Optimized Packet Filtering Honeypot with Intrusion Detection System for WLAN

Amandeep Singh
Asstt. Prof., C.S.E Deptt.
GZS PTU Campus,
Bathinda
amanmithri82@gmail.com

Pankush Singla
Asstt. Prof., C.S.E Deptt.
GZS PTU Campus,
Bathinda
pankush21singla@gmail.com

Sukhpreet Singh
Asstt. Prof., C.S.E Deptt.
SLIET University
Longowal
Sukhpreet.manshahia@gmail.com

Navdeep Kaur Khiva
Asstt. Prof., C.S.E Deptt.
GZS PTU Campus,
Bathinda
navdeep07khiva@gmail.com

Second A
Name of Dep
Institution's
Institution's
email-

Abstract: *A honeypot is used in the area of computer and Internet security. It is an information system resource which is intended to be attacked and compromised to gain more information about the attacker and the used tools. It can also be deployed to attract and divert an attacker from their real targets. Compared to an intrusion detection system; honeypots have the great advantage that they do not generate false alerts because no productive components are running on the system. This fact allows the system to log every byte and to correlate this data with other sources to draw a picture of an attack and the attacker. Traditionally honeypots are connected with end clients to detect the uneven behavior of traffic. Activities such as port scanning can be effectively detected by the weak interaction honeypot but many applications such as packet scanning, pattern scanning cannot be detected by weak honeypots. In our research we will propose a strong honeypot mechanism along with intrusion detection system to achieve maximum security in the wireless network. To achieve the objective of our research we placed the honeypot just after the Firewall and intrusion system have strongly coupled synchronize with honeypot. Monitoring will be done at packet level and pattern level of the traffic. Simulation will filter and monitor traffic for highlight the intrusion in the network.*

***Keyword**: honeypot*

INTRODUCTION

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks- most of these measures are based on known facts, known attack patterns. As in the military, it is important to know, who your enemy is, what kind of strategy he uses, what tools he utilizes and what he is aiming for. Gathering this kind of information is not easy but important. By knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather as much information as possible is one main goal of a honeypot.

Generally, such information gathering should be done silently, without alarming an attacker. All the gathered information leads to an advantage on the defending side and can therefore be used on productive systems to prevent attacks.
A honeypot is primarily an instrument for information gathering and learning. Its primary purpose is not to be an ambush for the blackhat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, purpose of attack and the blackhat community itself. All this information is used to learn more about the blackhat proceedings and motives, as well as their technical knowledge and abilities. This is just a primary purpose of a honeypot. There are a lot of other possibilities for a honeypot - divert hackers from productive systems or catch a hacker while conducting an attack are just two possible examples.

Honeypots are not the perfect solution for solving or preventing computer crimes. Honeypots are hard to maintain and they need operators with good knowledge about operating systems and network security. In the right hands, a honeypot can be an effective tool for information gathering. In the wrong, inexperienced hands, a honeypot can become another infiltrated machine and an instrument for the blackhat community.
This paper will introduce some basic terms, types as well as possibilities which can be used to implement a strong working honeypot.

History

The concept of Honeypots was first described by "Clifford Stoll" in 1990. The book is a novel based on a real story which happened to Stoll. He discovered a hacked computer and decided to learn how the intruder gained access to the system. To track the hacker back to his origin, Stoll created a faked environment with the purpose to keep the attacker busy. The idea was to track the connection while the attacker was searching through prepared documents. Stoll did not call his trap a Honeypot; he just prepared a network drive with faked documents to keep the intruder on his machine. Then he used monitoring tools to track the hacker's origin and find out how he came in.
In 1999 that idea was picked up again by the Honeynet project, lead and founded by "Lance Spitzner". Unfortunately it is not clear who founded the term "Honeypot". Spitzner's book lists some early Honeypot solutions, but none of these had Honeypot in their name.

