International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Honeypot based Secure Network System

Prof. Leena Patil[1], Swapnil Desai[2], Ayushi Singh[3]

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

Abstract - *Honeyword (decoy passwords) was proposed by Juels and Rivest to detect attacks against hashed password databases. The legitimate password for each user account is stored with several honeywords in order to detect impersonation. If honeywords are selected properly, a cyberattacker who want to access someone's system will see the fake account. Also, logging in with a honeyword will set off an alarm notifying the administrator about a password file breach. At slight expense of increasing the storage requirement, the author introduces a simple and effective solution to the detection of hacking of user account. Our study highlights various honeypot implementations and we provide a starting point for persons who are interested in this technology.*

Key Words: **Honeypot, Honeywords, Password Hashes, Intrusion Detection System, Login, Authentication**

1. INTRODUCTION

Password based validation remains as the most popular form of identity authentication because of its better usability standard[4]. Password files leak is a severe security problem that has affected various users and companies[3]. Although, various attack models have been implemented over the time to decline the security standard far below to the desired level. Recent events have revealed that the weak password storage systems are currently in place on many web sites. Some recent password data breaches include Adobe (150 million), Evernote (50 million), 000webhost (15 million), Anthem (40 million), Gmail (4.9 million), etc[4]. Honeypot acts as a computer security process which is set to detect, deflect or counteract attempts at illegal use of data systems. Honeypot is a sacrificial system that is pre-planned to attract cyberattacks and utilizes their intrusion attempts to gain data about cybercriminals. Honeywords is a webpage security mechanism[1].

2. LITERATURE REVIEW

To increase the security of hashed passwords, a simple method was proposed in which a additional honeywords which are false passwords was associated with each user's account. A hacker who robs a hashed password's file and then inverts the hash function cannot distinguish if it is the original password or a honeyword. When the honeyword is used to login, it sets off an alarm. The secondary server can distinguish the password from honeywords for the login process and will set off an alert if a honeyword is entered . A contender is forced by using honeychecker to either risk logging in with a higher chance of causing the detection of the compromised password-hash file or to attempt compromising the honeychecker as well. As the honeychecker's interface is very simple, one can readily secure the honeychecker. When honeychecker is used it forces an adversary to either risk logging in with a greater chance of causing the detection of the compromise of the password-hash file or else to attempt compromising the honeychecker as well. In spite of their benefits over common ways for password management, honeywords aren't a guaranteed to user authentication[1].

Table-1: Comparison of honeyword generation methods

Comparison of honeyword generation methods			
Method	**DoS Resistance**	**Flatness**	**Storage**
Tweaking	weak	(1/k) if U constant over T(p)	1
Password	strong	(1/k) if U ≈ G	k
Tough nuts	strong	N/A	k
Take-a-tail	weak	(1/k) unconditionally	k
Hybrid	strong	(1/k) if U ≃ G & U constant over T(p)	√k

There have been various severe password leaks including LinkedIn, Yahoo and eHarmony. While you want to make sure that if the hashes are compromised, it is not easy for hackers to generate passwords from the hashes, you also never want to have vulnerabilities that can allow hackers

