ENHANCING IDS – Honeypot Systems

A. Bielko[1], D. Rainys[1,2], A. Čenys[2]

[1]UAB "BlueBridge", Jasinskio str. 16, Vilnius, Lithuania

{andrej.bielko, darius.rainys}@bluebridge.lt

[2]Information Systems Laboratory, Semiconductor Physics Institute

A.Gostauto11, LT-2600, Vilnius, Lithuania, cenys@uj.pfi.lt

Abstract: In this paper we present statistical results recorded by the honeypot system deployed at Vilnius Academy of Sciences library's computer network. The system was functioning for two months in the network's DMZ (demilitarized zone) to be able to detect both local area users and intruders from outside. More than 30 attempts to compromise the system were recorded daily. Most of attempts were scans and probes by automated script-kiddies from the geographically close countries. However, more serious and remote attacks were recorded as well. In the paper we also discuss advantages and risks related with honeypot technology. Biggest advantage of honeypot systems as compared with usual intrusion detection systems (IDS) is absence of false positives making interpretation of obtained data comparatively easy - any activity from or to honeypot is suspicious one or an attempt to compromise the system.

Keywords: honeypot, intrusion detection systems

1 Introduction

Illegal intrusions to computer systems are becoming a common feature of our everyday life. Two main types of intrusion can be mentioned:

- Illegal access to forbidden information. In this case hacker gains access to forbidden information: he could read it, delete it, edit it or do something only he thinks about.
- Illegal access to services (starting, restarting or denial of services).

One or another way intruder prevents normal job of organization's server. Most organizations use firewall as a main defense tool against illegal intruders. However, even advanced and well configured firewalls can not deter all attacks. The second line of defense is intrusion detection system (IDS). Most of attacks to computer networks are based on known vulnerabilities and methods. As a result malicious software can be detected from known "signatures" and illegal intrusion can detected recording untypical or suspicious activities in the system. In our days, however, hackers improve their tools, methods and skills very fast. Nowadays hackers can compromise the system without owner even noticing that, since all log files or even operating system itself can be modified. As a result intrusion detection systems should adapt very fast as

well, including development of new methods of intrusion detection. One of very promising methods receiving very wide attention recently is deployment of the traps to intruders or so called honeypots (Cheswick 1991, Stoll 1990). The honeypot is a service or a system in the network without any real use. According to L. Spitzner *honeypot is a resource whose value is in being attacked or compromised. This means that whatever we designate as a honeypot, it is our expectation and goal to have the system probed, attacked, and potentially exploited* (Schroder, 2002). The main goal of honeypot systems is to gather information about intruder's methods, tools, and habits remaining invisible.

In this paper we present the brief overview on the honeypot systems and statistical data gathered using this technology in Lithuania.

2 Honeypot systems

2.1 Production and research honeypots

As it was stated above a honeypot is a resource pretending to be a real system, with real services but with weakened defense system to attract attention of attackers. The main goal of honeypot systems is to gather information and/or to protect company's productive servers. According to these goals two types of honeypot systems can be distinguised: *production* honeypots and *research* honeypots. The purpose of production honeypot systems is to minimize the danger of an intrusion into organization's servers. The research honeypot systems are used for the information gathering. Research honeypot alone is not a security solution protecting your network. However, this is a very useful tool while deployed with other intrusion detection systems.

2.2 Value of honeypot systems

Honeypot systems like any security systems have some advantages and disadvantages. The biggest advantages of the honeypot are related with the simplicity of idea. They can be summarized as follows:

- Any activity towards the honeypot is an attempt to scan, probe or even compromise the system. Of course people can make a mistake, they can write wrong IP address or wrong DNS name but such cases are very rare. Any outbound activity from the honeypot can appear is only if the honeypot system is compromised since it doesn't have any productive activities. Therefore most of the data collected by a honeypot is relevant. The system collects very little data of high value unlike usual IDS (Raikow 2000). This feature is most evident for isolated honeypots since these are systems unknown to the outbound world. Only an attempt to sniff or compromise the system can find such honeypot. Any activity to or from isolated honeypots is unauthorized. Low number of false positives is a biggest advantage of the honeypots as compared with IDS. Honeypot systems also generate false positives, but the number of false positives is very low.
- Honeypot system can be used to test and to evaluate an intruder. The biggest part of an activity from Internet is scanning and probing. Recorded data allows to de-

tect what kind of vulnerabilities are most often attacked, what type of tools are used and so on. This kind of information can help to eliminate or hide known system's vulnerabilities.

