Honeypot: a Supplemented Active Defense System for Network Security

Feng Zhang, Shijie Zhou, Zhiguang Qin, Jinde Liu
College of Computer Science and Engineering
University of Electronic Science and Technology of China
Sichuan, Chengdu 610054, P.R.China
E-mail: {ibmcenter, sjzhou, qinzg, jdliu}@uestc.edu.cn

Abstract Honeypot is a supplemented active defense system for network security. It traps attacks, records intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Integrated with other security solutions, honeypot can solve many traditional dilemmas. We expatiate key components of data capture and data control in honeypot, and give a classification for honeypot according to security goals and application goals. We review the technical progress and security contribution of nowadays production honeypot and research honeypot. We present typical honeypot solutions and prospect the technical trends of integration, virtualization and distribution for the future honeypot.
Keywords honeypot, honeynet, attacks deception, network security

I. Introduction

Web applications are broadly deployed. More traditional services are extended to Internet. E-commerce and e-government quicken up the process. At the same time, attacks and intrusions to the web application system become more popular. Hackers exploit more tricky and obscure methods [1]. Automated attacking tools and Trojan horse appear at a more rapid rate. Some of them such as worms, attack scripts and DDoS attacks are truly powerful and destruct [1, 2, 3, 23]. Traditional security technologies and defense system for network security are blunt while facing new attacks and intrusion.

Round the clock is one of the most important properties of web application, but attacks and intrusions change the situation. IDS can't give alert when intrusion occurred using new signature. Even worse, we can't down the service system to check it completely because there still many online users making their deals. To prevent, detect and react to intrusions without disturbing existing system is a severe problem for web application and network security. Traditional security technologies can't solve the problem. Firework gives flexible policy according to proper service ports to control out and in connections regarding the protected network or system. It does nothing to attacks using proper service ports [4]. IDS work well on detecting and alerting attacks of known signatures [8]. Most IDS can't detect unknown intrusions [7, 8, 9]. Though some can do anomaly detection by training a clean data set of normal action, clean data set is difficult or costly to get [8]. Information on Unknown signature of intrusion can't be attained unless attacks are analyzed. It is a contradiction that laggard attaining of unknown signature and signature matching based IDS. Honeypot system attempts to solve the problem by setting up a controlled environment similar to the service system, inveigling attackers, gaining information about new type intrusions to aid the corresponding security system [13, 14, 15, 16, 18]. Industry and academia show growing interests in honeypot and related technologies. In industry field, a variety of honeypots with different extent of interaction appear including BOF [25], Spector [26], CyberCop Sing [27], Honeynet [29], Open Source honeyd [28] etc. In academia, there are number of projects in progress such as ISIC Honeypot Project [10], Distributed Honeypot Project [11], honeynet Project [12]. Honeypot is a valuable tool aiding traditional security technologies to improve corresponding performance.

This paper introduces honeypot and honeypot related technologies from the viewpoint of security management for network. Basic conceptions, general model and taxonomy for honeypot are given in section 2. Key problem and focuses in honeypot research are addressed in section 3. Typical honeypot system is reviewed in section 4. Finally, trends of honeypot and the features that should be taken into account while designing future honeypot are summarized.

II. Honeypot Basics

This section refers to the basic conceptions, the general model and taxonomy of honeypot.

1. Conceptions and Ideas

A. Honeypot

Different researcher may give different definitions according to particular scenarios. We incline to take the following definition, "honeypot is a security resource who's value lies in being probed, attacked or compromised" [15]. It catches the nature of honeypot--if no one attack honeypot, it is nothing. Still, honeypot is valuable security tool by some active nature. Other security tools such as firewall and IDS are completely passive for that their task is to prevent or detect attacks. Honeypot actively give way to attacker to gain information about new intrusions. This nature makes honeypot outstanding to aid other security tools. Honeypot is also integrated technology. Later we will demonstrate honeypot exploits IDS, firewall, routing control to realize an integrated active defense system. Therefore, We define honeypot in three folds. As a security resource whose value lies in being scanned, attacked or compromised, As a security tool whose value lies in actively luring attacks to attain intrusion

information and improving performance of other security tools such as IDS, As one technology whose value lies in being an alternative methods for network security.

