Article can be accessed online at http://www. publishingindia. com

Efficient Security Services of Honeypot using Kerberos for Detecting Intruders

Dinesh S. Kapse*, Vijay Bagdi**

Abstract

Internet security is a vital issue of recent times. It is necessary to protect our assets or valuable data from unauthorised person. There area number of techniques 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 give the vital information to the unauthorised 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. This paper would also give introduction about Kerberos. Finally we shall conclude by looking at the future of honeypot using Kerberos.

Keywords: Internet Security, Unauthorised Person, Honeypot, Attacker, Kerberos.

Introduction

In recent years global communication has become more significant in everyday life, so that computer crimes are growing rapidly as well as demand for more aggressive form of security also increases. One of these security methods involves the use of honeypots. To 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. More the information from honeypot servers, more appropriate attack pattern we can generate and can find the source of attack. Honeypot is an outstanding technology that helps us to secure our valuable data from the attacker.

Literature Survey

According to Rao (2013) and Vinay Hedge the web-based honeypot gives brief introduction to honeypots, its types and uses.

According to Balas and Viecco (2005) the third generation data capture achitecture for honeypot gives new data collection architecture that addresses the need for both rapid compression and detailed analysis by accessing methods of relational model fast path and canonical slow path. According to Liu (2012), the application virtual honeypot on mining enterprise network security gives modified algorithm which provides high degree of interactivity level of virtual honeypot helpful for network maintenance as needle-man wunsch algorithm which compare sequences.

What is Honeypot and Honeynet?

The honeypot is basically a virtual machine for information gathering and learning to emulate real machine. Honeypots do not have any untrusted, un-useful servers, workstations on network because they are closely watched by administrator. Fig. 1 shows general diagram of honeypot.

* Dept. of Wireless Communication & Computing, A. G. P. C. O. E, Nagpur, Maharashtra, India.
Email:dinesh25. kapse@gmail. com

** Dept. of Wireless Communication & Computing, A.G.P.C.O.E, Nagpur, Maharashtra, India.
Email:bagdi. vijaysingh@gmail. com

Fig 1: Deployment of Honeynet

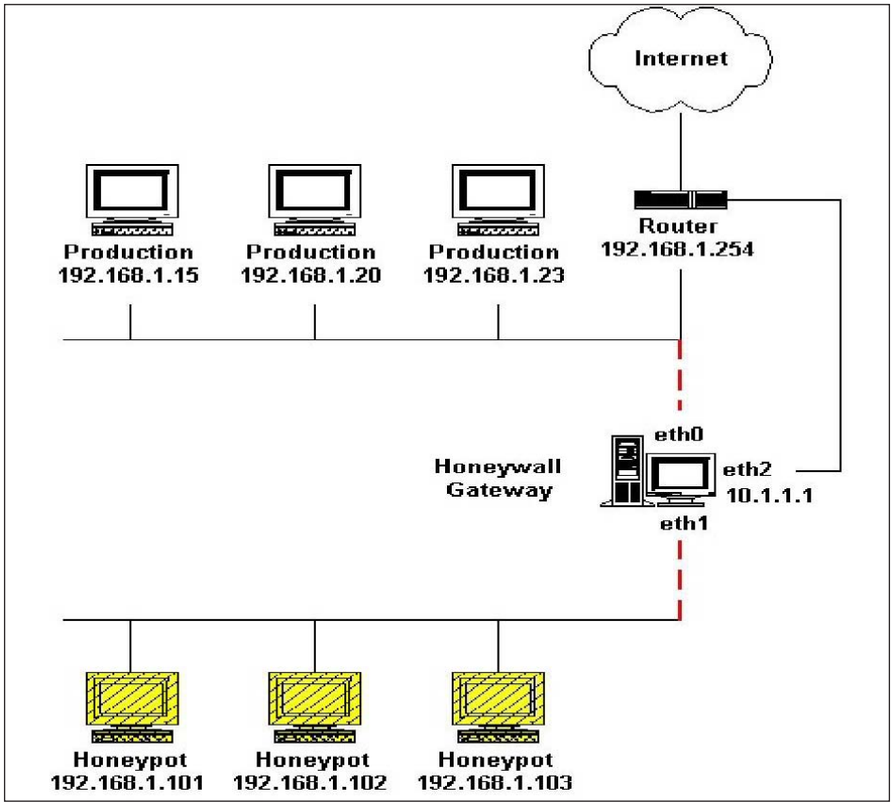
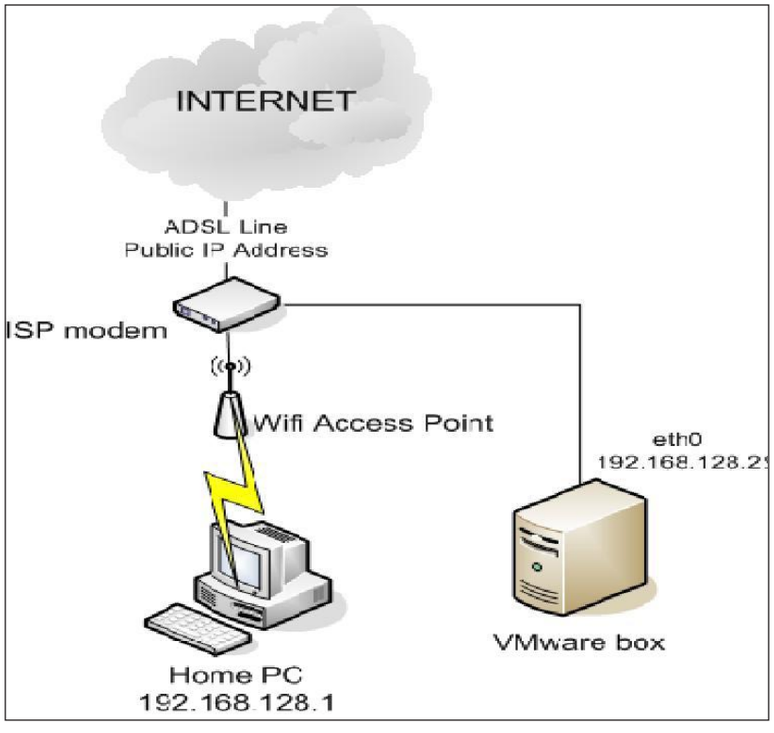


