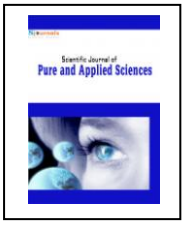
Sjournals
Scientific Journals
Scientific Journal of Pure and Applied Sciences (2012) 1(3) 84-89
ISSN 2322-2956

Contents lists available at Sjournals
Scientific Journal of
Pure and Applied Sciences
Journal homepage: www.Sjournals.com



Original article

Information precautions using intellectual honeypot instrument

L.S. Arul[a,*], K. Lecturer[b]
[a]*Director-CA, T.John College, Bangalore, India.*
[b]*T.John College, Bangalore, India.*

[*]Corresponding author; *Director-CA, T.John College, Bangalore, India.*

ARTICLEINFO

Article history:
Received 03 November 2012
Accepted 24 November 2012
Available online 28 December 2012

Keywords:
AODV
Blackhole
Honeypot
Intrution Detection
Honeynets
Production honeypot
Research honeypot
Gen I honeynet
Gen II honeynet

ABSTRACT

A honeypot is used in the area of computer and Internet security. It is a resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques. It can also be used to attract and divert an attacker from the real targets. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts as all traffic is suspicious, because no productive components are running on the system. Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defence to supplement the existing methods. One of these methods involves the use of honeypots. In computer terminology, a honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. In this paper, examine types of Honeypots, detection scheme, advantages and disadvantages of honeypots and generations of honeynets.

1. Introduction

In this day and age, information security is an ever-increasing concern. One of decoy-based intrusion protection is through the use of honeypots and honeynets. A honeypot is valuable as a surveillance and early-warning tool. While it is often a computer, a honeypot can take other forms, such as files or data records, or even

unused IP address space. A honeypot that masquerades as an open to monitor and record those using the system is a sugarcane. Honeypots should have no production value, and hence should not see any legitimate traffic or activity. Whatever they capture is therefore malicious or unauthorized. One practical implication of this is honeypots that thwart spam by masquerading as the type of systems abused by spammers. Blackhole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. A blackhole attack is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming afresh routeto the destination and absorb them without forwarding them to the destination. Two kinds of attacks can be launched against ad-hoc networks, Passive and Active. In passive attacks the attacker does not disturb the routing protocol. It only eavesdrops upon the routing traffic and endeavours to extract valuable information like node hierarchy and network topology from it. In active attacks, malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes. An on-demand routing protocol which initiates a route discovery process only when an originating MR desires to send some traffic to an unknown destination. The algorithm's primary objectives are to broadcast discovery packets only when necessary, to distinguish between local connectivity management and general topology maintenance, to disseminate information about changes in local connectivity to those neighbouring mobile nodes that are likely to need the information (Prathapani, 2009; Honeynet Project, 2011).

2. Honeypots

Honeypots is roaming virtual software agents that generate a dummy Route Request (RREQ) packet to lure and trap blackhole attackers. It acts as synonymous to secret police officers who conduct random investigation.

3. Types of Honeypots and Purpose of Honeypots

Honeypots can be classified based on their deployment and based on their level of Interaction. Basedon the deployment, honeypots may be classified as Production Honeypots and Research Honeypots

3.1. Research honeypots

Research honeypots are for the hardcore hacker hunters. It is designed to gain information about the blackhat community and does not add any direct value to an organization (Li-juan, 2009). They are used to gather intelligenceon thegeneral threats organizations may face, allowing the organization to better protect against those threats. Its primary function is to study the way in which the attackers progress and establish their lines of attack, it helps understand their motives, behavior and organization. They are typically used by organizations such as universities, governments, the military or large corporations interested in learning more about threats research. It adds tremendous value to research by providing a platform to study cyberthreats.

3.2. Production honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations; Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. It is one used within an organization's environment to protect the organization and help mitigate risk (Honeynet Project, 2011). Their main benefit is in the area of detection. Due to its simplicity, it addresses the challenges of IDS's – there are minimal false positives and false negatives.

3.3. Level of Interaction

Interaction defines the level of activity a honeypot allows an attacker.

3.3.1. Low-Interaction Honeypots

Low-interaction honeypots have limited interaction. They normally work by emulating services and operating systems. The advantages of a low-interaction are their simplicity, these honeypots are easier to deploy and maintain, take minimal risk, the emulated services mitigate risk by containing the attacker's activity, and the

attacker never has access to an operating system to attack or harm others. The disadvantages of low-interaction are log only limited information and are designed to capture known activity; the emulated service can do so much, easier for an attacker to detect a low –interaction honeypots.

