Secured Enterprise Network using Honeypot

Prof. Leena Patil[1], Kartikey Prajapati[2], Praveen Choudhary[3], Vishal Desai[4]

[1]*Assistant Professor, Dept. of Electronics and Telecommunication, Xavier Institute of Engineering, Mumbai, Maharashtra, India*
[2,3,4]*Student, Dept. of Electronics and Telecommunication, Xavier Institute of Engineering, Mumbai, Maharashtra, India*

---***---

Abstract - *The Honeypot was proposed by Lance Spitzner in 1999 to detect cyber-attacks. It is a security mechanism that traps attackers by creating a virtual trap. If the installation is successful, then the cyber-attacker trying to access the data will get access to false data. At that time, the organization is notified about the attack and the administrator can stay vigilant. The author introduced this technology to detect malicious practice, and since then it has kept on growing with the growing industry. Our study highlights various techniques used to design and implement an enterprise network with a honeypot, and we are introducing the topic for people interested in this technology.*

Key Words: **Enterprise Network, Honeypot, Intrusion Detection System, Firewall, Virtual Private Network.**

1. INTRODUCTION

With the increase in security awareness, organisations or individuals understand how to use a firewall to protect themselves when using the Internet, but the internal network has been invaded, and the phenomena of server attacks is infinite [1]. Even though different attack models have been implemented, recent events have shown that weak security measures have led to a major loss of data. A few recent breaches include Facebook (533 million), Microsoft (250 million), Broadvoice (350 million), Whisper (900 million), etc. A honeypot acts as a security system which is used to mimic, detect, or deflect an attacker from their target organization. It is a pre-planned system to attract cyber-attackers and then wait until they intrude on the system and try to gain access [2].

2. LITERATURE REVIEW

Software Defining Network (SDN) is a famous technology which is an approach to network management that enables dynamic programmability and controls the overall decision. SDN is divided into different types of layers as shown in fig.1.

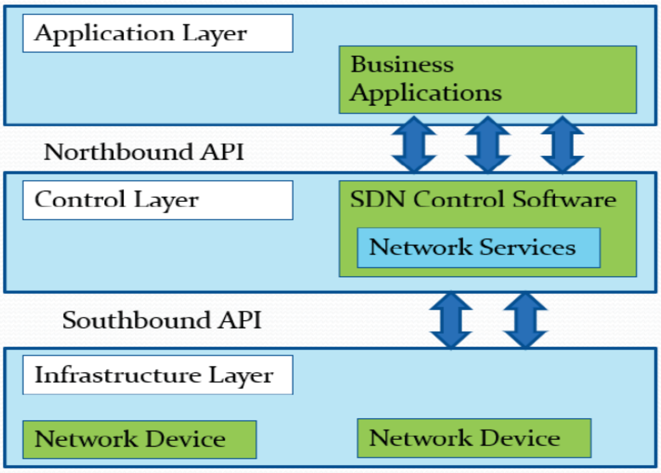


Fig -1: Three layered Software Defined Networking Architecture

The control layer takes the decision of routing of packet in network. Northbound interface, located below Application layer, exchanges information between control & Application layer. Lastly, Southbound interface, located between control layer and infrastructure layer, takes care of information exchange between these two layers. Selecting effective load balancing helps to smartly select the overburdened device and balance its load by distributing to other devices. Distributed controller is the best example of decentralised SDN since it is essential for normal functional activity of the system. A server load balancing is essential when there are multiple servers in a network. SDN brings innovative solutions to divide the traffic flow and increases network scalability and performance. SDN helps in improving network performance compared to traditional network and also helpful in automation of network management [1]. To emphasise a company's security, a firewall-based production can be developed covering reliability, confidentiality, manageability and scalability. The company's network system shown in fig.2 involves personnel, material management and production information and other departments. It was analysed that the structure of the enterprise network was a star structure. A second-level switch equipment is placed on each floor of the building and since the network command centre controls all the system, then if there is a damage, it will affect the normal operation of a company.

