Eph - International Journal Of Science And Engineering
ISSN (Online): 2454-2016
Volume 05 Issue 01 January 2019

DOI: https://doi.org/10.53555/eijse.v5i1.110

KERBEROS BASED DATA SECURITY IN RESEARCH & PRODUCTION HONEY POT

Ms. Apurva Saxena[1*], Dr. Pratima Gautam[2], Dr.Anubha Dubey[3]
[1]Research Scholar, Computer Science Engineering, Rabindranath Tagore University, Bhopal, India
[2]Dean of Computer Science and Application,Rabindranath Tagore University, Bhopal, India
[3]Independent Researcher and analyst, Bioinformatics,Independent Researcher,Gayatri Nagar,Katni,India

Corresponding Author:-
Email: apurvasaxena16@gmail.com

Abstract:-

A honey pot is a technique of cloud computing that is proposed for capturing hackers or tracking unusual methods of attack. This technique will seize, recognize and duplicate the hacker behavior. It works in Cloud environment where anything like technology, tool, and result can be offered as a service. Purveyors offer and deliver such services to their customers via the network. Production honeypot is one of the types of honeypot which is used to solve the problem of data security in organizations. Honeypot techniques are used to detains the actions of intruder and create a log-file for providing better security in to the cloud network. Kerberos is a protocol for validating the services which requests between true hosts across the network, such as the internet. Kerberos builds on symmetric key cryptography and needed trusted third party, Key Distribution Centre(KDC) which uses public key cryptography. This paper presents the concept of production and research Honeypot as a service in cloud environment by implementing the benefits of Kerberos Authentication system, which distinguishes between hackers and users, and to provide overall security to the data/network.

Keywords:- *Honeypot, Kerberos, Cryptography.*

INTRODUCTION

Cloud computing is a new technique put ahead from industry circle, it is the development of equivalent computing, distributed computing and grid computing, and is the amalgamation and[5]development of virtualization, utility computing, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)[6]. To users, cloud computing is a Pay-per-Use-On-Demand mode that can opportunely access shared IT resources through internet. Where the IT resources include network, server, storage, application, service and so on and they can be organized with much rapid and easy manner, and least management of and communications with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Virtualization is a solution point in the cloud system that provides multiple virtual illustrations of a physical resource and if a single instance of are source is vulnerable then connected patrons get affected [7]. A honeypot is designed for trapping hackers or tracking unconventional or new methods of hacking. Honeypots are used to identify vicious behavior performed over the Internet. If any attacker tries to invade or penetrate in the network by connecting this technique honeypot will ambush, detect and draw its activities. It is designed in such a way that if anything thrown at them will confine whether it may be tool or strategy. Honeypot has a special characteristic of uninterrupted monitoring the behavior of the intruder/attacker and requires minimal resources to trace the movement. Honeyd is an open source honeypot application that keeps virtual host on network. It's a type of a low interaction honeypot which perform services like FTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol).The greatest impact of the honeypot is it simplicity. It gives a smaller amount of traffic in the network. Whenever connection is sent to the honeypot it is being access by illegal activity [11].There are two different types of honeypot are as follows [8]:

1. Production Honeypot: The concept of production honeypots is to imitate real production systems and have attackers use time and reserve attacking them as opposed to the production systems and to learn the way they develop vulnerabilities in production environment. Production honeypots mainly follow specific services and occasionally operating systems to encourage hackers. They can also imitate different viruses and trojans to attract the attackers. For an example to examine attacks on web servers a production honeypot imitating the Web server and fake services can be organized. The further very appealing part of production honeypots is that, they can be very well deployed within to find out the inside ambiguity and attackers within.

Production honeypots can only follow and confine activities that directly interact with them; they cannot detain attacks beside the real systems. That is why they cannot swap any existing technology but can append a prevailing layer to the Defense in Depth architecture. They might become a compromised host. Specifically, they have the risk of individual taken over by the attacker and being used to damage other systems inside or out of the organization. It could be a very difficult situation if the honeypot is used beside third party systems but it scarcely applies to production honeypots because of the imperfect follower and interaction provided. It's a type of low interaction honeypot, which is simple to use and has only restricted information about the hacker's redirect and explanatory his attacks. It is applied in business corporations and organizations.

2. Research Honeypot: Research honeypots are fundamentally used for learning new methods and tools of attacks. Research honeypots are used to accumulate aptitude on the general threats organizations can face, which gives the organization a better protection alongside those threats. Its main goal is to gain info about the way in which the attackers development and performs lines of attacks. These types of honeypot are complex to construct, deploy and manage. They are basically used by organizations like universities, governments, the military and intelligence systems to learn more about threats. Research honeypots provides a strong platform to study cyber-threats and forensic skills. It provides detail information about the strategy and motives of the attacker. It is complex to implement. It is mainly used in military, research and government organization.

Honeypots are categorized into different forms:-

- Low-interaction Honeypots: It necessitates only one physical machine. This honeypot gives the information about the attacker who is recurrently access the network. They use hardly any resources on the multiple virtual machines with a minute response time. It requires less code by which difficulty of security gets compact.
- Medium-interaction Honeypot: In this invader is not in statement with real system. This honeypot did not give us feature information about the hacker. It provides fractional service as compare to low-interaction honeypot.
- High-interaction Honeypot: It works on remote network in which it hosts variety of services. It gives the most amount of attacker's information activities when interact with our system. This technique is implementing on one physical machine per honeypot which direct increase the cost and maintenance.

