Extended system of honeypots to detect threats

Roman Jasek, Martin Kolarik, and Tomas Vymola

***Abstract*—**Recently emerged threat type of Advanced Persistent Threats (APTs). APTs continuously gather information and data on specific targets, using various attack techniques examine the vulnerabilities of the target and then perform the data obtained by hacking. APTs are very precise and intelligent. Perform specific attacks on specific targets, and so differs from traditional forms of hacking. APT is precisely focused on specific targets, according to the knowledge of the environment and selects appropriate types of attacks. Therefore, it is very difficult to detect APT attacks. This article describes the methods and procedures APT attacks, analyzed and proposes solutions to detect these threats using honeypots system. In the second part of the paper discussed two possible solutions using classical detection system, honeypots and its modifications. The final section is conducted an experiment that compares the efficacy of these two variants.

***Keywords*—**Advanced Persistent Threat, Attack, Computer Security, Honeypot, Intrusion Detection System

I. INTRODUCTION

INSTITUTIONS and businesses always face new threats. One of the biggest problems lately is type of APT threats, which are sophisticated, multiple attacks at a specific organization. Threats type of APT (Advanced Persistent Threat) belongs to the category of cyber-attacks, their goals most often as commercial entities, political and state institution and the individuals. These types of threats require long-term high secrecy. They carried a group of attackers who are well privy to the problem. They use more types of vulnerabilities to break the key security systems. In the initial stage of the APT focus on getting information about the network configuration and server operating systems. Later, focus on installing rootkits and other malware to gain control and communication with C&C (Command & Control Server) attackers. The contested objects are long compromised to steal intellectual property, copying of confidential and sensitive data, or financial gain. Individual systems are often long infected, and the achievement of the objectives striker ever taken out of service.

R. Jašek is with Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic (e-mail: jasek@fai.utb.cz)

M. Kolařík is with the Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic (e-mail: martin.kolarik@email.cz).

T. Vymola is with the Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic (e-mail: vymola@gmail.com).

II. APT

Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below:

Advanced - Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.

Persistent – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.

Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well-funded. [3],[1]

A. Lifecycle APT

APT has been firmly defined methodology that has been proven in recent years. It begins phishing and social engineering ends and export large volumes of stolen data to the attacker's server. Attackers use techniques and methods are constantly evolving and have a great ability to adapt effectively. They keep their tools a step ahead than the current status of infected systems.

Attackers can have multiple campaigns running in parallel. Every consists of one or more operations. These operations are usually distributed into phases. For example, in the initial phase, the aim is to provide a striker initial entry point to the target system. The following phases are then usually parallelized and distributed among individual cells due to more

efficient attacks. The subsequent section describes the basic operation phases within a single APT intrusion. The following section describes the details of these phases and their possible detection. [4], [2]

Initial compromise - This is done using conventional practices of social engineering, spear phishing emails, and with zero-day virus. Next option is to infections websites, and forced the victim to visit them. Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it.[8]

Establish Foothold – install remote administration software in victim's network, create network backdoors and tunnels allowing stealth access to its infrastructure. Connection communication with the Command & Control server the attacker and as he controls remotely contested keeps updating machines and used malware.

Escalate Privileges – use exploits and password cracking to acquire administrator privileges over victim's computer and possibly expand it to Windows domain administrator accounts.

Internal Reconnaissance — collects information on surrounding infrastructure, trust relationships, Windows domain structure.

Move Laterally — expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.

Maintain Presence — ensure continued control over access channels and credentials acquired in previous steps.

Complete Mission — exfiltration stolen data from victim's network

Furthermore, in this article we will focus in detail on the stage Move laterally. Previous phase is detectable by standard quality tools. But if the attacker gets up to the current stage, it means that standard security techniques have failed. This phase is a standard security technique almost undetectable. The attacker behaves as a normal user and using common tools. One of the methods to detect the attacker is using the honeypots.

III. Basic Types of Security Solutions

In this chapter will be devoted to some of the security concept for solving APT attacks. We present a basic division and subsequently introduced as a type of honeypot technology IDS.

