SECURING WMN USING HONEYPOT TECHNIQUE

Priyanka Gupta
Dept. of Computer Science
RGGI, GBTU, India;
prsv123@yahoo.co.in

Paramjeet Rawat
Dept. of Computer Science,
IIMT Engineering College,MTU,India;
paramjeet.rawat@gmail.com

Suraj Malik
Dept. of Computer Science,
IIMT Engineering College,MTU,India;
er_surajmalik83@rediffmail.com

Sudhanshu Gupta
Dept. of Information Technology,
Bharat Institute of Technology. College, MTU, India
Sudhu_gupta2004@yahoo.co.in

***Abstract*- WMN has been a field of active research in the recent years. Lot of research has focused various routing mechanism but very little effort has been made towards attack detection or intrusion detection. In this paper, we propose an attack detection approach for wireless mesh network using Honeypot technique. A Honeypot is a security resource whose value lies in being probed, attacked or compromised. A honeypot is designed to interact with attackers to collect attack techniques and behaviors. A collection of such Honeypots laid to effectively trap the attacker is called a Honeynet. In our paper, we propose a honeynet, that is able to trap the attackers by analyzing their attacking techniques and thereby sending the logs to a centralized repository to analyze those logs so as to better understand the technique used for attacking.**

Keywords: security, honeypot, honeynet, wireless, mesh, network.

I. INTRODUCTION

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks, has emerged recently, which is being adopted as the wireless internetworking solution for the near future. WMN has characteristics such as rapid deployment and self configuration. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure, it can be various forms like (i) Client WMN (ii) Infrastructural WMN and (iii) Hybrid WMN. Typical wireless mesh networks (WMNs) consist of mesh routers and mesh clients [3]. Fixed or static Mesh routers, forms a wireless backbone of the WMNs and interwork with the wired networks to provide multi-hop wireless Internet connectivity to the mesh clients. Mesh clients access the network through mesh routers.

Wireless ISP's are choosing WMNs to offer Internet connectivity, as it allows a fast, easy and inexpensive network deployment. Wireless mesh networks can easily, effectively and wirelessly connect entire cities using inexpensive, existing technology. Traditional networks rely on a small number of wired access points or wireless hotspots to connect users. In a wireless mesh network, the network connection is spread out among dozens or even hundreds of wireless mesh nodes that "talk" to each other to share the network connection across a large area.

The development of this technology has to deal with the challenging security, architecture and protocol design issues. The emergence of new applications of WMNs necessitates the need for strong privacy protection and security mechanisms against attacks. Amongst the several security attacks, intrusion detection has been the

most common and challenging attack. Traditionally intrusion detection involved a defensive approach where systems were either dedicated computers like firewalls or host based detection systems aimed at detecting attacks or preventing them. These systems existed as a part of the commercial/in-use networks and used techniques like pattern matching or anomaly detection. Another type of security systems are system integrity checkers, which are, typically host based. The problem that these systems face is that they are running on computers, which are in use on a daily basis. These systems usually have to deal with large number of connections and data transfers which results in huge log files and also makes it difficult to differentiate between normal traffic and intrusion attempts accurately. A proactive approach would be to discover these malware before they cause any damage, or at least, before their damage progresses. Such an approach is a Honeypot technique.

II. BACKGROUND AND RELATED CONTEXT

A Honeypot is a technique used to trap the attacker by monitoring and analyzing the techniques used by the attacker to a attack a system. Almost any software or packet captured by this Honeypot is malicious, as Honeypot do not run any real software but works as a simulator that pretends to be a real node. Honeypot is a supplemented active defense system for network security [2 ,7]. It traps the hackers by recording all the activities of the hacker and thereby preventing attacks. When integrated with some security framework it proves to be an effective defensive technique. The more the number of Honeypots in any network, the higher the chances are to capture malware. Honeypot is great way to improve network security and learn how to get information from a victim system using forensic tools. These systems can be used as a learning tool that helps to gather information as to how the intruder is attacking, which technique is being used by the hacker to attack a system. By definition a Honeypot is "a security resource whose value lies in being probed, attacked or compromised". So the more the Honeypot is attacked the easier it is to trap the enemy.

Honeypots are classified basically into two [2]:

A. Research Honeypots

These type of Honeypots are used to gather information. They help in learning about the attacker's attacking techniques and the various threats to the existing network. By understanding the motives of the enemy, we can design a security framework that can deal with such type of attacks. Honeypot technique actually do not directly provide any security but by having the knowledge of the various attacking techniques a better security framework could be designed. Information provided by Honeypots could provide valuable information for forensic department. Research Honeypots are mostly used by military, research and government organizations.