- Honeypot is an excellent tool for teaching administrator almost everything about system's security. It can be used to teach how to react when an incident appears, to learn about vulnerabilities and patching of the known holes in services and systems. Moreover honeypot could teach the techniques of attackers.
- Just a deployment of the honeypot can prevent an intrusion. If the attacker knows that somebody is watching and recording all his activities he can stop attacking the system at all.
- Many of existing security tools can be overtaken by the advanced intruders. Intrusions detection can be unable to watch all activity in the net letting some packets ant attacks to pass throw. The main log server can be halted or logs file can be erased leaving no trace of intrusion. The honeypot system does not have such vulnerabilities.

Along with advantage honeypot has some disadvantages:

- Honeypot systems are useless if nobody attacks them. It is worthless if nobody is interesting in it.
- Deployment of the honeypot carries additional risk because honeypot system is the system with some vulnerable services. Level of the additional risk depends on the interaction level and on the place in the network where the honeypot system deployed.

Summarizing it can be concluded that honeypot system should be installed along other security system, IDS for example.

2.3 Level of interaction

Level of interaction is a term to define capabilities of different honeypots (Spitzner, 2003). It is a measure of how much functionality a honeypot provides to an attacker. When an attacker interacts with a honeypot, there are different levels of functionality that the honeypot can provide. Some honeypots may provide only a limited set of emulated services, while others not only provide full applications, but an actual operating system for the attacker to gain access to. There are defined several types of level of interaction for honeypots: *low-interaction, mid-interaction* and *high-interaction.* They all differ according to level of interaction between intruder and system with services. Of course the more honeypot could perform and intruder is allowed to do with the system the more information we will get and that information will be more interesting. On the other hand the more attackers can do with the system the more damage they could perform on our systems. Higher interaction is related with higher risk.

Low-interaction level honeypot is the system providing some limited fake services. For example, listening for a port and log all received packets. Attackers could potentially scan and connect to real ports. In this case information is very limited since we log only port activity and intruder has no possibility to do anything extraordinary.

Value of low interaction honeypot depends on the interest to the services it is emulating. *BackOffice Friendly*, *Specter*, *Deception Toolkit* are examples of the available commercial low-interaction honeypots (Reference Nr. 8).

Mid-interaction and high-interaction level honeypot systems are real systems. The only difference between mid-interaction and high-interaction honeypots is an amount of services provided by the system. Mantrap is an example of the high-interaction honeypot. It could produce about four honeypot systems like jails. Another example of high-interaction honeypot is honeynet project (Reference Nr. 8). It is a research project based on real systems and real servers with the main goal to provide tool for research and to learn tactics and tools of black-hat community.

It is impossible to say definitely which type of honeypot is the best since this depends on the particular organization's goals, needs, capabilities, and resources. Honeypot system is not a solutions it is a tool.

2.4 Honeypot location

Honeypot could be placed everywhere in the local network, however, some places are more convenient than others. There are three main places: before firewall, in demilitarized zone (DMZ), and behind firewall. If honeypot is deployed before the firewall it will provide a lot of data of no interest and will not detect local attackers. On the other such honeypot position caries minimal risk for local area network. Honeypot inside the local area network can provide very interesting information about local activity but is very risky. A good comprise is honeypot in DMZ with additional firewall settings. Of course additional security is needed because in DMZ production services are available. It is important to watch the honeypot carefully and to run it safely.

3 Honeypot system implementation

Below we will discuss a real working honeypot system. As a honeypot system or bait we choose the computer with following characteristics:

- Processor: Pentium 166MMX
- RAM: 32 Mgb
- Hard Drive: 3.2 Gb
- Extra tools: LAN card (10/100 Mb/sec), CD-ROM, Floppy Disk

We used another computer to watch the bait and to sniff any activity of the honeypot. As bait we choose Slackware 8.0 system for the following reasons:

- The system has lots of known vulnerabilities. Some of them were hidden because we did not want to make the attacker job to easy.
- Easy implementation.
- Free of charge.
- Is is easy to deploy a simple services making the system to look like a real server.

The system was running following services:

- Ftp Server – ProFTPD 1.2.2rc3
- Server, SSH server,
- Web server – Apache/1.3.20,
- Mail server – Sendmail 8.11.4/8.11.4 ,
- MySQL server.

As a result we had some open ports for intruders to make their attacks. Hoenypot system was deployed at the Vilnius Academy library of Science and was implemented in such away that it looked like a real server (Figure 1). The computer was registered with the address dbserver.mab.lt. This hostname was chosen specially to be more attractive for automatic scan machines.

