**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **03/August/2020** | **Name:** | **Prashantha naik** |
| **Course:** | **Coursera** | **USN:** | **4al17ec074** |
| **Topic:** | **Network Security &**  **Database Vulnerabilities** | **Semester & Section:** | **6th b** |
| **GitHub Repository:** | **prashanth\_course** |  |  |

|  |
| --- |
| **SESSION DETAILS** |
| **Image of session** |
| **Report – Report can be typed or hand written for up to two pages.**  **Ethernet networks work, describe the difference between the Layer 2 and Layer 3 addressing schemes. Greetings. Today we're going to discuss Ethernet and Local Area Networks. This lecture was developed by Moises Monge and is being presented by Ben Briggs. Let's talk about ethernet and LAN. This lesson will be an introduction to the Local Area Network.**  **Our objectives will be to; describe how the Ethernet networks work, understand the various network devices and differentiate between them, understand the difference between a collision and a broadcast domain, describe different ways of segmenting broadcast domains, understand how Virtual Local Area Networks work, understand the different addressing schemas used in modern networks. The two different addressing schemas just mentioned are shown here. One on Layer 2, the data link layer of the OSI model, and the other on Layer 3, the network layer. The data link layer, uses MAC addresses, while the network layer uses IP addresses, which could be IPv4 or IPv6 format.**  **The way a packet is delivered from one network to another, from one host to another, can be compared to the way the postal service delivers mail. We will put a message inside of an envelope, which is similar to the way the data is encapsulated within one packet header. Then the header is encapsulated within another header. The IP packet is then encapsulated on an Ethernet frame at the data link layer, or another type of Layer 2 frame if something other than Ethernet is being used by the network.**  **Finally, this is all encapsulated one more time with physical information added at the Layer 1, the physical layer. This is similar to the way we put the message we want to send inside of an envelope and write our address and the destination address on the envelope, including the city, state, country, and postal codes. The post office puts your envelope in a shipping crate destined for the postal code and marks that code clearly on the outside of the crate.**  **The post office will search for the shortest and most efficient route, to get the crate from its current location to the postal office designated by the destination postal code. This is similar to how a Layer 2 device, or router, searches for the most efficient route for sending your message across the network or the Internet. Once the shipping crate has been received by the destination post office in the country, state, and city you specified, your envelope will be removed and driven to the street and the house or apartment number specified and placed in a mailbox. Your friend will receive the envelope, open it, and read your message.**  **As you can see, each step taken to encapsulate your message prior to it actually being sent, is undone, one step at a time in reverse order at the receiving end. The Layer 2 address and Layer 3 address are quite different. Layer 2 addresses are known as Media Access Control or MAC addresses. MAC are also referred to as hardware addresses, physical addresses, or burned-in addresses, because they are permanently etched into every network interface card and are unique to that card. Of the billions of network interface cards ever produced, no two have the same MAC address.**  **This is an example of a MAC address which is a six octet address for a total of 48 bits. Every time a packet passes through a Layer 3 device, like a router, and passes from one network to another, the Layer 2 information in the packet header is stripped out and replaced with new physical source of destination addresses. The Layer 3 address is the IP address, which is also known as the logical address.**  **This is an example of a private IPv4 address that is not routable on the Internet. Layer 3 addresses identify computers or endpoints and do not change as the packets are routed. With the exception of substitutions made by NAT routers, of course. Let's look at how Local Area Networks work so we can better understand the connections between devices and the rules controlling their communication. In order to deliver information from one host to another within the same Local Area Network, we need to know the MAC address associated with the IP address of the destination device.**  **Ping or packet Internet groper, is a utility that measures the time it takes to send a packet to another computer and receive a response back. It's the easiest way to quickly test if there's an open communication route between your computer and another system.**  **You can see that the ping was successfully delivered and we've received a response. You can ping an IP address because the Address Resolution Protocol or ARP, is able to make an association between the IP address we typed in and the MAC address that you can now see on the screen. This works fine for communication or Local Area Network. But when we need to deliver a packet outside a Local Area Network, the default gateway is the device that will make sure the packet is forwarded outside of the local network. Now let's try to ping 4.2.2.2, an address which is outside of our LAN. But the default gateway address is not found in our ARP table, which is why the ping did not succeed.** |