Penetration Testing for Software Defined Networks against DOS Attack

N.Priyanka[#1], Dr.V.Vetriselvi[#2]

#1 PG Student, Department of Computer Science and Engineering, Anna University CEG, Chennai-25, India

#2 Associate Professor, Department of Computer Science and Engineering, Anna University CEG, Chennai-25, India

Abstract--*Penetration test is a great way to identify vulnerabilities in SDN network and DOS Mitigation can be done by identifying the attacks. Penetration testing is a specialized security auditing method where a tester manually creates attacks on software defined network. This test usually involves the use of attacking methods conducted by trusted individuals called penetration tester that are conducted in a similar manner as practiced by hostile intruders or hackers. The goal of this penetration testing is to identify attack surfaces, vulnerabilities, and other weaknesses from the perspective of an attacker. This is the most effective way to exploit and to prove that the network is vulnerable. Penetration testing allows the security analyst to find new vulnerabilities which is certified as highly secure. In this paper, we proposed penetration testing to identify vulnerabilities in software Defined Networks. Penetration Testing is more important and it is mandatory for every system or network in order make the system or network more robust.*

Keywords — Vulnerabilities, Penetration Testing, Security measures and attacker.

I. INTRODUCTION

Penetration tests can be done in any system, network and any hardware devices to prove that it is not secure and it is exposed to vulnerabilities a penetration test helps to determine whether a system is vulnerable to attack even though the defences were sufficient. Penetration test is to identify vulnerabilities that is impossible or difficult to find using application vulnerability scanning software or automated network tools. The test is conducted, which involves a scanning of IP addresses of target hosts that are offering services with unknown vulnerabilities. The results of the tests or attacks is then documented and given as report to the owner and the vulnerabilities identified can then be resolved in a suitable manner.

Depending on the organization which is conducting the tests, the time taken by each test varies. Penetration test is basically an attempt to break the security of a network or system and it is not a full security audit. It means that auditing the view of a system's security at a single moment of time.

Penetration testing is often done for two reasons. It is either to increase management awareness of security issues or intrusion detection and response capabilities. Penetration testing assists in management of an organization to make decision in terms for providing higher security to systems. The weaknesses that are found in a vulnerability assessment is costly and most organizations are not afford to budget. Penetration tests probes to serious consequences for the network on which they run. If it is conducted poorly it can cause congestion and the system will be crashed.

In the worst case scenario, it can result in exactly the thing which is intended to prevent. The penetration testing purpose is to discover that the network is susceptible to distributed denial of service. A denial of service is a very dangerous attack that prevents host from functioning in accordance with intended purpose. Hence it is very important to find and mitigate at the early stage itself.

II. RELATED WORK

A secure SDN architecture [1][9], in which each switch is controlled by multiple controllers and it also provides services to all the switches available in the network. Surveys the state-of-the-art in programmable networks based on SDN and provided a perspective of programmable networks which is noteworthy from the early ideas to current developments. Then, particularly presented the software defined architecture and also OpenFlow standard. Penetration Test [2][3] methodology and framework which is capable to identify possible exploitable vulnerabilities in every network layer and identified problems with the current network configuration, management mechanisms. The technologies described enable network operators in a high level language policy is implemented and also easily determine sources of performance problems. Chen et al[4].,designed organization method of the penetration attack tree and an algorithm of attack serialization is put forward. Chen also designed and realized a penetration attack system whose attack scheme is the instance of the model. Penetration attack plan established based on this model can effectively instruct the penetration attack and unify penetration

attack implementation. Onix[8] is a platform on top of network control plane which can be implemented as a distributed system that is operated on a global view of the network. In this paper, our aim is to test the software defined network and to find any flaws which is called as vulnerabilities. Finding vulnerabilities is more important to secure the software defined networks more effectively. Our work focuses only on white box testing of software defined networks.

III. PENETRATION TESTING ACTIVITIES

The purpose of penetration testing is to discover that the network is susceptible to distributed denial of service. A distributed denial of service attack is a very dangerous attack that prevents host from functioning in accordance with intended purpose.