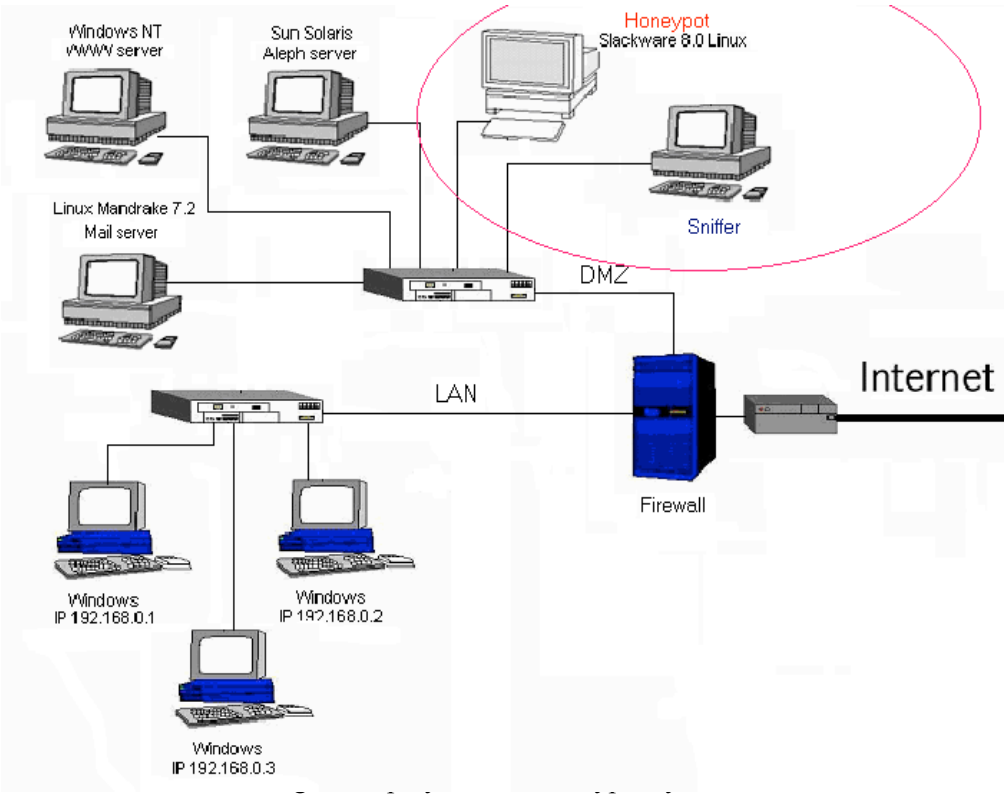
As a packet sniffer we used a computer with Windows XP platform and installed Ethereal 0.9.12 program (Reference Nr. 9) which overtake all inbound and outbound network traffic. The main reasons:

- Possibility to work under Windows XP
- Easy management
- Free of charge
- Has lots of useful tools
- There is a possibility to write specialized filters, if somebody wants to filter out obtained information.

One more update was needed before starting to run the system. Ethereal lacked the packet capture library. For this purpose WinPcap (winpcap.dll) was installed.

4 Results

Recording of the data from the honeypot system started on April 14th, 2003 and was carried on approximately two months. On the average we detected 35 attempts to scan, to probe or even to compromise the system per day. Most of attacks were attempts implement the "*Code Red*" virus and to get the system information using web server. Below we present obtained statistical data. As can be seen from Fig. 2 honeypot system was probed and attacked with more or less stable frequency during the day. Only small peaks can be seen, one at 8-9 p.m. and another at 4-5 a.m. The last peaks can be explained by the fact practically all probes and scans during night period were from foreign countries. The peak at 8-9 p.m. seems to be related with the convenient time for local attackers.