The following discussion deals with the threat detection capabilities in a virtual environment. This includes a basic overview of the classification of intrusion detection systems, and discusses some of the basic concepts.

A. Host and network-based systems

Detection systems and intrusion prevention systems are divided into intrusion detection IDS (intrusion detection system) and intrusion prevention systems IPS (intrusion prevention system). It is also possible detection systems and intrusion prevention divided into host-based (host based IDS - HIDS) and network-based (NIDS). For both categories is common continuous monitoring system, the ability to alert the administrator to the attack revealed a record during the attack. HIDS systems are deployed on individual servers and user workstations. It is a software product, which suggests that the possibility of their use is limited support for operating systems used on the monitored computers. These products monitor system calls, logs, error messages, and the like. They protect against attacks on the operating system and applications running on the computer. They can evaluate the success of any attack. A comprehensive NIDS that use information obtained from the local network segment. [10]

B. Intrusion Detection System

Intrusion Detection System IDS is used to detect intrusion attempts integrity, confidentiality and availability of data in the protected network. It is a set of tools, methods and resources that help us identify, disclose and report unauthorized and unapproved activities. It is a passive system which only draws attention to it and makes active countermeasures.

Through the warnings and statistics gives the operator information about the recorded attacks. It's just one part of the overall protection of the protection system. It also detects operating activities, which do not necessarily represent a threat to the system.

Some traditional IDS can also actively responding to the detected attack. In this case, mostly to work with a firewall that dynamically changing part of its policy to avoid the communication assessed as offensive.

IV. APT Honeypots

While there are many solutions to detect APT, are not all 100% effective. With the honeypot are able to some extent combat APT attackers. In this section we will discuss this problem and propose practical solutions that would form part of a system to detect APT. The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot": "A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated." [6]

Honeypot is an information system whose purpose is to attract potential attackers and record their activities. Honeypot is used to detect and analyze attacks on computer networks and systems. Honeypots servers are dedicated servers,

workstations and the network collects information about attackers and intruders who attack systems. Honeypots are most often used for the early detection of malware and subsequent analysis of its behavior. Malware is constantly changing its strategy of attack and different ways to hide and avoid finding. For these reasons, the malware somehow lure and then analyze their behavior. It is important to remember that the honeypot does not replace traditional security systems, but only complements it. Based on design criteria, honeypots can be classified as pure honeypots, High-interaction honeypots and Low-interaction honeypots.[5]

Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools

To detect APT incident is used by all types of honeypots, which are listed below.

A. *High-interaction honeypots*

Honeypot with a high degree of interaction shows a complete real system, with all services and functions. Unfortunately, this method of implementation allows the attack the whole system, including the honeypot.[7]

B. *Low-interaction honeypot*

These honeypots simulate only a few features transport layer operating system. In these systems, it is easy to identify the mapped threats, unfortunately detection of new types of attacks is impossible in most cases.[7]

C. *Medium-interaction honeypot*

This is the combination of low and high-interaction honeypot. It is not only the emulation of the protocol. Application's protocols are not detailed simulated as in the high-interaction honeypot, so the attacker thinks that this is the real system. [9]

D. *Honeypot on production systems*

It is a special version of honeypots, implanted in a production system. If the user does not have access to production systems, allow him to produce the system log. After verification, but is not admitted to the productive version, but in the sandbox, with imaginary data. The attacker feels that operates within the contested system, but is found only in the sandbox, which is monitored. All information about the activities striker transferred to the control system. Depending on the system administrator if this will be a honeypot to inform the user. It can also serve as an opportunity to capture unauthorized access to authorized systems.

Monitoring APT attacks honeyfarm used with any number of High-interaction honeypots, Medium-interaction honeypot Low-interaction honeypots and Honeypots on production systems, according to the current situation.

E. *Honeypot agent*

Next complement the above solution is a honeypot agent.

