Honeypot Mechanisam

Nimmy Mathew
Student of St. Mary's College
Department of computer science
Thrissur, Kerala, India

***Abstract*: - This paper shows possible implementation of honey pot in local network. The honey pot works as the 0-day malware detection system. It implements many of active or semi-active traps in local area network and DMZ in the company network. There are not defined the legal trace to the honey pot. That mean, that common connection does not be forwarded to the honey pot. The approved users and computers are not being able to detect the honey pot. This means that all communication with honey pot coming from the unauthorized devices. The common IDS system does not detect the 0-day vulnerabilities. The trap represented by the honey pot in the network might detect behavior of new exploits and hacker attempt.**

Key-Words: Security, honey pot, IDS, network, intruder, malware, exploit

1 INTRODUCTION

The World is represented as the many interconnected networks. These interconnections show rapid simplify of the common life. People occasionally use Internet as the global network. They used local networks as the common working tool. The interoperability of these networks represents the big potentially security issue; if there are everything connected to everything, the network does not have any borders. The intruder might misuse this connection from any place in the World.

Companies use some type of security systems occasionally. The antivirus and the firewall are the common standard [1][2]. The next level is represented with an anti-spam filter and a content analyses tool [6]. But how it is with protection against 0-day exploits? Is there any option or future, how to detect 0-day exploits, malware and hacker attacks?

2 PROBLEM FORMULATION

The main problem in computer security is the evolution. Many attack vendors had same signature and it is possible to create the definition of this attack. There are only a few the original examples of malware; each other is only the derivation of it [1]. The evolution brings the minimal probability of the original vendor of malware or attack. But the minimal probability is not the zero probability [6].

2.1 0-days exploit

The zero day exploit represents the new vulnerability of the tested system. This is the new vendor of the attack and is possible that these types of attacks could not be detected by the definition based computer security components.

2.2 Undescribed hacker attack

This new type of attack is combined with the 0-day exploit occasionally. The attacker behavior might be undetectable, because the commonly used system does not find this vendor in the definition database [7].

2.3 Honey pot

The honey pot represents the real computer system; this system is used as the trap for unauthorized communication in the computer network. *„Honey pots are systems that are designed to be exploited… By creating such systems, you can attract and log activity from attackers and network worms for the purpose of studying their techniques."[2]*
There are some types of honey pots. The classification is based on the amount of interaction of interaction. The interaction of the honey pot determines the system requirements for implementation.

2.3.1 Low-interaction honey pot

These types of honey pots represent the system which only simulates the specific protocols on transport layout of TCP/IP model. These systems could emulate open ports for common services such as FTP, HTTP and SQL. The main advantage of these types of honey pots is their minimal system requirements.

2.3.1 Medium-interaction honey pot

This is the combination of low and high interaction honey pot. It is not only the emulation of the protocol. Application's protocols are not detailed simulated as in the high-interaction version, so the attacker thinks that this is the real system. This takes the time for the IDS/IPS to detect this action.

2.3.1 High-interaction honey pot

This is the real computer system with specific real vulnerability. For example, this will be represented by the computer with the MS Windows without security updates. These types of honey pots are manageable hardly [7]. This honey pot represents the high sophisticate interactive part of the network and it is not possible to distinguish the real system from the honey pot.

3 PROBLEM SOLUTION

The main problem for the IDS/IPS system is 0-day exploits or 0-day vulnerabilities. The possible solution is implementation of traps; these traps might catch new malware or the new vendor of attack. If there is any unwanted communication with the honey pot, there is potential malware or attacker. The honey pot is invisible for legal communication in the network.

The high-interaction honey pot is occasionally used in production systems. The amount of interaction is necessary for the trustworthy target for attackers.

3.1 Honey net

The honey net is the network of honey pot. There are many high-interaction honey pots inside the LAN segment. The purpose is to emulate many of potential victims for the attack. These honey pots have a specific gateway and monitoring tool based on the IDS or IPS system. The solution is valuable for its isolation from other parts of network. This solution minimizes the risk of misused honey pot in legal LAN segment.

