***Snort – MIS311 Information Security Systems Design and Application Term Project***

And our group’s page on GitHub as follows;

<https://github.com/ArahmiAtalay/mis311_term_project>

And our presentation video link as follows;

<https://www.youtube.com/watch?v=P11Nf1RyE1o>

***Used Programs:***

Snort & Hydra

***Short Definition:***

Using Snort, we will consider some types of attacks and simulate them.

***Short Explanation:***

By using Snort and other programs that we have built on Linux distributions, we will enable us to detect and monitor common attack types, such as ping attack, brute force etc.

***Project Process:***

In this project, we covered basic attacks and their detection in a simple way using some tools such as snort, hydra. At the beginning of our project, we set up virtual machines to simulate attacks on our computers. For this, we used the program called “VirtualBox”. Afterwards, we installed various Linux distributions that we will use on our virtual machines. After the basic adjustments, our machines are ready for use. At this point, we installed Snort, the application that we will detect attacks. We made some adjustments to use Snort effectively. These are the "alerts.rules" content for notification of detected attacks and the "snort.conf" files and contents for basic network configuration. We have discussed these configurations in detail in the video we shot, and you can easily see the details in the video.

Above, we basically explained how we created the system, now we will consider various attacks and their detection using the system we have adjusted. First we want to start with Ping attacks. Ping attacks are a denial-of-service attack in which a malicious attacker repeatedly sends ICMP (ping) packet requests to render the system he has targeted unusable. In this way, unreal requests constantly enter the system and narrow the flow of the system. After a certain point, the system becomes unusable. At this point, we created a ping attack simulation. We defined the rules with the snort configuration files we created and added the warning text that we had determined in the alerts.rules file. Then we created and observed the attack. You can easily see the whole process in our application video. Then, we discussed our other attack type, the TCP Dos attack. Briefly, this type of attack works like this, it exploits TCP's 3-way handshake vulnerability. The source (Attacker) sends SYN packets to the target. (1st handshake) The target responds to the SYN packet as a SYN ACK. (2nd handshake) The source sends a new SYN packet without responding to the incoming packet, and the target remains in a constantly pending state. In this way, the communication network becomes inoperative and the attacker reaches his target. In our project, we wanted to consider and simulate this attack type, and we detected it with snort using the configuration and rules content that we used before. We have discussed this process in detail in our application video. You can find all the details of these processes in the application video. Finally, we want to talk about brute force attacks. A brute-force attack consists of an attacker sending many password combinations or username values ​​to the system interface in hopes of correctly guessing a combination. To simulate this attack, we first integrated a program called Hydra into our system. Then we created a "passwords.txt" file where possible passwords are kept and determined the path where this file is located. When we come to the terminal screen, we first run Snort according to the configurations we have determined, as we have discussed its creation before and as we have discussed in our previous examples. As an additional information, our work was done with root control rights. While Snort is running in the first terminal we opened, we open a new terminal window and first access the root control rights with "sudo su". Then we activate the program called hydra on the terminal. At this point, we are sending the password combinations in the “passwords.txt” we created before to our local IP. At this point, Snort, which is already working, detects this attempt and both shows this attack by Hydra on the console screen and prevents this attack. Additionally, you can find a video of this process in the presentation slide. In this way, we have simulated a simple brute force attack.

In conclusion, despite some technical glitches, we have covered several types of attacks and simply visually demonstrated how they happen. In this way, we have observed how the snort is used and its reactions to attacks.