Honeypot gives us important information about the attacker'saction [9]. The honeypot is a system or computer who sacrifices themselves to target the attacks of hackers. Like as honeypot, Kerberos is also one of the authentication protocols which executes on the network, increases the authenticity to protect the data of the client/host by a ticket or token granting ticket (TGT). It has time bound and[17]encrypts it by using secret key in the ticket granting service (TGS).Kerberos protocol is as a default verification method in Windows. Kerberos is a confirmation protocol in which user and server can usually validate to each other across an unconfident network connection, to guarantee data integrity of the message and privacy of channel communications. Therefore, here we use Kerberos authentication method in research and production honeypot to increase the protection and validation of the network.

METHOD

Data security is of utmost important for industries and Government organizations. So here an attempt is made to provide security to all the valuable data in cloud network. This is made possible by implementing [25] Kerberos (developed for Project Athena at the Massachusetts Institute of Technology) and Honeypot cloud computing technique.

[1] Kerberos: Itis a computer network validation protocol to all major operating systems, such as Microsoft Windows, Apple OS X, FreeBSD and Linux that works on the basis of tickets to allow users corresponding over an insecure network to confirm their identity to one another in a secure manner [10].Kerberos protocol is as a default verification method in Windows. This name Kerberos was taken from the Greek mythology "a three-headed dog" that guards the gates of Hades. These three heads represent a client, a server and a Key Distribution Centre (KDC). KDC act as a third-party authentication service. By default Kerberos uses UDP port 88. Kerberos builds on symmetric key cryptography and needed trusted third party (KDC) which uses public key cryptography.

Authentication Process of Kerberos: Kerberos protocol works based on the ticket system in which Key Distribution Center (KDC) is a Domain Controller (DC)[17]which keeps the information of each user who is in the network. NTP (Network Time Protocol) is a very constructive protocol which synchronizes the time in whole network between KDC, NFS and client. It may be possible that KDC may be in different country from the other server and client. KDC generate TGT for user in the network and it contains its possess key to encrypt the TGT [31]. This TGT sends back to the user in Kerberos tray which is a memory of the user. If system gets crash down by any reason this Kerberos tray will be safe from this. Now if customer wants to send data to file server, we need ticket for that. TGT will go back to KDC with request for the ticket for file server. KDC will not cross-check the client information, as it will decrypt the TGT by its own key. After decryption method applied on TGT, KDC will not check the identity of the client. This TGT was previously generated by the DC itself. This TGT also has its own Timestamp after which it gets damaged robotically. Consumer set this TGT copy in its Kerberos tray as its personality. KDC produce the ticket for the client which will be encrypting with its own key. File Server and KDC are connected with each other. Now KDC generate the ticket for the client who wants to share the data with the file server. This ticket will be stored in the tray, as ticket has its own timestamp. Within this time limit of the ticket, it sends its copy from tray to the file server[31].The file server does not be familiar with this client who sends the ticket, so the server decrypts this ticket by possess key. As file server and KDC check the accuracy of the client by confirm its individuality. If this procedure completes successfully then this ticket must be generated by KDC. As ticket generated by KDC whose key must only be with KDC and file server. After decrypt this ticket successfully from the file server then it will decide which resource must be given to the client to share it

The three parts of the Kerberos are as follows:

1. Key Distribution Centre(KDC):-It holds all the information about clients and secret key for the demanded service to validate the user. It is said to be a Domain Controller (DC) which is used to generate TGT and SGT. TGT is ticket granting ticket which is generated for the client. It is responsible to issue a ticket for the user to obtain the repair from the fileserver.
2. Client: -It's a customer who is present in the network, to share the data. In Kerberos only the client must be authenticated by generating the TGT.
3. File Server: -Whomsoever the client in the network wants to share the data by taking the permission from the server.

[2] Honeypot: It can manage and allowance security to the network activity like dropping of packets, system log files[12]. The idea of production honeypots is to copy real production systems, services and some operating system to promote the hacker. They can also duplicate different viruses and trojans to attract the attackers/intruders. The use of production honeypot [15] minimizes the data loss in an organization. Security conventionally has been about CIA (Confidentiality, Integrity, and Availability). It now also includes areas like Trustworthiness, Quality, and Privacy. Access control systems provide the essential services of identification and authentication(I&A), authorization, and accountability [25]. That's why it is tried to implement Kerberos with production honeypot. The process of working of Kerberos with production honeypot is shown in figure2 and research honeypot in figure 3.