to obtain your password hashes. According to the leaks, large companies are using weak hashing mechanisms that make it easy to crack user passwords. Kelly Brown has discussed the basics of password hashing, password cracking software and hardware, and discussed best practices for using hashes securely. Every year password leaks are becoming a frequent event on the internet with several large scale leaks. These leaks has disclosed various poor practices that many companies employ when storing their passwords. The widely available lists of common passwords, an expanding knowledge base on how user select passwords, and advances in password cracking technologies have made basic hashes more vulnerable than ever. However there are several security measures that can be put in place to increase the security password hashes: Use strong hashing algorithms, Salt Hashes, Employ techniques to slow password cracking & encrypt the password hashes[2]. There have been various severe password leaks including LinkedIn, Yahoo and eHarmony. While you want to make sure that if the hashes are compromised, it is not easy for hackers to generate passwords from the hashes, you also never want to have vulnerabilities that can allow hackers to obtain your password hashes. As these leaks have demonstrated, large corporates have been using weak hashing mechanism that can make it easy to crack passwords. Kelly Brown has discussed the basics of password hashing, password cracking software and hardware, and discussed best practices for using hashes securely. Every year password leaks are becoming a frequent event on the internet with several large scale leaks. These leaks has disclosed various poor practices that many companies employ when storing their passwords. The widely available lists of common passwords, an expanding knowledge base on how user select passwords, and advances in password cracking technologies have made basic hashes more vulnerable than ever. However there are several security measures that can be put in place to increase the security password hashes: Use strong hashing algorithms, Salt Hashes, Employ techniques to slow password cracking & Encrypt the password hashes[3].

Table-2: Comparison of the honeyword generator models

Comparison of honeyword generation models			
Method	**DoS Resistance**	**Flatness**	**Storage**
Tweaking	weak	weak	hN*
Password	strong	strong †,‡	khN
Proposed	strong	strong ‡	4kN + hN + 4N

To detect the breach at the server side, research strongly depends on honeywords. Though some significant efforts have been made, existing honeyword generation techniques never address all the issues affecting flatness. The proposed technique overcomes all the limitations and achieves much improved flatness. It resists the DoS attack with the probability more than 0.99 to meet all the security parameters. The advantage of this method is that the usability perspective of the passwords are formed based on the episodic memory of the users. Also, a high typosafety has been composed as a typing mistake can sets off a false alarm with lesser probability than 0.03. It provides an efficient way for storing the alternatives, which greatly helps in nullifying the cumulative storage overhead for incorporating the honeywords.[4] For real-time intrusion detection and prevention systems, a honeypot based system can be used on the network security. An effective software tool was developed for this proposed novel approach. It is a hybrid honeypot system that combines the superior properties of low and high interaction honeypots in a single structure. The developed system has been tested on a simulated campus network in real-time and successful results have been obtained. To reduce the installation, configuration, maintenance and management cost the virtualization technologies such as the usage of honeypots on the enterprise networks is implemented. A machine with at least a unique network interface for each VLAN should be deployed in networks with VLANs . The costs of installation increases as the utilization of a real machine for each VLAN and maintenance also increases for campus networks which deploy VLANs[5].

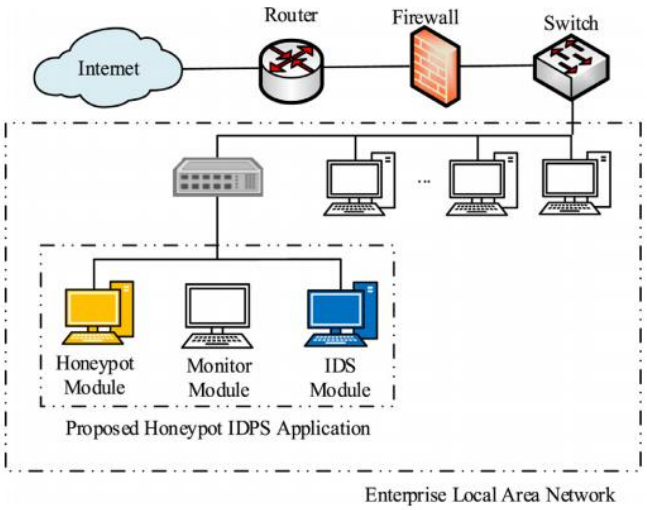

Fig-1: Localisation of developed honeypot IDPS on LAN.

