ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

An Efficient Technique to Improve the Data capturing Of Low-Interactive Honeypot Technology

Vidya Vijayan[1], M.Kalimuthu[2]

PG Scholar, IT Department, SNS College Of Technology, Coimbtore, India [1]

Associate Professor, IT Department, SNS College Of Technology, Coimbtore, India[2]

Abstract: Honeypot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system. Honeyd is an application which enables the setup of multiple virtual honeypots on a single machine with different characteristics and services. The possibility to generate different virtual honeypots on one system with even different simulated operating systems enhances the usability of this tool. .It is great for simulating victims and collecting a lot of interesting information. Honeyd is a low-interactive honeypot system could be used as an early warning system in a productive environment to catch some attacks and trigger an alert. The technique of attaching a script to a certain port allows a very flexible setup with unlimited capabilities and opportunities fortuning. Finally the logs generated as well as attacks came on virtual systems can be analysed and maintained. In the proposed system, bring out the essence of using honeynet in small scale organisation. And show how a fully functional low interactive honeypot technology could benefit your own system. Capture all the data's that passed through our network with the help of some tools like Snort, Wireshark, Nmap, Sebek.

Keywords:Low-interactive honeypots, Honeyd, Sebek, Nmap, Wireshark.

I. Introduction

Information security is today's growing concern for organizations and individuals alike. This led to growing interest in more aggressive forms of defence to supplement the existing methods. One of these methods involves the use of honeypots. A honeypot is a security mechanism whose value lies in being probed, attacked or compromised. Here examine different kinds of honeypots its concepts, and approaches to their implementation.

The traditional approach to security measurements has been largely defensive so far, but interest is increasingly being paid to more aggressive forms of defence. One of these forms is decoy-based intrusion protection through the use of honeypots and/or honeynets. The honeypot is a kind of safety resources, and its design can be used to observe how a hacker intrudes into a system, which has a very big allure. And we can describe it as a can with "honey".

For the information gathered by the honey pot system, on one hand, it can effectively forensics from computer crime and strike to the high IQ criminals. On the other hand, it can effectively analyze hacker intrusion process, reconstruction the hacker attacking process, and improve the ability of the security personnel that defense hackers. This design is very easy to provoke the hacker's interest, and it is easy to make hackers intrude this system.

This design is very easy to provoke the hacker's interest, and it is easy to make hackers intrude this Honeypots are closely monitored network decoys serving several purposes that includes they can distract attackers from more valuable machines on a network, provide early Warning about new attack and exploitation trends and allow in-depth examination of adversaries during and after exploitation of a honeypot.

Honeypot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into the system. It is important to remember that Honeypots does not replace any other traditional Internet security systems; they are an additional level for support to the system or network. Honeypots can be setup inside, outside or in the demilitarized zone of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes.

II. IDS (Intrusion Detection System)

An IDS is an application that detects attacks on the computer or network, and lets to know when the attacks occur.

A. *Benefits Of Running IDS*

- **Detecting attacks**: Attack detection is what an IDS is there for. An IDS can tell you if a worm is attacking your network, or if a computer system has been compromised.
- **Enforcing policies**: An IDS can monitor an internal network for behaviour that violates your organization's network security.
- **Resource justification**: An IDS can provide information on how well firewall is working and

exactly how many people are out to get you."

- **Providing an audit trail**: An IDS can provide an after-the-attack audit trail for seeing how far an attacker got, and where it came from.

B. *Key IDS Concepts*

- **False positives and false negatives**

  False positives are alerts generated by IDS because it assumes that it has detected a valid attack against a monitored system, but the attack was really not valid. False positives create problems, they made alert noise that can able to hide a real attack, and then it send on wild goose chases for attacks that never really happened. A false positive occurs when an IDS generates an alert on either network traffic that seems like an attack to the IDS, but is not an attack or a real attack.

  A false negative is a real attack that cannot be detected by the IDS, and therefore not alerted on. An IDS might miss an attack because the attack is not one that it recognizes, because the IDS is compromised, or because the attacker has successfully used a method of deception the IDS

- **Signatures and anomalies**

  Signature detection is an IDS that uses signature detection matches the network traffic it sees against a list of attack signatures. These signatures are typically important bits and pieces of the attack that the IDS should try to find for in incoming network packets and flag as "bad" traffic

  Anomaly detection is an Intrusion Detection System that works in a different manner. It learns what normal traffic for the network looks like, and will then alert when it sees something that looks abnormal. Properly tuned anomaly detection IDS might be low on false negatives, but higher on false positives.