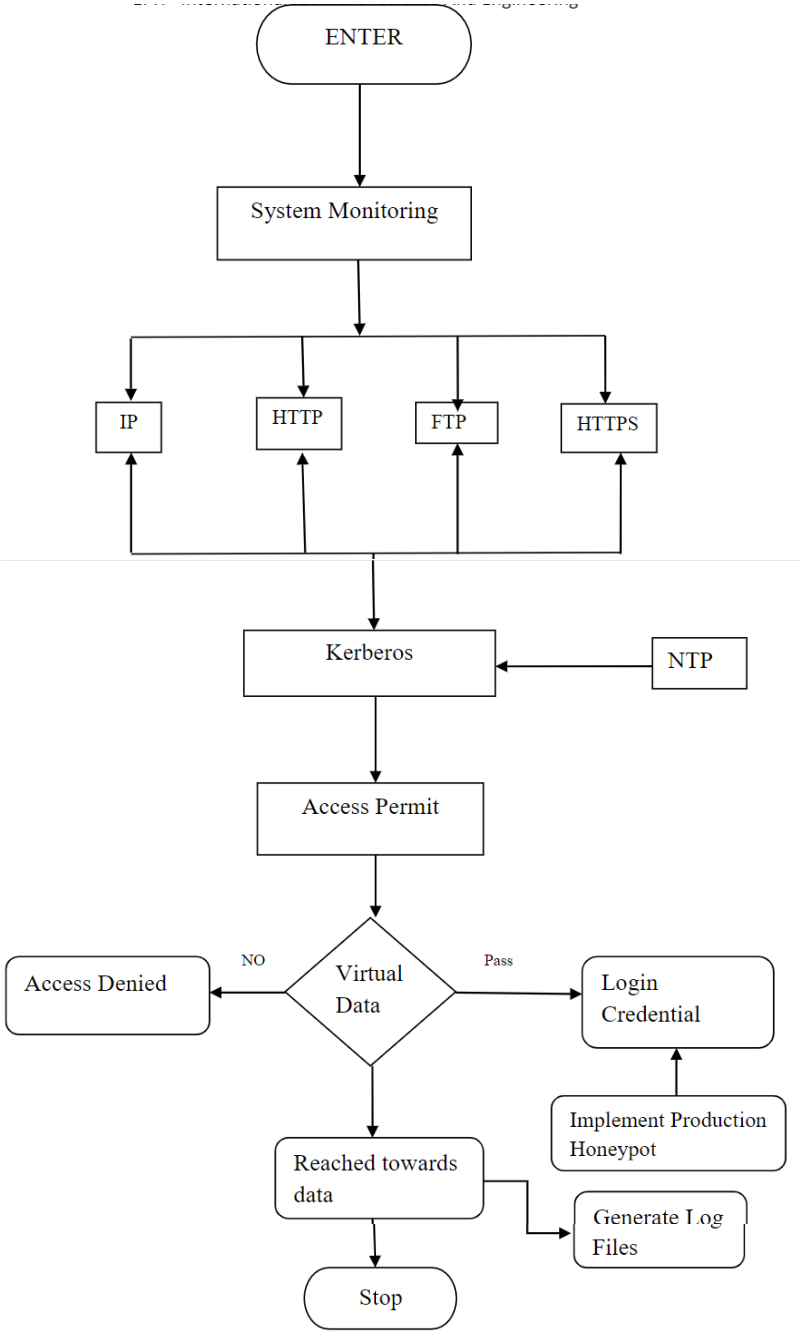
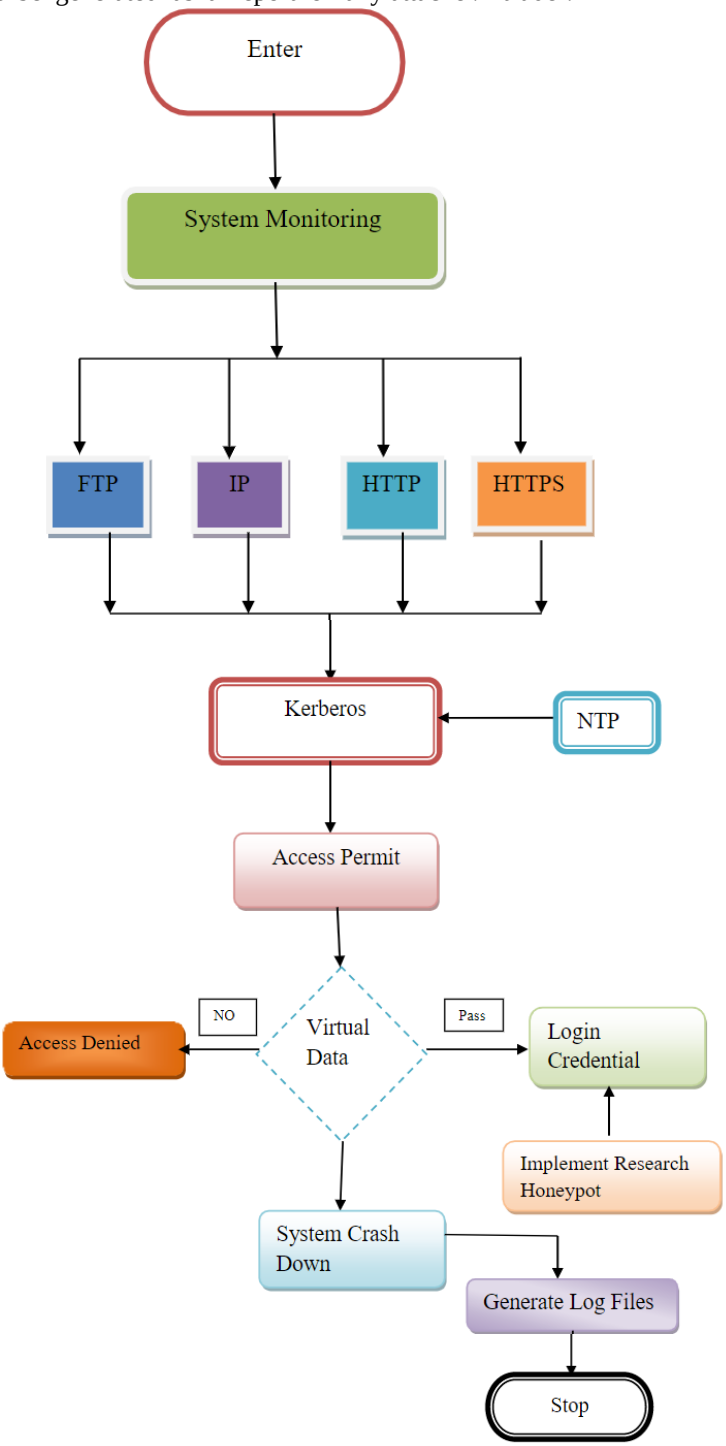