Penetration testing is divided into five stages which is shown in Fig 1. They are,

- Reconnaissance
- Scanning
- Obtaining access
- Maintaining access
- Finally erasing evidences

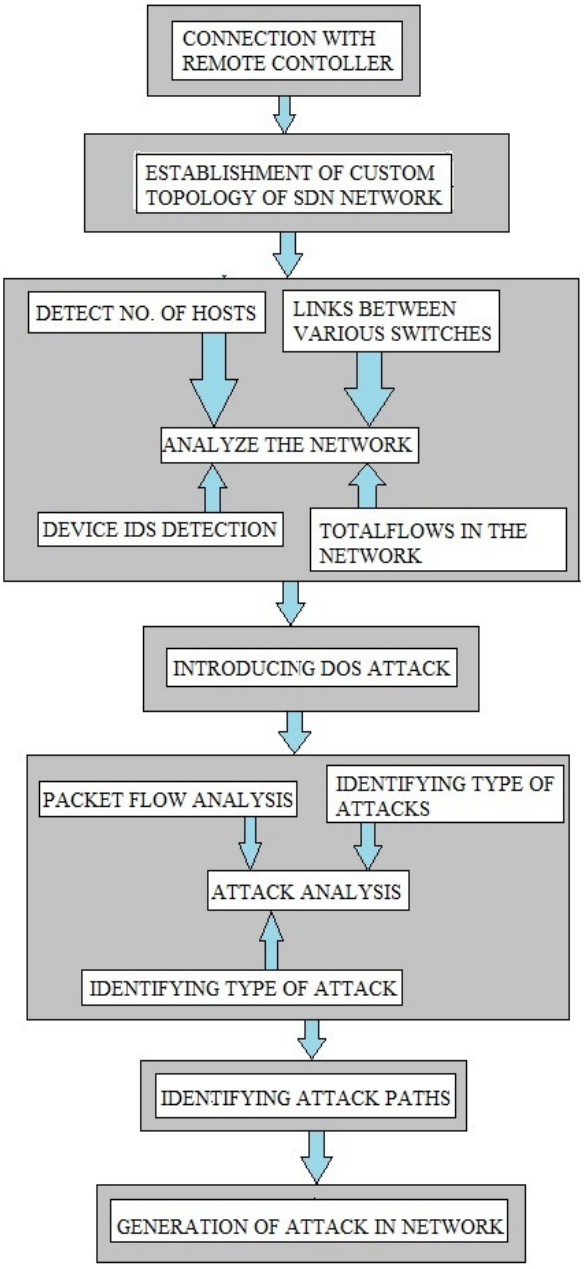

Fig. 1 Activities involving penetration testing

- Collection of the information about the network.Vulnerabilities are detected for the created network.
- Then scan the Software defined network and get the scanning report.Parse the scanning report and optimize the network for graph creation.
- Deduce the atomic attack path information from the report and map the paths into penetration graph.

In first stage, tester attempts to gather as much information as possible about the target host which must be prone to penetration testing. Here, customized software network is analysed completely for its device IDs, number of links between various switches, total flows in the networks, number of hosts and switches.

The goal of second stage is to scan the target host for vulnerabilities which can be exploited. It also scans for the services which are provided by the target host. As per white box testing, the target host is fixed. The service can also be transfer control protocol or user datagram protocol.

The third stage involves exploiting that weakness which is found during second stage of penetration testing. The fourth phase is maintaining. This stage involves providing or mitigating those vulnerabilities by using certain measures which is needed to secure software defined networks.

The fifth stage is clearing all the traces which we have done so far. This is done because the information which we gathered might be useful for hackers for exploiting the network.

A. *Testing activities for software defined network*

- Software defined network is created dynamically with various number of hosts and switches for testing.
- Once it is created, the network is connected with remote controller which will provide forwarding rules for the hosts and switches.
- Then the second stage of testing activity takes place.

IV. Experimental results

White box testing is done by varying the number of hosts in software defined networks. In Fig 2, Vulnerability present in the network during testing is detected and accuracy is represented in percentage. The vulnerabilities present in SDN vary for different number of hosts due to network complexity and the flow rules given by controller.

