Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Investigate the Use of Honeypots for Intrusion Detection Defense

[1]Dr. N. Balakumar, [2]C. Rangarajan, [3]M. Ragavi
[1]Assistant Professor, Head, [2]Associate Professor, [3]Assistant Professor,
[1,2,3]Department Of Computer Applications,
[1, 2,3]Pioneer College Of Arts And Science,
Coimbatore-47, India

Abstract :-There has been great amount of work done in the field of network intrusion detection over the past 20-30 years. With networks getting faster and with the increasing dependence on the Internet both at the personal and commercial level, intrusion detection becomes a challenging process. The challenge here is not only to be able to actively monitor large numbers of systems but also to be able to react quickly to different events. This paper aims at studying and analyzing various aspects of network intrusion and intrusion detection. This paper also explains the relatively new concept of "honeypot." Honeypots are computers specifically designed to help learn the motives, skills and techniques of the hacker community. This paper describes in depth the concepts of honeypots and their contribution to the field of network security. The paper then proposes and designs an intrusion detection tool based on some of the existing intrusion detection techniques and the concept of honeypots.

Keywords: intrusion detection,honeypots,networksecurity,monitoring

I. INTRODUCTION

An intruder can be defined as somebody attempting to break into an existing computer. This person is popularly termed as a hacker, blackhat or cracker. The number of computers connected to a network and the Internet is increasing with every day. This combined with the increase in networking speed has made intrusion detection a challenging process. System administrators today have to deal with larger number of systems connected to the networks that provide a variety of services. The challenge here is not only to be able to actively monitor all the systems but also to be able to react quickly to different events. Overall intrusion detection involves defense, detection, and importantly, reaction to the intrusion attempts.

Firewalls can be defined as sophisticated filters of network traffic. Firewalls are used to limit and regulate traffic entering and leaving a network. Historically firewalls are more concerned about the traffic entering the network than traffic leaving the network. Firewalls can be configured to allow/deny connection from/to certain hosts or allow/deny connections to/from certain ports and to filter out unwanted traffic.

The most serious threat of intrusion comes through the network. Until very recently internal networks were considered to be safe. But studies have shown that there are threats from within the network as well as from the Internet. A NIDS monitors packets on a network and attempts to detect any intrusion attempts using different kinds of techniques and methods.

System integrity checkers are typically host based intrusion detection systems which can be configured to monitor critical system files and detect inappropriate access or alteration of these files. Such intrusion detection systems are aimed to detect misuse by an authorized user. System integrity checkers are also helpful in the aftermath of an intrusion in determining which files got changed or damage done.

These are tools that monitor and scan system log files looking for specific patterns and trying to detect whether an intrusion was attempted occurred. Even though we classify these as intrusion detection systems they can be seen more as tools that help in parsing relevant information from log files that a firewall, a NIDS or system integrity checker generates.

A. Intrusion Detection Systems

An intruder can be defined as somebody attempting to gain un-authorized access into an existing computer. This intruder could be an insider or an outsider. An insider is a one who has legitimate access to your network or computer and is trying to misuse his privileges. Insider intrusion is usually an attempt to alleviate privileges or to gain information by probing misconfigured services or just to create mischief. An outsider attack is an attack from a person who is not a member of the organization. Usually the intruder is a hacker whose intensions are to cause harm or mischief. We can classify this intruder into two types, one who has something to gain by the intrusion and the other a curious person trying to probe the security of the system. The first type is popularly termed as a "cracker". Crackers attack web-sites or database servers in an attempt to gain critical information such as credit card or social security information. Some try to

deface government web-sites or deny normal service and may be backed by political motive. The second type is the "hacker" who can be further broken down into two types: - an extremely intelligent computer knowledgeable person or a "script kiddie". An intelligent hacker is one who studies protocols and algorithms and tries to detect vulnerabilities in them.

B. Software Bugs

Bugs in the form of buffer overflows are the single largest source of vulnerabilities in software. Internet worms, such as Code Red exploited buffer overflow vulnerabilities to spread across the Internet and to compromise thousands of systems. Most software applications (like web servers, web browsers) are extremely complex and it may not be practically possible to find all the buffer vulnerabilities in them. Also open source software sometimes helps since the source code is available for hackers to analyze. This doesn't mean that closed source systems are less vulnerable, since sometimes all you have to do check how the application behaves by feeding it various data. There are many known buffer overflow exploits for different services such as DNS, FTP, TELNET, SSH, HTTP etc.