Figure 2 Flow chart of Implementation of Kerberos with Production Honeypot

In fig.2 it shows the activity of the invader and tries to stop them by the use of honeypot with the Kerberos an authentication protocol. After continuous monitoring enters in the network, the system using different protocols and implement the Kerberos in the AWS cloud environment using Linux as an operating system. This Kerberos prevents the network by using Linux, and few know how to work on the CLI(Command Line Interface).In Kerberos also when TGT generate with a use of encryption technique, i.e. symmetric key is used at that time by the help of http protocol is also implemented[10].When we apply decryption technique on TGT ticket with time stamp we use asymmetric key with a use of https protocol. After the authentication of the client has been done successfully, then we get access permit in the network. As a client enters after the Kerberos authentication process completed, now pass from the login credential level I, here implement production honeypot. If it gets fail then access must be denied. If successful, then intruder reached towards data then log file must be generated as a report of any hacker/intruder.

Figure 3shows the activity of the invader and tries to stop them by the use of research honeypot with the Kerberos. After entering in the network by continuous monitoring the system by using different protocols we implemented, the Kerberos in the AWS cloud environment using Linux as an operating system. This Kerberos prevents the network by using Linux as very few know how to work on the CLI (Command Line Interface) In Kerberos also when we generate TGT with a use of encryption technique we implement symmetric key at that time by http protocol[10].When decryption technique applies on TGT ticket with time stamp, asymmetric key with a use of https protocol is generated. After the authentication of the client has been done successfully, then only access get authorized in the network. As a customer enter after the Kerberos authentication, now pass from the login

credential here implement research honeypot. If it gets fail then access must be denied. If successful then system crash down and log file must be generated as a report of any attacker/intruder.



DISCUSSION

As Kerberos [25] is verified the authenticity of the client to the server in the client-server environment, it is assumed that the user's password is shared securely to the client. Kerberos acts as a trusted third party in between the server and client to authenticate mutually. It creates on symmetric key cryptography. It can use public-key cryptography for authentication. To start with the Kerberos verification process, starts at the users ends a request to an authentication server for access to a service. In our proposed method, the verification between client and server is based on not only public key cryptography but also with honeypot techniques. Nowadays Amazon Web Services (AWS)[30]started offering IT infrastructure services to companies in the form of web services normally known as cloud computing which is free to access to everyone after simple registration process. One of the key benefits of cloud computing is the prospect to replace open capital infrastructure expenses with low changeable costs that scale with your business. With the Cloud, businesses no longer require to arrangement for and secureservers. Instead, they can immediately rollup hundreds or thousands of servers in minutes and deliver outcome faster. Amazon Web Services presents a highly reliable, scalable, low-cost infrastructure platform in the cloud that influence hundreds of thousands of businesses in 190 countries around the world.

Here we have used AWS [25] withKerberos5 (it's a version of Kerberos)with the three components like KDC, client, NTP (network time protocol) and file server. Cloud computing environment created by web services through AWS (Amazon Web Services).We have created four services of Kerberos through AWS by the instances. In which there will be DC, file server, NTP and client in the network through which TGT has been generated by DC for the authenticated user in the network which will be decrypt by its own key, as the name shows it's a controller of domain[24].When certified client wants to send data in the network, customers end request to the TGT, then with TGT,KDC came to know that it's an authorized client and generate another TGT with the timestamp or time limit which will be destroyed after lapse of the time period. We have use NFS(Network File Sharing) it's a protocol by which our file can be shared easily on the network with KDC. In network our file cannot be hacked by any malicious user as in fig.3shows the initialization of the Kerberos database with the password and its master key. In fig.4 it shows the host which is created by adding princs command.

