Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.181 – 185

RESEARCH ARTICLE

Network Monitoring and Forensics

[1]Subhay Chandra, [2]Rakesh Kumar Yadav
[1]School of Engineering & Technology, IFTM University, Moradabad, U.P, India
[2]Department of Computer Science & Engineering, IFTM University, Moradabad, U.P, India

subhaychandra@gmail.com

Abstract— In the study of network forensics Mostly tools give you view of movement in real time, But monitoring in real- time at any stage requires hardware resources and human significant, and doesn't ratio to workgroups larger than a single network. It is normally more practical to archive all intercommunication service and analyse subsets as necessary. This process is called as network forensics, or reconstructive traffic analysis. Practically, it is frequently limited to data digest and packet-level inspection supervision; in spite of, a network monitoring forensics tool can endow a richer look of the data gathered, permission you to inspect the intercommunication service from further up the protocol stack? the forensic network is very simple to monitor and identify problem conveniently. It is very useful to rummage security infringement. It is completely analysing the record of network traffic.

I. INTRODUCTION

Leakage and Steal of sensitive data Pose is a great business hazard to institutions processing and storing sensitive data. Many times institutions are unaware of their network and there are no security processes and controls in place to reduce data theft and leakage. Simulations of data leakage highlight in this document are assumed and were organised in a concept lab. The aim of the assumed events is to further clarify the process in network monitoring. Institutions that are considering step-in-aid of the execution in their network can get advantage by studying this document. They will get the help to develop their own methodologies and solutions to reduce leakage of sensitive data.

II. OBJECTIVE AND SCOPE

The given project focuses on the primary motive of the organizational setup to secure the network architecture from internal and external malicious activities. The basic objective is to catch the malicious intent of the employees within the organization and to detect the zero day attack scenarios made by black hat hackers operating outside the organization.

For internal employees the architecture is safeguarded through continuous monitoring and analysis. The monitoring will satisfy the following objectives:

- What software's are used by users?
- Which websites are accessed by users?
- On which time user accessed the particular system.
- What conversations are done by users of LAN?
- Find out malicious activity or user.

For external employees the network is safeguarded through placing the honeypot system which interacts with the hacker and records the activities and scripts run by him to recognize the zero day attack.

III. METHODOLOGY

The project is the combination of ore efforts which can be segregated in given five modules:

- 1st Phase

Development of LAN architecture

- 2nd Phase

Securing LAN architecture by implementing Honey pot

- 3rd Phase

Implement IDS system to Detect and prevent our LAN from malicious activities, Virus and Worm and monitoring the attacking system within the LAN

- 4th Phase

Analysing and investigating the packet flow with the help of Wireshark packet analyser for the purpose of Network Forensic

- 5th Phase

Checking the Admissibility of digital evidence in the court of Law

IV. TOOLS

There are opensource and freeware software in the proof of concept lab. Table shows the freeware and opensource software used in the table.

Tools Used:

- KFSensor

KFSensor is a Windows operating system based honey pot Intrusion Detection System (IDS).

- SNORT

Snort is created by Martin Roesch It is an open source network intrusion detection system (NIDS).it is a packet sniffer which monitors network traffic in real time, observe each packet closely to detect a riskful payload or suspicious anomalies.

- Wireshark

Wireshark is a free and powerful tool that investigates network packets and permit analysts to peer internal traffic for troubleshooting purposes and security evaluation.

V. FIRST PHASE

LAN architecture

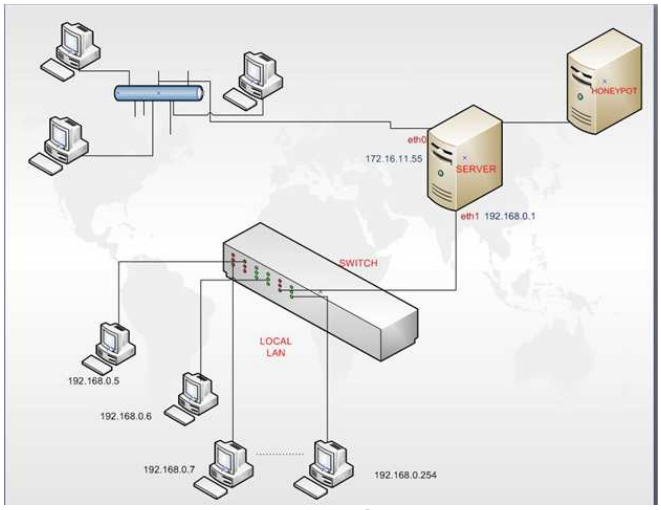

Fig. 1 LAN Architecture

SERVER:
IP Address: 172.16.11.55
Gateway IP Address: 192.168.0.1
IP Range: 192.168.0.2 to 192.168.0.254
Default Mask: 255.255.255.0
Configure servers:
• DHCP
• DNS
• FIREWALL
• IDS (Intrusion Detection System.