Honeypot differ according to different use. It could be an emulated application, a full functional operating system with default configuration or an actual net including different OS and applications, even an emulated network on a single machine. We will cover different kinds of honeypot in section 4.

One basic assumption for honeypot is that all connections outward and inward honeypot are considered conspicuous [15, 16]. That is rational for that honeypot itself doesn't provide public product services, and that Connections inbound and outbound honeypot are probably initiated from attacker to probe or attack the target. There maybe some mistyping IP but the chance is little.

B. Production Honeypot and Research Honeypot

Traditional honeypot is used to protect network of corporation. production honeypot is aimed to do so. Always does product honeypot come in company with production systems such as mail server and www server. They protect the target system by deceiving and detecting attacks, giving alert to administrator.

Research honeypot is primarily for learning new attacking methods and tools, gaining new information about attacks though it can be used for production honeypot. It provides more interactive chances for attackers and takes more risks being controlled at the same time. Research honeypot take an effective data control mechanism to prevent from being a jump to attack other computer system [16].

C. Honeynet

Honeynet has particular meaning corresponding to honeypot. Firstly, it is mainly used for research work. Secondly, there are multiple system in a honeynet. All systems placed within the Honeynet are standard production systems. Nothing is emulated nor is anything done to make the systems less secure. Honeynet is more interactive than honeypot and strongly resemble an actual net (it is truly an net with router, workstations, popular operationg systems and default configured service installed in default signature). Honeynet project focuses on honeynet related technologies. This organization give many useful advices making honeynet easier to deploy and difficult to detect. Honeynet and honeypot advance together by sharing attacks deceptions, data capture and data control technology.

D. Data Control and Data Capture

Data control and data capture are two essential requirements lie in all kinds of honeypot. The main task of honeypot is luring attacks and gaining intrusion information while preventing being used to attack other system. Data capture fulfill recording intrusions and attacks to honeypot. Data control measures up to prevent the compromised honeypot being an gangplank and protect the record data. Research works on data control refer to connection control and routing control technologies, and that data capture is a layered architecture to record data from link layer, IP layer and application layer. Related fields cover firewall, router and IDS.

2. General Model for Honeypot

In 2.1.4, we interpret two essential requirements of honeypot—data control and data caputure. the following model fulfills the basic two requirements and performs effectively.

We deploy IDS component, firework component, router control component, log component In the general model, target OS and applications with default configured. All of them cooperate one another to form a honeypot system. We will analyze it how to work and fulfill two requirements.

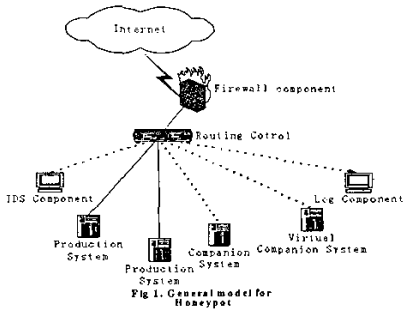

Fig 1. General model for Honeypot

Data control includes connection control and routing control. Firewall component (connection control) controls the outbound and inbound connections. Certainly, we allow all the inbound connections to the honeypot or we can't trap any attacks. Outbound connections should be controlled because connections initiated from honeypot is probably be used to attack other computer system. Alternative measures could be taken, just count and setup an threshold for outbound connections, add intelligence by analyzing activities of applications respectively to determine if an outbound connection should be blocked. Routing control component is the second layer for access control. It blocks any non-honeypot-IP packets so as to prevent most IP spoofed attacks to other system. Routing control component also supplements firewall component to control outbound connections.

Data capture uses a 3-layer hierarchy to capture and store data. Firewall component is the first layer (IP layer) to capture outbound and inbound connection data. All the connections are considered suspicious. These data are critically useful when watching and analyzing attack process. Second layer of data capture is IDS component, which captures all the network activities of honeypot in link layer. It lies in the same network with the target honeypot system and gather data in a hidden way. The third layer is log component which logs all the activities of the honeypot OS in application layer. Log data are stored remotely in strong access controlled log server. Experienced attacker would discover the remote log and try to destroy log server. It need more advanced skills to succeed compromising the security enhanced log server.