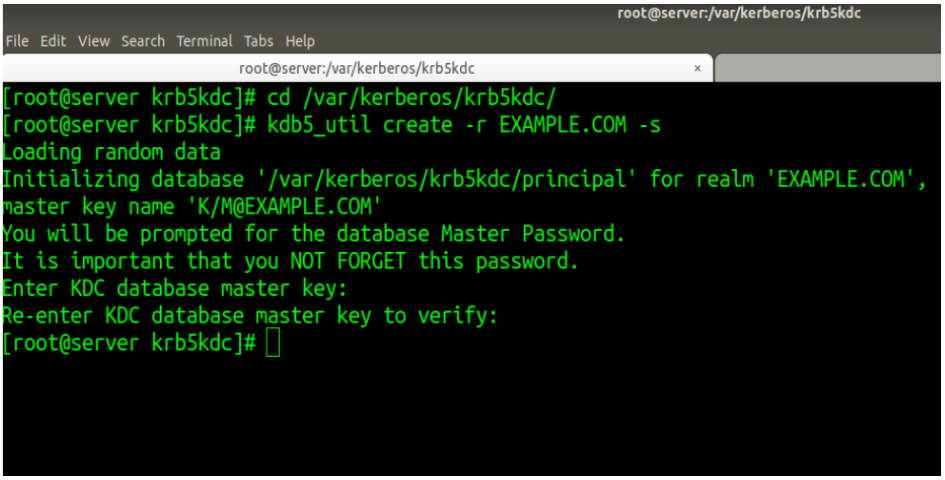


Figure 3. It shows the Kerberos database

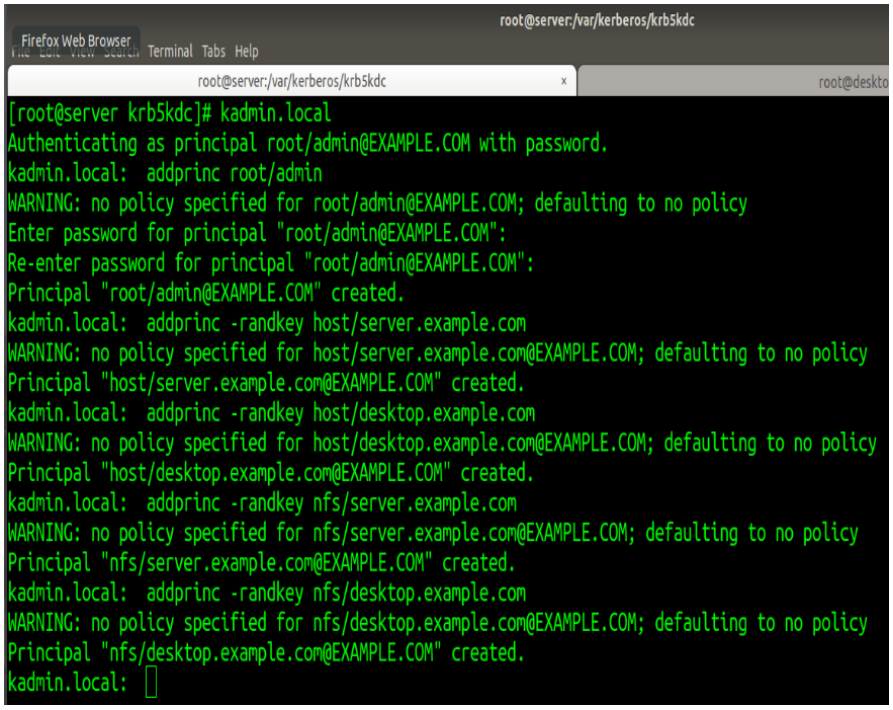


Figure 4 shows the host/client of Kerberos

In fig.5 KDC server which have configuration of time bound in which ticket has been generated. In this screenshot is defined the time bound of ticket which has 24 hours. Here in this fig.6 shows the NTP server created in which time is synchronized between host, KDC and server. In thefig.7 it shows the NFS client[30].In this NFS, serves the client when it demands the resources and then it become the NFS client. In fig.8 NFS mount the client at the starting of the system when connectivity is establish between them. In fig.9 shows the config of the NFS server and its connection with the KDC.