Buffer overflow vulnerability exists whenever a destination buffer is too small to hold the data. Most software applications have fixed-size buffers to hold data. If the program does not check its input then an attacker can overflow the buffer by sending too much data. The server may then execute the data that overflowed as if it were a program. If such an exploitable buffer exists in a privileged program, the attacker could then take full control of the server and execute arbitrary commands on the machine to steal passwords or other confidential information.

1.TCP Connect Scan – This is the most basic of scans. All this scan does is to try to connect to a system on a specified port. The connection will be successful if the port is listening.

2. SYN Scan or Half-open Scan – This is a popular scan method. By definition and design, a full TCP connection is established after completing the TCP/IP handshake. In this scanning technique only the SYN packet is sent. If a SYN+ACK is received in reply to the SYN then it indicates that the port is listening. This scan requires root privileges on the system and the ability to create custom SYN packets. Nowadays many intrusion detection systems and firewalls log or detect such type of scanning.

3. TCP FIN Scan – This is an even more clandestine method of scanning. Here the attacker sends a FIN packet to the target port. The default on many systems is to ignore this packet if the port is active and to send a RST (reset) if the port is closed.

4. UDP Scan – In this method a zero byte UDP packet is sent to a port. It the port is closed the system replies with an "ICMP port unreachable". UDP scans can be used to detect RPC ports or NFS (network file system) services which are known to be vulnerable.