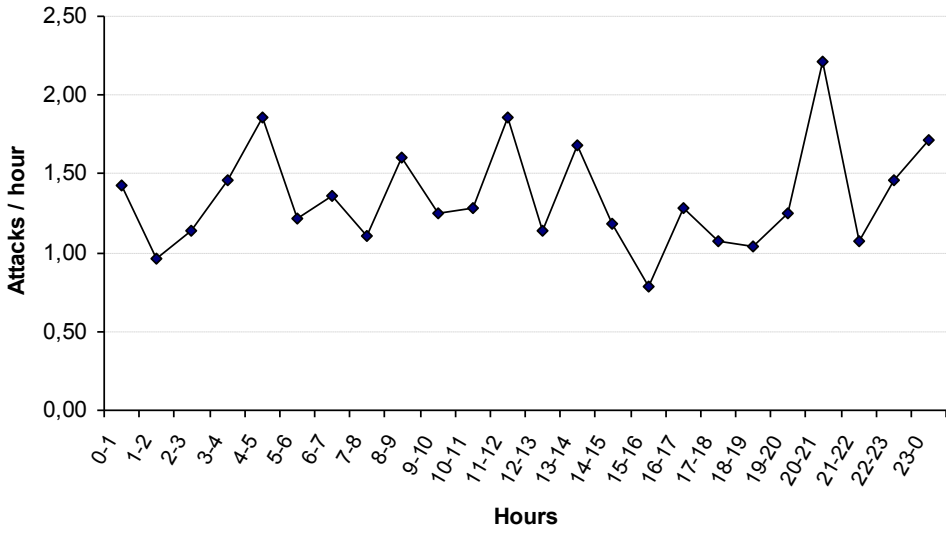


Fig. 2: Average daily statistics

Distribution of scans and probes during a week is shown in Figure 3. Again the distribution is more or less flat with small peak in the middle of the week. This result seems a little bit strange, but it can be related with the fact that most of attacks are coming from the computers at working place.

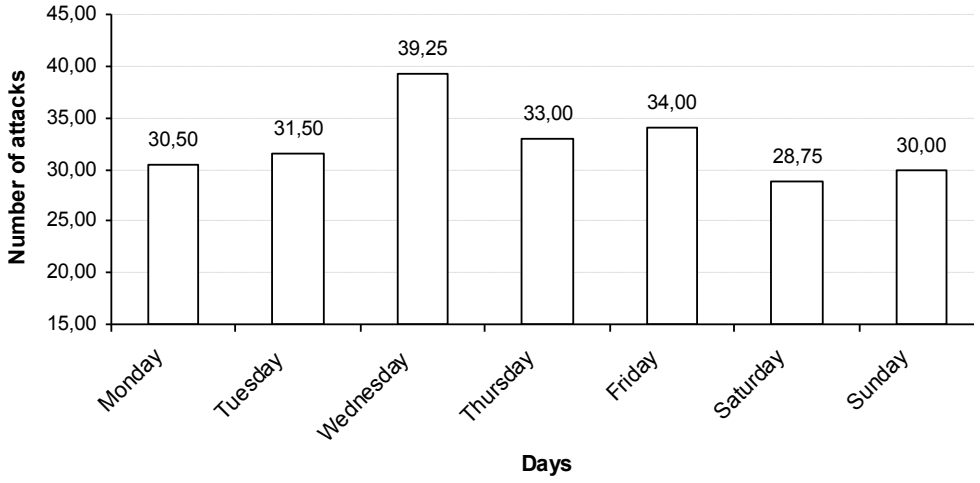


Fig.3: Weekly statistic

Distribution of the protocols used for the attacks are shown in the Figure 4. In this case attackers preference of HTTP and FTP protocols is very well pronounced. Other protocols are used not so often.

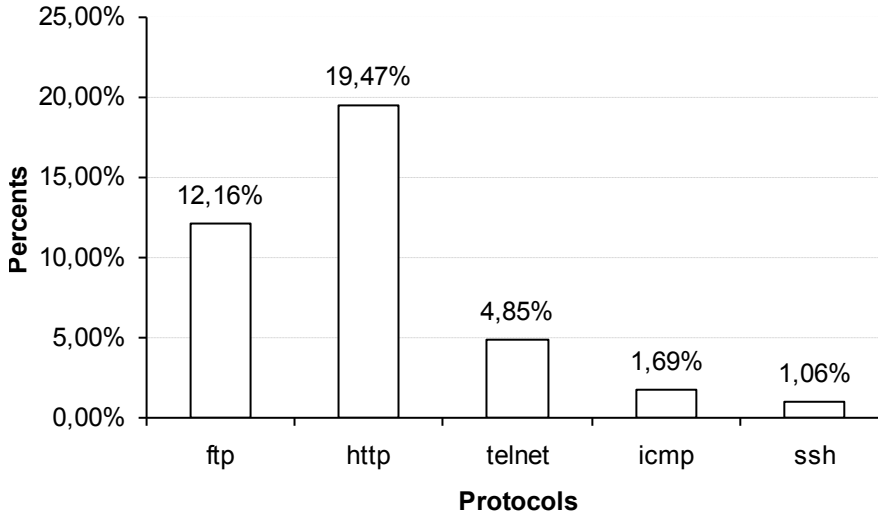


Fig. 4: Average distribution of the protocols

Using the recorded log files during a week we were able to define origin of the scans and attacks. The results are presented in Figure 5.

