
* **Network Routing**
  1. Which routing protocols use distance as criteria? **Distance-vector routing protocols include RIP and EIGRP.**
  2. Which routing protocols use speed as criteria? **Link-state routing protocols include OSPF.**
  3. Using the shortest number of hops, determine the shortest path from A to O: **A > C > F> J > M > O**
  4. Using the least time, determine the shortest path from A to O: **A > D > C > E > J > K > N > S > R > Q > P > O**

### **Part Six: Network Addressing:**

Answer the following questions:

1. Define binary. **Binary is a numeric system that uses only two digits. Binary is the most basic form that data travels along a network.**
2. What are the two binary states? **On (1) and off (0).**
3. What are IP addresses used for? **A numerical identifier associated with each device on a computer network.**
4. What are the two primary versions of IP addresses? **IPv4 and IPv6.**
5. How many octets are in a IPV4 address? **Four.**
6. Use a web tool to determine the IP of the following binary representation: 11000000.10101000.00100000.00101011. **192.168.32.43.**
7. What is the difference between primary and public IP addresses?

**A public IP address can be accessed through the internet, while a private IP address is assigned to a device in a private space such as an office or home. Typically, private IP addresses are not directly exposed to the internet, so other people cannot navigate to your personal device.**

1. What is CIDR? **Classless Inter-Domain Routing is a method for assigning out IP addresses.**
2. What is the range of IP addresses in: 192.18.65.0/24? **192.18.65.0 - 192.18.65.255.**