IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCED RADIOWAVE QUICKSAND

Nadesh .S
UG Student
Department of Computer Science & Engineering
SRM Valliammai Engineering College, Tamil Nadu, India

Akash Karthik .B
UG Student
Department of Computer Science & Engineering
SRM Valliammai Engineering College, Tamil Nadu, India

Godwin .E
UG Student
Department of Computer Science & Engineering
SRM Valliammai Engineering College, Tamil Nadu, India

Mr.S.VENKATESH, B.TECH., M.E.,(Ph.D.)
Assistant Professor
Department of Computer Science & Engineering
SRM Valliammai Engineering College, Tamil Nadu, India

ABSTRACT

Now more than 20 years after its inception, Wi-Fi isn't going anywhere.In addition to supporting short-distance connectivity the Wi-Fi Alliance is working on interoperability certifications for Wi-Fi 6 products, which operate over the recently opened 6 GHz frequency band. Still in India we are lagging in the security aspects of the internet, Wifi is a weak link to a network of devices and with the expansion of free wifi as a part of Digital India, privacy and security is getting vulnerable day by day. As a Part of the campaign , GOVT OF INDIA has launched a series of partnerships with Google to provide free internet in public railway stations. This has a lot of potential to attract unwanted surveillance of the public by criminals and there is always a threat to the privacy of people connected to these public networks. To enhance the security and protect the user from getting vulnerable to traps , Wifi quicksand aka Honeypot is the only efficient option. The aim of the project is to automate all the processes taking place after the installation and a user enhanced dashboard to overlook the operations taking place so that any such criminal activities taking place can be monitored and put to stop.

Keywords-HOTSPOT, HONEYPOT, FTP server, NMAP, ESP CANARY

I. INTRODUCTION

A brief overview of the system for securing wireless railway public networks using a low budget honeypot. The module is built using ESP-8266 wifi module that runs on a rechargeable lithium ion battery. The module is incorporated with a fake FTP server that acts as a vulnerability for our system but actually it does not provide the option to exploit it. The trigger point to make admins notified about any intrusion is made using a canary token . A Canary token is a File,url,API key or other resources that is monitored for access.once the resources has been accessed an alert is triggered notifying the object owner of said access. In our module we use Canary token as an API key , and it is linked to our module using a url. The module for accessing triggered incidents are provided by the canary token provider and they contain lots of valuable information. The programming of network and canary token API are done in objective c and C , also Python modules for wifi repeater are used via Arduino IDE.

II. LITERATURE SURVEY

Honeypot systems are not used for intrusion detection systems nor the firewall for a direct specific problem. Honeypots are used as a part of security systems and what kind of problem they will offer a solution depends on the design and usage purposes. Hence to the contrary other information security equipment is not to be able to mention a honeypot that is able to give a general answer to every problem solution [10, 11]. Riboldi et al. have developed a low interaction honeypot system to monitor illegal activities on VOIP systems in their study. During 92 days on the system whose performance has been monitored, related to SIP protocol 3502 events have been gathered. They have interpretered their system as available like a firewall and intrusion detection system VOIP environment [12]. Shukla et al. have performed a honeypot system to detect malicious web URLs in their studies. The system that has been developed in the Python language is served on the client side. By means of crawler on the client side the URL addresses are gathered and thereafter if there is a need for a visit, web sites are visited. If these URLs are malicious or contain vulnerability by the signature based intrusion detection system a trigger is activated. Thus the malicious URL addresses

