**Task 5**

**Research Pipeline**

**Sampling Criteria**

The main scope of this research is to identify which IPS is the most effective when operating an SDN network so that the industry will be able to protect their SDN infrastructure. In order to accomplish this, an investigation needs to be done from the implementation by measuring and comparing certain datasets that are necessary. the data set that will be investigated was mentioned in the previous task which is the total time taken for the IPS to start mitigating the DOS attack for each scenario. If one of those solutions takes less time to start mitigating the DOS attack will result into being more efficient than the other solution. Apart from those data sets, flow of packets will also be investigated in bits per second before performing the mitigation technique and the change in values (bits per second) is speculated to increase which proves that the different types of DOS attacks are flooding the network. Afterwards, an another experiment will be performed by launching the DOS attack but with the mitigation of each method. Change in values are expected to happen but instead the value of the bandwidth will be decreased on both methods as DOS attacks are getting mitigated and the victim is not getting flooded from malicious traffic. With this experiment being successful on both scenarios, one can verify the most effective IPS method by depending if the values are less than the other method, therefore comparison can be made based on the results. This signifies that the victim is not getting flooded with different types of packets and the industry will be able to determine which IPS should one use when operating an SDN network.

The idea behind my research samples were taken from other research papers. From (Baihaqi, Dwiputra Purba and Fahmi, 2018), testing was done to find out the delay ratio of the packet sent by the host that is attacking to the victim’s host before the DOS attack is carried out where the average delay is carried out before attempting the DOS attack. This research paper also evaluates the results by calculating the average speed of the mitigation technique when DOS attacks takes place. In my case, instead of calculating the average speed of the blocking technique, measurements will be taken to calculate the total amount of time taken for the IPS to start mitigating attacks as has been previously mentioned before. This will prove if the mitigation is taking place immediately once an attack has been detected from the IPS or not. The idea behind the bits per second sample was taken from (Busuttil, 2020), where he compared the bandwidth when launching the different types of DOS attacks in different SDN controllers. From this research paper since the setup is different and it was about mitigation, some ideas were taken where I discovered I can examine the amount of bits per second that the victim is accumulating on every type of DOS attack.

**Sampling Population**

This study is eventually aimed to serve as a guide for potential students that are studying in the security of SDN but mostly it is mainly focused to the industry. The reason behind this is that in the modern world, companies are opting to upgrade their network in SDN as it offers greater scalability and enables more efficient network management. However, unfortunately SDN as a technology suffers from a lack of security, therefore attacks are more prone to happen against the SDN controller. This study will aid the industry in implementing the most effective Intrusion Prevention System so that their SDN infrastructure stays secured against possible DOS attacks.

**Sampling Design**

A total of two utility tools has been used to gather the samples that are required for the data analysis. Although Snort is an IPS in itself, after mitigating the attack of the first solution, Snort has the ability to provide a result output that states the duration of the mitigation and the amount of blocked packets. Apart from that the duration of the mitigation process has been mostly noticed from using the monitoring tool of SFlow-RT. From there a real-time graph showing the amount of bits per second can be launched along with the time being captured during the mitigation of each method.

**Ethics**

**Prior to beginning the study**

One of the main principles of action/participatory research is that the researcher will not further treat the research subject to be insignificant or disempower them. To avoid this, proposal writers can perform test projects with participants to build trust and respect, allowing inquirers to discover any insignificance throughout the research before the proposal is written and the study is begun.

**Beginning of the study**

Proposal developers must explain the purpose of the study that will be described to the participants when drafting the purpose statement or the main principles and the questions for the study. When participants understand one purpose and the researcher has a different purpose in mind, deception may occur. It’s also crucial for researchers to mention who sponsored their study as sponsorship can create confidence and credibility.

**Collecting Data**

Many ethical issues may arise during this stage. It is important to let people identify you by your name or your organization along with a reason on why you are collecting that particular data of your research.

You should get permission from participants (those who provide the data) and make them aware that their participation is completely optional. Participants are allowed to leave any active data collecting or intervention program at any time, without feeling any pressure or fear.

When gathering data, it is common to assume that the information submitted would be kept private and that the results will be anonymous. You should inform participants when you will need to break confidentiality (for example, if they or someone else is in danger) and whether or not the results will be anonymous.

**Analysing Data**

Once data has been examined, it must be stored for an appropriate amount of time. The data should subsequently be discarded so that it does not end up in the hands of other researchers who may misuse it.

**Reporting, Sharing and Storing data**

The ethical issues are applied as well to the actual writing and dissemination of the final report.

Ethical issues may include the potential for hiding, misrepresenting or invent findings to satisfy the needs of a researcher or an audience. These deceptive techniques are not tolerated and they are considered as a scientific misconduct. A proposal can include a researcher’s deliberate decision not to engage in these behaviors.

It is also critical to consider the ramifications of doing research on certain audiences when arranging a study, and to avoid misusing the results to benefit one group over another. The researcher must send a preliminary copy of any study publications to those at the research site.

References

Busuttil, R., 2020. The effects of Distributed DoS intrusion on Software-Defined Networks – An approach to network security. *MCAST Institute of Information and Communication Technology in partial fulfilment of the requirements for the Bachelor of Science (Honours) in Computer Systems and Networks*, pp.1-51.

*2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 2018. Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm. [online] pp.55-59. Available at: <https://ieeexplore.ieee.org/document/8684039> [Accessed 23 March 2022].

**Task 6**

**Experimental Protocol & Design**

An experimental protocol are essential data structures that support the description of each process that leads to the generation of results in the experimental research. The experimental design on the other hand is the process of doing research in an objective and controlled manner in order to optimize the scope of the research and derive particular conclusions about a hypothesis statement.

As has been mentioned before, the scope of this research is to find the most effective IPS solution to protect an SDN network from harmful DOS attacks as SDN itself lacks security and is prone to data breaches. For this to be possible, two similar SDN networks were required and were both conducted by making use of the utility tool Mininet. Different types of DOS attacks are simulated inside those networks and a different type of IPS solution is initiated on each network so that a comparison can be made between them to determine which IPS is the most effective to use when an industry is suffering through a DOS attack.

**Independent variables & Dependent variables**

In research studies, variables resemble any type of attributes with multiple values, such as height, age, temperature or other metrics that can be changed upon testing. The independent variable is the variable that does not depend on any other variables and the dependent variable is the variable that depends on the independent variable.

In our scenario, the independent variable for this research paper is the total time in seconds for the IPS to mitigate the DOS attack as this variable will be triggered once the DOS attack is active. Afterwards, the bandwidth of the victim will be identified and calculated depending on the duration of the IPS to mitigate the attack. Therefore the dependent variable is clearly the bandwidth which is measured in bits per second (bps).

**External validity of an experiment & Sampling types**

External validity of an experiment resembles the generated results from the context of your research. The experiment that is conducted will be validated depending on the design of the experiment. There are a diversity of sampling types and in total there are four of them. Random sampling is a sample where everyone has a chance to be targeted within that population. Stratified sampling