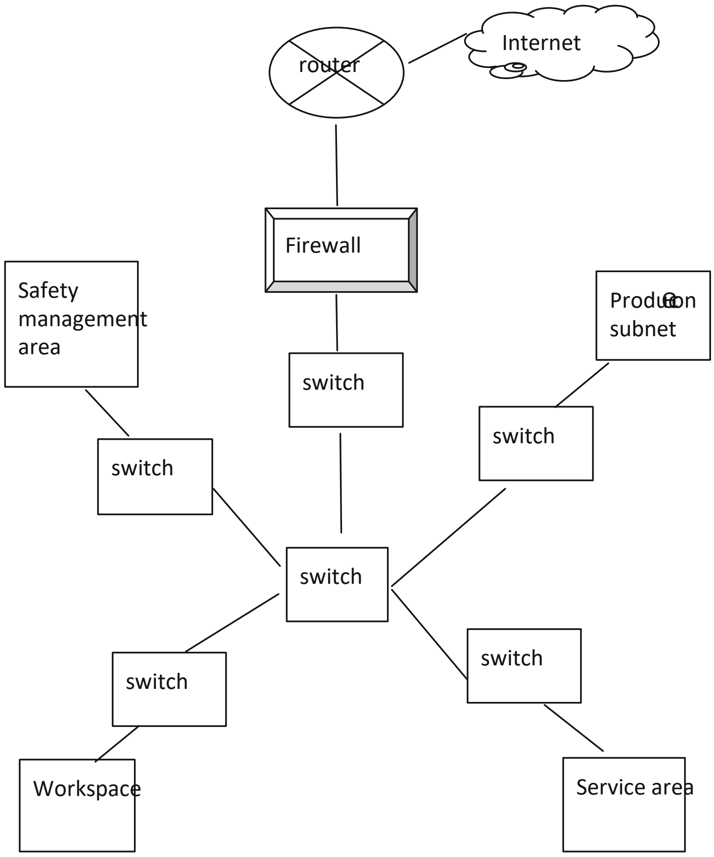
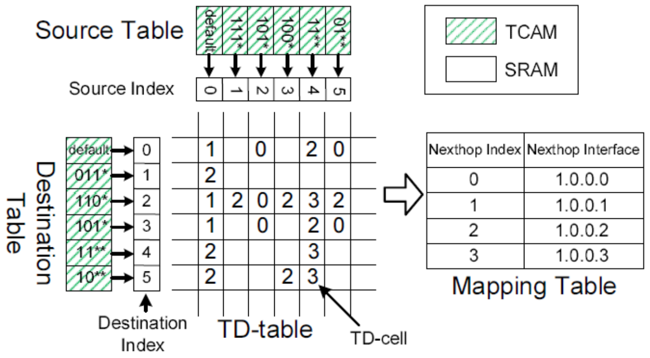


Fig -2: L company's original network topology

Thus, the company needs to implement some measures such as rationally planning the structure to ensure physical safety, deploying Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), combination of firewall and waterproofing to protect the sub network, installation of vulnerability scanner for the scanning of application and system layers on a regular basis, configuration of Virtual Private Network (VPN) to provide smooth external entry to isolate the intranet and external network, and using the network security management software to manage the server and terminal system [2]. Cowrie's default configuration has weak deceptive capabilities since an end-user running the honeypot with default settings could be easily detected by attackers. Also, renaming the hostname, server name, and configuring the endpoints may make the honeypot less deceptive, but it can't be completely viable for deployment. Thus, the Cowrie instance was downloaded from the official GitHub repository and the configuration was carried further. The variables assigned were differentiated based on their usage characteristics. For instance, a variable to identify the architecture or operating system on which the honeypot is running was assigned the name *arch.* All variables were examined to determine the functionality of each variable and what kind of deception was used. The methodology aimed to modify and determine Cowrie variables in order to better understand their functionality and to lay the groundwork for future research into how the variables can be potentially configured to make the Cowrie honeypot more deceptive when attacked [3]. To overcome the ever-increasing demands for much more flexible routing policies in enterprises, a forwarding table structure can be used to handle the expanded policies in an enterprise network. The forwarding structure used was the FIB Structure for Enterprise (FISE). The use of this technology was to shift from ternary content-addressable memory (TCAM) to static random-access memory (SRAM), since SRAM has a larger memory. A matching rule technique was used to test the functionality of the SRAM shown in fig.3. The destination prefixes were matched first since they needed to be guaranteed reachability and avoid routing loops.



1		0		2	0
2					
1	2	0	2	3	2
1		0		2	0
2				3	
2			2	3	

Nexthop Index	Nexthop Interface
0	1.0.0.0
1	1.0.0.1
2	1.0.0.2
3	1.0.0.3

Fig – 3: FISE: A forwarding table structure for enterprise networks

The forwarding was evaluated through experiments using real datasets. With the help of separation between TCAM and SRAM, FISE was able to reduce the TCAM storage and kept fast lookup speed. The positive part of this experiment is that it doesn't require new device since it can be implemented on an existing hardware router. The research was focused on Layer 3 two-dimensional table because of the importance of source address in routing [4]. To increase the security of network, three honeypots were used, both low and medium interaction, to offer a wide range of service. The implementation was done using operating system level virtualization, known as containerization. A container is a virtual environment that isolates an application and its dependencies. Containers are lighter than virtual machines because they can share the kernel and necessary libraries with the underlying operating system. A docker was used which supports many architectures such as x86-64 and ARM to fulfil the requirement for interoperability. The first honeypot deployed was "Cowrie," a medium interaction SSH and Telnet honeypot that is a successor of the Kippo honeypot. It provides a fake shell and a fake file system and also supports downloading files using SFTP. Furthermore, Dionaea, low interaction honeypot, emulates and supports many protocols such as FTP, TFTP, HTTP, HTTPS, etc. It is capable of capturing malware sample by using the libemu library for x86 emulation. Lastly, Glastopf, low interaction web application honeypot, does not emulate specific vulnerabilities. It responds to the attacker about expected answer in order to convince them of any vulnerability. On the honeypot server, Beats was installed, a shipping utility that collects all sources and then streams them using public key cryptography shown in fig.4.

