ASEE 2014 Zone I Conference, April 3-5, 2014, University of Bridgeport, Bridgpeort, CT, USA.

Honeypots and Mobile Technology: Discovering the Attacker

Breno Fabrício Lira Melo Sousa
Coordination of Computer Science
Centro de Ensino Unificado de Teresina - CEUT
Teresina, Brazil
breno_fabricio23@hotmail.com

Raimundo Pereira da Cunha Neto
Coordination of Computer Science
Centro de Ensino Unificado de Teresina - CEUT
Teresina, Brazil
netocunhathe@gmail.com

Francisca de Fátima de Lima Sousa
Coordination of Computer Science
Centro de Ensino Unificado de Teresina - CEUT
Teresina, Brazil

***Abstract*— This paper is mainly focused on presenting one of the techniques of defense against invasions communications networks, which can affect both small, medium and large enterprises as for ordinary users. Exposing their characteristics, strengths and weaknesses, and honeypots for mobile devices.**

Keywords— honeypots; honeynet; android; device mobile.

I. INTRODUCTION

The computing over the years gained a tremendous growth ever since the first computers emerged, that had military purposes. The information became accessible to everyone, anytime, anywhere.

Over the years, computers increasingly, have been gaining improvements, the processing power and storage, and even size. Reached a point of changing the way of life of the world population, providing greater convenience and troubleshooting problems that hitherto could be almost impossible to be solved without the use of them.

Every day we are faced with the increasingly smaller and more powerful machines. Commonly, we can see that the growing number of people who own devices with a lot of processing power and storage in the palm of the hand, from the mobile technology grows every day.

Users are increasingly exchanging information over the internet, which goes from simple transactions such as exchanging email, for example, to confidential transactions that deserve more attention and greater data protection, such as transactions banking, for example.

For this, we use the concept of Intrusion Detection System (IDS), Firewall and honeypot so we can have a greater knowledge of which technique to use in a possible attack.

With the use of a honeypot, as a defense, we came across some questions that we can not leave out, as follows:

- The honeypot is an effective technique for identifying intruders?
- How to identify an intruder using honeypot?
- What types of services are major targets of the invaders?

We will talk in section two of this paper its definition, describing its history, characteristics, ratings, their strengths and weaknesses, ending the section with honeynets and honeytokens. In section three, we will have a brief introduction to the android operating system. Following, we discuss in section four of this article threats to mobile devices. Continuing, in section five, we discuss honeypots aimed at mobile devices. And finally, we have our conclusion and references.

II. HONEYPOTS

Honeypots are tools used for monitoring attacks, collecting important information on trends and allowing enhance the methodology used the security of a company [1].

We also have to point out that, unlike a firewall or IDS (Intrusion Detection System), a honeypot will not solve just one problem or another specific security flaw but rather interpret the network as a whole, thus helping to other defense mechanisms to identify where and what a particular system has flaws.

Initially, the concept was presented by Cliff Stoll, with the publication of his book in 1990, "The Cuckoo's Egg: Tracking the Spy Through the Maze of Computer Espionage"[2].

In later year, Bill Cheswick published his paper "An EveningWithBerferd, In which the Hacker is Lured, Endured, and Studied" [2]. Cheswick in this text relates how was able to fool hacker with a bait, and while studying it.

A. History

For a better understanding of how this powerful technique has developed over the years, we have to keep in mind some facts that contributed to its development.

In 1997, the scholar Fred Cohen, launched the first honeypot, which had the characteristics: open source and free.Já of the following year, the CyberCop company produced the first product, Sting, which was later acquired by NAI, in the end year the same year. In 1998, Martin Rash created a honeypot for the U.S. government. In 1999, Lance Spitzner created the Honeynet Project, along with a team of about fifty security experts [1].

B. Characteristics

Regarding its features, we may have the honeypots: production honeypots and research [1].

The "production honeypots are used to distract malicious activity of machines with highest value on the network or as an alert mechanism" [1]. Yet we must bear in mind that the production honeypots may give aid for security mechanisms, such as IDS and Firewall [4].