B. *NIDS(Network Based IDS)*

A network-based IDS (NIDS) analyzes packets coming across a network connection for data that look like it's part of an attack.NIDS analyze network traffic for attacks, using signature or anomaly detection .

Its network interface card (NIC) runs in disapproved mode, which means that it captures all network traffic that goes by its NIC, not just the traffic destined for the IDS system itself. It generates alerts to inform attack in real-time. It generates logs to tamp down deeper into an attack, typically after the attack has occurred.

C. *HIDS(Host Based IDS)*

A host-based IDS (HIDS) only monitors for intrusions on the system it running on HIDS perform one or more of the tasks. HIDS look for incoming network traffic to find out attacks, using signature or anomaly detection. It examines system logs for unusual events, such as multiple invalid login attempts. HIDS check the unity of files on the system. Integrity checking will also let to know if files have been created or deleted.

III. GSN (GPRS SUPPORT NODE)

A GSN is a network node which supports the use of GPRS in the GSM core network. All GSNs can have a Gn interface and support the GPRS tunnelling protocol. The GPRS core network provides mobility management, session management and transport and for Internet Protocol packet services in GSM and WCDMA networks. There are two key variants of the GSN, one the GGSN and the SGSN.

A. *GGSN(Gateway GPRS Support Node)*

A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks (radio network and the IP network). It converts the GPRS packets coming from the SGSN into the suitable packet data protocol (PDP) format (e.g., IP or X.25) and sends them out on the corresponding packet data network. In the next direction, PDP addresses of incoming data packets are converted to the GSM address of the destination user. The readdressed packets are again sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and their profile in its location register. The GGSN is responsible for IP address assignment and is the default router for the connected user equipment (UE). The GGSN also performs authentication and charging functions.

B. *SGSN (Serving GPRS Support Node)*

A serving GPRS support node (SGSN) is responsible for the delivery of data packets from and to the mobile stations in its geographical service area. It has certain functions include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions.

The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address(s) used in the packet data network) of all GPRS users registered with this SGSN. The SGSN detunnel GTP packets from the GGSN (downlink) and tunnel IP packets toward the

GGSN (uplink).Carry out mobility management as Standby mode mobile moves from Routing Area to Routing Area .it also have the capacity to billing user data. GSM/EDGE have specific SGSN functions like it have the capacity to carry traffic per subscriber up to about 60 kbit/s (150 kbit/s for EDGE) .

GSM/Edge connect via frame relay or IP to the PCU using the Gb protocol stack .Accept uplink data to form IP packets and encrypt downlink data and decrypt uplink data. WCDMA specific SGSN functions like it has the capability to carry up to about 300 kbit/s traffic per subscriber (R99) and carry up to about 7.2 Mbit/s traffic downlink and 2.0 Mbit/s traffic uplink (HSPA).It can tunnel or detunnel and downlink or uplink packets toward the radio network controller (RNC). Carry out mobility management to the level of an RNC for connected mode mobiles.

IV. AP(ACCESS POINT)

Access point is an IP network to which a mobile can be connected and have a set of settings which are used for that connection. When a GPRS mobile phone sets up a PDP context, the access point is selected. At this point an access point name (APN) is determined. This access point is then used in a DNS query to a private DNS network. This process (called APN resolution) finally gives the IP address of the GGSN which should serve the access point. At this point a PDP context can be activated.

V. PDP CONTEXT

The packet data protocol context is a data structure resides on both the SGSN and the GGSN which contains the subscriber's session information when the subscriber has an active session. When a mobile wants to use GPRS, it must first attach and then activate a PDP context. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscribers access point. The data recorded includes Subscriber's IP address, Subscriber’s IMSI and Subscriber's Tunnel Endpoint ID (TEID) at the GGSN and Tunnel Endpoint ID (TEID) at the SGSN.

The Tunnel Endpoint ID (TEID) is a number allocated by the GSN which identifies the tunnelled data related to a particular PDP context. There are two kinds of PDP contexts, one is Primary PDP context it has a unique IP address associated with it second is Secondary PDP context that shares an IP address with another PDP context.

V. SNORT

Snort (affectionately known by its designers and users at “the Pig”) is a network based IDS that uses signature detection; it sniffs and examines network data packets for content that matches known attacks. Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. Snort has three primary uses: It can be used as a straight packet sniffer like tcp dump, a packet logger or as a full blown network Intrusion prevention system. Snort is used here to generate alerts and to capture more information about the attacks.

