ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IDENTIFICATION OF ATTACKERS BY USING SECURITY SERVICES OF HONEYPOT

Dinesh S. Kapse*, Prof. Vijay Bagdi
* WCC DEPT. A.G.P.C.O.E, NAGPUR.
WCC DEPT. A.G.P.C.O.E, NAGPUR.

ABSTRACT

Internet security is vital issue recently. it is necessary to protect our assets or valuable data from unauthorized person. There are number of techniques are available, one of them is honeypot. Honeypots are modern approach to give high level security to our data. Honeypot can be deployed at victim's site to attract and divert an attacker from their intended source or targets. Honeypots have the big advantage that they do not gives the vital information to the unauthorized person because each traffic is observed by this security mechanism. This fact enables the system to log every byte that passes from network as well as from honeypot and it relates this data with other sources to find the real source of attack as well as attacker.In this paper the brief introduction of honeypots and the types and its uses are described. And also paper this paper would give introduction about Kerberos finally we shall conclude by looking at the future of honeypot using Kerberos.

KEYWORDS: Internet security, Unauthorized person, Honeypot, Attacker, Kerberos.

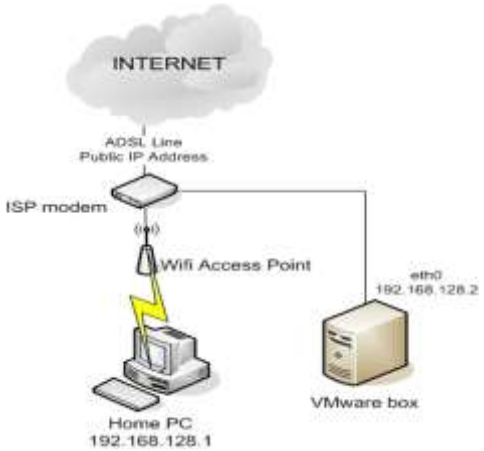
INTRODUCTION

In recent years global communication is more significant in every day. So that computer crimes are growing rapidly as well as demand for more aggressive form of security also increases. One of this security methods involves the use of honeypots to as gather as much information as possible related to attack and attacker is one main target of honeypot. Usually information gathering should be done without attacker's knowledge.

The much information is from honeypot servers, the more appropriate attack pattern we can generate and we can find the source of attack. Honeypot is an outstanding technology that helps us to secure our valuable data from the attacker.

WHAT IS HONEYPOT AND HONEYNET?

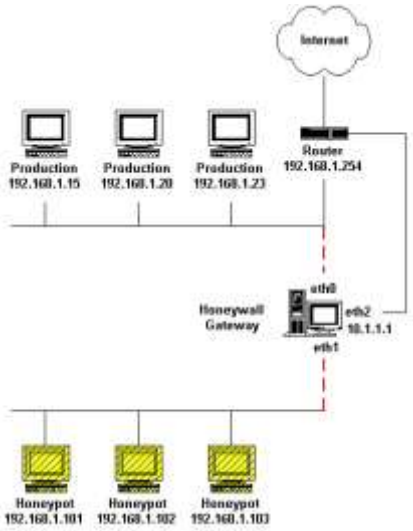
The honeypot is basically virtual machine for information gathering and learning to emulate real machine. Honeypots do not have any untrusted, unuseful servers , workstations on network because they are closely watched by administrator.fig1 shows general diagram of honeypot.



[1]Diagram2:honeypot

Its primary purpose is not to be avoid the attackers but gathers more information about it by giving information from the honeypot. All this information is used to learn more about the technical knowledge and abilities of the attackers. After gathering all this information we will give more security to our data.

Two or more honeypots on network from a honeynets. Basically Honeynet is used for monitoring a network in which one honeypot may not be sufficient. To successfully design a honeynet we must correctly arranged the honeynet architecture.



[2]Diagram1: deployment of honeynet

There are two main reasons why honeypots are deployed
I.To learn and gather information about attacker.
II.To gather forensic information required to aid in the prosecution of intruders.