These honeypots are easier to be implemented, since they have fewer functions, bringing a lower rate of risk to the system. However, obtaining information that the production honeypot will manage to collect will be lower compared to the honeypot research.

Differentiating the production honeypots, honeypots research "are used for monitoring of an attack with the objective of capturing the largest possible number of data for further analysis" [1].

To so, in order to develop research honeypots, is getting directly on the attackers as they will not only focuses on a single organization [4].

However, their main goal is to get the information highest capacity possible of an attack, not failing to capture "who are the attackers, how they are organized, where the attacks occur, what tools are used and how these tools are obtained" [4].

C. Classification

Honeypots can be a great benefit to companies, since their main focus is to deceive the attacker, giving you a system or any other service previously set to be invaded, which can be studied the techniques and mechanisms that the attacker used during invasion.

It is noteworthy that during the process of to set up a honeypot, we have to setting that the attacker does not realize that it is being monitored, if is flaw, an attacker will flee from our honeypot, making it unnecessary.

This study we are only allowed through logs that are constantly generated in a honeypot, where each log contains at least the information referred to "date and time of attack, source IP (attacker) and destination IP (wholesale) and type of attack "[3].

If the logs was generated, these are stored, so that administrator(s) of the network can analyze them in future and may or may not modify its settings for added protection time because if there is an actual failure, the honeypot can serve bridge so that the attacker can infiltrate the actual system.

Honeypots found in two classification levels: low-interaction honeypots and high-interaction honeypots, where the low-interaction will provide fake services, and interaction occurs with the attacker, giving you false information [3].

Differing from low-interaction, high-interaction honeypots, will provide a real environment for the attacker, where it can interact with both the operating system itself, or applications or services of the company. In this scenario, we will have to take greater caution, because if a security breach occurs, the system may be compromised [3].

These rating levels, the author [3] points out that some authors also consider an intermediate classification of honeypots, lying between the low and high interactivity.

D. Strengths and Weaknesses

The author [3] states that some authors highlight some of the advantages of using honeypots, such as small data sets, new tools and tactics, information capture and ease of use.

For small data sets (although of great value), any information obtained on our honeypot will bring us useful because any information generated by it, is that an intruder tried to perform an unauthorized action.

In new tools and tactics, network administrators, can stay abreast of new forms of invasion, since the honeypot will generate logs that will be studied later.

Regarding ease of use using the low-interaction honeypots, due to its characteristics, we will not need more complexity in its implementation.

As a disadvantage, since our environment of honeypot is compromised, if it has not been configured correctly, the attacker can use it as a gateway to compromising the actual system of the company.

E. Honeynets and Honeytokens

The idea of honeynet was initially proposed by Lance Spitzer (founder of the Honeynet Project) in 1999, with the publication of his work "To Build a Honeypot", whose "purpose was to learn from the tools used, tactics and motivation of the attackers "[2].

A Honeynet is a cluster of honeypots, thus becoming a virtual computer network with the goal of being compromised [1]. Such involvement of the network will serve as study mechanism to observe the behavior of the invaders, enabling thus further analysis of the tools used, the goal of the attacker and which vulnerabilities were indeed exploited.

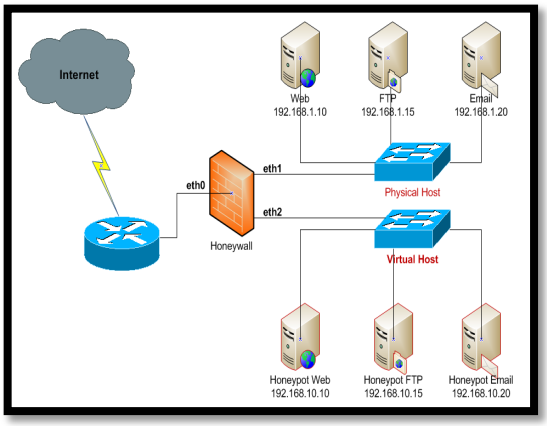
As in honeypots, all traffic to a honeynet network is captured and stored in files, in order subsequently to be

studied, as well as a honeypot, if there is a real security flaw a honeynet can be used as door entry to a real system.