Objective

To achieve or set proposed scheme and ideas, we will target our objectives given below:

- Monitoring of the traffic in wireless networks.
- Implementation of intrusion detection system in WLAN networks.
- Implement honeypot mechanism on IDS for comprehensive detection of IP terrific flow.
- Compare the simulation of proposed scenarios by analyzing performance metrics.

Methodology for research

Our research will start with study of intrusion detection system implementation and will proceed with honeypot implementation and avoidance of malfunctioning in wireless networks in following steps.

1st Phase: This phase will contain the basic functionality and collection of information (simulator, basic honeypot functions etc). Layout for comparison will be done in this phase.

2nd Phase: In this phase we will create a network with intrusion detection environment in OPNET simulator and will fetch the difference in the performance of the wireless network.

3rd Phase: We will implement the proposed scheme for honey pots to avoid the malfunctioning and achieve good monitoring measures. We will implement a strong honeypot mechanism along with intrusion detection system to achieve maximum security in the wireless network. Honey pot will be placed just after the Firewall and intrusion system will have strongly coupled synchronize with honeypot. Monitoring will be done at packet level and pattern level of the traffic. Simulation will filter

and monitor traffic for highlight the intrusion in the network.

4th Phase: Final step will be comparing of the proposed schemes with different scenario of network.

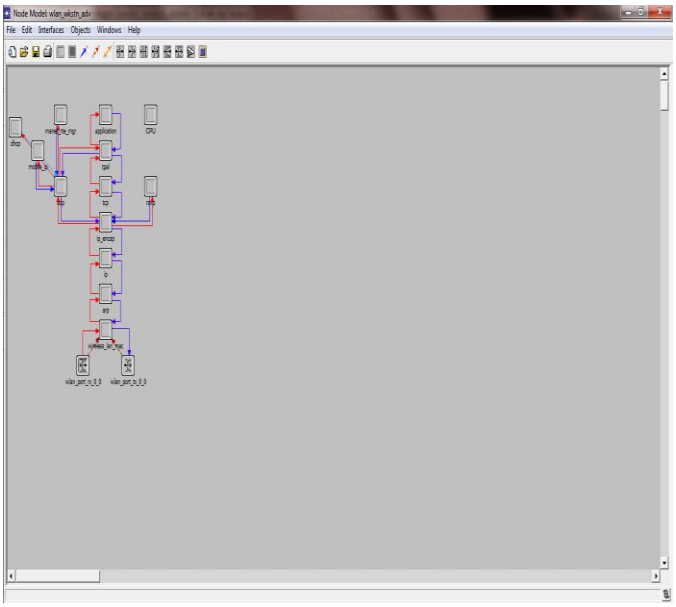
1. Simulation parameters

The network designed consists of basic network entities with the simulation parameters presented in table 1.

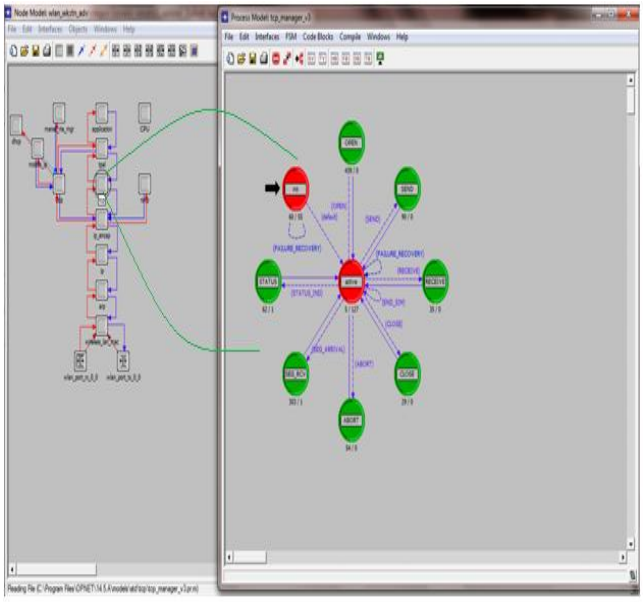
Simulation Parameters Table 1

Area of the sensor field	10×10km
Simulation Time	3600 second
Traffic type	FTP
Performance Parameters	Throughput, Delay and Network load
Security Protocols	MD5, DES,RSA
Application servers	Email server, FTP server, Web Browsing
No. of ATM Backbones	6
Attacking Nodes	4

Below is the node architecture for normal scenario network in figure 1.



