International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Deception Technique Used in Cyber Security (Honeypots)

Nidhi Yadav, Ram Singhal Verma
Assistant Professor Department of Computer Science, Baba Bhimrao Ambedkar University, Luck now, Uttar Pradesh, India

ABSTRACT

Our cyber world is going to converge in a very rapid manner, all the data and information is presented in digital format. As everything is on computers attackers easily predicts the information and attack the computer system. Here in this paper, we are going to discuss what ways deception play a most important in cyber security. Computer breaches can be prevented through this deception technique. .Honeypot used as a deception technique to prevent computer attacks. In this Paper we will discuss Advantages and limitation of this deception technique.

Keywords : Cyber Security, Honeypots, Advanced Persistent Threats, DBIR

I. INTRODUCTION

Organizations save its data in servers. And these servers are the easiest targets to the attackers advanced persistent threats (APT), corporate espionage, and other forms of attacks are very common and continuously increasing. Fortinet reported 144 million unsuccessful attacks in 2013. In addition, a recent Verizon Data Breach Investigation Report (DBIR) reported that currently deployed protection mechanisms are not adequate to address current threats [1]. The report by (DBIR) states that 60 to 70% of the breaches took months or years to discover. Furthermore, 80% of these attacks only took hours or less to infiltrate computer systems [1]. In Addition, the report states that only 5% of these breaches were detected using traditional intrusion detection systems (IDSs) while 70% were detected by external parties [1].These numbers are only discussing attacks that were discovered. Because only 5% of the attacks are discovered using traditional tools. But in reality, scenario is worse as there is number of undiscovered attacks. Current security threats cannot be prevented by the traditional security tools. We need more sofaciticated security tools .Each and every interaction with the computer system are monitored by protocols and software. These protocols and software uses error detection and correction method to find reasons why the interaction with the computer system fails. Attacker's uses error and detection mechanism to refine its tools and re-attack again and again until it does not penetrate the system. These kind of systems are helpful to the attackers and they get the guideline from the system to attack the system again after refinement of tools, hence targeted systems are not aware of these attempts but there is a panic in the security team.

There is number of advantages of deception technique over the tradition tools. In present, most of the security tools act as responsive measures to the attackers that probes over the known vulnerabilities of the systems. The attacker fined all the week points to penetrate the system. Through the deception technique attackers were attracted by system to attack it so that attacker is misled with the false information. There is number of differences in tradition based security mechanism and deception based mechanism. The latter focuses on the attackers actions detection and prevention measures.traditonal

method works on the attackers perceptions and manipulate them.

Computer security deception definition given by Yuill[2]; Computer Deception is "Planned actions taken to mislead attackers and to thereby cause them to take (or not take) specific actions that aid computer security defences". We add word "confusion" in the definition of computer security defence.

Computer Security Deception final definition is; "Planned actions taken to mislead or to confuse attackers and thereby cause them to take (or not take) specific actions that aid computer security defences."

II. HISTORY

Deception is one of the part our society from ancient time and deception also used in the technical world now a days to deceive attackers. Deception and decoy based mechanism used from decades, these decoy based mechanism is honeypot and honey token. Cheswick in his paper defined- "An Evening with Berferd" [3] He tells how the interaction with the attacker in the real time give him with fabricated responses. Fred Cohen developed a toolkit used for deception in 90's was the first publicly available tool used in computer defences. Cliff Stoll's book "The Cuckoo's Egg" shows the uses of deception technique in computer security. Honeypot concept comes in the late 1990's

Honeypot tools lured the attackers to attack the computer system .some of the files that need high security are stored at safe places, these files can't accessed by the normal user, another files with same or interesting and location name to deceive the attack are placed as bait that shall trigger an alarm if these files are accessed by the attackers.

- **HONEYPOT (Tool Used In Deception Technique)**

Honeypot is used in number of security applications, it is used in detecting, stopping spam and malwares. Databases are also secured by the honeypot. There is two types of Honeypot –Server Honeypot and client Honeypot. Server honeypot is the computer system that have no important information, it is mainly used to lure attacker to attack the server honeypot .Client Honeypot is highly active in comparison to the server honeypot .client honeypot are user agent moves over many computer system which are suspected to get compromised as the incident occur client honeypot inform the server that it has infected users'.