VI. SECOND PHASE

Implementation of HONEYPOT

A honey pot is a computer system. Honey pot is expressly set up to attract and "Entrap" people who attempt to come through other people's computer systems.

To set up a honey pot:
• Install the operating system
• Make sure that there is no data on the system
• Add application

We are using honey pot For Two purposes in our project:-
First before IDS system to prevent network:

- Track and Trace attacker.
- Maintain log file and store various script and code use by the attacker to exploit various server generate
- For IDS system set signature and rule

Second honey pot after IDS system to detect false alarm and reduce them;

KFSensor
KFSensor is a Windows based honeypot Intrusion Detection System (IDS). Its action as a honeypot.

How it works?
A signature rule gives a set of conditions which must be met in order for the precept to be matched. There are so many types of condition which can be defined, such as stipulated service port or a text piece to be found.

When KFSensor gets a connection from a visitant it passes knowhow on the connection and the data received from the visitant to the Signature Engine. The Signature Engine compares data with each Signature Rule. If it is found the signature ID is stored with the event in the event log.

The signature rule's report is then made available to the user along with the rest of the event information, by the email alerts and user interface.

KFSensor is flexible and highly configurable.

There are two main components of the KFSensor system:

- KFSensor Server
- KFSensor Monitor

KFSensor save your network by many of the perpetrators. These are as following.

- Virus
- Worm Trojan
- Root Kit
- Hybrids
- Scanners
- Hacker

VII. THIRD PHASE

Network Monitoring Using GUI Based IMonitor:

IMonitor EAM permits you invisibly monitor your whole network, such as Email(SMTP, POP3, web based email), instant message, screenshots, print Jobs, keystrokes, websites visited, FTP, computer devices,

applications used, software's, system services, system hotfixes etc. IMonitor EAM also can log file manipulation on client's computer. Gives alarm to console computer when client do a file operation on storage disk, open an unwanted website, add or remove a removable disk, transfer file with FTP protocol, send or receive mail, etc. The screenshots of network computers will be available on main computer and pick a control of a client computer by controlling its keyboard and mouse, it is specifically helpful when you need to help the person who uses the client computer, and you can open file, edit file, upload file and download file remotely. IMonitor EAM also can conditional remote computer's browsing, restrict remote computer's application using, send instant message and command to remote computer. Additionally this provides a powerful remote task manager, permits you to view all processes on client computer.

Implementation in The project

- The IMonitor Server Module is installed on the main server with IP 192.168.0.1
- The IMonitor Client Module is installed in other clients in the network
- While installing the client module the server IP is provided

Advantages of IMonitor

• The client program cannot make any configuration changes in the client module as the file does not exist in the Program Files.

• The all the activities of the client accessing the system can be monitored at the server end including: sites visited, directory analysis, etc.

Analysis:

The GUI Based tools help the network Administrator to analyse the activities of the client in silent mode.

All the logs generated are stored in the database server that can be analysed for latter review.

The tool generates the functionality for the administrator to review the remote desktop of the client and carry out functions like: Task Manager, Software installed, hardware information etc.

Limitation:

The tool only accommodates two computers as client in the demo version.

Implementing Intrusion Detection System (SNORT)

Objective: Discover and inhibit our LAN from malevolent activities, Worm and Virus and monitoring the attacking system within the local network.

