**ICT Project Assignment**

**Task 1**

**Introduction**

* Software defined networking is a technology which is being more approachable in the modern world. It eliminates the limitations of a physical network device by recreating them as programmable objects that are software defined, making this technology suitable in the current networking industry as SDN. However since this is a new technology security is a major issue as it can become prone to attacks such as a Denial-of-Service (DOS) attack.
* This research will analyse the classifications and effectiveness of different network intrusion prevention systems to mitigate DOS attacks in an SDN network and will investigate the security and performance by launching DOS attacks that will act as the attacker. This study will also analyse the challenges that will be encountered when detecting DOS attacks in the SDN network.

**Completed Work**

**Research Aims**

* The aim of this study is to identify which security methods such as Intrusion Prevention Systems (IPS) or mitigation firewalls are most effective for the modern industry when implementing an SDN network infrastructure
* Possible solutions for any challenges when detecting a DOS attack in an SDN network.

**Shaping of Literature Review**

* Research in academic papers was done before attempting to write the plan of the literature review and a variety of research papers which were related to DOS attacks taking place in SDN were considered and studied. Essential information and datasets were taken out and noted from these papers so that the formation of the literature review can take place.

**Literature Review Pipeline**

* for the first stage general information on how an SDN architecture operates is provided by taking key points from the paper (Zammit 2020). This also shows how effective the transition is from traditional networks to SDN.
* From the research paper (Busuttil, 2020) more details regarding SDN were carried out which includes how the architecture is divided into three layers which are the data plane, the control plane and the infrastructure layer. This information is essential to have a deep understanding on how to deploy a software defined network.
* In order for the SDN controller to communicate with the hosts, the openflow protocol is required as according to (Sayeed, Sayeed and Saxena, 2015) and (Alharbi, Layeghy and Portmann, 2017), the infamous key component where SDN can operate from in today’s standard is by using the Openflow protocol which provides a distinction between the control application and the fundamental data or forwarding plane.
* Before mitigating a DOS attack, that particular IPS or mitigation firewall needs to first detect it by creating two different types of alerts on their prevention system, therefore a differentiation between signature-based detection and anomaly-based detection was carried out and taken from the research paper of (Pratama et al., 2018).
* Signature-based detection is used for threats that are already acknowledged from the database and anomaly-based detection can detect malicious traffic from unknown sources.
* (Yan, Yu, Gong and Li, 2016) addresses the current issue that DOS attacks are always increasing due to the fact that bots and botnets are turning up to be more effective over time especially since SDN is prone to DOS attacks which has the ability to cripple the whole network. This essential information was listed down as it describes what are the issues about DOS attacks.
* After reading (Wani et al., 2021)’s research paper, I discovered that there are different types of DOS attacks that can take place. It can be either a Resource Exhaustion Attack, an Application Layer attack or a Volumetric Attack.
* A resource exhaustion attack drains computing resources such as CPU power, memory and I/O bandwidth, an application layer attack takes advantage of an application or system vulnerabilities which will cause the network to be volatile and volumetric attacks is when large amount of data is sent to the user by making use of botnets or by DNS amplification methods that will exhaust the bandwidth of the network. All of those attacks are relevant as in order to launch a DOS attack, one of those methods needs to be deployed.
* In order to mitigate DOS attacks, (Holl, P., 2014) mentioned that Defense mechanisms needs to be placed in order to defend the network. Certain key points were taken out from this paper which includes different defense mechanisms that have the ability to block a DOS attack when it is happening in real time and performing an analysis on an attack by finding patterns in it to discover the attacker.
* There are different techniques on how to mitigate a DOS attack, according to (Al’aziz et al., 2020) and (Baihaqi, Dwiputra Purba and Fahmi, 2018) describes that by using a tool defined as Snort is one of them. Snort is mainly an IDS which has the ability to monitor incoming traffic inside a network and detects for anomalies, however Snort can be configured to act as an IPS as well where it will be able to detect and stop malicious traffic from entering the network. According to (Haymarn Oo, 2019) and (LIN and WANG, 2016), An another method can also be created by making use of a custom script to act as an IPS to stop malicious traffic as well as to enhance the controller’s security itself by monitoring it using a utility tool that is defined as Sflow-RT.

