International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Web-based Honeypot Tool for Website Analysis

Prof. Manoj Dhande[1], Prashant Patil[2], Supriya Mhashelkar[3], Avanti Patil[4], Shweta Jadhav[5]

Abstract: ***Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize this threat, it is necessary to have a security system that has the ability to detect zero-day attacks. "Honeypot is the proactive defense technology, in which resources placed in a network with the aim to observe and capture new attacks". This paper proposes a honeypot-based model for intrusion detection system (IDS) to obtain the best useful data about the attacker.Honeypots are a modern approach to network security. Ahoneypot is used in the area of internet security and cryptography. It is a resource, which is intended to be attacked and compromised to gain more information about the attacker and the used implementations. It can be deployed to attract and divert an attacker from their real targets. Honeypots have the big advantage that they do not generate false alerts as each observed traffic is doubtful, because no productive components are running on the system. This fact enables the system to log every byte that flows through the network through and from the honeypot, and to relate this data with other sources to draw a picture of an attack and the attacker.***

Keywords: Methodologies, Honeyd, Spammers, Proxies, Knowledge

1. Introduction

Computer crimes are growing rapidly, counter measures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. As in the military, it is important to know, who your enemy is, what kind of strategy and plan he uses, what tools he utilizes and what he is aiming for. Gathering this kind of information is arduous but important. By knowing attack strategies, countermeasures can be improved and anomalies can be fixed. To gather as much information as possible is one main target of honeypot.

Generally, such information gathering should be done without the attacker's knowledge. All the gathered information provides an advantage to the defending side and can therefore be used on productive systems to prevent attacks.

2. What is A Honeypot?

A honeypot is basically an instrument for information gathering and learning. A honeypot is an information system resource whose value lies in the unauthorized or illicit use of that resource. More generally a honeypot is a trap set to divert or discover attempts at unauthorized use of information systems. Essentially, honeypots are resources that allow anyone or anything to access it and add production value. Honeypots do not have any unprotected, unused workstation on a network being closely watched by administrators.

Its primary purpose is not to be an ambush for the black hat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, and the black hat community itself. All this information is used to learn more about the black hat proceedings and motives, as well as their technical knowledge and abilities. This is just a primary purpose of a honeypot. There are a lot other possibilities for a honeypot- divert hackers from productive systems or seize a hacker while conducting an attack are just two possible examples.

The two main reasons why honeypots are deployed are:
1) To learn how intruders probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems.
2) To gather forensic information required to aid in the apprehension or prosecution of intruders.

3. Types of Honeypots

Honeypots came in two flavors:
1. Low interaction
2. High interaction.

Interaction measures the amount of activity that an intruder may have with honeypot. In addition, honeypots can be used to combat spam. Spammers are constantly searching for sites with vulnerable open relays to forward spam on the other networks. Honeypots can be set up as open proxies or relays to allow spammers to use their sites.

We will break honeypots into two broad categories, as defined by

Snort, namely:
- Production honeypots
- Research honeypots

The purpose of a production honeypot is to help alleviate risk in an organization. The honeypot adds value to the security measures of an organization. Think of them as 'law enforcement', their job is to detect and deal with intruder.

4. Honeypot Architecture

1. *Structure of a LOW-INTERACTION HONEYPOT (GEN-I)*:- Atypical low-interaction honeypot is also known GEN-I honeypot. This is a simple system which is very effective against automated attacks or beginner level attacks Honeyd is one such GEN-I honeypot which emulates services and their responses for typical network functions from a single machine, while at the same time making the intruder believe that there are numerous different operating systems. It also allows the simulation of virtual network topologies using a routing mechanism that mimics various network parameters such as delay, latency and ICMP error messages. The primary

architecture consists of a routing mechanism, a personality engine, a packet dispatcher and the service simulators. The most important of these is the personality engine, which gives services a different 'avatar' for every operating system that they emulate.

Drawbacks

- This architecture provides a restricted framework within which emulation is carried out. Due to the limited number of services and functionality that it emulates, it is very easy to fingerprint.
- A flawed implementation also leads to reduce itself to alerting the attacker.

It has constrained applications in research, since every service which is to be studied will have to be re-built for the honeypot.