Fig 2: Honeypot



Its primary purpose is not to avoid the attackers but gather more information about them 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 forma honeynet. Basically honeynet is used for monitoring a network in which one honeypot may not be sufficient. To successfully design a honeynet we must correctly arrange the honeynet architecture. 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.

System Design

How it works?

Kerberos is a trusted third party for the secure verification. It contains the following parameters

Fig. 3: Data Flow of Project Work

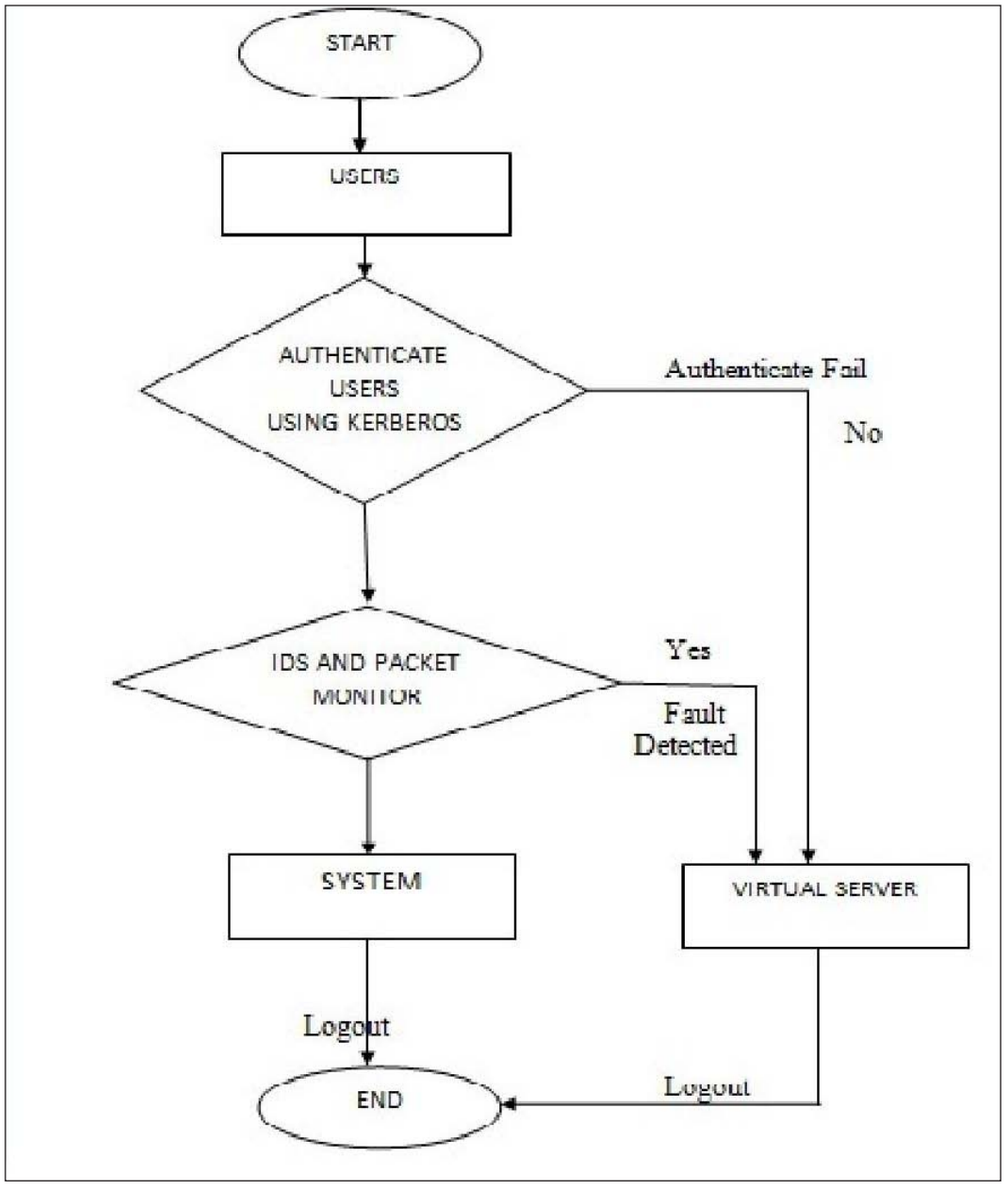
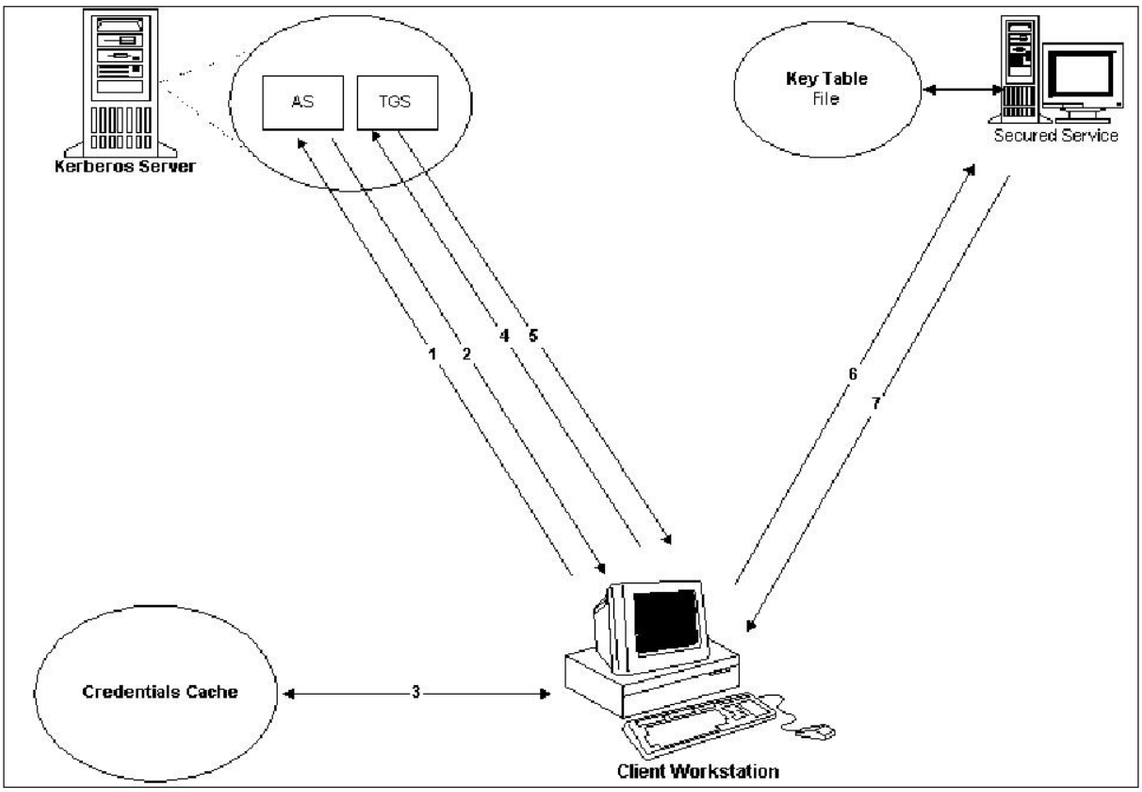