**First step of the Research Methodology and Prototype Development**

* Evaluating different methods to use to mitigate DOS attacks in an SDN network
* The first method was deployed, using one of the techniques that was mentioned in the literature review along with one type of attack which is a resource exhaustion attack and a reactive defense mechanism.
* A basic topology was created with a single switch connected to 5 hosts and a controller using the tool Miniedit which is the same tool as Mininet but provides a GUI.
* As one of the mitigation techniques from the literature review, the Snort tool was implemented and was configured to act as an IPS by inserting DAQ modules and by modifying ICMP rules to drop the traffic instead of just alerting.
* The RYU controller was setup as the chosen controller for our topology and was configured accordingly to sync with Snort.
* Pulledpork was installed in Snort which is an addon to update all of the listed rules in real-time.
* A test demonstration was done by attempting an hping3 (DOS attack) from one of the hosts in mininet and ICMP traffic was being mitigated by Snort.
* All of the mentioned concludes method one and has been done by using the research paper of (Baiju, Yahiya, Raj and Farooq, 2021) and by videos that serve as guides having a similar implementation.

**Work to be done**

**Research Methodology and Prototype Development Continuation**

* Evaluating other methods to use to mitigate DOS attacks in an SDN network so that comparison can be made to identify which method is best to use in the industry.
* Try and create other rules on Snort so that mitigation from HTTP Flood and UDP Flood will be mitigated as well to enhance method 1.
* Try and launch the DOS attack of method one from a Kali Linux machine so that the attack will be sourced externally.
* A write up of the methodology and prototype development needs to be done along with an explanation of the tools that were used and the type of controller that was used.
* Further research regarding the next method needs to be done to deploy a mitigation of a DOS attack with the use of a javascript to act as an IPS which will be based by creating a similar topology of method one using Mininet using a POX controller as an RYU controller mostly supports only Snort.
* Prototype Development of the second method needs to be implemented when the research is done and testing is implemented.
* A third method is in consideration as well by implementing a similar topology using Mininet along with a Floodlight controller embedded with Sflow-RT where a python script will be created to mitigate a DOS attack and Sflow-RT will mark the traffic being dropped.
* Sflow-RT is a monitoring tool where you can see a variety of values being monitored in real-time.

**Findings and Discussion**

* Wireshark will be used to develop the results after a successful mitigation of a DOS attack for each method.
* An addon will be installed within Wireshark where it can view graphs in real-time to determine the traffic precisely to evaluate the effectiveness of each method.
* After finalizing all of the methods, a comparison will be discussed between the three defence mechanisms and will determine which method is best suited in the industry when it comes to protecting an SDN network from malicious attacks. The comparison will be based on the accuracy of the way those approaches are able to mitigate DOS attacks and afterwards, the results are compared by making use of the graphs from Wireshark to identify the suitable method.

**Conclusion**

* The main cause of this research is to find a suitable method so that the industry can identify the most effective method that can mitigate DOS attacks fluently. As mentioned, a DOS attack is an attempt to make a user unable to access system resources by overwhelming it with traffic from a specific source.
* According to this report two of the mitigation methods are still being discovered and and requires further investigation on functioning the mitigation. Evaluation of results for each method are still undergoing.

**Task 2**

Diagram, schematic

Description automatically generated

**Bibliography**

Zammit, S., 2020. Investigating Software-Defined Networks performance in contrast to simulated fixed vertical networking methods. *Institute of Information and Communication Technology in partial fulfilment of the requirements for the Bachelor of Science (Honors) in Computer Systems & Networks*, pp.1-15.

Baiju, B., Yahiya, S., Raj, P. and Farooq, S., 2021. DDos Attack Detection Using SDN Techniques. *Turkish Journal of Computer and Mathematics Education*, 10, pp.326-335.

Gogoi, M. and Mishra, S., 2018. Detecting DDOS Attack Using Snort. pp.1-8.