B. Production Honeypots

Production Honeypots are used to protect the company from attacks, they are implemented inside the production network to improve the overall security. In this type of Honeypot interaction is very low. The security administrator keeps a watch on the various types of threats that may be trapped in the types of Honeypots. While testing the security of the systems existing in an organization, unexpected actions may happen such as misusing other systems using Honeypot features. If the network administrator is not aware of this problem, they put organization in a big trouble. So production Honeypots basically implemented by the companies in order to prevent their systems from various attacks and thus minimizing threats.

III. ISSUES RELATED TO HONEYPOTS

A. Security issues

Honeypots [2] can be considered to be one of the latest technologies in network security today. There are various things that need to be considered, like Honeypot should be hidden from unauthorized users , honeypot should be protected; it should not be open and easily accessible as it may create some security problems.

B. Configuration issues

Things to consider while configuring a Honeypot are what will your Honeypot look like, where do you deploy your Honeypot , what is the best location of your Honeypot, what should be structure of the network in which

Honeypots are made, how many nodes should be made as Honeypot, to whom will they report the logs and in what form will they store the log etc.

C. Legal Issues

There are at least three legal issues [1] that you must consider:
• Entrapment - Attackers may argue entrapment
• Privacy – Laws exist that might restrict your right to monitor users on your system
• Liability - Realize that attackers may misuse your honeypot to harm others.

IV. PROPOSED WORK

We propose to create a HoneyPharm for trapping the activities of hacker in order to build a more secured WMN. Our proposal is based on a Clustered Honeypot approach where the entire network is divided into clusters. Each cluster consists of at least one Honeypharm that comprises of one or more Honeypot (i.e. Honey mesh clients and Honey mesh routers). These Honeypot traps all the activities of attacker and sends this information to the Remote Gateway(RG) which is a central place for collecting all the malwares. This remote gateway analyzes all these activities and stores all the data in log files. After the analysis, all these files are normalized and stored in a central database in the form of tables from where readable information can be presented in a proper way to the end users. This information can be viewed in two ways:
User View : where user can view Honeypot information of single cluster
Admin View : where administrator can view the information of all Honeypot's of all Cluster's.

A. Preliminaries:

1) The total functionality is client-server based architecture.
2) We consider a Infrastructural WMN which is divided into several clusters where each cluster consists of a Honeypharm that comprises of one or two Honey Mesh Clients (MC's) and one or two Honey Mesh Router's (MR's).
3) There is a central repository in which all data is stored in form of tables.
4) Nepenthes is used as a software for creating Honey MC's and Honey MR's.
5) A unique id is assigned to all the logs send by the Honeypots in order to distinguish between normal message and Honey message.

V. PROPOSED ALGORITHM

We propose to use a HoneyPHARM which is a system that manages, reports, and analyzes all distributed Honeypot . Honey MC's and Honey MR's captures malware's that attacks on their systems and reports about the same to their Gateway, that in turn sends this information to a central repository. This central repository gathers the data from various Honeypot's from various cluster's and analysis them and finally gives a report for the same in a web portal from where it can be viewed (by administrators managing the HoneyPharm or users working in the network). The web portal works in two modes : User mode and Administrator mode. In the Administrator mode, the Administrator's can view the information of security attacks of all clusters but in the User mode, the users can view the information about their cluster only.

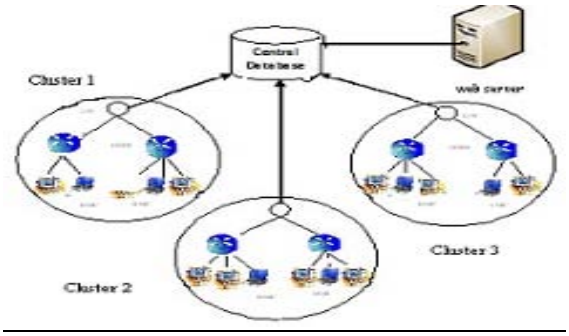

Fig. 1: Clusered WMN containing Honeyclient and Honey Routers

ALGORITHM

Step 1. Start Nepethes on each designated Honeypot in each cluster to trap the malware activities.
Step 2. If Honey MC's or Honey MR's captures the malwares, then
(i) Assign an unique id to each activity along with the cluster id.
(ii) The corresponding Honeypot stores this information in a log file and send it to its corresponding Gateway.
(iii) The Gateway after checking the special id attached to the message, sends this information to the central repository.
(iv) The central repository normalizes these log files and store them to the database for better analyses of these log files.
(v) After analysis data is sent to a web portal from where it could be presented to the users to give them knowledge about various security attacks going on currently in their cluster.
Else
(i)Keep running Nepethes and keep checking periodically that it is working properly or not.
Step 3. End

