ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Intrusion Detection System using SSH Protocol

Saumya Lahera[1], Dwij Bhatt[2], Jigar Patel[3], Vinit Patel[4]

B.E. Student, Dept. of Computer Engineering, Shah and Anchor Kuchhi Engineering College, Mumbai,India [1,2,3]

B.E. Student, Dept. of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India[4]

ABSTRACT: Intrusion Detection System is Gathering Information and Maintaining Log of huge Network. It is a strong new technology with great potential to help companies to focus on the most important data in their Network. It captures the browsing behaviour of users at a Company. So, proposed system is used to find most frequent combinations of item present in company. This will help in Gathering Information and Maintaining Log. This system can be used to discover different paths and routes . The proposed system uses SSH Protocol which will make System more efficient. The Intruder can perform Intrusion Detection System and Gather information and Maintain log and make system secure for company.

KEYWORDS: Intrusion Detection System (IDS), SSH Protocol , Maintaining

I.INTRODUCTION

Intrusion Detection Systems are a modern approach to network security. A Intrusion Detection System is used in the area of internet security and cryptography. It is a resource, which is intended to be attacked and compromised to gain more information about the attacker and the used implementations. It can be deployed to attract and divert an attacker from their real targets. Intrusion Detection Systems(IDS) have the big advantage that they do not generate false alerts as each observed traffic is doubtful, because no productive components are running on the system. This fact enables the system to log every byte that flows through the network through and from the Intrusion Detection System, and to relate this data with other sources to draw a picture of an attack and the attacker. This admittedly document attempts to propose a brief introduction to Intrusion Detection Systems-the types and its uses.

The security of network is required for endurance of the industries which are dependent on the internet to enhance the business and providing services on the network. So security of network is primary concern of the industries for securing the critical information. The main target of Intrusion Detection System is to maintain the valuable information of the attackers .Generally, such information gathering should be done without the attacker's knowledge. All the gathered information provides an advantage to the defending side and can therefore be used on productive systems to prevent attacks .Giant sums of attacks are noticed in recent years on these kinds of industries. Intrusion Detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alert the administrator. IDS and Intrusion Detections are used for protecting the system and network from attacks, but after so many efforts for security still the network is not fully secured so different types of solutions are proposed by the researchers .

II. LITERATURE SURVEY

The two main reasons why Intrusion Detection Systems are deployed are:

1.To learn how intruders probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems.

2.To gather forensic information required to aid in the apprehension or prosecution of intruders.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

2.1 DIFFERENT PROTOCOL ATTACKS

A. ICMP

ICMP is used by the IP layer to send one-way informational messages to a host. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. There are a few types of attacks that are associated with ICMP shown as follows:

B. TCP

TCP SYN or TCP ACK Flood Attack - This attack is very common. The purpose of this attack is to deny service. The attack begins as a normal TCP connection: the client and the server exchange information in TCP packets.

C. ARP

ARP maps any network level address such as IP Address to its corresponding data link address.

D. UDP

UDP uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagram may arrive out of order, appear duplicated, or go missing without notice.

E. FRAGGLE

A fraggle attack is similar to a smurfing attack with the exception that the User Datagram Protocol (UDP) is used instead of ICMP.

TEARDROP
A teardrop type of DoS attack The attack works by sending messages fragmented into multiple UDP packages.

2.2 TYPES OF ATTACK

A. PASSIVE ATTACK

A Passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

B. ACTIVE ATTACK

In an active attack**,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

C. PASSWORD ATTACK

Password attack an attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

2.3 DRAWBACKS OF EXISTING SYSTEM

1. The analysis of the current situation of campus network security
In addition to the common occurrence of virus, campus network has to face three major security hidden dangers.

2. The limitation of the Intrusion Detection**:** Many campuses only install a layer barrier-Intrusion Detection, but there are many limitations in the Intrusion Detection. The Intrusion Detection System technology has the active defence characteristics, and can help campus network avoid being attacked.

3. Internal attack: According to relevant materials statistics, the percent of campus network attack by inside is more than 80%. With computer universalness, some students' computer level is already beyond school network management personnel's imagination, and these students affected by curiosity or motives eavesdrop someone else's code and other important information. This mischief damage even malicious attacks school management system.