Fig. 4: Kerberos Workstation



Realm: It is a user defined administrative boundary.

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

Principal: It provides unique name for each user service.

Tickets: Helpful for client authentication to a server.

Modules

Module 1

(Registration Process using Kerberos) In our system, module one is taken for the registration process for the all clients. In this module we have used the Kerberos protocol for the security purposes because it can provide various levels to add on the single system as the part of security. Following are the different forms for the three levels of registration process. Whenever user has to complete the registration process,he/she can access the system.

1. Personal: In this form all information about user is to be filled necessary for using the system such as name, address, city, mob_no, email_id. Email_id is mandatory for this which should be valid to use our system. We have provided three passwords to the user, to be used for the login purpose. The first password is 5 character long, second is 8 character, and third is 10 character long. The specialty of our system is that in every existing system they just provide single password for the login purpose but we are providing three passwords for this as the passwordneed not remembered.
2. Identification for User: It is the first level of system. It contains different identity proofs for the correct verification of user which can be driving license, PAN card, Aadhar Card,or Election Card number required to be filled during the registration process.

Psychometric Questionnaires

It is the second level for security which contains various questions related to information about the user like childhood nickname, favourite childhood friend, mother and father's first meeting, city or town, first job, mother's maiden name. These are the simple questions related

to the user's personal life and known only by the user. These are very helpful to identify the user while logging to the our system after registration otherwise the user is considered as fake user.

3. Image Optimisation It is the third level for security which contains the group of images. The images should be visible to the user and out of those the user has to select five images. There is no importance of sequence but the proper images are to be selected by the user. When the user has furnishedall this information for the registration process, the user id is provided to the user for using the system. When the user clicks on the save button of last level the OTP is generated for that user for login. The OTP is usedfor a particular instance of login only. When the user finishes the login, the next OTP is generated.

Module 2 (Login Process)

The second module of honeypot system contains the login procedure for the user to use the system. When the user finishes its registration then one OTP is generated by using random number of three passwords of 5, 8, and 10 characters. Here the user does not know which passwordis generated whenever he/she opens the email account. In that one OTP is generated and password is character matching for that OTP which was given by the user at the time of registration. After that in the login screen, a colour code box of 8 colours is displayed and an OTP is generated whose character of code is entered depending upon the length of OTP as each colourhas 2 characters. After that the next form is open which is the second security level for login purpose and user has to provide the password having the number of OTP characters which the system has sent to the user's email ID. Then identification information has to be entered as mentioned in registration. Psychometric questionnaires similar to that at the time of registration and at last 5 images have to be selected to complete a perfect authenticated login trusted user. Then the user can use the utilities as provided in the system.

Module 3 (Client System Utilities)

Once the trusted user is logged in, two of the system utilities are to be available for the user as Upload and Download. Also the number of clients which are working in the particular organisation is shown in the system and user can communicate directly with them by simply selecting the user.

Upload: In this menu, user has the facility to send the attachment to a number of usersor client can communicate directly with the user without packet loss.

Download: In this menu, user has the facility of downloading authenticated files. He can directly download the files from the main server without interrupt but the limit of file downloading is 5 files only and if he wants more then he needs to login again

Module 4 (Administration)

In the server side of system there are four utilities to be performed.

Main IDS

This utility keeps record of all authenticated or trusted users and continuously monitors the activity of all users viz. tasks performed by the user, login time, logout time, type of activity performed. It also maintains each record of user in the database by simply selecting user details.

Honeypot IDS

This utility keeps record of all unauthenticated or untrusted users and continuously monitors the activity of all users viz. tasks performed by the user, login time, logout time, type of activity performed. It also maintains each record of user in the database by simply selecting user details and the main entry of the task done by user to the database. In this way the intension of each user can also be verified.

