The Use of Honeynets to Detect Exploited Systems Across the Wireless Networks

Mahmood I*
CS Department, Aptech Computer Education, Wah Cantonment, Punjab, Pakistan

Abstract

Any internet is target of hackers and intruders. Every organization/institution system connected uses some kind of network security software to protect its data from unauthorized use. Software’s used by organization/institution are antivirus firewall etc. There are many types of services that are run on organization/institution networks and it is important to detect intrusion. Due to large bandwidth, monitoring is very hard and impossible. In developing, where the cyber-crimes are very easy to commit and there are not very strong lows Honeynet scheme, is use to help system administrator in detecting intrusion or malicious content. Honey net is only deception. They deceive the attacker that he is conquering the real systems or applications. But there every activity is closely watched and monitored, this information is used to improved the system security and avoid such attacks in future. Honeynet can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice versa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless, if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis. Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

Honey net is a better solution because it is set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to improve the system security and avoid such attacks in future. Honeynet is not tool used for offence or defense. It allows us to measure flaws or vulnerabilities in our system. Honeynet provide an information gathering approach to security; there sole purpose is to gather Information about threats in the network. A Honeynet is an interactive type of honeypot which provides real systems and application for attackers to attack and thus capture real information on a real attack [1]. Technically the Honey is only deception. They deceive the attacker that he is conquering the real systems or applications. But there every activity is closely watched and monitored, this information is used to improved the system security and avoid such attacks in future. Honeynet can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice versa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless, if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis. Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

Honeynet is a better solution because it is set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to improve the system security and avoid such attacks in future. Honeynet is not tool used for offence or defense. It allows us to measure flaws or vulnerabilities in our system. Honeynet provide an information gathering approach to security; there sole purpose is to gather Information about threats in the network. A Honeynet is an interactive type of honeypot which provides real systems and application for attackers to attack and thus capture real information on a real attack [1]. Technically the Honey is only deception. They deceive the attacker that he is conquering the real systems or applications. But there every activity is closely watched and monitored, this information is used to improved the system security and avoid such attacks in future. Honeynet can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice versa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless, if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis. Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

Keywords: Cyber; Cyber crime; Hacking; Intrusion detection; Honeynet

Introduction

Honeynet is not tool used for offence or defense. It allows us to measure flaws or vulnerabilities in our system. Honeynet provide an information gathering approach to security; there sole purpose is to gather Information about threats in the network. A Honeynet is an interactive type of honeypot which provides real systems and application for attackers to attack and thus capture real information on a real attack [1]. Technically the Honey is only deception. They deceive the attacker that he is conquering the real systems or applications. But there every activity is closely watched and monitored, this information is used to improved the system security and avoid such attacks in future. Honeynet can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice visa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless, if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis. Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

Honeynet is a better solution because it is set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to improve the system security and avoid such attacks in future. Honeynet can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice versa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless, if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis. Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

High interaction honeynet

This is aggressive approach which allows the attacker to penetrate in a system. The attacker is allowed to attack on real time environment which actually exist in our organization. The attacker is allowed to have actual servers and applications to play with but he is monitored very carefully. Log file are created for future use and for creating pattern or signature based IDS. The benefit of using High interaction honeynet is collection of real time data [7,8]. Give the detail of a low-interaction honeynet, developed by Niels Provos, Honeyd which is designed to run

| Features | Low-interaction honeynet | High interaction honeynet |
|----------|--------------------------|--------------------------|
| Knowledge to Develop | Low | Mid high |
| Knowledge to Run | Low | High |
| Risk | Low | High |
| Real Operating System | No | Yes |
| Degree of Involvement | Low | High |
| Maintenance Time | Low | Very high |

Table 1: A comparison between High interaction and low interaction Honeynet.
primarily on unix systems, Honeyd works on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the attacker, pretending to be the victim. By default, Honeyd detects and logs any connection to any UDP or TCP port. In addition, you can configure emulated services to monitor specific ports, such as an emulated FTP server monitoring TCP port 21. When an attacker connects to the emulated service, not only does the honeynet detect and log the activity, but it captures all of the attacker’s interaction with the emulated service. In the case of the emulated FTP server, we can potentially capture the attacker’s login and password, the commands they issue, and perhaps even learn what they are looking for or their identity. It all depends on the level of emulation by the honeynet [9]. Most emulated services work the same way. They expect a specific type of behavior, and then are programmed to react in a predetermined way. If attack A does this, then react this way. If attack B does this, then respond this way. The limitation is if the attacker does something that the emulation does not expect, then it does not know how to respond. Most low-interaction honeynet, including Honeyd, simply generate an error message [10-12].