A. *Benefits Of Using Snort*

Snort is configurable. All of Snort’s inner workings, configuration files, and rules are laid bare so you can tune Snort to your specific network architecture. You can create your own rules for new attacks. Snort is free. Snort is released under the GNU GPL, which means you can use it for free. There are tens of thousands of downloads of Snort each month from the http://www.snort.org/ Web site. Snort runs on multiple platforms. Snort not only runs on all the major Unix operating systems (including Linux), but also runs on Microsoft Windows.Snort is constantly updated. Maintenance releases for Snort come out as needed, typically once every few months. The Snort rules are regularly updated with new attack signatures and can be downloaded from www.snort.org/.

B. Snort Components

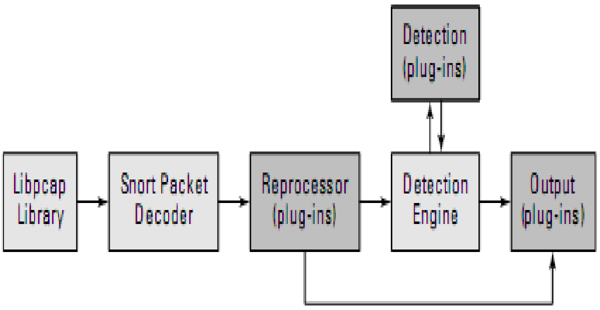

Fig.1. Snort Components

1) Packet capture library: Illustrated as “Libpcap library” in Figure the packet capture library is a separate piece of software that tosses Snort network packets from the network card. There are unprocessed Data-Link Layer (Layer 2 of the OSI model) packets, such as Ethernet frames. On Linux and UNIX systems, Snort uses libpcap. On Windows systems, Snort uses WinPcap. .

2) Packetdecoder: The packet decoder takes the Layer 2 data sent over from the packet capture library and takes it apart. First it decodes the Data Link frame (such as Ethernet, Token Ring, or 802.11), then the IP protocol, then the TCP or UDP packet. When finished decoding, Snort has all the protocols information in all the right places for further processing.

3) Preprocessor: Snort's preprocessor has several plug- ins that can be turned on or off. Preprocessing operates on the decoded packets, performing a variety of transformations making the data easier for Snort to digest. Preprocessors can alert on, classify, or drop a packet before sending it on to the more CPU-intensive detection engine.

4) Detection engine: The detection engine is the heart of Snort. It takes information from the packet decoder and pre-processors and operates on it at the transport and application layers these rules contain signatures for attacks.

5) Output: When a preprocessor or rule is triggered, an alert is generated and logged .Snort supports a variety of output plug-ins.

VII. DYNAMIC HONEYPOT SYSTEM

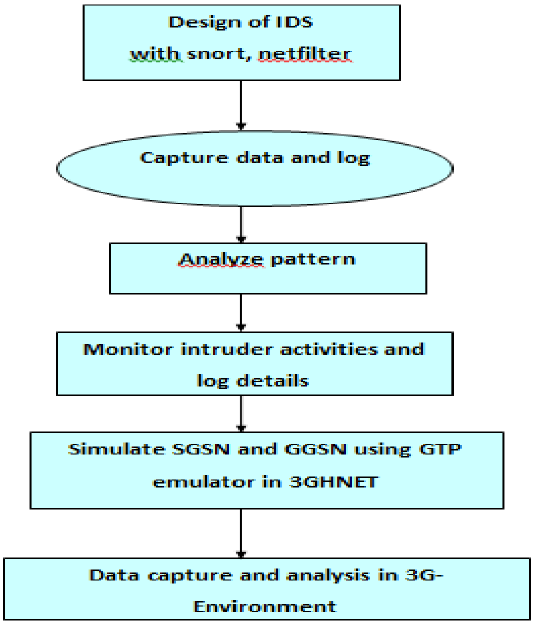

Fig.2 .Dynamic Honeypot System

VII. RESULTS

Low-interactive honeypot system are easy to implement, cost effective and maintain but the data capture under this system is very low .In high-interactive honeypot system the data capturing capacity is higher compared to low-interactive honeypot technology, but implementation is quite complex and cost is high. Here increase the data capture capacity of low-interactive system by adding additional tools named snort and wireshark. Snort is an open source data capture tool.

Configuration of snort is a major task, then initialize the snort. After snort initialization it can monitor any system that connected to the LAN with its IP address or analyzed the virtualized system. Monitoring means capture the data that pass through the network and saved the data's in the log file. The characteristics of log files are used in further deployment.

VIII.COMPARISON

Here compare existing system and proposed system, existing system is low-interactive so data capturing is very low. Data capture of low- interactive honeypot system is incremented by the use of data capturing tools Snort and Wireshark. By implementing these tools ,it can capture all the data's that pass through the network. These Captured data and its characteristics is stored in log files.