In order to trap the adversaries as well as investigate cyber attacks, a honeypot system is a vitally important security facility created to be probed, attacked and compromised. The innovation of this paper is the compact honeypot architecture i.e. HoneyDOC which differs from the traditional honeypot architectures by using the novel Decoy Orchestrator Captor perspective to dissect and decouple the honeypot, allowing all round honeypot design, which has been presented by the powerful SDN enabled architecture. The heterogeneous decoys supported by the SDN switches can be integrated into the versatile honeypot system flexibly by taking advantage of the SDN

technology. The diverse security applications can be developed and integrated upon the SDN controller's APIs, particularly, the traffic control can be adaptively and transparently conducted by the SDN controller applications according to the requirements. The sensibility test shows the arbitrary tragic classification rules and the fine-grained actions. The countermeasure and stealth tests demonstrate that a much stealthier tragic migration function is added but the performance does not decrease compared to existing solutions. Also, for real production network, we conducted the system deploying virtual honeypots for capturing live attacks. The real data based validation shows the efficiency of data reduction and the effectiveness of the tragic redirection for data analysis[6]. There are different kinds of attacks in each layer and protocol and there should be a different kind of honeypot for each of them. A honeypot which was proposed on port 80, is a web-based HTTP service which includes the weak password module and the SQL injection module. A group of honeypots detect the whole security level of the network and also helps to get the index of network security situation. A honeypot-based IPv6 security situation awareness system was developed that acts as a trap to catch attackers. The platform can observe the IPv6 system security situation in real time and capture the behavior of illegal users. It uses the honeypot system to transfer attacks from the main system to the trap system[7].

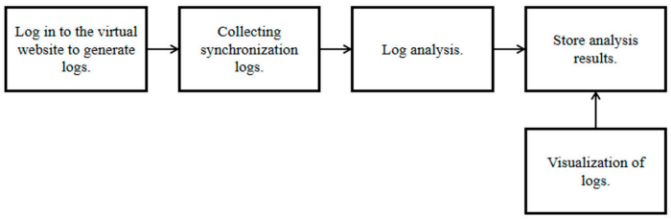

Fig-2: Framework of flow chart

3. CONCLUSION

In this research, honeypot and various honeywords generation techniques to provide network security are described. The improved security of hashed passwords by additional auxiliary server called "honeychecker" which can distinguish the user password from honeywords. The basics of password hashing, password cracking software and hardware and best practices for using hashes securely. Implementation of honeychecker, in order to provide realistic honeywords and also to reduce storage cost of the honeyword scheme. Questionnaire Based technique overcomes all the limitations and achieves much improved flatness and it resists the DoS attack with the probability more than 0.99 to meet all the security parameters. A developed IDS application can protect the network from attacks by blocking the delivery of the packets if they match with an attack signature. By using the SDN technology, the heterogeneous decoys sustained by the SDN switches can be combined into the versatile honeypot system flexibly. A web-based honeypot in IPv6 network environment with the main benefits of calculating the security situation awareness with SSI. The objective of the paper regarding awareness of database breaches and the importance of honeypot system to ensure the security of the network. d. The paper gives a brief study of Honeyword Generation techniques like Tweaking, Tough nuts, Take-a-tail, password-model, etc.

REFERENCES

[1] A. Juels and R. L. Rivest, "Honeywords: Making Password cracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS'13. New York, NY, USA: ACM, pp. 145–160, 2013.

[2] K. Brown, "The Dangers of Weak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.

[3] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," IEEE 2015.

[4] Nilesh Chakrabortya, Shreya Singh ,Samrat Mondal, "On Designing A Questionnaire Based Legacy-UI Honeyword Generation Approach For Achieving Flatness", Journal of LATEX Templates, 3 Aug 2017 .

[5] Muhammet Baykara, Resul Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems", Journal of Information Security and Applications 41 (2018) 103–116.

[6] Fan, Wenjun, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design" IEEE Journal on Selected Areas in Communications, 37 (3). 683 - 697. ISSN 0733-8716 (2019).

[7] Keyong Wang, Mengyao Tong, Dequan Yang, Yuhang Liu, "A Web-Based Honeypot in IPv6 to Enhance Security" MDPI Information 2020, 11, 440.