Cybersecurity

Activity File

Module 9 Day 2

Activity File: Networking Review Part 1

Part 1: HTTP

Open reviewpackets.pcapng.

- 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? HyperText Transfer Protocol
2. What is the port number for HTTP? 80 for HTTP, 443 for HTTPS.
3. What types of services does HTTP provide? HTTP provides services for viewing web pages.
4. Which OSI layer does HTTP exist in? Application
5. What website is being accessed? example.com
6. What is the source port being used? 58424
7. What is the port number range that this port is part of? Private/Dynamic port

B. Select packet number 419, which should be the first HTTP packet. View the packet details to answer the following questions:

- Under Ethernet II is a value of `Destination: Technico_65:1a:36 (88:f7:c7:65:1a:36)`.
    i. What does this value represent? MAC address
    ii. Which OSI layer does this exist in? Data Link
    iii. What networking devices use these values? Switches and NICs

Part 2: ARP

Continue viewing the same PCAP.

- Filter for ARP traffic.
- There should be 115 ARP packets.

A. Answer the following questions on ARP:

1. What does ARP stand for? Address Resolution Protocol
2. What service does ARP provide? Converts IPs to MAC addresses
3. Which OSI layer does ARP exist in? Data Link
4. What type of networking request does ARP first make? Broadcast

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

1. What is the IP of the device that is responding? 10.0.0.32
2. To what IP is the device responding?10.0.0.31
3. Write out in simple terms what has taken place, describing the request and response. 10.0.0.32 is telling 10.0.0.31 that it's MAC is a0:a4:c5:10:ac:c0

Part 3: 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? Dynamically assigns IPs to devices on the network.
3. Which OSI layer does DHCP exist in? Application
4. What are the four steps of DHCP? Discover, Offer, Request, 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? It does not have an IP yet.
3. What is the original destination IP? 255.255.255.255
4. What does that value signify? It is broadcasting across the network.

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

1. In simple terms, what is happening in this packet? Final confirmation
2. What is DHCP lease? The time to live of the IP address
3. What is the DHCP lease time provided in this packet? 7 days

Part 4: 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 connectionless? Connection-oriented
3. Which OSI layer does TCP exist in? 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 appear in the packets displayed? SYN > SYN/ACK > ACK
7. For what type of activity/protocol is TCP establishing a connection? HTTP
8. What is the website name 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 connectionless? Connectionless
3. What type of services would UDP provide a benefit for? Video and gaming

Part 5: Network Addressing

Answer the following questions.

1. What is binary? Basic computer readable language
2. What are the two binary states? 0 and 1
3. What are IP addresses used for? Identifying devices on a network
4. What are the two primary versions of IP addresses? IPV4 and IPV6
5. How many octets are in an IPv4 address? 4
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? Public IP is accessed through the internet, a private IP is assigned within the LAN and are not typically exposed to the internet.
8. What is CIDR? Classless Inter-Domain Routing it is used to assign IPs
9. What is the range of IP addresses in `192.18.65.0/24`? 192.18.65.0 - 192.18.65.255.