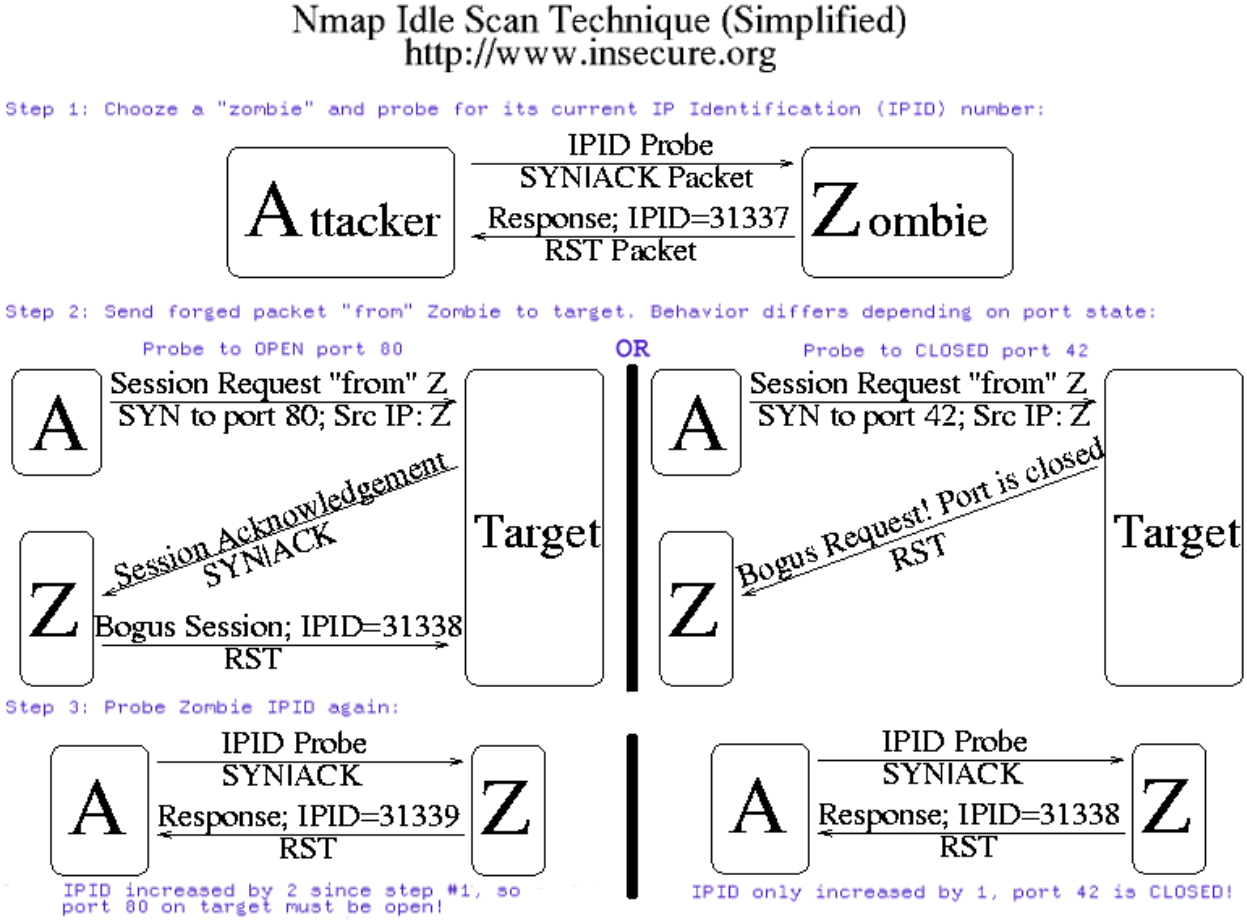

Figure -1 Idle Scan Technique

C. Neural networks and artificial intelligence

Neural networks are a totally different paradigm for computing. They can be defined as "algorithms that learn about the relationship between input-output vectors and "generalize" them to obtain new input-output vectors in a reasonable way". They are used to express nonlinear relationships between different constraints of a system. A neural network can be used to help a behavior-based system build a regular usage model. Similarly various pattern matching techniques from artificial intelligence can be incorporated into both signature-based and behavior-based systems. Neural networks and artificial intelligence techniques are still computationally intensive methods and are very much in the embryonic stage as far as their use in intrusion detection is concerned.

D. Statistical Approach

Statistical-Based systems use statistical models to detect malicious packets. Statistical models are primarily used to relate information regarding occurrence and variables related to factors that influence occurrence. Statistical systems adapt to different system behaviors or occurrences and try to develop a usage pattern. Then they monitor pre-defined variables over a time period and calculate a test value. If this value is above the user-defined threshold then they trigger an alert. This approach does not require any predefined attack patterns and is capable of detecting new attacks. Also depending upon the number of variables processed it can detect evasion attacks or slow attacks. Like behavior based approaches the system must "learn". So the effectiveness of the system depends on the learning process. Another concern with statistical approach is the fact that it will not pinpoint the attack or the problem. It will only flag a packet as being anomalous and either drop the packet or trigger an alert. The administrator will then have to perform the necessary analysis on it and will require reasonable amount of expertise.

II. HONEYPOTS

Traditionally intrusion detection involved a defensive approach where systems were either dedicated computers like firewalls or host based detection systems aimed at detecting attacks or preventing them. These systems existed as a part of the commercial/in-use networks and used techniques like pattern matching or anomaly detection. Another type of security systems are system integrity checkers, which are, typically host based. The problem that these systems face is that they are running on computers, which are in use on a daily basis. These systems usually have to deal with large number of connections and data transfers which results in huge log files and also makes it difficult to differentiate between normal traffic and intrusion attempts accurately. Many of these systems are also known to generate many false positives or in some cases false negatives. Moreover these systems provide very little insight to the tools and methods employed by the blackhat community.