With the use of a honeynet, we can enhance the ability of detection, reaction and analysis of the system because "the techniques used are subjected to constant analysis after each attack carried out in order to be perfected" [1].

The honeytokens, in general, are data and/or information provided attractive way to draw the attention of an attacker, may be a simple failure in the security of a given system of the company, or even 'information' available purposely by administrator network. For we can have a greater vision of how to constitute a honeynet, follows a basic example of how it arises:

Fig. 1 - Example of architecture of a honeynet



Source: (http://uitnetwork.com)

Such honeytokens will help the work of the attacker, as he will think you are invading the real system itself, however is not the case, because the information that it is accessing are false [1].

For our honeytoken is functional, our honeynet must be configured so that "any attempt to use the resources provided to Honeytokens should be monitored and recorded for later analysis" [1].

Honeytoken has the advantage of not being dependent on a single technology because "any repository of information with recursos of traceability can house honeytokens" [1].

III. ANDROID OPERATING SYSTEM

Android operating system is complete architecture for mobile devices because it was developed primarily for smartphones, what their platform is made up of the following components: operating system, middleware, applications and user interface [3].

In 2008, the android operating system was launched on the market of mobile phones developed by Google. Then, it created links with various companies in the field of mobile phone, thus giving continuity to your project. This link has been labeled Open Handset Alliance (OHA), currently with 84 companies [3].

The basic reasoning of Android, as mentioned [3], is based and grounded in the Linux operating system kernel. However, some changes had to be made, since its emergence, so that present your features of a mobile phone, such as [3]:

- Binder - which is used by the communicating processes. Ensure that no process has access to the memory space of other processes;
- Ashmem - characterized as a new way to have get shared memory between two processes, enabling it to communicate through this shared memory region;
- Wakelocks - occurs the detection if the device is being used or not, if not, convert it to energy-saving mode;
- Oomhandling - will be responsible for control the use of system memory, and termination of cases, if not acting memory available for its execute.

IV. THREAT TO MOBILE DEVICES

We keep in mind that threat to mobile devices is something new, that emerged with the advent of smartphones, but in reality this is not the truth.

The dangers faced by users of mobile devices is not something new. The first virus designed for digital mobile phones appeared in the year 2004, "Cabir", which was spread via Bluetooth, and had the exclusive focus attack the Symbian operating system [3,6].

Because a non-universal standardization of such threats, Dunham, K., et al (2009), cited by [3], make use of own termologias to define mobile security, as follows:

- Ad/Spyware - unwanted programs that can perform many actions without the user's authorization;
- Bluebug - its function is to exploit vulnerabilities in Bluetooth, "to make phone calls with differentiated value (highest)";
- BlueChop-constitutes the denial of a Piconet network service;
- Denial-of-Service (DoS) - characterized an attack aiming to disrupt and/or deny the use of a mobile device, network or service;
- Exploit - can be characterized as either a software or actions that seek to use apertures of a system to perform unauthorized actions;
- Hacking default - its function is to invade devices or software that has password or default configuration, such as security;
- MalwareMóvel - "is software that performs malicious actions on mobile devices."
- Snarf - "is the unauthorized data theft".

As we can see, were exposed some of the threats most varied with which we commonly find ourselves today. According to [3], based on Enck, Ongtang and McDaniel (2009), the reported threats, had their basis in personal

computers, which had to undergo some changes that they should put be used in handsets.

V. HONEYPOT FOCUSED ON MOBILE DEVICES

Regarding honeypots for mobile phones, there are still few works related "due to the limited hardware resources of mobile devices and their software vulnerabilities" [5].

Collinet *et al*. (2011), cited by [3] created a honeypot for mobile devices called HoneyDroid. These authors, rather than working with the software itself, chose to work directly with the hardware, because then they could have a greater visibility of honeypot.

Using the HoneyDroid were virtualized flash memory, modem and WiFi , so they could control the interactions between the android operating system and the hardware device. Thus, obtained an "efficient monitoring, generating log files and store these in a non-accessible location Android operating system" [3].