are saved in blacklist and so the security is available [13]. Koniaris et al. have used honeypot systems for the analysis and visualization of malicious activity and connections. In their performed application they have set up two alternate search honeypots. The first of these, generally has a self-propagation option and has been intended to gather malicious software and the second has been intended to gather malicious activities as a trap system [14]. Song Li et al. have deliberated to set up a mixed interaction honeypot based intrusion detection system. They explain the purpose of the system that they have developed to stabilize the network and enhance the security [15]. Chawda et al. have proposed a distributed honeypot system to search for new vulnerabilities. In their performance system to be exposed to further vulnerability as a front end content filter they have used low interaction honeypot systems [16]. Xiangfeng Suo et al. have deliberated how to practice honeypot technologies in intrusion detection systems. In research work, they have submitted a proposal to practice honeypot systems to remove the intrusion detection system problems [17]. Paul et al. have performed a honeypot based signature generator for computer network security. The developed system especially has been used for the purpose of protecting against polymorphic worm attacks. The developed system also has the skill to isolate suspicious traffic and gather much useful data about malicious traffic and worm attacks [18]. Beham et al. have benefited from the advantages of virtualization technologies. In their study, they have searched the intrusion detection and the nested virtualization environment of honeypot systems. [19]. Liu et al. have performed an intrusion detection system, which is honeypot based and uses IP traceback technique. To introduce the limits of conventional intrusion detection systems on honeypot systems an intrusion detection design has been offered [20]. Auttopan Pomsathit in his study, he has handled the usage of honeypot systems and intrusion detection systems on distributed networks. He has explained his main purpose has been measurement of effectiveness intrusion detection systems by using together both intrusion detection systems and honeypots [21].Jiang et al. have handled honeypot system applications for the enterprise business networks. They have combined the methods that are used in intrusion detection systems with a new honeypot system thereby to view current honeypot systems [22]. Mitsuaki et al. have designed a high interaction and effective performance scalable client honeypot. By this means in–depth analysis and capture capability have been aimed [23]. P.Fanfara et al. have focused on the technology called honeypot and the issue of the implementation process of its autonomous version, which is able to create virtual honeypots and thus rapidly increase a security level of distributed heterogeneous computer systems in their study [24]. Markert J. et al. have presented an effective analysis of a honeypot for WSN and show detection capabilities in the categories of known and unknown attacks in their paper [25]. Musca C. et al. have presented methods for isolating the malicious traffic by using a honeypot system and analyzing it in order to generate attack signatures automatically for the SNORT intrusion detection/prevention system in their study [26]. Sadasivam G. K. et al. have deployed several honeypots in a virtualized environment to gather traces of malicious activities in their paper [27]. Djanali S. et al. have proposed a low-interaction honeypot for emulating vulnerabilities that can be exploited using XSS and SQL injection attacks. The proposed honeypot tries to overcome the techniques that hide the attacker identity [28]. Haltaş F. et al. have presented a novel automated bot-infected machine detection system BFH (BotFinder through Honeypots), based on BotFinder that identifies the infected hosts in a real enterprise network by learning approach in their paper [29]. Bashir U. et al. have made a survey on the overall progress of intrusion detection systems in their paper. They survey the existing types, techniques and architectures of Intrusion Detection Systems in the literature. Finally they outline the present research challenges and issue [7]. Benmoussa H. et al. presented a survey of distributed Intrusion Detection Systems based on intelligent and mobile agents; it also proposes a new concept of proactive IDS in their study. First, they introduce the topic. Then, they present limitations of classical IDSs. In the third part, they study the technologies of agent and multi-agent systems and present benefits of using it to address shortcoming of classical IDSs. Finally, they present their approach and future work [8]. A variety of researches and studies have been done for information security . As it is seen in current technical literature, to provide information systems and network security, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls and honeypots are not used by themselves alone. When the current studies, which are related to the subject, are viewed as security systems like those, hybrid designs that interact with each other are proposed. A Survey on Honeypot Technologies Used in Intrusion Detection Systems Proceedings of 16 th ISERD International Conference, Prague, Czech Republic, 10 th November 2015, ISBN: 978-93-85832-28-4 16 Within this study in our investigated applications also considering the proposals in technical literature, honeypots, intrusion detection and prevention systems are used together. Thus security system performance has grown and especially false positive level, which is one of the most significant disadvantages of anomaly based intrusion detection systems, has been reduced and unknown new attack patterns detection has been possible with these studies.

III.PROPOSED SYSTEM

The proposed system contains a wireless access point replication that replicates the wireless packets to the main router that in turn gives a closed internet connection to the user to avoid suspicion. The backend of the honeypot archives a ftp server that usually does not appear on any network scanning searches on the public network , this looks like a vulnerability to the eyes of the attacker and it attracts people to exploit it . This is the factor contributing to triggering of our honeypot. The trigger used in our module is a Canary Token. A Canary token is a File,url,API key or other resources that is monitored for access.once the resources has been accessed an alert is triggered notifying the object owner of said access. In our module we use Canary token as an API key , and it is linked to our module using a url. About the module to host these attributes , we use ESP-8266 wifi module that is used on Arduino boards to provide it with wifi access. Instead of using the whole arduino module we use a wifi only module to make convenient and easy planting of the device to a 4*4 inch wooden block or any 4*4 inch wall slots for the purpose of security . .