The original design of honeypots has one major limitation. Honeypots are waiting for the attacker. Role honeypot is passive. The design of this solution becomes the attacker honeypots notice and carries out its activity without being detected by the system. Therefore, this solution we extended the agent who directs the attacker to the system honeypots. As these types of attacks simulate the behaviour of users, the attacker slip agendas and users little trap. The essence trap lies in the difference between continuous user behaviour and bot. The user of the system is using the agent set a trap. The average user is hidden at first sight, or not interesting for his work. For example, a typical user ignores file system, various TMP directories, and the like. Bot trying to do the contrary, collecting information about invaded system, it searches every corner of systems. This is the stage where they come onto the scene Honeypot systems that offer interesting information for bots. The next chapter will present all the steps of how the system works.

F. *Step-by-Step Description*

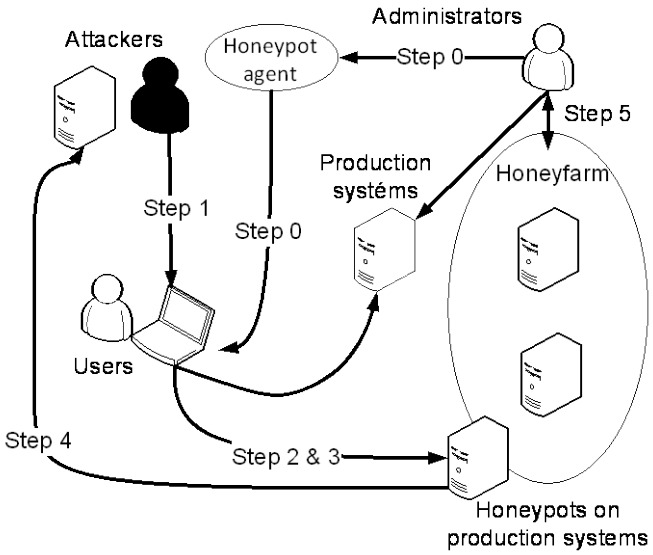

Fig.1 The procedure the attack on Honeyfarm

1) *Step 0*

Institutions will connect own network with Honeynets, containing various types of honeypots. Activated systems on Low interactive honeypot, Medium-interaction honeypot, High interactive honeypot and Honeypot on production systems. Agent activates a trap for attackers on selected systems.

2) *Step 1*

The attacker had risen to attack the weakest phase Internal Reconnaissance and compromised systems. Subsequently seeks to expand its activity to other parts of the network or systems which are the main interest of the attacker. It is highly likely that decodes any of the trap set by the agent. It explores the system, decodes passwords and collects a wealth of

information. Standard command can find e.g.: List the services that have started on the victim system, list currently running processes, list accounts on the system, list accounts with administrator privileges, list current network connections, list currently connected network shares, list other systems on the network, list network computers and accounts according and other.[2]

But for example in list currently connected network share finds the shared disks planted agent.

Once an attacker has any legitimate authority, subsequently proceeds to stage Lateral Movement. At this stage, according to the information obtained may legitimately be in the network. If he has the law, he can connect to share resources on other systems, he can run commands on other machines without arousing suspicion.

3) Step 2

The attacker logs on to a honeypot systems, according to information obtained on compromised systems from the previous step.

4) Step 3

The attacker invades honeypot systems and compromises them.

5) Step 4

The attacker collects data from infected systems and honeypots. Furthermore sends the information to its Command & Control server.

6) Step 5

Administrator detects accesses to the honeypot system and applies safety rules on production systems, misused blocking honeypot, misused blocking accounts. It can then analyses the process of attack and establish rules and procedures to defend the weak spots.

G. The activity of attacks

The following chart recorded a number of anti-virus detection systems and antimalware a number of incidents captured by honeypots running in the selected time period for a non-homogeneous network. The environment consists of 400 systems under the control of the administrator, as well as about an average of 300 to 400 devices on private property without the possibility of influencing their management. Honeypot agent was installed about 15% of the stations.

