**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 when the mitigation of each method starts taking place.

**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 time taken for the IPS to start mitigating 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 divides the target population in multiple groups and propose the samples based on the characteristics of each group. Opportunity sampling uses the researcher’s knowledge to recognize a sample and the last sampling is the systematic sampling where the samples are selected after calculating the probability of those samples such as formulas.

In my research paper, the external validity of my experiments are all dependable on the SDN networks that are created along with the IPS methods that are running inside those networks. Apart from those factors, a type of DOS attack needs to be running as well to be able to successfully generate the samples that are required which is the bandwidth of the victim before the mitigation and after the mitigation. As discussed before, the total time for the IPS to start mitigating the attack is also measured in seconds.

In terms for the sampling type, the target group of my research is referred to large corporate companies that are operating an SDN infrastructure, therefore random sampling can take place as different type of DOS attacks has a chance to occur on everyone who is operating an SDN network infrastructure in their enterprise.

**Coding**

In the case of my thesis, it was more focused on configurations when using certain utility tools rather than coding, however as a part of my methodology a script was also used to meet the requirements of my implementation.

Diagram

Description automatically generated

For the purpose of this research, a total of two SDN networks were created by making use of Mininet, where both of them include a single controller connected to three switches along with five hosts. Both networks were the same in terms of design to prove that several type of IPS solutions can be implemented in the same type of network. Two IPS scenarios were produced. One of the IPS is Snort and a configuration file defined as “AFpacket” was implemented to make it act as an IPS along with the pre-defined rules where it will be able to detect and block a variety of attacks.

The second IPS method was implemented by using a freely available javascript where it was able to detect and block a variety of DOS attacks from being reached to the victim. The javascript was modified to my own network by configuring the required flows inside the script so that serve as rules to mitigate the type of attacks.

From these two methods that were mentioned a comparison was done between the IPS methods by evaluating metrics that were mentioned previously. Most importantly the comparison was done to identify the difference between the solutions and to verify which of those solutions is the most effective method to mitigate a variety of DOS attacks.

**Research Triangulation**

Research triangulation can help researchers by providing a variety of datasets to explain various elements of interest. It also helps with the confirmation of a hypothesis when a set of findings is linked with another set by confirming with each other. Triangulation has the possibility to aid in the interpretation of research findings. The idea behind triangulation is that approaches that produce identical results give researchers more confidence in their conclusions.

In the case of my thesis, we know that the bandwidth of the victim in bits per second will be monitored before the mitigation of an attack takes place which is predicted to be increased as a value as well after the mitigation takes place which is expected to be decreased as a value. Apart from that, the total amount of time till the Intrusion prevention systems starts mitigating the attack is calculated as well and will be compared with each other which proves their efficiency. As discussed before, the independent variable is the total time that is calculated between intrusion prevention systems and the dependent variable is the bandwidth. All of these metrics will be automatically calculated when the DOS attack is initiated, which makes them being linked with each other. Those metrics also evaluate the hypothesis, which has been implied that Snort IPS will be the most effective IPS as a solution to mitigate a variety of attacks. With the DOS attacks being launched along with both IPS solutions, those metrics have proven otherwise as javascript that is acting as an IPS (second solution) is more effective than Snort IPS.

**Task 7**

**Research Paper 1**

The scope of this study is to develop a packet filtering firewall to enhance security over a Software Defined Network through a floodlight controller and the application of sample rules to identify the patterns along with the data that is passing through the firewall. In this research the pre-defined rules that were implemented inside the firewall were investigated as with those rules, specific malicious traffic can get mitigated. Apart from that variable, an algorithm was also used to identify the association rules.

For the first investigation, I personally agree by applying pre-defined rules on the firewall. This is because it provides ease and certainty when it comes to mitigating a type of attack as the type of rules can be designed to mitigate a wide range of attacks from reaching a destination. However, the firewall got designed there were specific paths that allowed the traffic to be passed to certain destinations.

In my opinion the conclusion was vague on this paper, the author clearly did not test many metrics to test if the firewall is successfully mitigating DOS attacks. I also do not agree that the author chose to use an algorithm to determine if the attacks are getting mitigated or not due to the fact that it is too complex to implement and other easier testing resources such as testing the bandwidth of the network or monitoring the percentage of allowed and blocked packets in real-time with a DOS attack could have been much more well designed.