3.3.2. Medium-Interaction Honeypots

Medium-interaction honeypots are slightly more sophisticated than low interaction honeypots, but less sophisticated than high interaction honeypots. Like low-interaction honeypots they do not have an operating system installed, but the simulated services are more complicated technically. They provide the attacker with a better illusion of an operating system since there is more for the attacker to interact with.

3.3.3. High-Interaction Honeypots

High-interaction honeypots are totally different. They are usually complex solutions as they involve real operating systems and applications. Nothing is emulated and attackers are given real thing to interact with. The advantages with such a solution are two fold. The advantages of a high interaction are it can do everything low-interaction honeypots can do and much more,tend to be research honeypots ,normally are for the hacker hunting purposes,Can captureextensiveamounts of information and can learn the full extent of their behavior, Make no assumptions on how an attacker will behave. The disadvantages of a high Interaction includes normally take hell of a work to do, nothing is emulated and attackers are given real thing to interact with, more complex to deploy and maintain.

4. Legal Issues and Challenges

There are many factors which determine whether or not the use of a honeypot is legal. If deploying a honeypot in the United States, then there are at least three legal issues that must be considered:

i) Entrapment - Applies in a criminal case in which the government acted in a manner that actually caused the defendant to committhecrime. Attackers may argue entrapment.

ii) Privacy – Laws exist that might restrict your right to monitor users on your system.

iii) Liability - Realize that attackers may misuse your honeypot to harm others.

5. Advantages and Disadvantages of Honeypots

Honeypots have several powerful advantages that include: Small data sets: Honeypots collect small amount of data, but almost all of this data is real attacks or unauthorized activity. Reduced false positives: With most detection technologies a large percentage of our alerts are false warnings, making it very difficult to figure out what is a real attack. False negatives: It's very easy for honeypots to detect and records attacks or behavior never seen before in the wild. Cost effective: Honeypots only interact with malicious activity; we do not need high performance resources. Simplicity: Honeypots are very simple; there are no advance algorithms to develop, nor any rule bases to maintain.

Disadvantages of Honeypots are Limited Vision: A honeypot is tracked and captured when the attacker directly interacts with them. Attacks against other parts of the system will not be captured unless they honeypot is threatened also. Discovery and Fingerprinting: When an attacker can identify the true identity of a honeypot, a fingerprinting is donned. Risk of Takeover: If taken over, the honeypot may be used to attack other systems, within or outside the organization. The honeypot could be used to store and distribute contraband.

6. Honeypot Detection System

The system architecture of the proposed honeypot detection scheme (Prathapani, 2009) consists of several components.

Route Module: It consists of a Route Reply Analyzer, Dummy Packet Generator, and Constant Bit Rate Unit. This module analyzes the RREP packet and makes a note of the sequence number and the hop count in the REP packet. It then triggers the Dummy Packet Generator to generate dummy packets to be given to the testee. These dummy packets are used to determine whether the 'testee' under consideration is malicious or reliable. Such

traffic is sent towards a ' testee' to be forwarded to a given destination. Feedback Module: The feedback module plays a critical role in the detection of the blackhole MR. It gives the information that it has learned from the alternate path and dispatches a query packet to the known destination to determine if it has received any traffic packets from the testee. If the packet is received by the destination MR, it acknowledges the receipt of the traffic and unicasts a trace.

Alert Module: The alert module broadcasts the identity of the malicious blackhole to all MRs in the network so that they stop forwarding traffic through it and discard any route reply packets originating from the blacklisted blackhole MR. An alert is issued by the alert module to block the intrusive activity, when an attack is detected.

Interactive log: It gathers information on the route replies. It gives the information about the strategies that the honeypot has applied to lure the malicious MR. Honeypot System Architecture attacker uses to lure other MRs in the network. The report of the entire route discovery phase and alerts are lodged in the Interactive log.

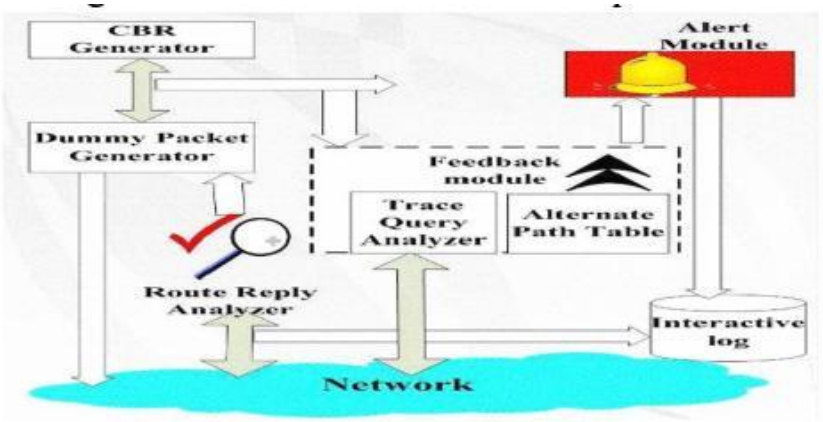


Fig. 1. Honeypot System Architecture.

