**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **04/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.**  **differences between stateful and stateless inspection. First, we will focus on how firewalls and routers work in modern enterprises. Then, we are going to talk a little about the differences between an intrusion detection system or IDS, and an intrusion prevention system or IPS. Finally, we will cover some of the basics of network address translation routers or NATs. Regular routers and some firewalls utilize the stateless way of filtering packets. Stateless means that each packet is inspected one at a time with no knowledge of previous packets. No session table is maintained, so each packet is inspected independently of all other packets. So what is inspected in the packet? The source IP address is examined to see if it's allowed. We may have an ACL rule, an access control list rule that will determine if that source IP address is allowed into our network, or if the destination address is allowed to be accessed. A check is made to see if the destination port or the service is allowed into the network. Basically, this proceeds packet by packet. Stateless inspection doesn't know anything about session. We will discuss sessions later. There is no database with details of the packets that have already been inspected. Here is an example of a stateless inspection event. We will have our source computer, the client system, bring up its web browser. The web browsers operate in the network application layer. The browser can create TCP or UDP traffic, but TCP is the most common traffic we will see traversing our network. Since our packet is using TCP on network layer 4, it is going to have an IP address. The packet header will contain the source IP address of our client machine, and the destination IP address of our receiving computer or web server. Then, the layer 2 information will be added to the packet header. This is information about our local network segment added by the network, such as the physical or MAC address of the source and destination computers, and the MAC address of our gateway. Then, the encapsulated packet will be sent to the physical layer, which could be wired or wireless ethernet. The packet will go to the router and the router will evaluate the packet. If the source IP address, in this case, our client machine, is allowed to access our server, and TCP or UDP are allowed, and if the destination port is allowed, in other words, if our server is listening to that specific servers for traffic from outside or even within our company's network, then the packet will be forwarded to the server. What are some of the benefits of a stateless inspection? For starters, stateless inspections are faster than stateful inspections. A stateless inspection gives us a degree of control over what's going on and what is going to be allowed within our network. Stateless inspections are great for troubleshooting purposes when we want to classify packets. Also, they are helpful when we have a router that supports virtualization. We can tell if we have a flow of traffic coming from a specific source trying to go to a specific destination. Then we can send it to a specific virtual instance within our router. Also, we can perform some QRS or quality of service switches which will prioritize traffic.** |