Below is the process architecture for simulation network in figure 2.



Below are the throughput results for normal network scenario, attacked network scenario and finally network scenario with security.

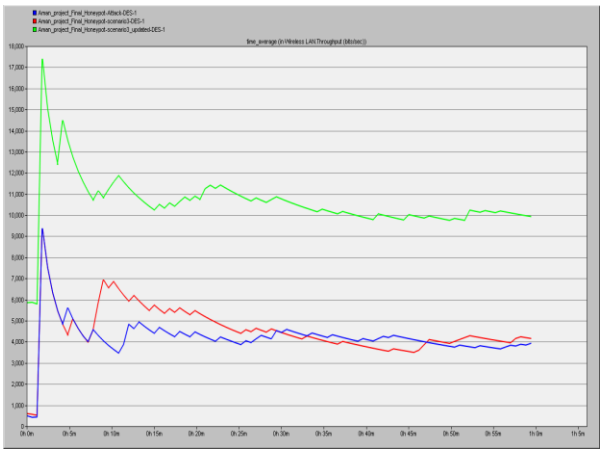


Fig. 3 Comparison of Throughput in Normal, Attacked and Security scenario

In fig. 3 throughput results of all three scenarios are compared. We have seen in fig. throughput of third scenario is maximum as compared to the first and second scenario. In showing graph x-axis shows the time and y-axis shows the throughput in term of seconds.

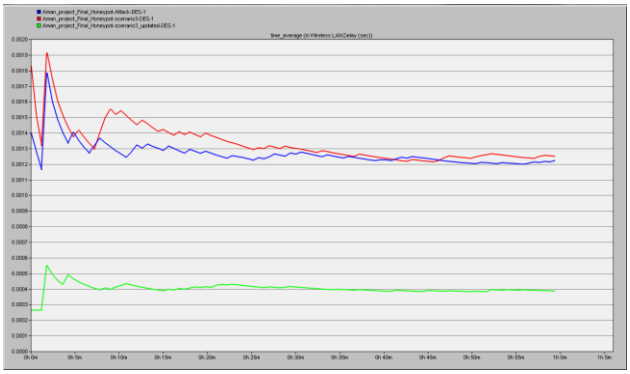


Fig. 4 Comparison of delay in simple, Attacked and Security scenario

In this figure the delay results of all three scenarios are compared. The three scenarios are simple scenario, Attacked scenario and Scenario with security. During simulation delay is found at different intervals. In showing graph x-axis shows the time and y-axis shows the delay in term of seconds. Maximum delay is finding in simple scenario and lowest delay finding in scenario with security. Value of delay in third scenario becomes constant after the starting point throughout the simulation process. It is concluded that during simulation for delay there is more fluctuation in first and second scenario and find more delay when there has no technique applied.

Load is the amount of traffic being carried by the network. In the figure below all three scenarios are compared. During simulation network load is found at different intervals. In showing graph x-axis shows the time and y-axis shows the network load in term of seconds. Maximum network load is finding in third scenario and network load is decreases gradually till the end of simulation.