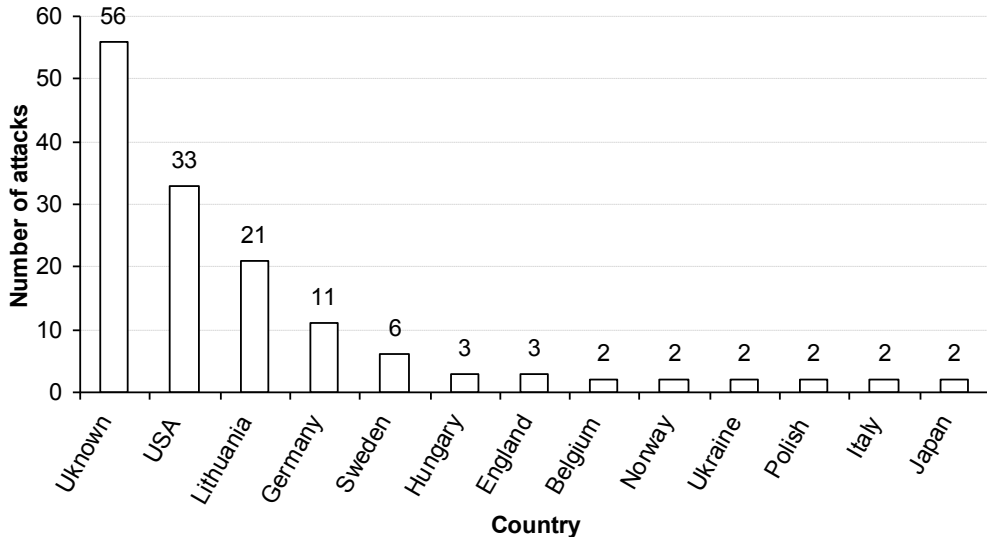


Fig. 5: Number of weekly attacks by countries

In the most cases, however, it was impossible to determine the country of attack. The most often attacks with defined country were coming from USA and naturally Lithuania. The USA result is quite surprising. Some of these attacking computers, however, can be only pretending to be in USA. Most attacks from Lithuania were simple scans, probes or script kiddies were trying to hack the system with standard hack tools from the internet. We assume this results from the fact that sophisticated attackers were able to successfully hide country of origin. It was far lees activities from other countries. In total we detected about thirty countries, which IP addresses were recognized using DNS.

We have noticed from our analysis, that very often we were attacked from geographically nearest countries: Lithuania, Poland, Russia, Latvia and etc. This fact demonstrates that intruders are trying to scan their own subnet or local arena network more frequently than wide area networks. Also most of the tools intruders are using are designed for local area networks. We can conclude that it is vitally important to protect not only from outside world, but from inside local area network as well. Honeypot technology fits for this purpose very well.

While most of the attacks were simple scans or probes, we have also detected quite significant number of attempts to compromise the system. None of these attempts was successful meaning that no attacker was able to compromise and to get control of the honeypot system. Taking into account vulnerabilities of our system we can conclude that computer system of the library are not attracting attention of the most skilled hackers. The system is of interest only for amateurs, students and attackers trying to

use the compromised system as a proxy for further attacks. For the last there is no reason to try hard since they can find easier target somewhere else.

5 Conclusion

Using the honeypot system we were monitoring security situation in the computer network in Lithuania. During two months significant number of scans, probes and attempts to compromise the system was detected. Most of the attempts were simple scans, so called "script kiddies", trying to hack the system using automated tools. Rate of attacks was more or less flat during a day as well as during a week. One of the most popular attempts was to implement "*code red*" virus and other worms. We will continue the project and will try to implement honeypot in other organizations which are of interest for more sophisticated attackers.

6 References

1. Cheswick B. *"An evening with Berferd in which a Cracker is Lured, Endured, and Studied*", http://www.tracking-hackers.com/papers/berferd.pdf , 1991.
2. Raikow D., "*Building your own honeypot",*
3. http://www.zdnet.com.au/newstech/security/story/0,2000048600,20106785,00.htm, 2000.
4. Schneier B., Wiley J., "*Secrets And Lies: Digital Security in a Networked World"*, 2000.
5. Schroder C., "*Bait Crackers With A Honeypot",* http://networking.earthweb.com/netsecur/article.php/1365031, 2002.
6. Spitzner L., "*Honeypots: Definitions and Value of Honeypots"*,
7. http://www.tracking-hackers.com/papers/honeypots.html, 2003.
8. Stoll C."*Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage",* Pocket Books, New York, 1990.
9. http://www.cerias.purdue.edu/homes/kaw/projects/honeynet/HoneynetTutorial/
10. honeypots/procon.html.
11. http://project.honeynet.org/book/
12. http://www.ethereal.com/docs/user-guide.pdf