Even if attacker really hack the log server, we have firewall and IDS component record the attacking process.

Layered data control and data capture gives attackers great flexibility to interact with honeypot and provides a more secure way protecting intrusion process data. Data control and data capture can be deployed in a distributed layered net environment for secure reason or deployed in one single machine for portability.

3. Honeypot Taxonomy

honeypot can be classified by security goals or application goals. Related research work focuses different fields accordingly. We break honeypot into four broad categories according to security goals, prevention, detection, reaction and research. The first three focuses different cycles in security, while the last one focuses the whole attacking process.

Prevention honeypot stops attacker compromising production system indirectly. It applies effective attacks deception methods such as IP address deception (using multi-homed capability in a single LAN interface), network traffic simulation and information deception. Hacker wastes time attacking honeypot system instead of production system. In this way, honeypot deters attacks in and protects production system from being comprised. It's true that new automated attacks and worms can infiltrate the production system. honeypot still more easier to capture the auto-rooters and worms because of know vulnerabilities to provide information in advance.

Detection honeypot gives alert when attack occurs. Main difference between detection honeypot and IDS lies in that honeypot detects compromises by virtue of system activities while IDS compares intrusion mode with known signature. So detection honeypot is effective in detecting new or unknown attacks. The other contribution to intrusion detection is that it can reduce both false positive rate and false negative rate. False positives are alerts that were generated when IDS sensor recognizes "signatures" are intrusions but are valid in reality. False negatives are opposite meaning, IDS fails detects valid intrusions. Reducing false positive rate is a big problem IDS facing. Outbound and inbound honeypot connections can be attacks to honeypot or attacks initiated from compromised system. Thus alert generated from honeypot is lower false positive rate and false negative rate. Detection honeypot can't be deployed solely because honeypot itself would be comprised and controlled. Detection honeypot can be a powerful tool supplements IDS in attacks detection.

Reaction honeypot is a companion system for production system. It provides a environment similar to production system for taking measures to find the cause and patch vulnerabilities after the production system is attacked and compromised. It is always a great loss to take production system off-line for a full analysis after intrusion occurs, but we can't have a completely check on on-line target system for that there are active users making their deals and perhaps the attacker is just active in system. Reaction honeypot removes the difficulties. Incident team can take off-line the reaction honeypot and investigate in detail what failed, what damage was done, what entrance of attacker used and what he did. Lessons learned from reaction honeypot can be used to identify faults and recovery production system.

Research honeypot focuses threats information including motives, tools, methods and skills. It is a platform with common vulnerabilities and OS holes to attain information from the opponent. Unlike the above three honeypot, research honeypot doesn't always company with production system but give attacker great flexibility. The goal of research honeypot is security research. Researchers analyze new attacking tools as well as worms extracted from recording information. Remedies or solutions can be applied to enhance normal system security.

One honeypot maybe carry several responsibilities of both security goal and research goal. We know that prevention, detection and reaction relate one another in security life cycle. Research honeypot can be modified and adapted to particular security life cycle too.

Honeypot can be classified according to application goals. The kind of application-oriented honeypot dedicate to solving a certain application security problem. The following are several application-oriented solutions. A case in point is antispam honeypot, which filters spam without eliminating legitimate mail [20, 21]. DoS and DDoS honeypot detect attacks by signature matching and actively directing attacking packets to honeypot through transparent packet forwarder [22]. Worm honeypot traps a robot intruder indefinitely by manipulating the TCP session parameters. Almost no intruder could escape [24].

III. Research Focus

The total goal of improvement is making honeypot easier to deploy and more diffcult to detect. Present research points to the following fields.

1. Detection Method

Tracking attacker's activity instead of merely counting their outbound connections. An activity is asserted to be an attack according to actual activity in honeypot. Assertion is made basing on common-use command sequence or tools such as ftp, telnet. Data mining method of sequence analysis is introduced to add intelligence for attacks detection [9].

