**Project Documentation**

**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 Sections**

* 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, (Al’aziz et al., 2020) 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.1-9.

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**

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 association rules to identify the patterns along with the data that is passing through the developed firewall. This research paper describes the intrusion detection mechanism for OpenFlow based on SDN.

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).