4. Hacker attacks: The internet is a connection from one gateway to another gateway. Due to the safety consciousness and capital reasons, many campus exist the "heavy technology, light safety, light management tendencies, and the builders of the campus network does not pay much attention to the security problems, and often set up one Intrusion Detection.

III.PROPOSED SYSTEM

Intrusion Detection System is a non-production system, used for exploiting the attacker and notice the attacking techniques and actions. The objective of Intrusion Detection Systems is not only to notice but to tackle the risk and abate it. There are various definitions of Intrusion Detection Systems are available as few people take it as a system to lure the attackers and inspect their activities where as other take it as a technology for detecting attacks or real systems formed for getting attacked.

In network security, Intrusion Detection Systems are used to detect the attackers and learn from their attacks and then modify and develop the system accordingly for security. The loop holes of the network security can be covered with the help of information provided by Intrusion Detection Systems.

Intrusion Detection System can be figured as a computer system connected with a network for inspecting the vulnerabilities of a computer or a complete network. as it is a exclusive tool to study about the attackers and their strategies on the network. Intrusion Detection Systems are normally virtual machines which acts like a real system. Intrusion Detection Systems are classified into two categories on their use.

3.1 PURPOSE

The two main reasons why Intrusion Detection Systems are deployed are:

1.To learn how intruders probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems.

2.To gather forensic information required to aid in the apprehension or prosecution of intruders.

3.2 TYPES OF INTRUSION DETECTION SYSTEM

A . HIGH INTERACTION.

Intrusion Detection Systems that provide only some fake services, these acts as an emulator of the operating system and services. These Intrusion Detection Systems are simple to design but also simply detectable. Attacker can just use a simple command to identify it that a low involvement Intrusion Detection System does not support.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

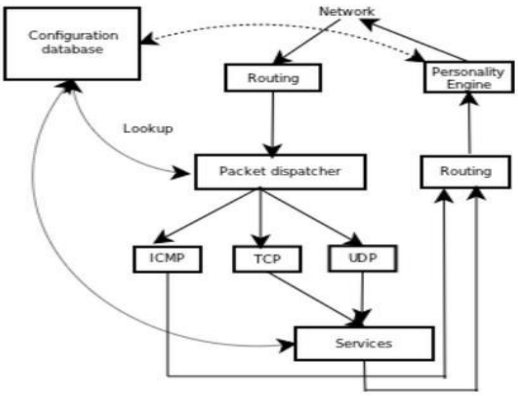

Fig. (3.2.A) Honeyd

An example of this type of Intrusion Detection System is Honeyd.Honeyd daemon receives a packet for one of the virtual Intrusion Detection Systems , it is processed by a central packet dispatcher. The dispatcher checks the length of the IP packet and verifies its checksum

The daemon knows only three protocols: ICMP, TCP and UDP.Packets for other protocols are discarded.

B. LOW INTERACTION.

Low level interaction Intrusion Detection Systems provides the real like operating systems and some real services with some real uncertainties. These allow the capturing of information of attacker and record their activities and actions. These are the real machine with one system, with one network interface on network. An example of this type of Intrusion Detection System is Honeynet.

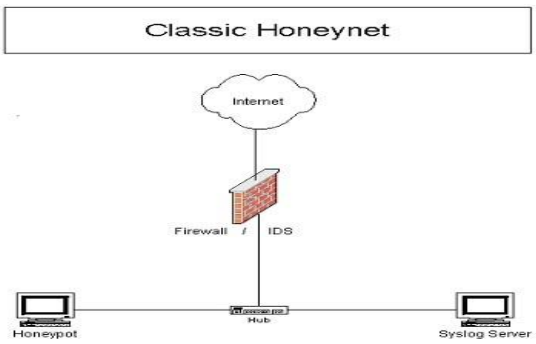

Fig. (3.2.B) Honeynet

VMware is software that allows you to set up 'Virtual Machines' within the confines of one computer. So, if you have a Linux system, you can run that Linux system and run WindowsNT inside of Linux. It is different than dual booting because you can have both operating systems (OS) running at the same time. The OS on which VMware is installed is called the HostOS. The OS that is installed on a virtual machine is called the GuestOS. You can have several Virtual Machines running simultaneously.