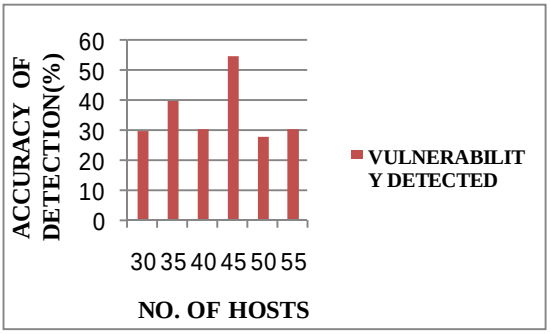

Fig. 2 Testing with respect to hosts

The packets entering during Dos attack is given based on time which is given in Fig 3. During Dos attack there will huge amount of packets entering the network. This packet has characteristics of normal packets. There will be huge amount of packets which are used for the attack. This abundant packet is the vulnerabilities which attack the network.

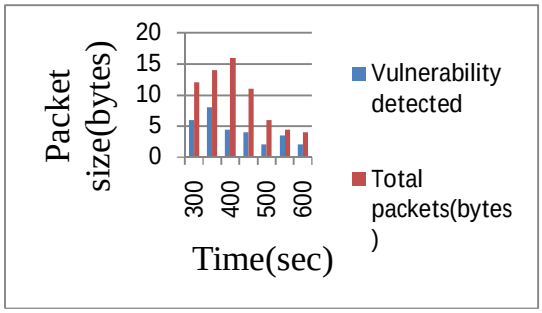

Fig. 3 Time based vulnerability detection

V. Conclusions

In this paper, penetration test for software defined network is done in order to find the vulnerabilities. The main objective is to prove that software defined network is less secure and it can face security threats easily. After finding vulnerabilities, necessary step is taken in order to secure the network. Here, White box penetration testing is done by creating network manually and dynamically.

ACKNOWLEDGMENT

I express my sincere thanks to my project guide, Dr.Vetriselvi**,** who provided consistent support and motivation for the successful completion of the project. From the very beginning, her insight and expertise greatly assisted us in carrying forth the project. This acknowledgement would be incomplete if we fail to show my gratitude to our parents and almighty god.

References

[1] Amiya Nayak,Li,Peng Li and song Guo,"Byzantine-Resilient Secure Software Defined Networks with multiple controllers in cloud",IEEE Transactions on cloud computing,Vol.2,No.4,pp.436-447, 2014.

[2] A.Bechtsoudis and N.Sklavos,Aiming at higher network security through extensive penetration tests.Latin America Transactions,IEEE(Revista IEEEAmaerica Latina)10(3):pp.1752-1756 , 2012.

[3] A.R.Curtis et al,"Devoflow:Scaling Flow Management for High-Performance Networks,"Proc. ACM SIGCOMM'11,New York,NY, pp. 254-65,2011.

[4] Chen.X,N.Zhu,Y.Zhang, and S.Xin,"Design and application of penetration attack tree model oriented to attack resistance test",computer science and software engineering,2008 International conference ,pp.622-626,2008.

[5] H.Kim,N.Feamster, "Improving network management with software defined networking",IEEE communication.Mag.,vol.51,no.2,pp.114-119,2013

[6] ONF White paper.Software Defined Networking.The New Norm for Networks[EB/OL].2012.https://www.opennetworking.org/

[7] Teemu Koponen,Casado Martin,Scott Shenker,Amin Tootoonchian Fabric:on Evolving SDN.In HotSDN 2012.

[8] T.koponen, M.casado, N.gude, J.Stribling, L.Poutievski, M.Zhu, R.Ramanathan, Y.Iwara, H.Inoue, T.Hama and S.Shenker(2010), Onix:a distributed control platform for large-scale production networks. In Proceedings of the 9th USENIX conference on operating systems design and implementation, OSDI'10, Pages16,Berkeley, CA, USA, 2010.USENIX.

[9] Xuan Nam Nguyen, Bruno Nunes, Marc Mendonca, K.Obraczka, and T.Turletti(2014),"A survey of software-defined networking:
Past, present, future of programmable networks,"Communications Surveys Tutorials",IEEE,vol.16,no.3,pp.1617-1634,Third 2014.