Date	Common solutions (CS)	captured by CS and HS	Honeynet solutions (HS)
26.1	1	0	0
27.1	2	0	1
28.1	7	0	1
29.1	8	2	3
30.1	6	1	2
31.1	2	0	0
1.2	1	0	0
2.2	4	0	1

Tab.1 Number of incidents captured during the period

Incidents labeled as Common Solutions (CS) are captured using conventional anti-virus and anti-solutions. Honeynet solutions (HS) attacks are detected only by the honeypots. Captured by CS and HS is indicated by the intersection of the two types of detection. The attack was detected using the Common solutions and Honeynet solutions. More successful Common solutions is expected, an attack captured in the beginning. These attacks are mostly in documented and there is a defense for them. Unfortunately, some new types can bypass this protection, and then it can only be detected using the honeypots. These intersections are the most targeted, more destructive and more dangerous.

H. Some Interesting Features

Compared with other antimalware and anti-spyware solution, the solution proposed some interesting features:

1) Function 1

Standard detection solution is supplied from external suppliers, and directly targeted attacks are to learn to do without. APT attacks can in some cases outperform. Honeypot system offers an additional level of defense and detection, after overcoming a standard solution. It is able to detect the effects of charge from the 0-day exploits on days vulnerabilities, for which standard solutions can not react in time.

2) Function 2

This solution can be independent of the operating systems of individual users. Omitting the agent is decreasing its ability to detect, but on some systems cannot use any standard solutions. For example: operation systems in printing devices.

3) Function 3

This addition to the standard security solutions can, in combination with other systems to improve their performance and increase the efficiency of detection of the attack.

4) Function 4

By intercepting attacks on honeypots can be analyzed for the attack and using the information collected we can better secure vulnerabilities of systems.

5) Function 5

After analyzing captured on honeypots can determine which accounts were compromised, then you can only block the system. We do not exclude the operation of the whole system, just fix the compromised section. Saving considerable financial resources.

6) Function 6

Basic setup honeypots without an agent does not have any additional requirements (software or hardware) to the user. Users do not even know about this defense system. This solution is for him invisible, which is the case of standard detection systems, the exact opposite.

7) Function 7

Possibility of detection of attacks on mobile devices, which are beyond the control of the administrator network segment. Detects attacks that are not specifically targeted.

Detection solution using honeypots is unnecessarily

expensive and complicated as most systems to detect attacks. This is the use of standard techniques and instruments. To detect APT use their own shortcomings APT system attacks.

V. COMPARISON OF SOLUTIONS HONEYPOTS VS. HONEYPOTS WITH THE AGENT IN THE EXPERIMENT

We have created a virtual experimental system simulating a real institution. It was implemented using virtualization server and multiple physical workstations. Scope of the network simulated secondary network behind the firewall using NAT. This network was separated by a firewall with strict rules. Data flows were controlled by IDS in the case of suspected dangerous situation or when you try to abuse the laboratory experiment was suspended. Was inserted into the network compromised machines and were followed in a certain time interval. The network was divided into five virtual VLAN. Infected machines could interact with each other, and have a wide network of honeypots.

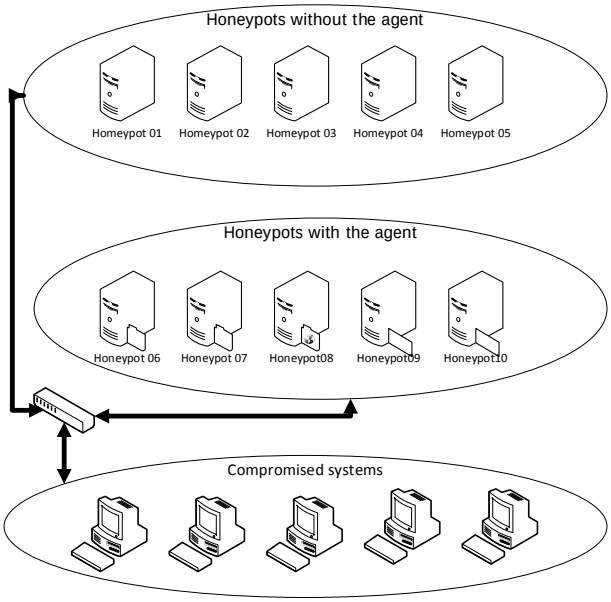

Fig.2 Schematic experimental virtual networks

The system includes a source of infections and is the gateway for attackers. It follows the Lifecycle APT (Internal point Reconnaissance). Sources of infection for these sets were collected of the following sources:

The real environment was partially virtualized infected machines from lecture or from of users who give their consent to the operation. They were first removed sensitive data and change credentials. Laboratory network that resembled the structure of the source network from which comes the contested machines. Furthermore, these machines were deployed agents. If this type of infection permitted the machines were virtualized and run in a virtual environment. If not, some types of infection tested, whether it is a virtual machine that was used to clone their similar physical machine, and then connected to the laboratory network.

Have been tested source of infection from the Internet. From Internet sources were downloaded real disease and implemented on a clean system with appropriate software programs. Additionally, this machine was operated as a physical machine or was virtualized, depending on the type of infection.

Another type sets the virtual machines that were made available to validate the real and the man who tried to get as much information about the laboratory network.

A. The honeypots

These segments are connected together to simulate real network. There were implemented other real devices such as printers and real workstations and servers. It was because research to verify the infected device will try to spread to other resources.

1) The traditional honeypots

In the system are referred to as honeypots without agents. This part of the system was performed using light sensors honeypot. These honeypots on infected computers had no record of the activities and continuously changing its IP address using DHCP. They are detectable only in a forward scanning and browsing the network. In the experiment, it is honeypoty01 – 05.

2) The system of traditional honeypots mapped agents

This part was realized by the middle honeypot. Unlike traditional honeypots of these honeypots in some way mapped to the infected computer via an agent. It is a medium type of honeypots, which are allowed to login and follow-up is mapped. The following table is a list of honeypots and their primary focus. All of these honeypot courses register other services such as classic honeypot. The experiment was a honeypot06-10. These honeypot to focus on the next one service: microsoft-ds, ftp, pop3 and http. The experiment tested the services that are most vulnerable to APT attacks.

Name	Main focus	Service	Port
honeypot06	mapped agent	microsoft-ds-permanent.	445
honeypot07	mapped occasionally	microsoft-ds-occasionally	445
honeypot08	FTP	ftp	21
honeypot09	POP3	pop3	110
honeypot10	webmail system	http	80

Tab.2 List of honeypots mapped agents

B. Experiment

The main objective of the experiment was to observe the differences between the detection performance between the traditional design of honeypots, which were honeypot of information which was not anywhere on infected computers and the honeypot agent mapped according to Tab. 1.

The result of the experiment is expressed by the following graph.

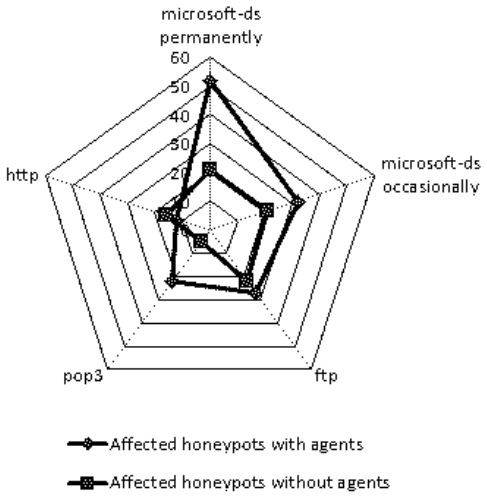

Fig.3 The result of the experiment

C. *The conclusion of the experiment*

Solving system honeypots, which are referred, infected systems i.e. (Affected honeypot with agents) - HPA 63% had incident detection experiment more than segment Affected honeypots without agents - HP. It was detected from 37%. Better results can be attributed to HPA data entered about honeypots HPA system in the infected system. Incidents are no longer focus on complete scanning and reconnaissance networks where these intrusions detected. But today's incident draws information from the attacked system and those used for other activities. This section is the most obvious at the detection port 445 (Services Microsoft-DS Active Directory, Windows shares), wherein the ratio of segments HPA / HP 76% / 23%.