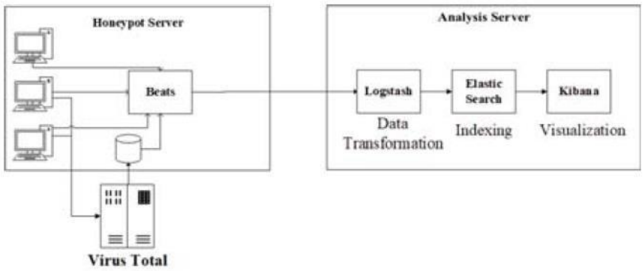


Fig – 4: Architecture of the Proposed System Setup

The Cowrie honeypot was able to capture 291,726 sessions to the SSH service, out of which the successful number of logins to the system was 262,434. 129 unique samples of malware were collected by the Cowrie honeypot, and it was found that all were categorised as malicious. It is possible that Docker may be deployed to multiple IoT devices in an organization's environment just as it supports different architectures [5]. Dynamic multipoint virtual private network (DMVPN) is a technology that is used to create more scalable VPNs because it supports IP unicast, IP multicast, and dynamic routing protocols. This technology ensures the data transmission security and constructs a dynamic tunnel layer network shown in fig.5.

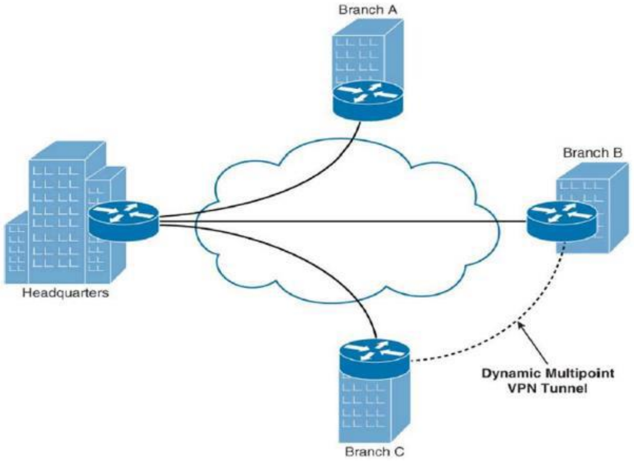


Fig – 5: Dynamic tunnel between spoke to spoke

Host standby routing protocol (HSRP) method provides network repetition to IP systems to guarantee that the client activity starts from the first jump to organise edge devices or access circuits. A central network station travels to the main centre of all systems in an enterprise. If the match between the HUB routers is successful, then the information of the branches is ready to communicate with Headquarter router and other branch router. The paper studied the issues related to VPN rented for line strategy and rule of DMVPN and HSRP system which will be applied to broader fields and transport into important function [6].

3. CONCLUSION

In this research, we have described various techniques to design and implement an enterprise network while considering the honeypot network security system. It has also covered the current security methods such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN), and static random-access memory (SRAM). The implementation of a honeypot in an enterprise is a good alternative as it provides an extra layer of security that can be broken, but the loss of data and privacy can still be maintained. The container-based honeypot experiments prove that the honeypot is capable of catching a suitable number of attacks and presenting the details to the organisation to help them study the attacks and implement precautionary measures for such kinds of cyberattacks in the future. The paper gives a brief analysis of honeypots, specifically the Cowrie honeypot, and various security methods as mentioned earlier.

REFERENCES

[1] Rout, S., Patra, S.S., Patel, P. and Sahoo, K.S., 2020, December. "Intelligent Load Balancing Techniques in Software Defined Networks: A Systematic Review." In 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC) (pp. 1-6). IEEE.

[2] Yuan, H., Zheng, L., Qiu, S., Peng, X., Liang, Y., Hu, Y. and Deng, G., 2019, February. "Design and implementation of enterprise network security system based on firewall." In The International Conference on Cyber Security Intelligence and Analytics (pp. 1070-1078). Springer, Cham.

[3] Cabral, W., Valli, C., Sikos, L. and Wakeling, S., 2019, December. "Review and analysis of Cowrie artefacts and their potential to be used deceptively." In 2019 International Conference on computational science and computational intelligence (CSCI) (pp. 166-171). IEEE.

[4] Yang, S., Cui, L., Deng, X., Li, Q., Wu, Y., Xu, M., Wang, D. and Wu, J., 2019. "Fise: A forwarding table structure for enterprise networks." IEEE Transactions on Network and Service Management, 17(2), pp.1181-1196.

[5] Kyriakou, A. and Sklavos, N., 2018, October. "Container-based honeypot deployment for the analysis of malicious activity." In 2018 Global Information Infrastructure and Networking Symposium (GIIS) (pp. 1-4). IEEE.

[6] Alam, T., Refat, C.M.M., Imran, A.Z.M., Rashid, S.Z., Kabir, M.H., Tarek, R.H. and Gafur, A., 2018, October. "Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol." In 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET) (pp. 367-371). IEEE.