2. Reaction Method

We have mentioned that all outbound connections above the threshold would be blocked. In this way, we prevent the comprised system being a gangplank but risks implying the existence of connection control (firework). Valuable information on attacker's activity after compromising a system can't be attained. We hope a way that is effective and far more difficult to detect. Data control can be replaced by a 2-layer gateway, which would modify several bytes of packets considered to be attacks [16]. Attacker still can create connections with other system send ordinary request but can't receive

proper response packets. This is a preferable response way without knocking the attacker.

3. Data Capture and Data Store Method

How to capture and store data in a trick way is permanent problem. Honeynet project propose an artful solution to data capture. Attcker's activity is captured by kernel module of honeypot OS, which encapsulates the captured data with a spoofed IP and common use protocol such as NetBIOS. Honeypot gateway actively captures, decrypts, and reconstructs these data. Capture data in kernel module make it independent of the communication means, such as SSH, SSL, or IPSEC. Spoofed ip and encapsulation are used to trick attackers [16].

4. Virtual Honeypot

It combines data capture and data control as well as other components of honeypot in a single machine. Virtual honeypot even can simulate different kinds and different number of honeypot in a device. Related technologies includes virtual environment in home OS, IP stack simulator and application simulator.

IV. Honeypot Examples

We select several honeypot systems to show the status of honeypot products. Each is a sample of one kind. We investigate different honeypot system concerning security value, interaction and virtualization.

1. BackOfficer Friendly (BOF)

BOF is developed by Marcus Ranum. It is a lightweight honeypot and free to distribute. We choose BOF because it represents an accurate distillation of the ideas and insights of honeypot. BOF emulates several common services such as http, ftp, telnet, mail and BackOrrifice. BOF logs, alerts and responses a fake reply whenever someone connects to such ports. BOF user can have clear view of the attacking process [25].

2. Specter

Specter is a commercial production honeypot whose value lies in detection. Spector can simulate 13 different operating systems in application level including Windows, Linux, Aix, Solaris, MacOS etc. It's a windows based software which offers 14 different network services and traps. The other character is actively gathering attackers information such as Whois and DNS lookup. Specter is a low interactive honeypot which fakes the reply of attacker's request. Attacker can't utilize the application to interact with the OS [26].

3. Honeyd

Created by Niels Provos, Honeyd is an powerful production honeypot, which can be used for attacks detection and reaction. It represents today's level of production honeypot in many fields. First, it can emulate over 400 kinds of OS at IP stack level. This hides the guest OS before attacker. Second, emulating hundreds of computers at a single machine by use of Arp spoofing. Third, Honeyd is Open Source honeypot system. It is free to use and easy to modify for particular requirement. Honeyd still use the simulated service reply to attacker's request, but administrator can customize the reply script to provide attacker more flexibility [28, 30].

4. Honeynet

Honeynet represents the highest level of research honeypot. We have pointed out that it is a high interaction honeypot which is primarily used for research. It can also be modified to production honeypot for attacks detection and reaction. New methods of data capture and data control proposed by Honeynet project show greater flexibility and higher access contrl ability, which can be applied both research honeypot and research honeypot [29].

V. Conclusion

Honeypot is not a solution to network security but a good tool supplements other security technologies to form an alternative active defense system for network security. Working with IDS and firewall, Honeypot provides new way to attacks prevention, detection and reaction. Honeypot can serve as a good deception tool for prevention of product system because of it's ability of trapping attacker to a decoy system. Supplemented with IDS, honeypot reduces false positives and false negatives. Intelligence routing control provides flexible response to attacks. Different kinds of honeypot share the common technologies of data control and data capture. Researchers focus the two to make honeypot easier to deploy and more difficult to detect. From the advances in research and production honeypot nowadays, we predict the future honeypot has the features of integration, virtualization and distribution. Integrated honeypot encapsulates all the components in a single device. Virtual honeypot creates large number of honeypot systems in one machine. Distributed honeypot comprises different honeypot system in an actual network to offer high interaction between attacks and system. All of them make future honeypot cheaper to apply and easier to maintain.