VI. CONCLUSION

APT attackers will always have an interest in your data. They are highly adaptable and monitor deficiencies in the security of your systems. If they are able to penetrate the defense can monitor your systems and collect data. This data is then used to infiltrate into other systems. The information obtained could be used for business meetings, and can have economic and strategic implications. Analysis of incidents will help us improve our infrastructure and can focus on fixing vulnerabilities. We can then better focus on the monitoring and audit of specific systems. Planning these strategies forward, it will be much harder for attackers to infiltrate systems and obliterate his tracks. Maintenance IT environment, effective patch management are important steps to eliminate opportunities for initial penetrations. With increased awareness of users can mitigate attempts by social engineering. Removing local admin rights to users, we can reduce the risk of privilege escalation. Simulation threats through penetration testing and test exercises are good grounds for the creation of effective security strategies. Without a thorough understanding of the threats and good security strategy, security spending will be ineffective and an inefficient.

REFERENCES

[1] *Advanced Persistent Threats (APT): What's an APT? A Brief Definition*. DAMBALLA. [online]. 2010 [accessed on 2013-05-11]. Available at: https://www.damballa.com/knowledge/advanced-persistent-threats.php

[2] APT1 Exposing One of China's Cyber Espionage Units. [online]. p. 74 [accessed on. 2013-05-11]. Available at: http://www.mandiant.com

[3] COMMAND FIVE PTY LTD. *Advanced Persistent Threats: A Decade in Review*. [online]. 2011, p. 13 [accessed on 2013-05-11]. Available at : http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

[4] DELL SECUREWORKS. *Lifecycle of the Advanced Persistent Threat*. [online]. 2012, p. 16 [cit. 2013-05-11]. Available at: http://go.secureworks.com/advancedthreats

[5] Honeypot Background. PROVOS, Niels. *Honeypot Background* [online]. [accessed on 2013-05-11]. Available at: http://www.honeyd.org/background.php

[6] SPITZNER, Lance. *Honeypots tracking hackers*. Boston: Addison-Wesley, 2003. ISBN 0-321-10895-7.

[7] SPITZNER, Lance. *Honeypots: Definitions and Value of Honeypots. Virtual honeypots: from botnet tracking to intrusion dedction* [online]. Upper Saddle River: Addison-Wesley, 2008 [accessed on 2013-05-11].

[8] TREND MICRO. Targeted Attack Entry Points: Are Your Business Communications Secure?. [online]. 2012, p. 5 [accessed on 2013-05-11].

[9] MALANIK, David and Lukas KOURIL. Honeypot as the Intruder Detection System. In: 2013, pp. 96-101. ISBN 978-960-474-311-7. Available at: http://www.wseas.us/e-library/conferences/2013/Rhodes/COMPUTE/COMPUTE-14.pdf

[10] SU-HYUNG, JO, KIM JEONG-NYEO a SOHN SUNG-WON. Security Management System for Intrusion Detection. p. 4. Available at: http://www.wseas.us/e-library/conferences/joint2002/451-130.pdf

[11] SILVA, TAMER A. DA, ROBSON DE O. ALBUQUERQUE, FÁBIO M. BUIATI, RICARDO S. PUTTINI a RAFAEL T. DE SOUSA JR. Trapping, Blocking and Redirection of Network Security Attacks Against a Network using a Community of Intelligent Agents. p. 4. Available at: www.wseas.us/e-library/conferences/2005argentina/papers/503-223.doc

[12] KIHO, LEE, LEE WANSOO a JANG SANGSOO. Developing Online Self-Training Info rmation Security Program for Web Hosting Administrators Using Virtual System. In: AL]., Editors Subhas C. Misra ... [et]. Recent advances in education and educational technology: proceedings of the 7th WSEAS International Conference on education and educational technology (EDU'08), Venice, Italy, November 21-23, 2008. S. l.: WSEAS Press, 2008, s. 289-293. ISBN 9789604740291ISSN 1790-5109. Available at: http://www.wseas.us/e-library/conferences/2008/venice/edu/edu50.pdf