*Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia* | *Paper No. 057*

# DEVELOPMENT OF A SINGLE HONEYPOT SYSTEM INTERFACE

**Siti Rohaidah Ahmad[1], Arniyati Ahmad[2], Nazatul Naquiah Ahba Abd Hamid[3], Mohd Sharif Ab Rajab[4], Nor Fatimah Awang[5], and Muslihah Wook[6]**

[1]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, sitirohaidah@upnm.edu.my*
[2]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, arniyati@upnm.edu.my*
[3]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, nazatul@upnm.edu.my*
[4]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, sharif_liger@yahoo.com*
[5]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, norfatimah@upnm.edu.my*
[6]*Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia, muslihah@upnm.edu.my*

**ABSTRACT**. Networking is crucial to any organization which interconnecting systems all around the globe. However, networking is exposed to the increase of threats that have been detected which reducing the organization's security level. Perpetrators of cybercrime will take this advantage to exploit other systems in their network. To enhance the security level of networking, Honeypot technology has been created to detect the unauthorized use of network. This paper focuses on development of batch files that execute a normal computer as a Honeypot. The main goal of this system is to capture information on every network attacks. Technically, this paper will guide user in Honeypot configuration process.

**Keywords**: Honeypot technology, cybercrime, Honeypot interface

## INTRODUCTION

Network Intrusion Detection System is a system used to detect any illegal activities occurred in a computer network. There are various malicious network traffic and computer usage for instance network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malwares.

In the advance of systems and superb technology, most users ignore the security part when using the technology. Honeypot is not new in cyber-technology. Honeypot acts as surveillance and manage to detect and capture the attackers of computer network system. The development of batch scripting which contains instructions for generating a single Honeypot will be introduced in the next section in this paper.

## HONEYPOT

Referring to the definition of Honeypot by the author of Tracking Hackers, "*A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource"* (Spitzner, 2003). In a computer jargon, Honeypot is a tool to get information about the attacker. It is designed for inspection and attacked. Furthermore, network administrators can learn about activities that can harm and monitor the trends of these activities. Honeypot will give early warning if the system encountered with attacks. Despite that, Honeypot has its own drawback. If Honeypot is not walled off appropriately; this can benefit the attacker to break into a system by using it.

**Type of Honeypot**

Honeypot can be categorized based on its use. There are two types of Honeypot for this category; Research Honeypot and Production Honeypot. Research Honeypot are run by volunteer non-profit organization whose aim is to gather information about the black hat community. Compared to Research Honeypot, Production Honeypot is easy to use. It captures only limited information and usually used by companies or corporations. Production Honeypot falls into low interaction honeypots which means it is easier to deploy but give less information about the attack or attackers. Both honeypots help to mitigate risk in an organization by working independently.

Different level of interaction classifying Honeypots into:

*Low-interaction honeypots* have limited interaction. They normally work by emulating services and operating systems (Kyi Lin Lin Kyaw & Gyi, P., 2008). Tools are installed to emulate operating system and services. This type of honeypot has a small chance of being compromised. Low-interaction honeypots are useful to gather information at a higher level, *e.g.*, learn about network probes or worm activities, analyze spammers or for active countermeasures against worms.

*High-interaction honeypots* give complex solutions as they involve real operating systems and applications (Kyi Lin Lin Kyaw & Gyi, P., 2008). It observes the attacker's behavior, their tools, motivation and explored vulnerabilities.

**BATCH SCRIPT**

Batch files or it could be called batch programs or scripts are text files containing a series of commands that executed by command interpreter which also known as shell program such as command.com or cmd.exe. The shell program is a computer program that reads line of text that is entered by the user. It interprets line and the text was in the context of a given operating system or programming language. In simple terms, it can be said that the batch file ease work that requires repetition or a certain routine to allow user to create a batch script to automate a lot of orders. Commands for example *for, goto,* and *if*, allow us to perform conditional processing of commands in batch files.

Different platforms come with different batch file's extensions. DOS batch files have the filename extension **.bat**. Meanwhile, for Microsoft Windows NT family and OS/2, the batch files may have the filename extension **.cmd** or **.bat.** 4DOS and 4NT related shells use **.btm**. In OS/2, a file with a **.cmd** extension can also be a Rexx file and shell script is similar to batch file in Linux.