REFERENCES

[1] Gary McGraw, Greg Morrisett. Attacking Malicious Code: A report to the Infosec Research Council , May. 2001. http://citeseer.nj.nec.com/498998.html

[2] Felix Lau, Stuart H. Rubin, Michael H. Smith, Ljiljana Trajovic. Distributed Denial of Service Attacks. IEEE International Conference on Systems, Man, and Cybernetics,pp. 2275-2280,Oct. 2000.

[3] CERT Coordination Center, "Results of the distributed systems intruder tools workshop," Nov.1999. http://www.cert.org/reports/dsit_workshop.pdf.

[4] Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, Jonathan M. Smith.Implementing a distributed firewall. ACM Conference on Computer and Communications Security, pp.190-199, 2000.

[5] Dan Schnackenberg, Kelly Djahandari, D. Strene. Infrastructure for Intrusion Detection and Response. Proceedings of DISCEX, January 2000

[6] Alan M. Christie. The Incident Detection, Analysis, and Response (IDAR) Project. http://www.cert.org/idar/papers/IDAR_paper.pdf
[7] Gene Spafford, Mark Crosbie, COAST group. Dept. of computer science. Active Defense of a Computer System using Autonomous Agents Technical report no.98-005, Dept. of Computer Science, Purdue University.
[8] Eleazar Eskin. Anomaly Detection over Noisy Data using Learned Probability Distributions. Proc. 17th International Conf. on Machine Learning. Morgan Kaufmann, San Francisco, {CA}, pp.255—262. 2000.
[9] Terran Lane, Carla E. Brodley. Temporal sequence learning and data reduction for anomaly detection. ACM Transactions on Information and System Security, Vol.2, No.3, pp. 295—331. 1999.
[10] Ireland Security Information Center and DuBlin City University. ISIC Honeypot Project. http://www.isiclabs.com/honeypot/.
[11] Distributed Honeypot Project. http://www.lucidic.net.
[12]honeynet Project. http://www.honeynet.org/misc/project.html.
[13] Reto Baumann, Christian Plattner. Honeypots, Diploma thesis. Feb, 2002. http://security.rbaumann.net/download/diplomathesis.pdf
[14] Reto Baumann, Christian Plattner. White Paper: Honeypots. Feb, 2002. http://security.rbaumann.net/download/whitepaper.pdf
[15] Lance Spitzner. Honeypot: Definitions and Values. May, 2002. http://www.spitzner.net
[16] Honeynet Project. Know Your Enemy: Honeynets. http://www.honeynet.org/papers/honeynet/
[17] Honeynet Project. Know Your Enemy: A Forensic Analysis. http://www.honeynet.org/papers/forensics/
[18] Honeynet Project. Know Your Enemy: Motives. http://www.honeynet.org/papers/motives/
[19] Michael Clark, Virtual Honeynets. Nov, 2001. http://online.securityfocus.com/infocus/1506/
[20]Spencer, Fighting Relay Spam the Honeypot Way. http://fightrelayspam.homestead.com/
[21]Jack Cleaver. Jackpot Mailswerver: a SMTP Relay Honeypot. http://jackpot.uk.net/
[22]Nathalie Weiler. Honeypots for Distributed Denial of Service Attacks. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02). P.109, Jun, 2002.
[23]Information Security Inc. 2001 Industry Survey on Computer Attacks. http://www.infosecuritymag.com/articles/october01/images/survey.pdf
[24] Tom Liston. Trapping Worms in a Honeypot: The Tarpit. http://www.threenorth.com/LaBrea/
[25] Marcus Ranum. BackOfficer Friendly (BOF). http://www.nfr.net/products/.
[26]Spector. http://www.specter.com/default50.htm
[27] CyberCop Sing. CyberCop Sting Getting Started Guide. http://www.um.es/ftp/mirror/ftp.mcafee.com/security/ccsting/manual/Cstguide.pdf
[28] Niels Provos. Open Source honeyd. http://www.citi.umich.edu/u/provos/honeyd/
[29] Honeynet. Tools for Honeynets. http://www.honeynet.org/papers/honeynet/tools/
[30] User-Mode Linux: an OpenSource solution to create a virtual Machine. http://user-mode-linux.sf.net/honeypots.html.