IV. SYSTEM DESIGN

A. System architecture

A System Architecture is the conceptual model that defines the structure behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

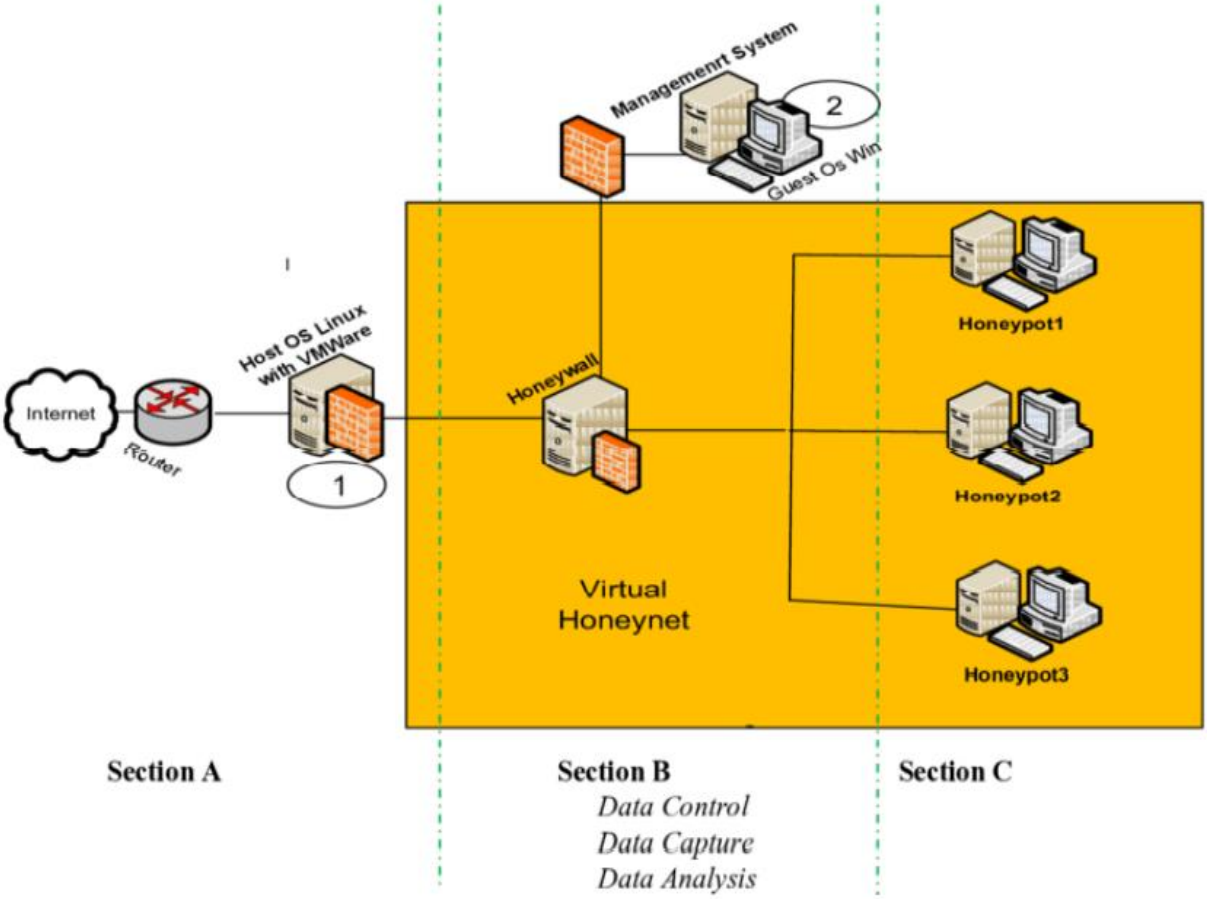

Fig. 1. wifi Honeypot system architecture

B. Use Case Diagram

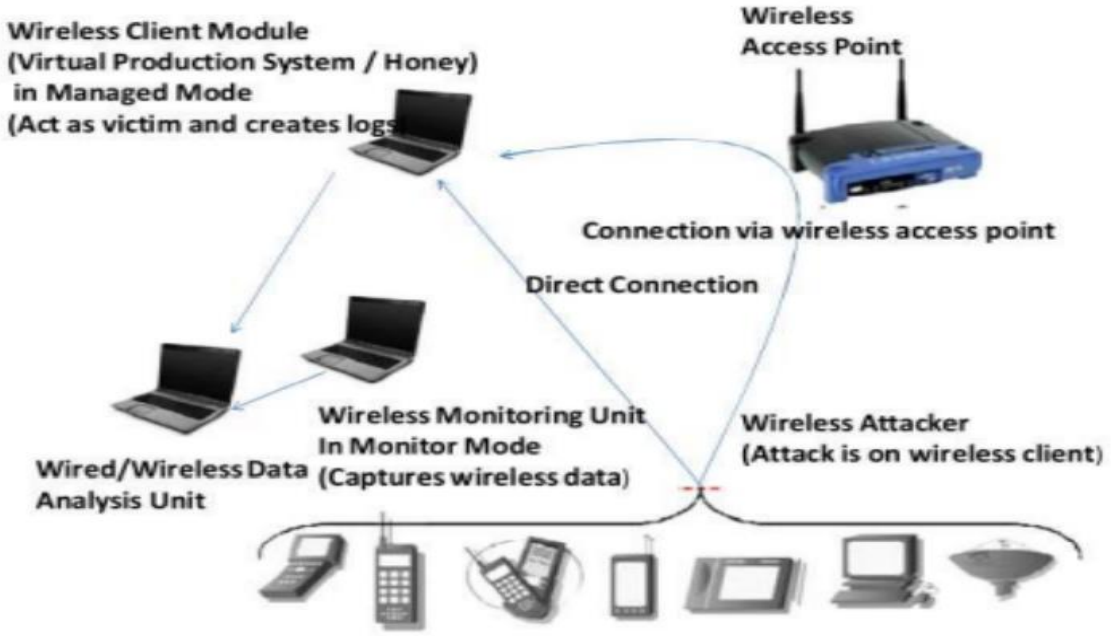

Fig. 2. Use Case Diagram

V.CONCLUSION

With the exponentially increasing usage of wireless devices, the threat of wireless attacks is also growing. This paper presents a comprehensive survey of previous wireless honeypot systems that have been deployed to assess the security scenario in the wireless domain. Then, a framework is given which describes the whole process model of a generic wireless honeypot. The possible attack scenarios in the wireless domain are identified and the honeypot architectures compliant with each scenario are given. A comprehensive analysis (classification and comparison) of existing projects is presented. As part of observations made from classification, the paper poses the need for worldwide deployment of more comprehensive wireless honeypots, incorporating all the three- deceptive, detection, and deterrence mechanisms, to control the wireless attack scenario.

REFERENCES

[1] Virtual CMS Honey pot capturing threats in web applications International Journal of Scientific & Engineering Research, Volume 4, Issue 4,April2013 ISSN 2229-5518

[2] THE RESEARCH AND DESIGN OF HONEYPOT SYSTEM IN THE LAN SECURITY International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 ISSN 2229-5518