**SPECIFICATION OF SYSTEM**

The system has been developed using Visual Basic programming language version 6.0 (VB6.0). The development of this system involved the design on how to generate a list of command codes that will produce a batch script. This batch files will be applied in configuring a computer as a single Honeypot.

```
If stopWinDef = vbChecked Then List1.AddItem "NET STOP Windows Defender"
```

**Figure 1. Example of Program Code in VB6.0.**

Figure 1 shows one line code that displays check box for the selected service. NET STOP or NET START command codes are used in the command prompt (cmd.exe) to stop or to turn on any services in Windows operating system. Switched or ended the service in the system is intended to make the computer more vulnerable and to attract hackers to intervene into the computer.

Users can also select a list of ports to be opened for the construction of a Honeypot. Here is an example of segment code for setting an instruction to open a port in the system as shown in Figure 2.

```
If port137 = vbChecked Then List1.AddItem "netsh firewall add portopening TCP 137 NetBios137"
```

**Figure 2. A Segment Code To Open A Port.**

**Development Process of a Single Honeypot**

The flow of the process to generate a batch file is illustrated in Figure 3. Initially, user has to decide which services and ports they need to choose to attract hackers to attack Honeypot system.

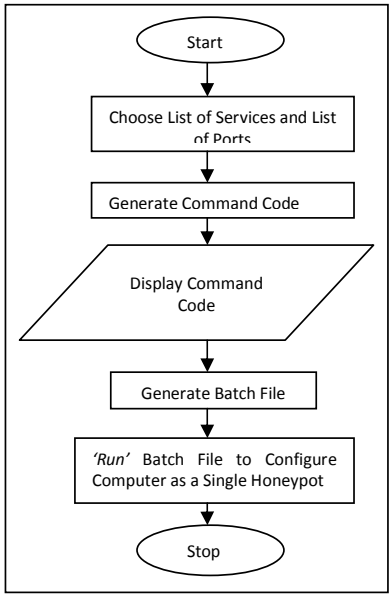


**Figure 3**. **Flowchart Of Generating A Batch File.**

Once the required list of services and port are selected, a command code will be produced and displayed. Batch files are delivered and stored in the specified directory. Eventually, the batch file runs the computer as a single Honeypot. The yielded batch files affected the starting or termination process of the computer, and opening the port for a computer that has a connection to the internet. Figure 4 demonstrates a segment code which output the direction.

```
@ECHO off
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName /v
ComputerName /t REG_SZ /d SERVER
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName /v
ComputerName /t REG_SZ /d SERVER
NET STOP wuaUserv
NET STOP WindDefend
NET STOP wscsvc
NET STOP nla
NET STOP ProtectedStorage
NET START RemoteRegistry
NET START RemoteRegistry
NET START LanmanServer
NET STOP SamSs
NET START TermService
NET START RemoteAccess
NET STOP Netlogon
NET STOP PolicyAgent
netsh firewall set opmode mode=ENABLE
netsh firewall add portopening TCP 137 NetBios137
netsh firewall add portopening TCP 138 NetBios138
netsh firewall add portopening TCP 8193 Sophos8193
```