7. Honeypot Agents in Detection

To detect such attack, it deploys the honeypots on MRs to lure the malicious attackers and these honeypots are synonymous to the network cops.

7.1. Proposed Scheme

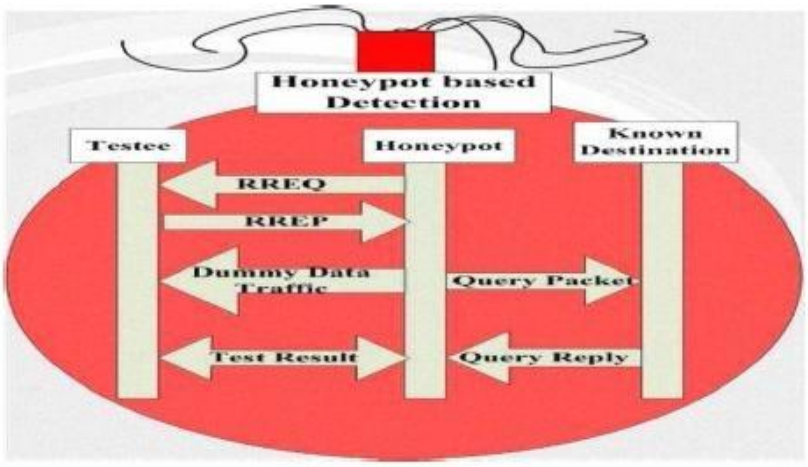


Fig .2. Honeypot Based Blackhole Attack

The steps followed in Figure 2 are:

1. The Honeypot agent sends a RREQ packet to the 'testee'. The source address is that of the MR on which honeypot is residing and the destination address is that of a randomly chosen known destination.

2. The 'testee' sends a RREP packet back to the honeypot that could be valid or spurious. Hence, in the subsequent steps, our honeypot detection scheme enables to distinguish the integrity of RREP packets.

3. Next, the honeypot prepares a testee data packet and forwards it to the ' testee'. The testee packet is like any other regular data packet. However, its payload is masked and padded with random data stream because of which it is not possible for the testee to conclude that it is originating from the honeypot.

4. The honeypot sends a 'Query packet' to the destination about the packet it has already forwarded to the 'testee' in Step 3. It then sends the query packet through this known route. Various fields in the query packets consist of:

a.) Sequence Number: It is the sequence number of the packet generated from the source.

b.) Source IP address: The source IP address is the address of the MR on which the honeypot resides.

c.) Destination IP address: It is the address of the known destination as per the honeypot detection scheme.

d.) Testee id: Source IP address of the testee being evaluated.

5. When a destination receives such a trace query, the destination processes it by examining its most Recently Received Traffic Cache, including the source ids, a timestamp when it was received and count of number of packets received from this source

6. If the destination finds the testee id in its traffic cache, it prepares a "Query reply packet", the destination address of which is equal to the source address of honeypot from which query packet came. The query reply packet also includes the following data in its information field: count of number of packets received and the timestamp of last received packet. Thus, the Query reply packet is unicast to the honeypot using the same route on which trace packet came (Know Your Enemy, 2003; Pirzada, 2005).

8. Honeynets

Honeynets are Information System that deploys honeypots to track footprints of attackers.

Honey nets can be divided into two generations (Karthik et al., 2009). Gen I Honeynets and Gen II Honeynets.

8.1. Gen I Honeynets

The Gen I Honeynet was implemented in an isolated network. A firewall and a router were used as access control devices. Data Control was implemented at the routing firewall. However, Gen I Honeynet has the high risk of intruder exploiting its data control mechanism.