TYPES OF HONEYPOT

Honeypots has two types –

1) Low interaction
2) High interaction

Basically interaction measures the amount of activity that an intruder may have with honeypot. Depending on this interaction we categorize honeypots in above two types

Low interaction:- Typical low interaction honeypot is also known as gen-I honeypot. They had only basic mechanism for capturing requirements and data control. The firewall is used to data control requirement in this type. In IDS also has two major roles the first role is capture all network traffic and second is to parse network traffic.

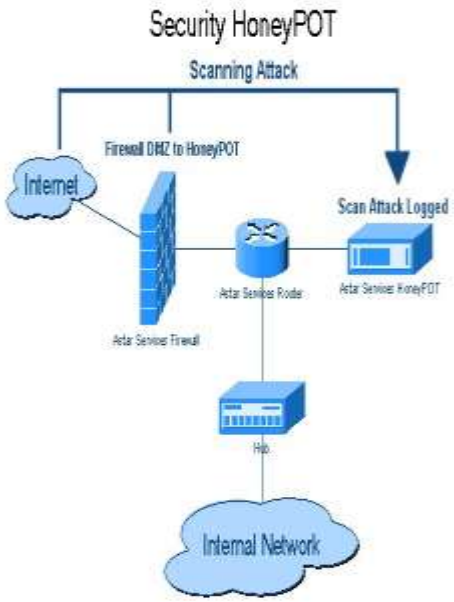
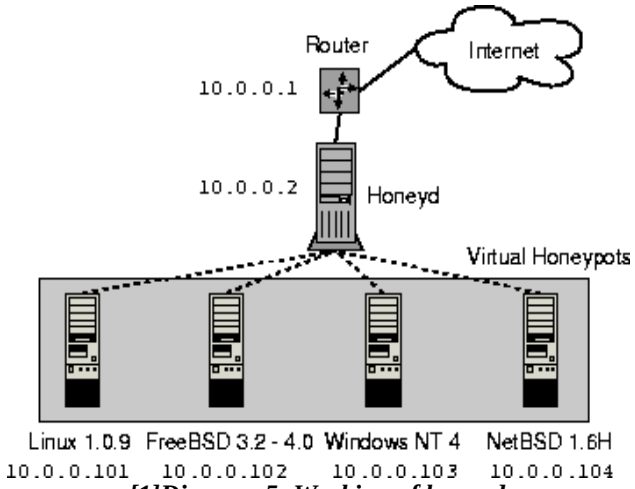


Diagram3: gen-I honeypot

2)High interaction:- A typical high interaction honeypot consist of following elements: Resource of interest, Data Control , Data Capture and Data loss.Once honeypot is compromised malicious user may try to attack from the honeypot but firewall avoids and captures the data and alert the administrator.

HONEYPOT ARCHITECTURE

GENERATION-I HONEYPOT(LOW INTERACTION): This generation honeypot is the beginner for the automated attack against the network. It only providing the services of honeypot not actually honeypot and by providing the services. It does not provide the actual operating system so the attacker can not have gain to the system. In this IDS only captures the network traffic there is no modification can be perform in the system for network traffic. Examples of this are Honeyd for stimulating large structured network and Specter works on application layer for large enterprise.



[1]Diagram 5: Working of honeyd

GENERATION-II HONEYPOT(HIGH INTERACTION)

This generation proving better mechanism of data capture and control. It providing the actual operating system to collect the target attacker to gain collect more information against the attacker and analyzing by monitoring log information about the attacker.

Example of this is Honeynet which is used for research purpose for Forensic lab to know in which pattern the attacker will attack and collecting the information about the attacker.

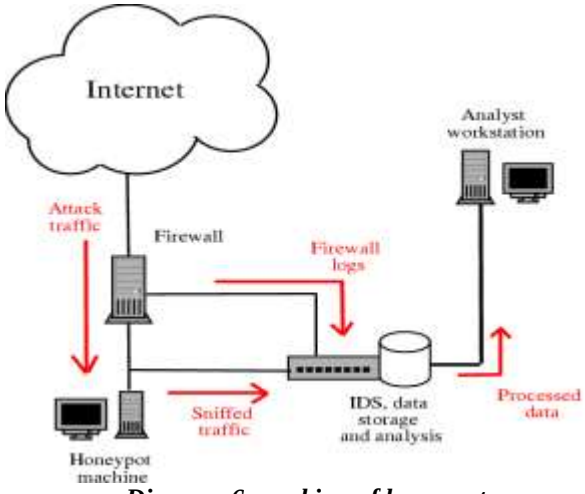


Diagram 6: working of honeynet.