Reference of Paper 1

Sayeed, M., Sayeed, M. and Saxena, S., 2015. Intrusion Detection System based on Software Defined Network Firewall. Next Generation Computing Technologies (NGCT), [online] pp.379-382. Available at: <https://ieeexplore.ieee.org/document/7375145> [Accessed 3 March 2022].

**Research Paper 2**

In this research paper, DOS mitigation techniques were proposed using Snort and BRO as Intrusion Prevention Systems taking place in an SDN network to enhance its security. The performance of the network was evaluated before and after a mitigation took place against a DOS attack where packet loss, average time and round-trip time was observed.

By investigating the packet loss with average time simultaneously, I agree that this information links to the scope of this study as with packet loss and average time, they will be able to detect the number of packets that got lost during the transmission between the source and destination on a given average time. When the DOS attack was initiated, the number of packets that got lost got increased to 100% in an average time of 5 minutes which shows that the IPS is successfully mitigating the DOS attack.

The investigation about Round-trip time is also acceptable and made sense to this study as it confirms if the victim is getting flooded or not. This was confirmed as the role of the round-trip time is basically the amount of time that it took for a packet to be travelled from a source to destination. A test was conducted where a DOS attack was launched and the packets that were sent from the attacker and the victim had a high round-trip time but once the IPS was launched, the victim host became unreachable.

Reference of Paper 2

Ombase, P., Kulkarni, N., Bagade, S. and Mhaisgawali, A., 2022. DoS Attack Mitigation Using Rule Based and Anomaly Based Techniques in Software Defined Networking. IEEE, [online] pp.469-475. Available at: <https://ieeexplore.ieee.org/document/8365396> [Accessed 5 March 2022].

**Research Paper 3**

When referring to this research paper, its purpose is to implement Snort IPS along with a Genetic Algorithm as a solution to detect the duration of the mitigation taking place from the DOS attack to secure SDN networks. The results that were investigated was the calculation of the network bandwidth being consumed before the attack and after the attack with the IPS being launched measured in Gbps, the delay ratio of the packet being sent to the victim before and after the DOS attack is carried out and the average speed being calculated while mitigating the attack.

In my opinion, the bandwidth consumption being calculated looks to be triggered accurately as a table of 5 comparison tests were provided. I personally agree with the researcher’s decision to find the bandwidth consumption as when a DOS attack takes place, it will consume a lot of your bandwidth’s network to perform the attack. Therefore whenever the IPS is taking place, the bandwidth consumption is expected to decrease when the malicious traffic is being dropped.

I also agree with the second metric being calculated which is that of packet delay ratio. The reason behind this is that its role is to confirm that the attacker’s host is indeed flooding the victim with malicious traffic as after the attack was initiated, it shows that a large volume of packets are destined to be directed to the victim.

Personally, I do not agree with the other metric being calculated as although the scope of this research is to calculate the duration of the Genetic Algorithm (IPS), it would have made more sense to calculate the total time that was taken until the IPS started mitigating the attack to see if it is being effected immediately or not.

Reference of Paper 3

Baihaqi, S., Dwiputra Purba, R. and Fahmi, F., 2018. Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm. IEEE, [online] pp.55-59. Available at: <https://ieeexplore.ieee.org/document/8684039> [Accessed 7 March 2022].

**Justification for my Research**

Since all of those papers are related to the thesis, those 3 papers helped me to create my own ideas on how to investigate my own metrics when investigating the performance of the DOS attack getting mitigated to be able to compare both IPS methods. Paper 3 influenced me to calculate the metric of bandwidth consumption of the victim that is running in an SDN network so that I could verify the exhaustion of the network before and after launching the chosen IPS. From the results of both IPS, I would be able to compare their effectiveness as bandwidth consumption is expected to decrease. The idea behind calculating the total time taken for the IPS to start mitigating the attack was taken directly from both Paper 1 and Paper 2. Both of these papers included the calculation of average time taken of the IPS running along with other metrics taking place. In my case, I switched this idea and made it my own by instead calculating the total time for the IPS to start mitigating the attack as in my research paper, a comparison needs to be made as discussed previously. Apart from that, one of the IPS methods is using Snort IPS, therefore the idea of using pre-defined rules was taken directly from that paper but the rules were adjusted to my own network to be able to detect and mitigate the different types of DOS attacks.