All incoming and outgoing traffic from this honey pot network is monitored and deeply analyses at the potentially dangerous communication. There is the issue flowing from transformation of the honey pot to the sniffing device by the attacker.

3.2 Integration in network

There are some methods for integration of the honey pot into the company network. The best practises in these solutions are based on the desired property of implementation [8].

3.2.1 Honey pot in the LAN

The honey pot is on the same segment as production servers, and it has the same gateway. This solution is the best for using a small number of honey pots inside the network infrastructure. The main advantage is: the honey pot can detect the attackers from Internet and from local network. The honey pot might detect the illegal communication and attacks coming from outside and inside. It is possible to detect intruders from the local network.

This solution is the best way for wide networks. There is significantly growing risk of local intruders [10].

Honey pot on the LAN detect the active node scan; this scan is the starting point for the ARP poisoning attack.

If there are VLANs defined inside the infrastructure, the honey pots must be implemented in each VLAN.

3.2.2 Honey pot in the DMZ

This type of location is appropriate for detection intruders in DMZ. The DMZ occasionally contains production servers and every attempt for live host scanning and the network mapping. The advantage of this solution is isolation the DMZ from the local network. The compromited honey pot is not able to intrude security of computers in the local network.

This scenario is not recommended as the only one solution. If there is the attack to the local network, this type of honey pot could not detect unwanted communication to the local network. The DMZ is protected, but there is suggested to implement the other honey pot in the local network.

3.2.3 Honey pot in the Internet

. This situation represents the location of the honey pot outside the company network. The honey pot is connected before the firewall and it is totally unprotected.

The position is totally isolated from the local network. This is safe for the local infrastructure. But the local infrastructure is unprotected.

3.3 Communication with IDS/IPS

There must be authorized the two-way communication between installed honey pots (or honey nets) and IDS/IPS security components. The common IDS/IPS detects the known attack vendors or known behavior of malware. The IDS/IPS is responsible for analyses of the communication. It could detect unwanted communication. But the new vendor does in the definition database.

On the other side of the security system, there is the honey pot. The honey pot might detect the security treads, but it is not necessary. The fact is that all communication to the honey pot is unwanted. The IDS/IPS system analyse all communication to the honey pot. All of this communication is illegal.

The interaction rate between the honey pot and IDS/IPS system is important for two main specifications of the honey pot. It there is no interaction, all analyses is on the IDS/IPS system. The IDS/IPS system must be able to detect any suspicious behaviour on the honeypot.

This case simulates the real system; the attacker could not detect any outgoing suspicious communication from the honey pot. The honey pot is clearly undetectable. But the honey pot does not report any attack vendor. The detection and prevention routines are managed by the IDS/IPS completely.

The second option of interaction between the honey pot and the IDS/IPS system is the direct connection with reported services. This generates some communication between the honey pot and the IDS/IPS system, but this solution might detect any suspicious behaviour faster than the solution based without connection. The main issue in this scenario is the securing of the communication. The attacker might detect this communication and the honey pot might be compromised.

The direct LAN interconnection is unsecure method, because these communications might be detected.

The option used the serial port as the cable interconnection. The maximum length might limit the interconnection device.

3.4 The main roles of honey pot

This part describes the main 3 roles of honey pot in the production systems; these roles cover the master parts of computer security systems.

3.4.1 Prevention

This role might distract attention from the real system. The honey pot works as the trap for intruders. The position of the honey pot is so important. The prevention has 2 different levels of working.

The first is the trap for potential intruders. The honey pot must be the attractive target for the attacker. It must be the weakness point of infrastructure.

The second is the prevention based on the knowledge of intruder. If the intruder detects, that this system is only the honey pot, the intruder might leave this system, because the honey pot might report the unwanted behaviour and the security system starts defence routines.

The both of these levels help improve the infrastructure security.

3.4.2 Detection

The detection role is the basic role of each honey pot. If the prevention role failed, the most important operation is the detection of intruder. These detection routines contain method for: detection of malware and other intruders, collection of information about the attack and its source.