As the HoneyDroid used virtualization to utilize the services of the Android operating system, CPU overhead problems of the mobile device were found. Should consider that this overhead can be perceived by the attacker, ie, authors such as [3] concluded that its creation would be feasible for mobile devices, but both would have to use virtualization to achieve a complete system.

The authors Ahmed *et al.* (2013), also reported that the HoneyDroid has the disadvantage of not behave like legitimate Android operating system. This disadvantage can be understood as malware, which may cause the termination of the attack, causing the attacker to escape the honeypot.

O'connor and Sangster (2010), cited by [3], developed a framework for virtual HoneyClient (a type of honeypot) to mobile devices, with the goal of finding the weak points or "malicious code that affects a machine or application client, such as a web (browser) "[3].

According to [5], several problems are faced when building a honeypot for mobile devices, such as system configuration, part tracking, containment and visibility.

The system configuration depends on how you actually develop a honeypot system for mobile phones, and will depend on which operating system mobile phone we will develop the honeypot.

Monitoring is the key part, because our honeypot only be useful to us if we can get full view of what occurs in the network, and we wonder what the attacker is doing.

Containment allows us to have control of the honeypot will not be used as a mechanism for the attacker to actual attacks, thus jeopardizing our system, and ultimately the visibility is very important because our honeypot will have to be visible to our invaders . We'll have to have compelling information, eg, "the publication of phone number, email address, account name and instant messages in as many ways as possible" [5].

VI. CONCLUSION

However, we realize that honeypots can be useful in protecting against external threats of a business or mobile phones. Their limitation of data capture will depend on your configuration.

As we can see, mobile phones became targeted by invaders from 2004, with the advent of so-called smartphones. Over the years, were gaining more and more processing power, features that did not have before.

Have become increasingly essential in everyday the world population requiring increasingly protective of users' information, because due to the great features that such devices are able to have, if one is stealing your information, it may suffer various problems, once on your handset, you may have sensitive data and saved passwords.

REFERENCES

[1] C. M. O. Junior; F. S. Deco; S. da S. Antonio. Honeypots: enganando e conhecendo o inimigo. 2004. 61 f. Monografia (Graduação) - Curso de Bacharelado em Informática, Universidade do Grande Rio, Duque de Caxias, 2004. Available in: <http://www.apostilando.com/download.php?cod=3164>. Acessed in: 16 nov. 2013.

[2] S. Simões; F. Silva. Estudo de Ferramentas para HoneypotsInstaláveis em Máquinas Virtuais Perfazendo uma Honeynet Virtual. Available in: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Sidney%20Simoes%20e%20Silva%20Filho%20-%20Artigo.pdf >. Acessed in: 16 nov. 2013.

[3] V. B. Oliveira. HoneypotLabsac: um framework de honeypot virtual para o android. 2012. 86 f. Dissertação (Mestrado) - Curso de Engenharia de Eletricidade, Universidade Federal do Maranhão, São Luís, 2012. Available in: <http://www.bcc.unifal-mg.edu.br/bibliotecabcc/files/Discentes/Monografias/Monografia_Lucas Tardioli.pdf >. Acessed in: 16 nov. 2013.

[4] L. T. Silveira. Detecçãode Intrusão Atravésde Configuraçãode Honeypot de Baixa Interatividade. 2011. 105 f. TCC (Graduação) - Curso de Bacharelado em Ciência da Computação, Universidade Federal de Alfenas, Alfenas, 2011. Available in: <http://www.bcc.unifal-mg.edu.br/bibliotecabcc/files/Discentes/Monografias/Monografia_Lucas Tardioli.pdf>. Acessed in: 16 nov. 2013.

[5] H. M. Ahmed; N. F. Hassan; A. A. Fahad. A Suvery on Smartphone Honeypot. ISSN 2277-3061.2013.

[6] C. C. Ho; C. Y. Ting. A Conceptual Framework for Smart Mobile Honeypots. Available in: <http://www.academia.edu/download/31058450/KasperskyConferencecchocyting.pdf> Acessed in: 14 mar. 2014.