VI. RELATED WORK

A honeypot is a new and challenging technology and it can be involved in different aspects of security such as prevention, detection and information gathering. Honeypots serve as a learning tool for system administrators and also involved studying issues[2] concerning intrusion detection systems the challenges that these systems faced. Various types of honeypots like: Virtual honeypots [3] that simulate different types of honeypots in a device, Distributed honeypot that consists of an set of honeypot systems in a network in order to trap the attacker with good success ratio. Honeypharm implemented in paper [4] collects and reports the malwares to a centralized repository in order to monitor all malicious activities but this was implemented on Wireless Sensor Network which have energy and power constraints. Honeycomb[5] technique, another approach that produces attack signatures automatically by analyzing traffic on a honeypot. The system produces good-quality signatures, it lays more emphasis on analyzing the attacking technique by exploring the signature rather than detecting the attacker. This approach took lot of time to detect attack on quiet nodes whereas it works well at busy nodes. Combination of [6] correlated logs and flow based attack that gives high level of performance in detecting worm based attack. HoneyBow [11] is based on the high-interaction honeypot principle and has a capability of automatically collecting malware which propagates by exploiting new vulnerabilities.
But most of these techniques were generally implemented for any wireless network and not based on any particular type of network. Our proposal is specifically designed keeping in mind the Infrastructural WMN, and to the best of our knowledge, no such work has been done at this end for WMN.

REFERENCES

[1] "Honeypots: Concepts, Approaches, and Challenges", Iyatiti Mokube Computer science Armstrong Atlantic State University Savannah, Michele Adams, Computer Science ,Armstrong Atlantic State University Savannah, GA 31419.
[2] "Honeypot based Secure Network System", Yogendra Kumar Jain , Surabhi Singh Research Scholar Computer Science & Engineering Department Samrat Ashok technological Institute Vidisha, M.P., India, Yogendra Kumar Jain et al. / International Journal on Computer Science and Engineering (IJCSE).
[3] "Honeypot: a Supplemented Active Defense System for Network Security , Feng ."Zhang, Shijie Zhou. Zhiguang Qin, Jinde Liu, College of Computer Science and Engineering, University of Electronic Science and Technology of China, 2003 IEEE.
[4] "COLLECTING MALWARE FROM DISTRIBUTED HONEYPOTS HONEYPHARM,Ahmad Hassan and Majid Al Ali{ahmad.hassan,majid.alali}@aecert.ae , 2011 IEEE GCC, Dubai, United Arab Emirates.
[5] "Honeycomb . Creating Intrusion Detection", Signatures Using Honeypots Christian Kreibich, Jon Crowcroft University of Cambridge Computer Laboratory JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom.
[6] "Flow-based Worm Detection using Correlated Honeypot Logs", Falko Dressler, Wolfgang Jaegers, and Reinhard German, Computer Networks and Communication Systems, University of Erlangen, Martensstr. 3, 91058 Erlangen, Germany {dressler,german}@informatik.uni-erlangen.de.
[7] "Hybrid Honeypot System for Network Security" Kyi Lin Lin Kyaw, department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay, World Academy of Science, Engineering and Technology 48 2008.
[8] From Wikipedia en.wikipe,"en.wikipedia.org/wiki/Wireless_mesh_network
[9] " Threats and Vulnerabilities in wireless mesh networks", Dr. M.S. Aswal, Paramjeet Rawat, Tarun Kumar, International Journal Of Recent Trends in Engineering, November 2009.
[10] "An Integrated Security Framework For Open Wireless Networking Architecture" Jongmin Jeong And Zygmunt J. Haas, Cornell University, IEEE Wireless Communications , April 2007.
[11] "Collecting Autonomous Spreading Malware Using High-Interaction Honeypots", Jianwei Zhuge1, Thorsten Holz2, Xinhui Han1, Chengyu Song1, and Wei Zou1,
[12] Institute of Computer Science and Technology,Peking University, China.
[13] Laboratory for Dependable Distributed Systems,University of Mannheim, Germany.