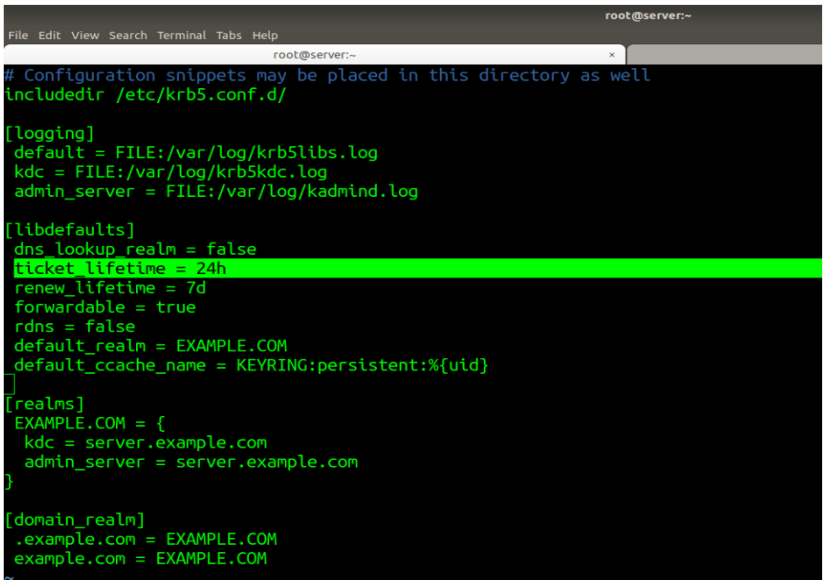


Figure 5 Kerberos Server Config

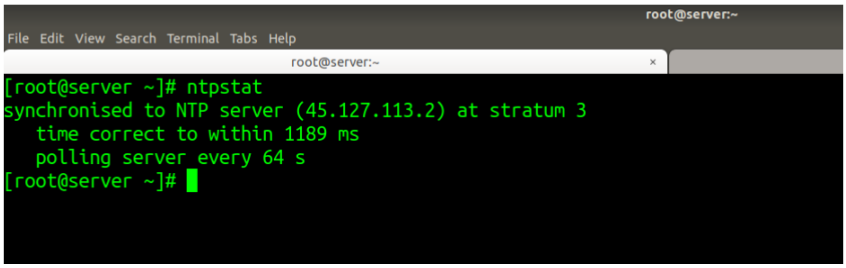


Figure 6 NTP Synchronization

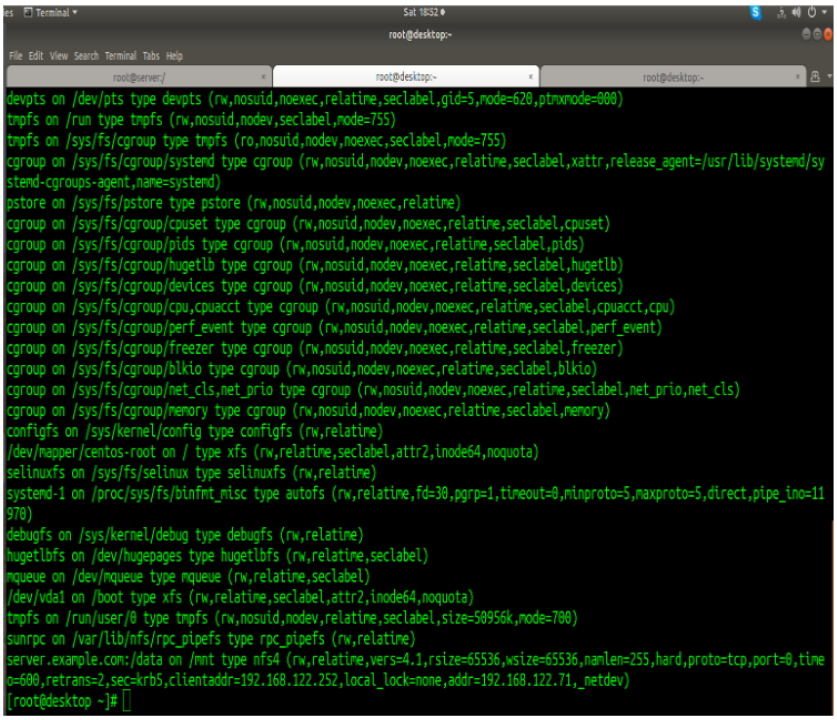


Figure7 Shows the NFS client

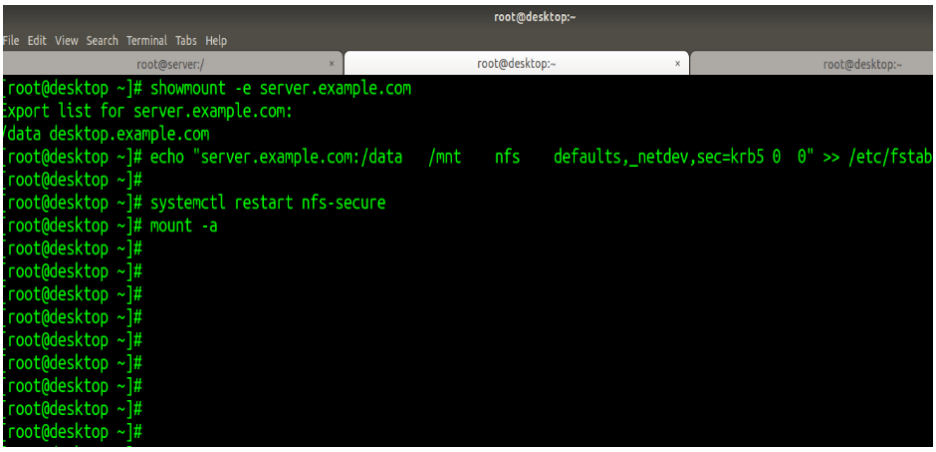


Figure 8 NFS mount the Client

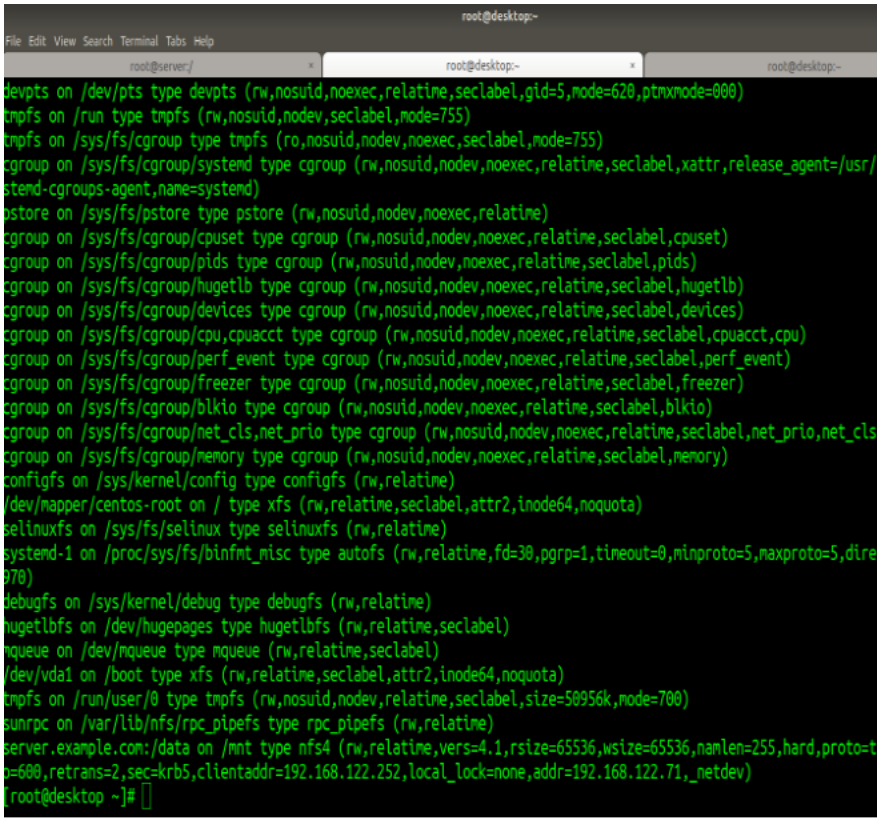
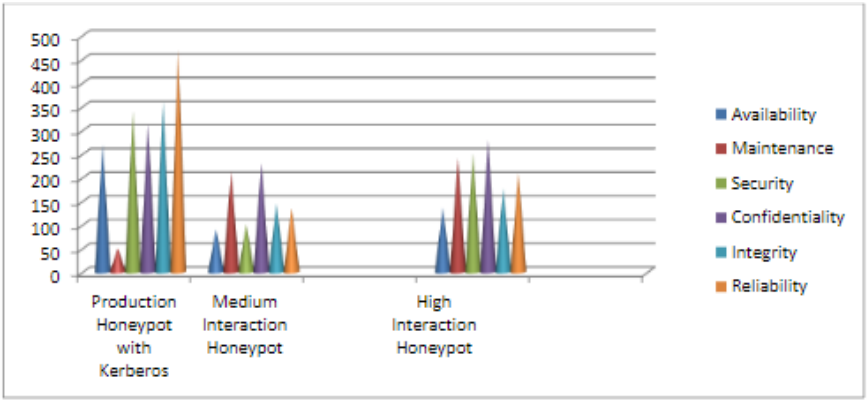