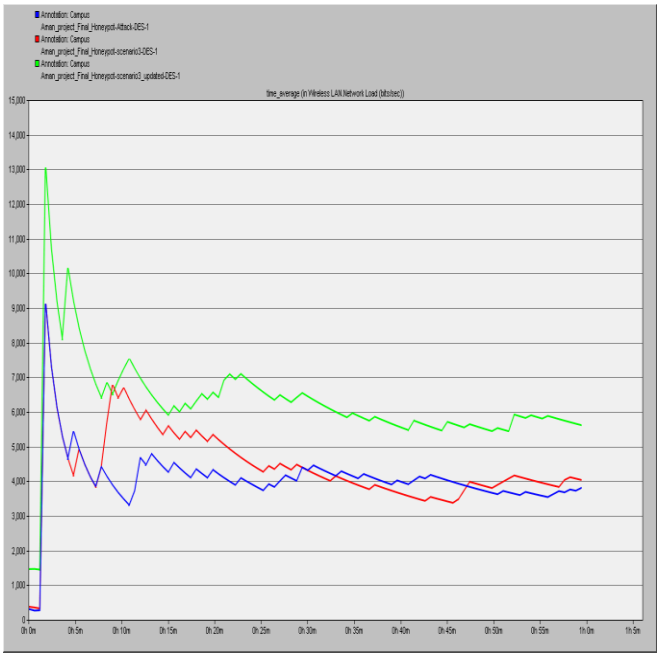


Fig. 5 Comparison of Network Load in Simple, Attacked and Security scenario

FUTURE SCOPE

In time, as security officials understand the benefits, honeypots will become an essential element in an operation of enterprise-class security. We believe that although honeypots have legal problems now, they do provide useful information regarding the security of a network. It is important that new legal rules be formulated to promote and support research in this area. This will help solve the recent challenges and make possible to use honeypots to benefit the Internet community at large.

In future this honeypot can be embedded in real time websites so that it gives effective detection rates for packet attacks and spoofing types of attacks. In future this honeypot is extended to find web application vulnerabilities for electronic applications. This research work can be extended by using different security algorithms.

REFERENCES

[1] YashikaBirdi," A Review of Honey Net Technology", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013

[2] Navita Sharma, Gurpreet Singh, ''Intrusion Detection System Using Shadow Honeypot'', International Journal of Emerging Technology and Advanced Engineering, August 2012, vol.2, issue.8, pp.17-19

[3] BalajiDarapareddy, VijayadeepGummadi," An Advanced Honeypot System for Efficient Capture and Analysis of Network Attack Traffic", International Journal of Engineering Trends and Technology. May 2012, vol.3, issue.5, pp.616

[4] MuktaRao and DrNipur, "Network Security in Organizations Using Intrusion Detection System Based on Honeypots", Global Journal of Computer Science and Technology Network, Web & Security, August 2012, vol.12, issue.16, pp.78-81.

[5] Gajendra Singh Chandel, PriyankaMurotia, "Manet Threat Alarming Based On System Statistics & Support Vector Machine", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4, July-August 2012, pp.1722-1726

[6] Matthew L. Bringer, Christopher A. Chelmecki, and Hiroshi Fujinoki,"A Survey: Recent Advances and Future Trends in Honeypot Research",I. J. Computer Network and Information Security, 2012, 10, 63-75 Published Online September 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012

[7] Heberlein, L.T., G. Dim, K. Levilt, B. Mukhejee, J. Wood, and D.Wolber, " A network security monitor,'' Proc., 1990 Symposium on Research in Security and Privacy, Oakland, CA, May 1990, vol.3, no.2, pp. 296-304.

[8] LIN Ying,ZHANG Yan, OU Yang-Jia," The Design and Implementation of Host-based Intrusion Detection System", Symposium on Intelligent Information Technology and Security Informatics, 2010 IEEE Computer Society.

[9] Cliff C. Zou Ryan Cunningham, "Honeypot-Aware Advanced Botnet Construction and Maintenance', Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN'06) 0-7695-2607-1/06 $20.00 © 2006 IEEE.

[10] Chunmei YIN, Mingchu LI, Jianh MA, Jizhou SUN," HONEYPOT AND SCAN DETECTION IN INTRUSION DETECTION SYSTEM", Mayhai 2004 0-7803-8253-6/04617.00 02004 IEEE