2. Structure of a HIGH INTERACTION HONEYPOT (GEN-II):-A typical high-interaction honeypot consists of the following elements: resource of interest, data control, data capture and external logs.These are also known as GEN-II honeypots and started development in 2002. They provide better data capture and control mechanisms. This makes them more complex to deploy and maintain in comparison to low-interaction honeypots.

High interaction honeypots are very useful in their ability to identify vulnerable services and applications for a particular target operating system. Since the honeypots have full-fledged operating systems, attackers attempt numerous attacks providing administrators with very detailed information on attackers and their methodologies. This is essential for researchers to identify fresh and unknown attack, by studying patterns generated by these honeypots.

Drawbacks

- The number of honeypots in the network is limited.
- The risk associated with GEN-II honeypots is higher because they can be used easily as launch pads for attacks.

5. Research Using Honeypots

Honeypots are also used for research purposes to gain extensive information on threats, information few other technologies are capable of gathering. One of the greatest problems security professionals face is lack of information or intelligence on cyber threats. How can your organization defend itself against an enemy when you do not know who the enemy is? Research honeypots address this problem by collecting information on threats. Organizations can use this information for variety of purposes including analyzing trends, identifying the attackers and their community, ensuing early warning and prediction or understanding attacker's motivation.

Advatages of Honeypots

1) They collect small amounts of information that have great value. This captured information provides an in-depth look at attacks that very few other technologies offer.
2) Honeypots are designed to capture any activity and can work in encrypted networks.
3) Honeypots are relatively simple to create and maintain.

Disadvantages of Honeypots

1) Honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.
2) There is also level of risk to consider, since a honeypot may be comprised and used as a platform to attack another network. However this risk can be mitigated by controlling the level of interaction that attackers have with the honeypot.

6. Conclusion

Honeypots are positioned to become a key tool to defend the corporate enterprise from hacker attacks it's a way to spy on your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they have accessed a corporate network, when they are actually hanging around in a honeypot-- While the real network remains safe and sound.

Honeypots have gained a significant place in the overall intrusion protection strategy of enterprise. Security experts do not recommend that these systems replace existing intrusion detection security technologies; they see honeypots as complementary technology to network-and host – based intrusion protection.

We do believe that although honeypots have legal issues now, they do provide beneficial information regarding the security of a network. It is formulated to foster and support research in this area. This will help to solve the current challenges and make it possible to use honeypots for the benefit of the broader internet community.

References

[1] Honeypot: Concepts, Types and Working- 1Maitri Shukla, 2Pranav Verma,1Research Scholar, 2Assistant Professor 1Department of Computer Engineering,1SOCET, Ahmedabad, India © 2015 IJEDR | Volume 3, Issue 4 |ISSN: 2321-9939
[2] Honeyware: a web-based low interaction client honeypot YaserAlosefer, Omer Rana School of Computer Science & Informatics, Cardiff University, UK {Y.Alosefer, O.F.Rana}@cs.cf.ac.uk 978-0-7695-4050-4/10 $26.00 © 2010 IEEE DOI 10.1109/ICSTW.2010.41
[3] Research of Attacks on MySQL Servers Using Honeypot Technology-Artem Taran1,DmitryS. Silnov2 Institute of cybernetic intellectual systems National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia 1devil.tem@gmail.com, 2ds@silnov.pro978-1-5090-4865-6/17/$31.00 ©2017 IEEE
[4] Design Considerations for a Honeypot for SQL Injection Attacks- The 5th LCN Workshop on Security in Communications Networks (SICK 2009)Zürich, Switzerland; 20-23 October 2009.
[5] Honeytokens as active defense- A.B. Robert Petrunić, bacc.ing.comp., Algebra university college for applied computer engineering, Zagreb, Croatia

robert.petrunic@racunarstvo.hr MIPRO 2015, 25-29 May 2015, Opatija,Croatia.

[6] Development and Implementation of a HoneypotTrap-Aleksey A. Egupov1, SergeyV. Zareshin2, Igor M. Yadikin3, Dmitry S. Silnov4 Department №12 "Computer Systems and Technologies" National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) Moscow, Russia 1 virus ingalex@gmail.com, 2svzareshin@gmail.com, 3imyadikin@mephi.ru,4ds@silnov.pro978-1-5090-4865-6/17/$31.00 ©2017 IEEE