Figure 9. The NFS Server

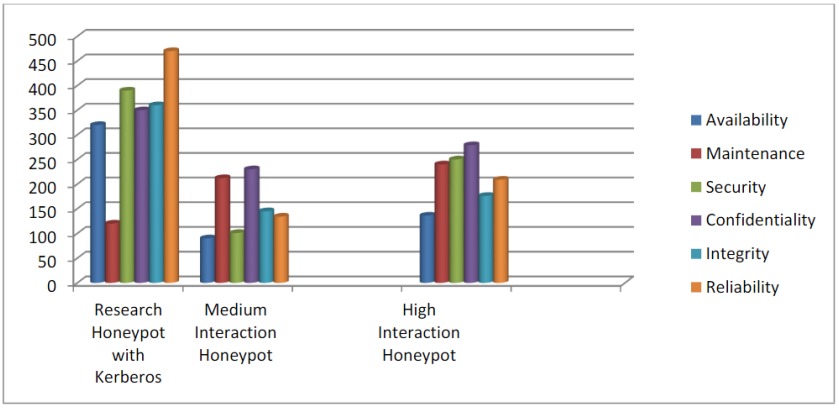
RESULT

Production honeypot is a low-interaction honeypot. Kerberos is client-server architecture, the server is liable to provide the service to client in a structured manner and client uses those services to achieve the preferred task which is allocated exclusively for the user[28]. An improvement of using [29] client-server is the capability to attach isolated users with distant resources to match the authorization and verification phase of protected distributed system. Our proposed method prevents the data by using [31] Kerberos with the production honeypot. After using Kerberos an authentication protocol which gives our method more secure, reliable and maintain confidentiality, integrity, availability of the network. These factors have been used with respect to production honeypots, a log-file is generated on every activity of the intruder. It is a form of report of the malicious user. This gives the network more secure when any malicious progress happens. Graph-1 shows the status of the system after the implementation of the Kerberos with the production honeypot from different types of honeypot.



Graph 1 Implement following factors on various types of honeypot with Kerberos.

According to graph1,the specific detail of the information of the system such as reliability is highest in production honeypot as compare with others. Maintenance is least over here as we have implemented cloud environment through AWS using Kerberos. In this graph x-axis shows the types of honeypot with respect to y-axis on which following factors have taken such as availability, security, confidentiality etc. In this graph it shows that some distant peaks increase the efficiency of the network during heavy traffic. Our foremost important factor is" the reliability" in production honeypot. By the help of Kerberos, implementation on the honeypot is used here to increase the security.



Graph 2 Implement following factors on various types of honeypot with Kerberos.

According to graph 2, the specific detail of the information of the system such as reliability is highest in research honeypot as compare with others. Maintenance is medium over here as we have implement cloud environment through AWS using Kerberos and it's a complex in structure. In this graph x-axis shows the types of honeypot with respect to y-axis on which following factors have taken such as availability, security, confidentiality etc. In this graph it shows the efficiency of the network during heavy traffic. According to the description of the research honeypot our main aim is on the designing of the algorithm with respect to graph is maintenance, as it can be use in military, army etc. By the use of maintenance our system credibility will be maintained and secured.

CONCLUSION

The present paper focused on to make the network more secure by the use of the production and research honeypot which protects the security of the services. The system becomes more efficient by the use of Kerberos-5in AWS Amazon cloud with research honeypot. Server based security has been implemented in our proposed technique, honeypot with Kerberos. In the near future, this can be implemented with the Machine learning technology with the cloud environment to increase the system security, confidentiality, availability and integrity. As it include speeding up digital transformation with faster access to promising technologies such as artificial intelligence, big data analytics and the Internet of Things. With the precisely public cloud platform, relations can be more cost-efficient, strategic and responsive, without sacrificing project requirements for availability, reliability, security, disaster recovery or regulatory agreement.