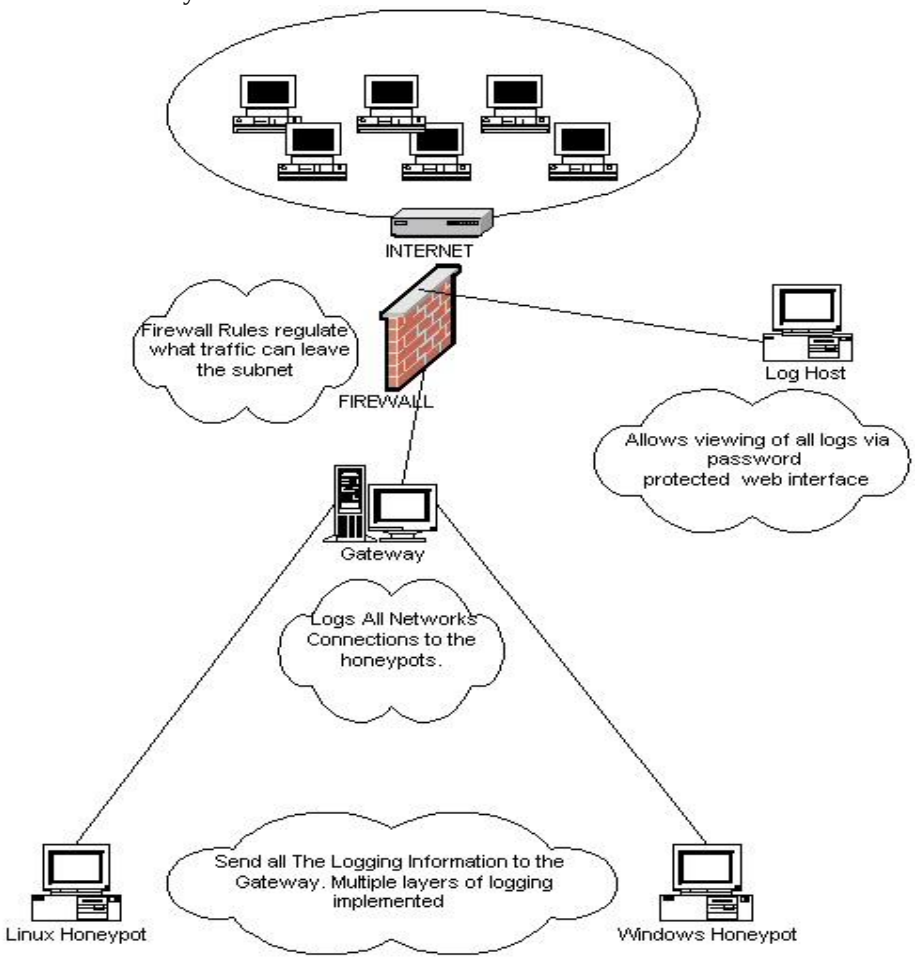

Figure -2 Working of the honeynet

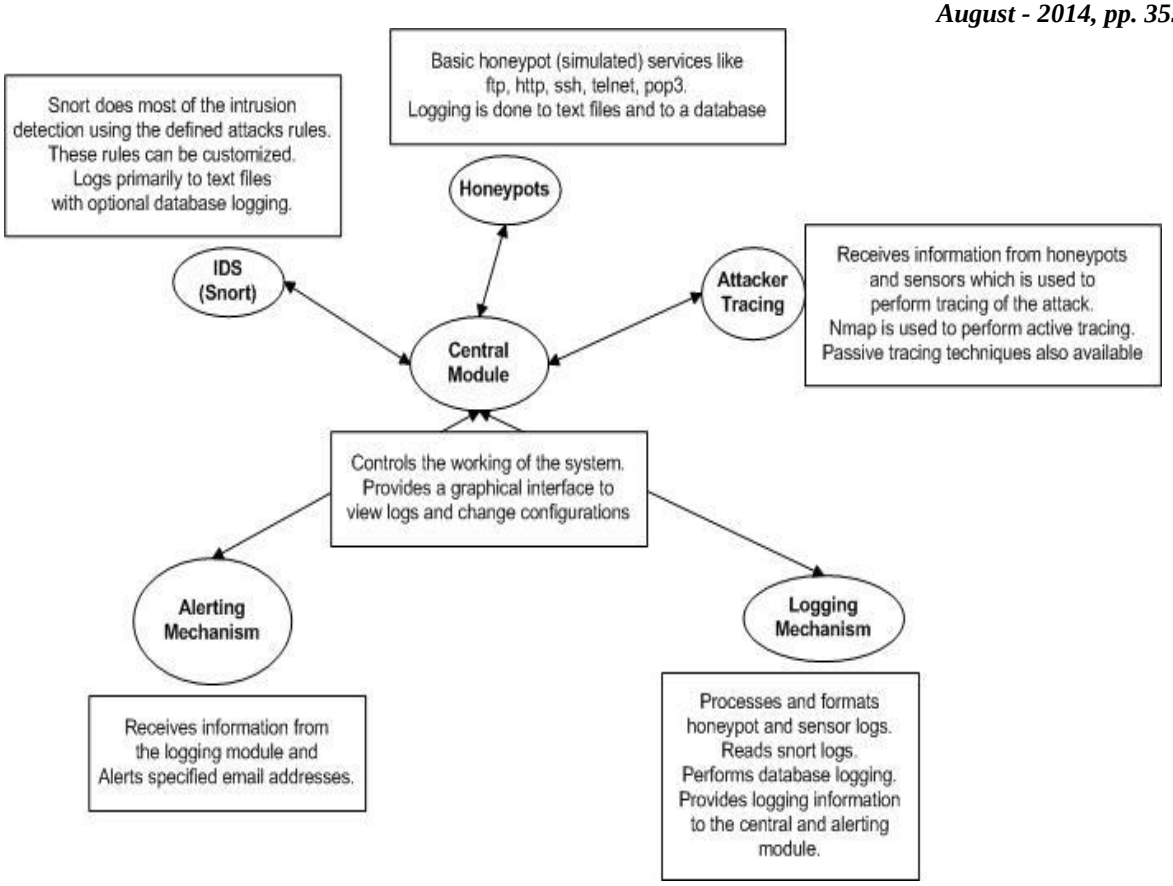

Figure -3 Design of lanCactus

The Central Module

This module controls the working of the entire system. It provides connectivity between different modules of the package. It also provides a graphical interface (See Appendix D1) to view logs and change configuration.

Working

The idea behind the entire package was to put together a set of tools that collectively work as an intrusion detection system and also as an early warning system. The honeypot module can be used to simulate many services.

- Apache web server
- IIS web server
- Three different kinds of FTP severs
- A simple telnet server
- A simple SSH (Secure shell) server
- A POP3 server

III. CONCLUSION

This paper involved studying issues concerning intrusion detection systems the challenges that these systems faced. The Internet has become indispensable both at the organizational and personal level and so it will be the case with security systems. We also explored the concept of honeypots in depth and saw how it might be useful to the field of network security. The concept of honeypots is an important addition to the security field. Honeypots offer an offensive approach to intrusion detection and prevention. Most importantly they serve as a learning tool for system administrators. Wireless technologies have opened up a whole new security threat. Wireless is the direction in which computers especially laptops, palmtops and other hand-helds are heading. The intruder can now compromise your system from your parking garage or a palmtop hidden in his backpack. At the on set this appears disastrous to security but there are quite a few solutions already available. Techniques like wired equivalency privacy (WEP), Extensible Authentication Protocol (EAP) have been developed and are subject to evaluations and studies. Many vendors like Cisco have also introduced proprietary technologies.