Holl, P., 2014. Exploring DDoS Defense Mechanisms. *Lehrstuhl Netzarchitekturen und Netzdienste Fakultaet fuer Informatik, Technische Universitaet Muenchen*, p.27.

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.1-5.

Alharbi, T., Layeghy, S. and Portmann, M., 2017. Experimental Evaluation of the Impact of DoS Attacks in SDN. *School of ITEE, The University of Queensland Brisbane, Australia*, pp.1-5.

Yan, Q., Yu, F., Gong, Q. and Li, J., 2016. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys & Tutorials*, 18(1), pp.602-622.

Mladenov, B., 2019. Studying the DDoS Attack Effect over SDN Controller Southbound Channel. *Faculty of Telecommunications at Technical University of Sofia 8 Kl. Ohridski Blvd, Sofia 1000 Bulgaria*, [online] pp.1-4. Available at: <https://ieeexplore.ieee.org/document/8825601> [Accessed 3 March 2022]..

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].

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K., Almotairi, S. and Gulzar, Y., 2021. Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry*, 13(2), p.227.

**Limitations in Concept Map**

For further investigations on how to mitigate DOS attacks in SDN, additional research on deploying different types of attacks that can get mitigated such as HTTP Flood and Slowloris could have been done as the only type of attacks that were manageable in terms of mitigation were only limited to UDP Flood and ICMP Flood. If further investigation was done on the mentioned deployment of attacks, it would be more beneficial for industries that are securing their SDN infrastructure, especially when it comes to web servers or application attacks.

An another recommendation is by researching on how to develop the SDN network and test the DDOS attacks using the IPv6 protocol instead of the IPv4 protocol as it is always an advantage to opt for IPv6 instead of IPv4 due to its built-in advanced security features which means it has the capability of being more resilient to DOS attacks.

**Task 3**

**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 developed firewall. This research paper also describes the intrusion detection mechanism for OpenFlow based on SDN.

The independent variable for this research paper is clearly the functions of the script that makes it act as a firewall and the association rules are dependable on the firewall which makes the rules being the dependable variable. Depending on the rules, they will discover and record the patterns among the data that is passing through the firewall, resulting that the patterns of the data being recorded is the control variable as they will change depending on the association rules.

Quantitative study The purpose of this \_\_\_\_\_\_ (experiment? survey?) study is (was? will be?) to test the theory of \_\_\_\_\_\_ that \_\_\_\_\_\_ (describes outcomes) or (compares? relates?) the \_\_\_\_\_\_ (independent variable) to \_\_\_\_\_\_ (dependent variable), controlling for \_\_\_\_\_\_ (control variables) for \_\_\_\_\_\_ (participants) at \_\_\_\_\_\_ (the research site). The independent variable(s) \_\_\_\_\_\_ will be defined as \_\_\_\_\_\_ (provide a definition). The dependent variable(s) will be defined as \_\_\_\_\_\_ (provide a definition), and the control and intervening variable(s), \_\_\_\_\_\_, (identify the control and intervening variables) will be defined as \_\_\_\_\_\_ (provide a definition).

**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**

The aim of this study is to detect and mitigate DOS attacks in SDN to improve the security infrastructure in SDN by implementing a Rule based approach using Snort and an anomaly based approach using BRO tool. This research paper also describes the use of those tools as well as the difference between those two approaches. The DOS attack was deployed by making use of the Hping3 attack and Low Orbit Ion Cannon (LOIC) tools.

The dependent variable for this research paper are the mentioned tools that are going to be used to detect the attack which are that of Snort and BRO. Those tools comes with a predefined set of rules for each method which will act once the DOS attack is launched making it dependable on the DOS attack. the independent variable is clearly the two tools that are used to launch the type of DOS attack (Hping3 and LOIC) as they can be launched without the need of Snort or BRO. The performance between the two tools that launches DOS attacks (Hping3 and LOIC) is evaluated using parameters such as packet loss, average time and round-trip time, resulting that those parameters are the control variable as their values will based on the outcome between the two tools that will launch the DOS attack.