Attacks

It is the main part of the system where the number of attacks can be shown where the administrator has the information about the attacks. There are two types of attacks which can be measured by our system.

A] DDOS Attack: This attack can be carried out in various ways and various strategies are mentioned. The underlying aspect would be to congest victim's network and thus make it inaccessible by other clients. Its objective is to deny or degrade users' ability to legitimately access

network. DoS attacks are accomplished by draining the limited resources of network bandwidth by flooding with packets or exhausting host resources by consumption of CPU cycles.

B] Fingerprints Attack: In computer science, fingerprinting algorithm is a procedure that maps an arbitrarily large data item (such as a computer file) to a much shorter bit string, its fingerprint, that uniquely identifies the original data for all practical purposes just as human fingerprints uniquely identify people for practical purposes. This fingerprint may be used for data deduplication purposes. Fingerprints are typically used to avoid the comparison and transmission of bulky data. For instance, a web browser or proxy server can efficiently check whether a remote file has been modified, by fetching only its fingerprint and comparing it with that of the previously fetched copy. Fingerprint functions may be seen as high-performance hash functions used to uniquely identify substantial blocks of data where cryptographic hash functions may be unnecessary. Audio fingerprint algorithms should not be confused with this type of fingerprint function.

Analysis

In this menu the number of attacks can be counted by the server against the users' activity. It keeps the record of all users. It will be shown in the graphical way of the attacks pattern to be mentioned in our system i. e. number of attacks by the user can be counted.

Module 5 (Honeypot Virtual Server)

This module is very important for our project as mentioned in the introduction part of our system. The actual use of honeypot is to collect more information from intruders. In this system whenever an user tries to make entry to the system after the registration, itis not possible because we have provided so much security in the project. Also if the user tries to make untrusted login to the system at every phase of the system, it directly goes to the honeypot i. e. the virtual server. It visualises like the actual server. If the user tries to do the illegal authorisation it is not possible.

Result Analysis TABLE I

Conclusion and Future Work

In this system we have provided a implementation of honeypot in terms of security provided in the various architecture in the generation of honeypot. It would be a useful tool for security purpose in the enterprise if honeypot can be used for web based clients because a number of attacker try to hack the system using Internet. This is very helpful for forensic labs to analyse the attacker's information. Kerberos is the mechanism which is very helpful for security purpose in the network. We have used Kerberos to implement the levels of security and OTP is the technique we applied for the better security purpose. This system has very strong security structure.

Future Implementation

In future we would like to add more modules related to the utility of the system. In this module we can add more security levels to increase more security provided to the system. We can implement this system for graphical representation for the entire section to view all users' information having the facility to maximise and minimise using pointer.

References

Balas, E. , & Viecco, C. (2005). *Towards a third generation data capture architecture for Honeynets.* IEEE 2005 Workshop on Information Assurance and Security United States Military Academy, West Point, NY, (pp. 15 -17).

Know Your Enemy: Honeynets (2006). Retrieved from http://www. honeynet. org

Know Your Enemy: Sebek (2003). Retrieved from http:// www. honeynet. org

Kulkarni, S. (2012). *Honeydoop - A system for on-demand virtual high interaction Honeypots.* IEEE 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012).

Liu, H. (2012). *Application of virtual honeypot on the mining enterprise network security.* IEEE Transaction, March, 13(3).

Mokube, I. (2007). *Honeypots: Concepts, Approaches, and Challenges*. Armstrong Atlantic State University Savannah, GA31419. *National Conference on*

Emerging Trends in Engineering & Technology (2014).

Rao, S. S. (2013). Web based honey pots network. *International Journal of Scientific and Research Publication,* 3(8), 1-5.

Patil, S. (2012). Honeyweb: A web-based high interaction client honeypot. *International Journal of Engineering Research and Applications.*

Sadamate, S. S. (2014). Review paper on Honeypot mechanism-The autonomous hybrid solution for enhancing. *International Journal of Advanced Research in Computer Science and Software Engineering,* January, 4(1), 854-858.

Sahu, N. , & Richhariya, V. (2012). Honeypot: A survey. *International Journal of Computer Science and Technology*, October-December, 3(4).

Zhai, J., & Wang, K. (2012). *Research on applications of Honeypot in campus network security*. 2012 International Conference on Measurement, Information and Control (MIC).