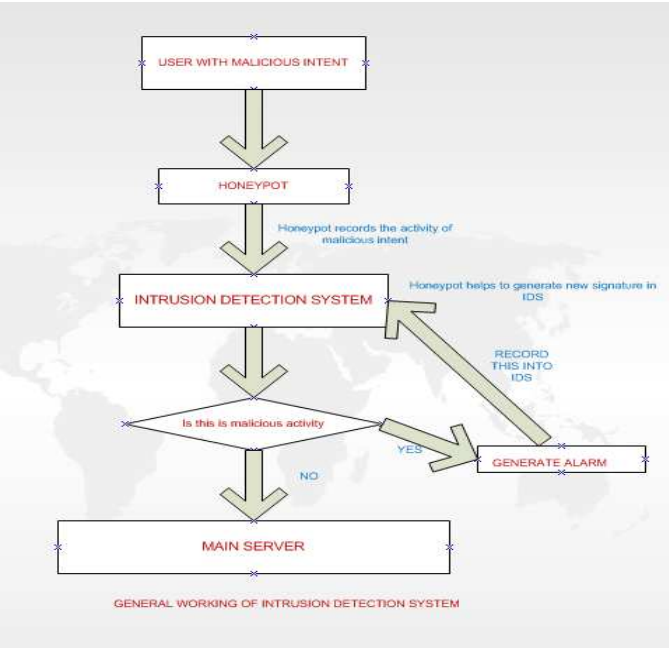

Fig. 2 General working of snort

Steps to configuring snort on our server.

Step1: Installation of snort on windows server 2008.

Step2: Configure snort according to our LAN architecture.

Step1: Installation of snort on windows server 2008.

Step a: Download the Snort_2_8_3_2.exe packages from snort.org
Step b: Click on Snort_2_8_3_2.exe installer.

VIII. FOURTH PHASE

Network Forensics

Wireshark:-Wireshark is a free and powerful tool that investigates network packets and permit analysts to peer internal traffic for troubleshooting purposes and security evaluation.

Apply filters to network packet captures

Analysis:

• The packet analyser can help in analysing the payload in depth so as to write snort signatures.

• The Wireshark provides the IO graph which can define any unusual traffic generated in the network nd which deviate from the set standard of the organization.

• The Wireshark provides the packet detail pane that helps the analysis of payload data.

• The facility to implement filters in Wireshark facilitate the forensic an examiner to narrow down the scope to relevant data.

IX. FIFTH PHASE

Integrating the facilities of Wireshark, Snort & Honeypot to Detect the Zero Day Attack Scenarios &Writing Snort Rule Set.

Use of Wireshark in Depth Analysis.

We watch the log file on snort and honeypot and which packet is comes in network for malicious intent, we analysis that packet on Wireshark packet analyser and find out the content in payload or develop different signatures to protect our network from that attack. Regular monitoring will help us to develop signature for new attacks and protect our network from zero day attack.

X. CONCLUSION

The aloft simulations are just some examples on how a network monitoring and forensic solution can provide an active solution in reduce sensitive web and data leakage and theft. It is not the author's Intention to push for the use of free tools for setting up a network monitoring forensics solution. Venture should plan and assess their own requirements. The main point of this entire document was to punctuate the main benefits and importance of having a network monitoring. Organizations are taken on wireless technology both for cost and for comfort.

These types of services reduce the false alarm rate a virtual honey pot can be performed after the IDS system that can check the period of alarm generated by IDS.

REFERENCES

[1] www.wikipedia.com
[2] http://www.securiour.com/2008/what-is-zero-day-attack-or-exploit/
[3] Grønland Vidar Ajaxon: "Building IDS signatures by means of a honeypot" Norwegian Information system Laboratory.
[4] http://www.vidarg.net/projects/Preliminary_thesis_report.pdf, Access on: 12-Apirl 2009
[5] Chi, Chi-Hung ,Li Ming , Liu Dongxi, A method to obtain Signatures From Honeypots Data, Volume 3222/2004,(Heidelberg/Berlin:Springer, October 2004) pp 435
[6] Bednarski M.Greg and Branson Jake: "Understanding Network Threats through Honeypot" Deployment, Carnegie Mellon University March 2004. Available from: http://www.infinitel00p.com/library/honeypot.pdf, Access on: 12- April 2009
[7] Hammer Richard,"Enhancing IDS using, Tiny Honeypot" SANS Institute InfoSec Reading Room, pp20-23, SANS Institute,2006
[8] Solution Base: What you need to know about honeypots Available form: http://articles.techrepublic.com.com/5100-22_11-5758218.html, Access on 18 April 2009