REFERENCES

[1]. G. E. Blonder: Graphical password,U.S.Patent5 559 961, (1996).
[2]. R. Dhamija, A. Perrig,: A user study using images for authentication.Proc. 9thUSINEXSecurity Symp. CO, pp. 45–58 Denver, (2000).
[3]. X. Suo, Y. Zhu, G. S. Owen,:Graphical passwords: A survey, Proc. 21stAnnu.Comput. SecurityAppl. Conf, pp. 463–472 (2005).
[4]. Paul. A.J, Varghese Paul, P. Mythili,: A Fast and Secure Encryption Algorithm For Message Communication, In: IET-UK InternationalConference on Information and Communication Technology in Electrical Sciences (ICTES 2007), pp. 629-634 Chennai, Tamil Nadu, India. (2007).

[5]. Junjie Peng, et.al, Comparison of Several Cloud Computing Platforms In: Second International Symposium on Information Science and Engineering 978-0-7695-3991-1 (2009).
[6]. Joshi Ashay M., et.al,:EnhancingSecurity in Cloud Computing. In: Information and KnowledgeManagement, Vol 1, No.1, (2011).
[7]. Ajeet Kumar G., et.al,: An Improved Hybrid Intrusion Detection System in Cloud Computing. Int: International Journal of Computer Applications (0975 –8887) Vol.53–No.6, (2012).
[8]. Stephen B., Rebecca L., Shishir P., Sivasubramanian R., and Josh S., : Honeypots in the Cloud,University of Wisconsin –Madison,(2012).
[9]. Nithin C., S.R, Madhuri, : Cloud Security using Honeypot Systems, In: International Journal ofScientific & Engineering Research Vol.3, Issue 3, (2012).
[10]. Aishwarya.S,et.al, Implementation of Honeypot using Kerberos Authentication In: International Journal of Computational Engineering Research (IJCER) ,(2012).
[11]. Michael Beham, et.al, :Intrusion detection and Honey pots in nested virtualization environments In: DSN, 43rd Annual IEEE/IFIPInternational Conference on Dependable Systems and Networks, pp1-6 Budapest (2013).
[12]. Hwan-Seok Y. ,: A study on attack information collection using virtualization technology,74:8791–8799, Springer Science + Business Media New York (2013).
[13]. Al Awadhi, E, et.al, : Assessing the security of the cloud environment, In: IEEE Conference,Page(s) 251 – 256 (2013).
[14]. Kumar S. , et.al, : A Prevention of DDos Attacks in Cloud Using Honeypot In: International Journal of Science and Research (IJSR) Volume 3 Issue11 (2014).
[15]. Muhammet Baykara, et.al,: A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems, Int : International Journal of Computer Networks and Applications (IJCNA) Vol.2, Issue 5 (2015).
[16]. Ramya.R,: Securing the system using honeypot in cloud computing environment, Int:International Journal ofMultidisciplinary Research and Development, Vol.2, Issue: 4, 172-176 (2015).
[17]. Hoa Quoc Le ,et.al, A New Pre-authentication Protocol in Kerberos 5: Biometric Authentication Conference Paper, (2015).
[18]. Romendrapal Singh Rathore ,et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, pg. 120-127(2015).
[19]. Marcin N., et.al,: A Survey on Honeypot Software and Data Analysis arXiv:1608.06249Cryptography and Security (cs.CR);(2016).
[20]. Sultan A. , et.al,: Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions Int :International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 7, No. 4, (2016).
[21]. Gagan, Dr. C. Rama K., Rohit H., :Dynamic Cluster based Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data 978-1-4673-8203-8/16/ 2016 IEEE Int:6th International Conference -Cloud System and Big Data Engineering (Confluence) (2016).
[22]. Akshay A. Somwanshi,et.al,Implementation of Honeypots for Server Security In: International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 03 (2016).
[23]. Yunfei CI, et.al,: Design and Implementation of the Components of the Symmetric Cryptographic Algorithm" Int:IEEE Second International Conference on Data Science in Cyberspace 978-1-5386-1600-0/17 IEEE (2017).
[24]. Liangxuan Zhang, et.al, : Privacy-Preserving Attribute-Based Encryption Supporting Expressive Access Structures Int: IEEE Second International Conference on Data Science in Cyberspace 978-1-5386-1600-0/17 IEEE (2017).
[25]. Ashok Kumar J, et.al, A Modified Approach for Kerberos Authentication Protocol with Secret Image by using Visual CryptographyIn: International Journal of Applied Engineering ResearchVolume 12, Number 21 pp. 11218-11223 (2017).
[26]. AZURE Homepage, https://azure.microsoft.com/en-in/overview/what-is-cloud-computing,last accessed 2018/09/27.
[27]. Chaimae S., Habiba C.: Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb, Int: International Conference on Computational Modeling and Security (CMS 2016), Morocco (2016).
[28]. Sushant M., Makarand K., Krantee J.: Application of Honeypot in Cloud Security: A Review, Int :International Journal on Future Revolution in Computer Science & Communication Engineering (2018).
[29]. Nooreen Fatima Khan, et.al, HONEY POT AS A SERVICE IN CLOUD In:International Journal of Pure and Applied Mathematics Volume 118 No. 20 (2018).
[30]. AMAZON Homepage ,https://aws.amazon.com/about-aws/,last accessed 2018/11/25.
[31]. Kerberos , https://cbt.gg/2CsnIRh,last accessed 2018/11/01.