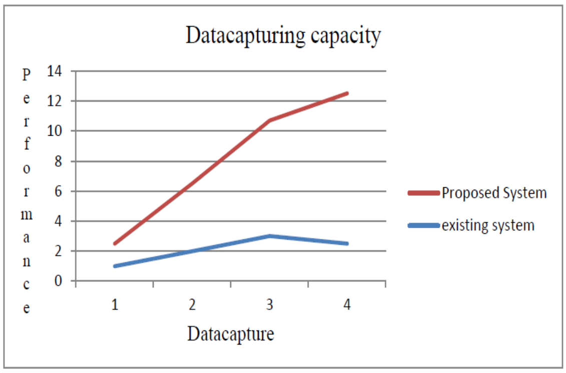

Fig 3.Comparison of Existing and Proposed Honeypot System

IX. CONCLUSION

Honeypot technology is used as one of the best intrusion detection system. By using snort, capture all the data the passed through a 3G network. The data captured is logged into log file. The alert file which contain the details about th3e attacker those come to attack the honeypot system.

In future enhancement wants to implement the emulated SGSN's and GGSN's with an open source emulator called OpenGGSN over Linux operating systems. Use Winpcap (packet capture library) we have captured packets from the network card and have had them analysed using Wireshark Network Protocol Analyser. Implementation of Wireshark protocol for high data capturing.

ACKNOWLEDGMENT

We would give thanks to Anna University Chennai and SNS Group of Institutions for giving support to fulfill the Project.

REFERENCES

[1] Almotairi.S, Clark.A, Dacier.M, Leita.C, Mohay.G, Pham .V.H,Thonnard.O, and Zimmermann .J,(2007) "Extracting inter-arrival time based behaviour from honeypot traffic using cliques," in The 5th Australian Digital Forensics Conference, Perth, Australia, 2007.

[2] Clark .A,Almotairi .S,Mohay .G and Zimmermann.J(2009)"A Technique for Detecting new Attacks in Low-Interactive Honeypot Traffic" © 2009IEEE, DOI:10.1109/ICIMP.

[3] Haifeng.W,Qinkui.C(2012),"Dynamic Deploying Distributed low-Interaction Honeynet" journel of computers vol 7,No.3,©2012 ACADEMY PUBLISHER doi:10.4304/jcp.7.3.692-698.

[4] Huang P.S(2009), "Design and implementation of a distributed early warning system combined with intrusion detection system and honeypot," in Proceedings of the 2009 International Conference .

[5] Jason Chih-Hun Chang, Yi-Lang Tsai.(2010)," Design of Virtual Honeynet Collaboration System in Existing Security Research Networks".

[6] Jingying Lan, Yongheng Wang," Snort Research and Improvement BM algorithm", Computer Engineering and Design, vo1.29, 2008, pp.2 199-2202.

[7] Jun Zhao, "High Camouf1age High Interaction of Honeypot Technology Research and Implementation", Computer Engineering,vol.36, 20 10, pp. 156-158.

[8] Kwong, L., Yah(2010)" Virtual honeynet srevisited"Proceedings from the Sixth Annual IEEE,vol.99.pp.230_240.

[9] Li Li,Hua Sun.Zhengu Zhang (2011),"The Research and Design of Honeypot System Applied in the LAN Security" ©2011 IEEE

[10] Liu .D,Zhang .Y,(2012)An Intrusion Detection based on Honeypot technology"©2012 IEEE DOI:10.1169 /ICCSEE. 2012. 156

[11] Min Ceng, Feng Li, "Design and Implementation of the Embedded Packet Capture Device", Computer Engineering and Design,vo1.30,2009, pp. 157 1- 1573.

[12] Ming shiue, Shang Juh,(2008) "Countermeasure for Detection of Honeypot Deployment"International Conference on Computer andCommunication Engineering .

[13] Mukkamala.S,Yendrapalli.K.Basnet.R," Detection of Virtual Environments and Low Interaction Honeypots". In Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC, 2007, p. 92 –98.

[14] Saurabh.C,Bhatia.J.S,Raj Kamal.Ramani.A.K(2011),"Deployment of a low interactive Honeypot in an Organizational Private Network"©2011 IEEE.

[15] Shubham.G,Vishal.S,Aswin.P(2011)" Honeypot-A trap of Hackers "Proceedings for 5 National Conference INDIACom-2011

[16] Stiemerling.M, J. Quittek, and L. Eggert,(2008) "NAT and firewall traversal issues of host identity protocol (HIP) communication," Network Working Group Request for Comments (RFC) 5207,

[17] X.Liu,L.peng and C.Li (2011),"The Dynamic Honeypot design and Implementation Based on Honeyd"CCIS 214©Springer-Verlag Heidelberg.