KERBEROS AS SECURITY PROTOCOL

The Kerberos comes from Greek methodology for network authentication protocol. It providing secure authentication, application, and network devices having password storage mechanism. In Kerberos message hiding while transferring in the network.

In TELNET, FTP and other protocols password are visible in network packets while transferring in the network and can be identified but Kerberos server provides in the encrypted form so which is unreadable and can not be easily identified helpful for large telecommunication network.

How it works?
Kerberos is a trusted third party for the secure verification. It contains the following parameters

Realm:- A user defined Administrative boundry.

Key Distribution Center (KDC):- It provides encrypted tickets to ensure a secret key to user.

Principal:- providing unique name for each user services.

Tickets:- Helpful for client authentication to a server.

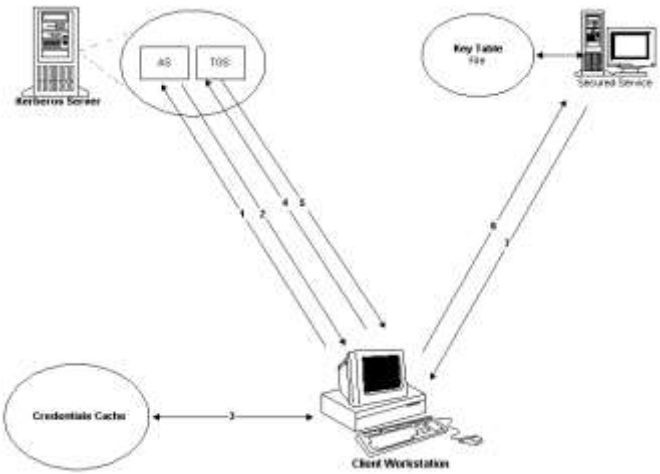


Diagram 7: Kerberos workstation

CONCLUSION

In this paper we have provided a brief overview of honeypot in terms of security provided in the various architecture in the generation of honeypot. It is a useful tool for security purpose in the enterprise if honeypot can be used for web based clients because number of attacker are trying to hack the system using internet this is very helpful for forensic lab to analyze the attacker information.

Kerberos it is mechanism which is very helpful for security purpose in the network as used in KDC which is powerful and fully secure as encrypted keys is provided as future if we use as security protocol to implements the honeypot.

REFERENCES

[1] Srivastha S Rao, ”Web Based Honeypots Network”, International Journal of Scientific and Research Publication, volume 3, Issue 8, Augest 2013.
[2] Iyatiti Mokube , ”Honeypots : Concepts, Approsches , and Challenges ” Armstrong Atlantic State University Savannah,GA31419.
[3] Miss. Swapnali sunder Sadamate “Review Paper on Honeypot Mechanism-The Autonomous Hybrid Solution for Enhancing”,IJAR,Computer Science and Software Engineering volume 4, Issue 1,Jan 2014.
[4] Haibo Liu, “Application of Virtual Honeypot on the Mining Enterprise Network Security”, IEEE Transaction vol 13, no.3, March 2012.
[5] Nehasahu ,VineetRichhariya , ”Honeypot: A Survey”, IJCST Vol. 3, Issue 4, Oct-Dec 2012.
[6] Edwards Balas and CamiloViecco,”Towards a Third Generation Data Capture Architecture for Honeynets”, IEEE 2005 Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 15 -17 June.
[7] http://www.honeynet.org”Know Your Enemy: Honeynets” May 2006.
[8] http://www.honeynet.org”Know Your Enemy: Sebek” 17 November 2003.
[9] JiqiangZhai ,Keqi Wang” Researh on Applications of Honeypot in Campus Network Security”, 2012 International Conference on Measurement, Information and Control (MIC).
[10] Saurabh Kulkarni ” Honeydoop - A system for on-demand virtual high interaction honeypots”, IEEE 2012 The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)
[11] Sainath Patil, ”Honeyweb: a web-based high interaction client honeypot”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
[12] National Conference on Emerging Trends in Engineering & Technology (VNCET-30