This might help the IDS/IPS system to detect these activities on other part of the infrastructure [6].

3.4.1 Reaction

The reaction phase is the last phase in the honey pot security system. This role is important in the cases, when the attacker breaks the production system security and might compromise the real server. The honey pot is the 1:1 copy of the production server in this case. The difference is only in contained data.

The honey pot does not contain the real data. It has only the collection of blank information. The system might be stopped and send to the forensic analyse every time. The honeypot contain the attack vendor and there were be information about attacker source address and its way back.

The examined attack vector is implemented to the IDS/IPS system and the 0-day vulnerability is detectable. The evidence received from the honeypot might be also used in the law process with the intruder.

3.5 Real application of honey pot

The most often implementation is based on the high interaction honey pot or honey net placed into the local area network of a company.

There is only one disadvantage; if the attacker compromises the honey pot, he will be able to use it for next phases of the attack. The IDS/IPS must periodically control the checksum of the honey pot. The detection and the reaction must be fast.

If there are many VLANs inside the network, it is necessary to implement the honey net with honey pots inside each network. The one honey pot with many VLAN interfaces might be identified as a honey pot very easily. The computer system inside production network with many VLANs is suspicious.

The IDS/IPS detects port scanning on “invisible” computer. The system reported it to the admin team. The message is clear; there is anyone who performs the port scanning on whole network. It is potentially the begin phase of the attack. The detection phase of honey pot was successful.

The honey net is configured for reporting any action. This report-level is hard constrains for the detection of any new attack vendors. The system is very sensitive for any potentially dangerous behavior; so the admin must evaluate every report. Because it is only the host alive scans from local admin account in many cases. The review from security admin is very important.

4 CONCLUSION

The honey pot represents the powerful weapon for unknown security vulnerability – 0-day exploits and not described method for hacking. The honey pot is not be implemented as the standalone system, the main purpose is; it is the trap. It necessary to implement IDS or IPS that monitors the honey pot and provide security functions inside the network infrastructure.

The implementation might be really variable. But there is some recommended solution.

The first, the honey pot or the honey net must be in any network in the company. The base implementation in DMZ zone works only in DMZ, the internal production server does not be secured. The internal intruders might be undetectable. If the internal intruders attack the server inside the LAN, the honey pot placed in DMZ could not detect this action.

The implementation of honey net across each network is hard to implemented and managed. But this solution is the best for the critical infrastructure. The risk of compromised honey pot inside the local network is minimal in this solution. External attackers might compromise DMZ zone primarily. The internal attackers have already local access.

ACKNOWLEDGEMENTS

The research work was performed to financial support by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

REFERENCES*:*

[1] McAfee LABS. McAfee Threats Report: Second Quarter 2012. c2012. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf
[2] LIGH, Michael Hale et al. Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code. Indianapolis: Wiley, 2011.
[3] SPITZNER, Lance. Honey tokens: The Other Honey pot. [online].2013http://www.symantec.com/connect/articles/honeytokens-other-honeypot
[4] SPITZNER, Lance. Honey pots: Simple, Cost-effective Detection. [Online]. 2013, http://www.symantec.com/connect/articles/honeypots-simple-cost-effective-detection
[5] SPITZNER, Lance. Honey pots: Tracking Hackers, 2012, ISBN: 9780321108951
[6] Singh A. N., Honey pot Based Intrusion Detection System, LAP LAMBERT Academic Publishing 2012, ISBN: 9783846583104
[7] Joshi R. C., Honey pots, Science Publishers 2011, ISBN: 9781439869994
[8] Cole, E: Network security bible, John Wiley, Indianapolis IN 2009, ISBN: 9780470502495
[9] Huang, S.:Network security, Springer, London 2010, ISBN:9780387738208
[10] Tipton, H.: Information security management.
[11] Elks, J.: Man in the Middle Attack: Focus on SSLStrip, GRIN Verlag 2011, ISBN: 9783640894721