There are a couple of different options for networking. One is bridge networking. Bridge networking gives the GuestOS direct access to the network. This means that the GuestOS will look like any other computer on the network. There are some disadvantages when using this method to set up a honeynet. For one, users cannot easily filter or log

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

traffic going to and from the GuestOS. As was stated in the Intrusion Detection System Project's Know Your Enemy: Honeynets paper, this is a very important capability.

The second option for networking is host-only. Host-only networking is a good choice for setting up a honeynet, as it forces the GuestOS to go through the HostOS to get to the network, so a Intrusion Detection can easily be set up on the HostOS. I will discuss how to do this later in this article.

An important thing to do when configuring VMware is to say no when it asks if you want GuestOSes to be able to access the HostOS's file system. Enabling this option would give an attacker who successfully compromises the Intrusion Detection System a way to get at the HostOS. If the HostOS is compromised, so is the integrity of the entire honeynet.

3.3 DATA FLOW DIAGRAM

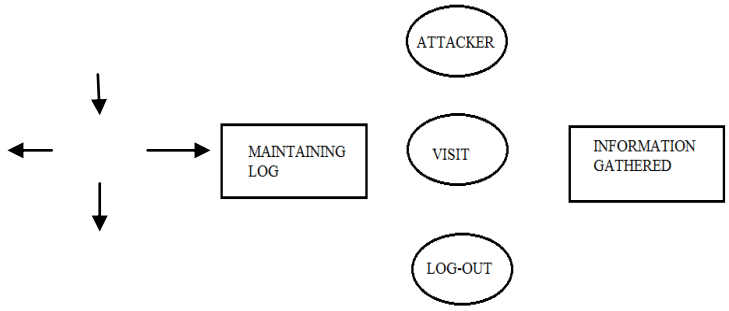

Fig. (3.3.1)DFD of Our System

IV.ADVANTAGES OF EXISTING SYSTEM

1.IDS monitors the operation of Intrusion Detections, routers, key management servers and files critical to other security mechanisms .

2.IDS allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs

3.IDS can make the security management of systems by non-expert staff possible by providing nice user friendly interface

4.IDS comes with extensive attack signature database against which information from the customers system can be matched

5. IDS can recognize and report alterations to data files

V.CONCLUSION

Intrusion Detection Systems are positioned to become a key tool to defend the corporate enterprise from hacker attacks it's a way to spy on your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they have accessed a corporate network, when they are actually hanging around in a Intrusion Detection System-- While the real network remains safe and sound.

The advantages that Intrusion Detection Systems bring to intrusion protection strategies are hard to ignore. In time, as security managers understand the benefits, Intrusion Detection Systems will become an essential ingredient in an enterprise –level security operation.

This will help to solve the current challenges and make it possible to use Intrusion Detection Systems for the benefit of the broader internet community.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

VI.FUTURE WORK

TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers operating systems such as Linux or BSD.

It allows host or subnet work IP addresses, names and/or indent query, replies, to be used as tokens on which to filter for access control purpose when TCP wrappers are closed in the system then all the ports are denied in the system.

REFERENCES

[1] Maximillian Dornseif, Thorsten Holz, and Sven Muller. Intrusion DetectionSystems and limitations of deception.
[2] Xiaoyan Sun, Yang Wang, Jie Ren, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Intrusion Detection System", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.
[3] C. H. Nick Jap, P. Blanchfield, and K. S. Daniel Su, "The use of Intrusion Detection System approach in software-based application protection for shareware programs", IEEE International Conference on Computing & Informatics, (ICOCI '06), pp. 1-7, 2006.
[4] Jian Bao and Chang-pengJi, and Mo Gao, "Research on network security of defense based on Intrusion Detection System", IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010.
[5] Anjali Sardana, R. C. Joshi, "Intrusion Detection System Based Routing to Mitigate DDoS Attacks on Servers at ISP Level".