A high-interaction honeynet is a conventional computer system, such as a commercial off-the-shelf (COTS) computer, a router, or a switch. This system has no conventional task in the network and no regularly active users. Thus, it should neither have any unusual processes nor generate any network traffic besides the regular daemons or services running on the system. These assumptions aid in attack detection. Every interaction with one of our honeynets is suspicious and could point to a possibly malicious action. This absence of false positives is one of the key advantages of high-interaction honeynet compared to intrusion detection systems (IDS). To quote Rutherford D. Roger, “We are drowning in information and starving for knowledge.” This may be a common phenomenon for IDS, but not for honeynet [13].

Further says that High interaction honey pot can be used to collect in-depth information about the procedures of an attacker. We can observe the “Reconnaissance phase” that is, how he searches for targets and with which techniques he tries to find out more about a given system. Afterward, we can watch how he attacks this system and which exploits he uses to compromise a machine. And finally, we can also follow his tracks on the honeynet itself. We monitor which tools he uses to escalate his privileges, how he communicates with other people, or the steps he takes to cover his tracks. Altogether, we learn more about the activities of an attacker his tools, tactics, and motives. This is an interesting field, and this methodology has proven to be successful in the past. For example, we were able to learn more about the typical procedures of phishing attacks and similar identity theft technique since we observed several of these attacks with the help of high-interaction honeynet.

**Proposed Honeynet Framework**

Honeynet work step by step using following techniques.

**Data control**

This very important function when implementing Honeynet, It is required that attacker feels that he is free to launch an attack. It is important to implement different data control layers (Figures 1 and 2) [13].

- Counting outbound connections.
- Intrusion prevention gateways.
- Bandwidth restrictions.

![Diagram](image-url)
Data capture

There should be a process of data collection which collects data of attack on Honeynet by attacker. The data is monitored and analyzed. A log file should be maintained for future use. These log files can also be used as proof of his attacks. Many tools can be used to capture the data. Examples can be Wireshark, sebek, etc. Here, W3af is used to collect the data about iqra website. Results indicate uninterrupted data capture from iqra university for 12 minutes 30 seconds.

An intrusion detection system

Very important part of Honeynet is IDS software called snort. It is used which is between the internet and Honeynet. It generates alerts and reports the data traffic (Figure 3).

Firewall logging

Firewall is used to log all data traffic coming in and out of Honeynet. It also maintains log files for connections denied or refused (Figure 4).

Data analysis

The final part of Honeynet is data analysis which is very important and final part in making a complete report of attacks and their pattern. Based upon the input data, the log attacker is blocked (Figures 5 and 6) [13].

Figure 2: W3af Data capture results.

Figure 3: Honey bot data log.
Figure 4: KFSensor firewall log.

Figure 5: Analysis of data KF sensor.

Figure 6: Data Capture.
Conclusion and Future Work

In this growing IT environment, there is also a need to strengthen its security. Preventive, Detective and Responsive measures have to be undertaken in order to improve IT Security. Technique used in the paper is well defined but the tool uses for instruction detection are not up to mark for an Enterprise environment, there is a need of comprehensive study to generate an integrated set of tools to fully implement the honynet. to detect new exploits launched against the organization/institution network. An area for further research would involve the establishment of a distributed Honeynet across the any Enterprise network.

References

1. Pravesh G (2018) Honeypots-and-Honeynets.
2. Zentyal (2018) Firewall configuration with Zentyal.
3. Spitzner L (2002) Honeypots Tracking Hackers.
4. Spitzner L (2018) Honeypots Tracking Hackers.
5. Warkentin M (2008) Enterprise Information Systems Assurance and System Security Cohen F. Internet Holes - Internet Lightning Rods Network Security Magazine.
6. Cohen F (1992) Operating System Protection Through Program Evolution Computers and Security.
7. Honeynet (2018) The Honeynet Project.
8. Cohen F, Phillips C, Swiler LP, Gaylor T, Leary P, et al. (1998) A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model. The Encyclopedia of Computer Science and Technology.
9. Honeynet (2018) The Honeypet Project.
10. IJCST (2018) Honeypot: A Survey.
11. Atomic Software Solutions (2018) HoneyBOT is a medium interaction honeypot for windows.
12. Honeynet (2018) The Honeypet Project.
13. Honeyd (2018) Honeypot Background.