[3] Summarization of Honeypot- A Evolutionary Technology for Securing Data over Network, And Comparison with some Security Techniques International Journal of Scientific & Engineering Research, Volume 4, Issue 3, March 2015 ISSN 2319-7064

[4] Study of Honeypots: Analysis of WiFi_Honeypots and Honeypots tools Article in Advances in Natural and Applied Sciences · December 2014

[5] Honeypots: Approach and Implementation International Journal of Scientific & Engineering Research, Volume 3, Issue 12, December 2014 ISSN 2319-7064

[6] Network Security Enhancement through Honeypot based Systems International Journal of Engineering and Technology, Volume 7 No 1, Feb-Mar 2015 ISSN 0975-4024

[7] Wireless Honeypot: Framework, Architectures and Tools International Journal of Network Security, Vol.15, No.5, PP.373-383, Sept. 2013

[8] Honeypots in Network Security Deniz Akkaya 2010-06-29 , 2DV00E

[9] Cloud Security using Honeypot Systems International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518

[10] Implementation of a Modern Security Systems Honeypot Honey Network on Wireless Networks International Young Engineers Forum (yEF··ECE) CapariCil, Portugal, May 5 , 2017 978·1·50904639..JJ171$31 ,00 C2017 IEEE

[11] An extensive study of Honeypot technique Article May 2020

[12] Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack International Journal of Scientific Engineering and Research Volume 3 Issue 8, August 2015 ISSN 2347-3878

[13] A Review on Honeypot Deployment London Journal of Research in Computer Science and Technology Volume 20, Issue1, Compilation 1.0 © 2020 London Journals Press

[14] Cloud Security using Honeypot Systems International Journal of Scientific & Engineering Research Volume 3, Issue 3, March - 2012 ISSN 2229-5518