Quantitative study The purpose of this \_\_\_\_\_\_ (experiment? survey?) study is (was? will be?) to test the theory of \_\_\_\_\_\_ that \_\_\_\_\_\_ (describes outcomes) or (compares? relates?) the \_\_\_\_\_\_ (independent variable) to \_\_\_\_\_\_ (dependent variable), controlling for \_\_\_\_\_\_ (control variables) for \_\_\_\_\_\_ (participants) at \_\_\_\_\_\_ (the research site). The independent variable(s) \_\_\_\_\_\_ will be defined as \_\_\_\_\_\_ (provide a definition). The dependent variable(s) will be defined as \_\_\_\_\_\_ (provide a definition), and the control and intervening variable(s), \_\_\_\_\_\_, (identify the control and intervening variables) will be defined as \_\_\_\_\_\_ (provide a definition).

**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**

Since SDN separates the control plane and the data plane, this type of network can be a target of DOS attacks. The main purpose of this research is to implement an IPS tool defined as Snort along with a Genetic Algorithm as a solution to detect the duration of the mitigation to DOS attacks in order to secure SDN networks. This research describes the security threats of SDN as well as the potential use of IPS to block malicious attacks. DOS attacks were launched to test Snort along with the Genetic Algorithm.

The independent variable for the selected research paper are the DOS attacks that will be launched as they do not require Snort to be running in order for the attack to be deployed. Snort comes with a predefined set of rules along with inline mode to make it act as an IPS. The dependent variable is certainly Snort and the Genetic Algorithm as they will function once the DOS attacks are executed. To evaluate the duration of the attack, a test was conducted by launching the DOS attack and the IPS simultaneously to calculate the average speed when it starts blocking the attacks which was that of 0.0278 seconds, making the average speed being the control variable.

Quantitative study The purpose of this \_\_\_\_\_\_ (experiment? survey?) study is (was? will be?) to test the theory of \_\_\_\_\_\_ that \_\_\_\_\_\_ (describes outcomes) or (compares? relates?) the \_\_\_\_\_\_ (independent variable) to \_\_\_\_\_\_ (dependent variable), controlling for \_\_\_\_\_\_ (control variables) for \_\_\_\_\_\_ (participants) at \_\_\_\_\_\_ (the research site). The independent variable(s) \_\_\_\_\_\_ will be defined as \_\_\_\_\_\_ (provide a definition). The dependent variable(s) will be defined as \_\_\_\_\_\_ (provide a definition), and the control and intervening variable(s), \_\_\_\_\_\_, (identify the control and intervening variables) will be defined as \_\_\_\_\_\_ (provide a definition).

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].

**Task 4**

**Research Design**

The main scope of the chosen study is to analyze and find the most effective solution on how to mitigate a DOS attack in SDN. As a type of dataset that is being tested are the different type of DOS attacks that will take place in real-time and the time taken (duration) for those malicious attacks to be mitigated will be noted to identify which of those solutions is efficient for the industry. Those kind of attacks affects specific targeted devices on the simulated network for each scenario. For this research, a variety of applications is used to gather results that shows the mitigation process from DOS attacks taking place in SDN. In total, two different scenarios will be produced so that analyzing of results can occur with the different techniques that were used.

As a type of design method, this research paper has been chosen to be quantitative for the simple fact that the type of results that will be analyzed are based on numbers since they will represent the total time duration in seconds for each IPS method to detect the attack on the SDN network which will start taking place once the type of DOS attack is launched as the IPS will automatically detect it. After both methods are tested accordingly, measurements will be taken from utility tools that are defined as Wireshark and Sflow-RT. I/O graphs will be generated as well by making use of the mentioned tools. The most efficient IPS method will be based depending on the least amount of time taken for the attack to be detected and mitigated.

When it comes to justifications, most of the ideas behind my datasets were taken from other research papers, an example can be seen from (Baihaqi, Dwiputra Purba and Fahmi, 2018), where 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 the DOS attack occur. This research paper also makes a test by calculating the average speed of the blocking 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.

An another justification is that this research is heavily based on statistical analysis techniques to examine the data collected. Such data can be either numeric or descriptive, but in this case there is a chance that numbers will be used to calculate the time taken for the mitigation process to occur, although this approach still needs further investigation. Other justifications include that by using a quantitative approach, it will help answer the research questions that are requested and the assumed hypothesis of this research.