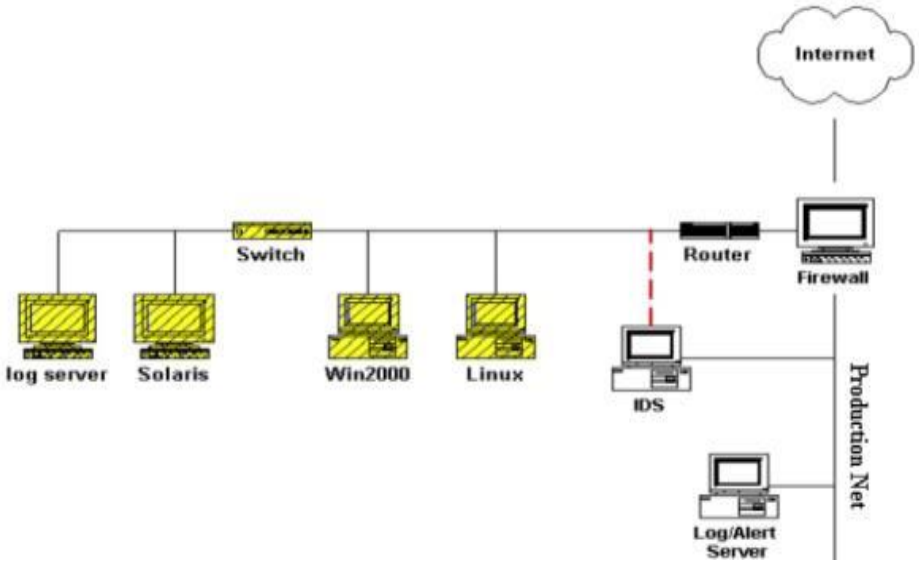


Fig. 3. Generation I Honeynet

8.2. Gen II honeynets

The Primary goal of a Gen II Honeynet is designated to ensure that compromised nodes of the Honeynet are not used to attack machines outside the Honeynet, and to ensure efficient data capture and to make the system hard to detect. The sensor is comprised of a firewall and an Intrusion Detection System. The presence of the IDS provides superior data control techniques. Alongside Gen II Honeypots, Redirection is a newly introduced concept that basis on redirection of unauthorized or malicious activity to production systems of a Honeynet as illustrated in figure.

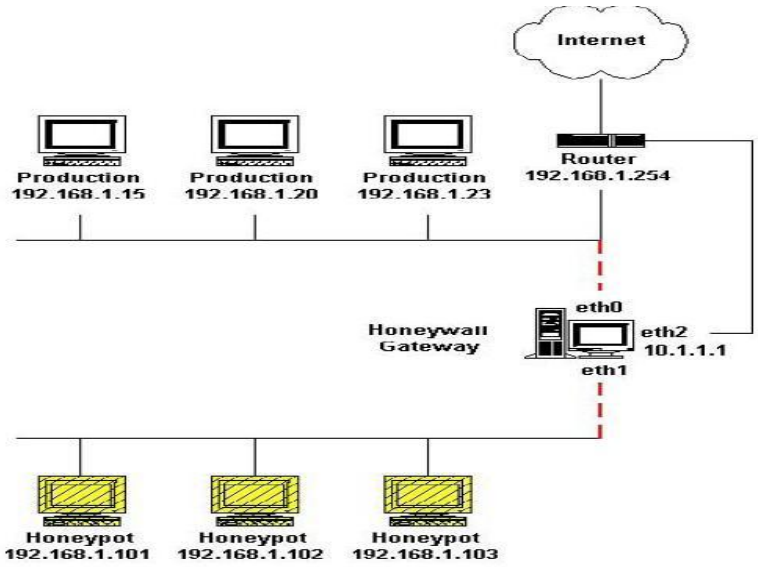


Fig. 4. Generation II Honeynets.

9. Conclusion

Honeypots are a new field in the sector of network security. Currently there is a lot of ongoing research and discussions all around the world. In this paper, an intelligent honeypot based detection system is using to identify the black hole attackers. A honeypot is an illusion that weaves for attackers. Future plan is to use honeypot detection agents to detect various other attacks. Also plan to use the Weighted Cumulative Expected Transmission Time as a routing technique to detect blackhole attackers in WMNs. AODV Protocol will be useful in applications for emergency services, conferncing, battlefield communications, and community-based networking. We look forward to further development of the protocol for quality of service, intermediate route rebuilding, and various interconnection topologies with networks and the Internet. Great deal of research is currently going on in devising the Honeynet architecture to track the activities of such hackers. Most of them are OS dependent. Coming up with a generic solution would be an appreciable task to perform.

References

Honeynet Project, 2001. "Know Your Enemy: Learning about Security Threats", 2nd Edition Addison Wesley Press.

Karthik, S., Samudrala, B., Yang, A.T., 2009. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 20, (4).

Know Your Enemy, 2003. Passive Honeynets. Honeynet Project. 18 January, 2003. http://project.honeynet.org/

Li-juan, Z., 2009. "Honeypot-based Defence System Research and Design", IEEE.

Pirzada, A.A., 2005. McDonald, C.," Secure Routing with the AODV Protocol", 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October.

Prathapani, A., 2009. Lakshmi and Dharma P.Agrawal : "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks", IEEE.