III. FUNCTIONS OF HONEYPOT

- **Detection**

Honeypot used in detection spams, malware and any intrusion on the server. Honeypot produce very less data as it is not to be interact by the normal user, honeypot is mainly intended to lure attackers. Angnostakis put forward the concept of shadow honeypot .it is very advanced detection architecture by using honeypot .In Shadow honeypots ,a dection sensors has been put in front of the real time system, when the request comes to the server ,detection sensors decided whether the request should be send to the normal machine or to the shadow machine. The shadow machine along with the honeypot integrate to the real system and diverted the suspicious traffic to the shadow machine to analysis it.Honeypot is widely used in the industrial attacks.

- **Prevention**

Prevention from the attackers is done by Honeypot, it lure the attacker to attack the system but unknowingly attacker attack on the deception system that is honeypot and attacker access false information from the system .

- **Response**

One of the best advantage of the honey pot is that it is an independent system, when it is attacked it is

easily separated from the given system and the expert's analysis the attacker after the attack happen. Concept of the honeypot is highly used in the network forensic.

- **Research**

Honeypot is used in the research of the new spam and malware families. With the help of honeypot number of spams and malware detected, after the detection tools are developed to prevent the malware and make the cyber world more secure. Honeypot also prevent distributed denial of service attack.

IV. HONEYPOT ADVANTAGES

- **Small logged data generated**

Any of the interaction with the honeypot is considered as malicious ,data collected and analysis , logged data generated is in a small amount.so it is very easy to maintain that data .

- **Reduced False Positives**

Honeypots help in reducing false positives. The larger the probability that a security resource produce false positives Or false alerts the less likely the technology will be deployed. Any activity with the honeypot is considered dangerous and making it efficient in detecting attacks.

- **Catching false negatives**

Catching false negatives with the help of honeypots is quiet easy because every connection made to honeypot is considered unauthorized. Traditional attack detecting tools become fail in detecting new attacks like signature based detection tools. These tools detect only those attacks whose signatures are already in their database. As per honeypot's approach, there is no need of predefined database.

- **Captured Encrypted malicious activity**

Honeypots have the capability to capture the malicious activity if it is in encrypted form. Encrypted probes and attacks interact with the honeypots as end point where the activity is decrypted by the honeypot.

- **Need minimum resources**

Honeypot requires a computer system, it does not require any database to capture malicious activity

- **Flexible**

It is highly flexible and adoptable in any kind of environment.

- **Working with IPV6**

Traditional security system not able to work with IPV6 but honeypot works with the IPV6 and IPV4-

V. LIMITATION OF HONEYPOT

- **Interaction needed**

Attacker need to interaction with the Honeypot then only honeypot is able to detect and prevent malicious activities .If the attacker does not interact with the attacker honeypot is worth less. Malware and attackers are more and more sophisticated they do not interact with the attackers.

- **Counter deception**

There is so many malware and spam are there, when they detect the honeypot they change their behaviour and deceive the honeypot and attack the productive system.

- **Risk**

If Honeypot is compromised by the attack, then the security of whole organization is on stake.

VI. CONCLUSION AND FUTURE SCOPE

The trend of using honeypot is very traditional in network security. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site, where real resources of information are available.

Even these honeypots could be extended to honey nets, where attacker deals with the bunch of honeypots. The log files analysed through these honeypots and honey nets could be used to enhance the Intrusion detection system to make it smarter in catching Intrusions.

VII. REFERENCES

[1]. Verizon,"Threats on the Horizon-The Rise of the Advanced Persistent Threat." http://www.verizonenterprise.com/DBIR/.

[2]. J. J. Yuill, Defensive Computer-Security Deception Operations: Processes, Principles and Techniques. PhD Dissertation, North Carolina State University, 2006.

[3]. B. Cheswick,"An Evening with Berferd in Which a Cracker is Lured, Endured, and Studied,"in Proceedings of Winter USENIX Conference, (San Francisco), 1992.

[4]. C. P. Stoll, The Cuckoo's Egg: Tracing a Spy through the Maze of Computer Espionage. Doubleday, 1989.

[5]. E. H. Spafford,"More than Passive Defense." http://goo.gl/5lwZup, 2011.

[6]. L. Spitzner, Honeypots: Tracking Hackers. Addison-Wesley Reading, 2003