**Research Questions :**

Which IPS is the most effective to mitigate external DOS attacks?

What are the challenges that were encountered when mitigating DOS attacks in an SDN network?

**Hypthoesis :**

Using Snort IPS to detect and mitigate DOS attacks is the most beneficial solution to provide more enhanced security and performance in Software defined networks.

**Research Methods**

Since this research paper is mainly focused on enhancing the security of an SDN infrastructure against malicious DOS attacks, the only best option to prove it is by first implementing a solution that is working and can be available as a guide for the industry to use on their infrastructure. To improve this further I believe that by finding other methods that are viable is essential so that comparison can be made by evaluating multiple tests. This will uncover which IPS solution is most effective to use to protect an SDN infrastructure.

The first chosen research method is to make an IPS solution in SDN from Snort by making use of RYU controller to control the SDN network. As previously mentioned, Snort originally is an IDS not an IPS. The idea behind this research method is taken out from (Baiju, Yahiya, Raj and Farooq, 2021), where in this paper the author produces an SDN network via Mininet using an RYU controller that can detect DOS attacks by creating rules that can be found inside Snort. RYU was chosen as a controller as it has an inbuilt python API script where it will sync the network directly to Snort which makes it ideal to use as a controller. DOS attacks are launched and Snort will just detect the DOS attack but will not block the traffic. When comparing it to my own concept, Snort was configured as inline mode using AFpacket where it will be acting as an IPS rather than an IDS. Snort rules were also configured to drop the malicious traffic once it detects it instead of just alerting. Wireshark will be used to confirm that the malicious traffic is being dropped.

The second chosen research method is to make an IPS solution in SDN by making use of Javascript that is using the RYU controller as well to control the SDN network. A javascript is created where it automatically targets a host so that when a DOS attack is being carried to that particular host, it will immediately automatically detect it and block the malicious traffic from being directed to that host. The idea behind this research method is taken out from (Haymarn Oo, 2019), where in this paper the author creates an SDN network via Mininet using a Floodlight controller and the javascript that is created will automatically block the malicious traffic from being directed to that host. The DOS attack will be launched from a specific host and upon launching the javscript, the author uses Sflow-RT to confirm if the packets are being dropped. When comparing this to my own concept, the javascript will be used but will be modified to sync with the RYU controller instead of the Floodlight controller and a different specific host will be marked as a target. An additional addon defined as Mininet-Dashboard will be installed in Sflow-RT to monitor all of the flows that the network is using instead of specific flows like the author was using. Just like the author of this paper, The DOS attack will be launched from a specific host as well and the javascript will block the malicious traffic from entering that host.

An another method was taken in consideration after reading the research paper of (Sayeed, Sayeed and Saxena, 2015) where a packet filtering firewall takes place in an SDN network. The firewall’s role is to block any type of traffic depending on what rules are configured inside the firewall. The only reason why I am not choosing this method for the simple reason that my research paper is about intrusion prevention systems and not about firewalls.

**Research Pipeline**

Diagram

Description automatically generated

When referring to this diagram, one can see the inputs, data processing and the outputs of my whole implementation. As for the inputs, all of the initiations that are required are listed which includes the creation of the SDN topologies linked with their respective controllers. An ICMP flood and UDP flood attack is being initiated to one of the network hosts using the following commands :

Command to initiate a UDP flood attack to a specific host (host 2)

h1 hping3 --flood --udp -k -s 53 h2

Command to initiate an ICMP flood attack to a specific host (host 2)

h1 hping3 -1 --flood h2

Upon launching the DOS attacks to the target hosts, data processing will start once the mitigation javascript or Snort IPS is launched. Once the mitigation techniques are initialized, we can confirm if the data processing has taken place by monitoring the attacks from Wireshark and Sflow-RT and if ICMP and UDP packets are marking as dropped, then evaluation will take place as both methods have successfully blocked ICMP and UDP attacks from either the packet capture of wireshark or from the I/O graph of Sflow-RT.