REFERENCES

[1] Robert Graham FAQ: Network Intrusion Detection Systems. http://www.robertgraham.com/pubs/network-intrusion-detection.html 1998-2000.

[2] Lance Spitzner Honeypots, Definitions and Value of Honeypots . http://www.spitzner.net.May, 2002.

[03] Biswanath Mukherjee, L.Todd Heberlein, Karl N. Levitt Network Intrusion Detection. IEEE Network May/June 1994.

[4] S.M. Bellovin Security Problems in the TCP/IP Protocol Suite. AT&T Bell Laboratories. Computer Communication Review, Vol19, No.2, pp. 32-48, April 1989.
[5] CERT® Coordination Center Denial of Service Attacks http://www.cert.org/tech_tips/denial_of_service.html
[6] The Honeynet Project. Know your enemy. (http://project.honeynet.org).
[7] Clifford Stoll The Cuckoo's egg. ISBN: 0743411463
[8] Bill Cheswick An Evening with Berferd, In which a cracker is lured , endured and studied AT&T Bell Labs. ISBN: 0743411463
[9] Brian Scottberg*, William Yurcik**, David Doss* Internet Honeypots Protection or Entrapment. *Illinois State University **University of Illinois at Urbana-Champaign
[10] Reto Baumann, Christian Plattner Honeypots. February 2002
[11] Intrusion detection systems: The evolution of deception technologies as a means for network defense. White paper Symantec Enterprise Security.
[12] Neil Provos Honeyd. http://www.citi.umich.edu/u/provos/honeyd/
[13] Fred Cohen Deception Toolkit. http://www.all.net/dtk/dtk.html
[14] Marcus Ranum and Andrew Lambeth Back Officer Friendly (BOF). http://www.nfr.com/products/bof/docs/