**Figure 4. Segment Code Of Registry Editor.**

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
/vComputerName /t REG_SZ /d SERVER
```

**Figure 5. Modification On Registry Editor.**

The registry file editor in Figure 4 has been modified as depict in Figure 5. When user enters the name of Honeypot, for example, 'SERVER', it replaces the computer name. The produced batch file runs the code and it changes the value of Active Computer Name REG_SZ as stated in the Registry Editor as shown in Figure 6.

**Figure 6. Registry Editor On Windows XP.**

The batch files should be placed in a computer and it does the computer system configuration to serve as a single Honeypot that has a connection to the Internet.

### Design of Single Honeypot System Interface

A single Honeypot system interface is designed to be user friendly and simple without having to remember all the commands to generate a batch file. A user only needs to select options through provided interface system.

**Figure 7. Naming A Honeypot.**

Figure 7 shows a user must name the Honeypot to attract hackers to attack the Honeypot system. The services listed in the *'Select Services in Your Honeypot'* have to be selected as presented in Figure 8. Cessation and initiation of any services listed aims to reduce the level of computer security that would act as a Honeypot. Hence, it eases hackers to intrude and interact with the system.

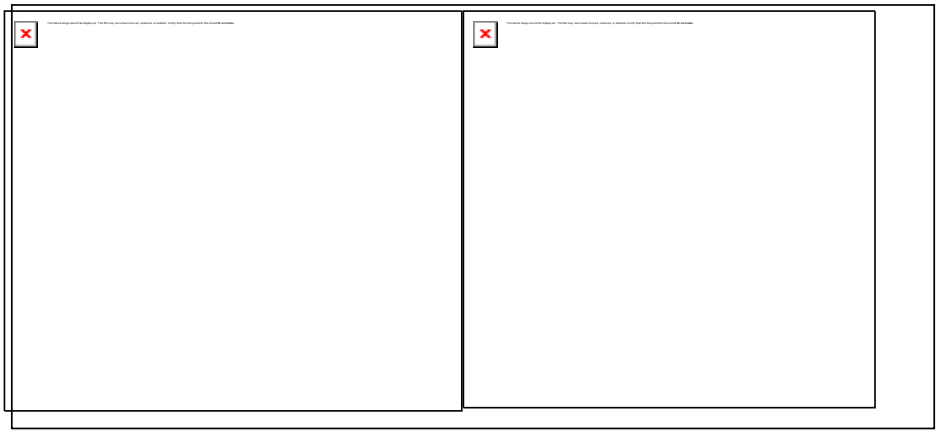

**Figure 8. List Of Services And Ports.**

Figure 8 shows the list of ports that need to be chosen by a user. These ports are used by hackers to break into a computer system which operates on Windows XP operating system.

**Figure 9. Batch Script Generated.**

Once the list of services and ports has been selected, the system will generates a batch file as displayed in Figure 9. This file is finally stored in a specified directory.

**Implementation of a Single System Honeypot Interface**

The system interface was developed to help user in generating a Honeypot without having to remember all the instructions to generate Honeypot. Although, there are a few disadvantages arise from the proposed system. Honeypot raises the possibilities of enabled services can be disabled by intruder, thus, user needs to restart the particular service. Testing of the services used in the project could damage a computer operating system. Therefore, the virtual operating system should be applied to overcome such problem. However, not all services that able to operate in a real operating system can run in virtual situation. Typically,

the problem arises when the test involves the use of network-based services, for example, Network DDE and Network DDE DSDM services which cannot be implemented because there is a problem of other services that do not operate in a virtual operating system.

## CONCLUSION

Due to the advancement of information technology, various forms of attack from hackers arise with intention to destroy data, information and so forth. Therefore, a system with improved security level is demanded with the purpose of protecting precious data and information. The development of low-interactive Honeypot system is an alternative method in learning the real circumstances in computer network. The aim of this research is to develop a system that can facilitate users in configuring Honeypot without entering any command codes. Apparently, users have options by selecting the list of services and ports in conjunction to build up a single Honeypot and run generated batch files.

## REFERENCES

Cenys, A., Rainys, D., Radvilavicius, L. and Bielko, A. (2004). Development of Honeypot System Emulating Functions of Database Server. *RTO IST Symposium*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA457668.

Even, L. E. (2000). Honeypot Systems Explained. Retrieved from http://www.sans.org/security-resources/idfaq/honeypot3.php.

Jones, J.K. and Romney, G. W. (2004). Honeynets: An Educational Resource for IT Security. *SIGITE'04*, Retrieved from http://portal.acm.org/citation.cfm?id=1029540.

Kaur, M. (2008). A Conceptual Honeypot Framework. Retrieved from http://www.rimtengg.com/coit2008/proceedings/NW36.pdf.

Kyi Lin Lin Kyaw & Gyi, P. (2008). Hybrid Honeypot System for Network Security. *World Academy of Science, Engineering and Technology*, 48, 266-270. Retrieved from http://www.waset.org/journals/waset/v48/v48-44.pdf

L. Spitzner (2003). "Honeypots: Definitions and Value of Honeypots". Retrieved from http://www.tracking-hackers.com/papers/honeypots.html

L. Spitzner. (1999). To Build a Honeypot. Retrieved from http://www.spitzner.net/honeypot.html.

Leary, M.O., Azadegan, S., and Lakhani, Jay. (2006). Development of a Honeynet Laboratory: a Case Study. *SNPD'06*. Retrieved from http://doi.ieeecomputersociety.org/10.1109/SNPD-SAWN.2006.35

Mikhalenko, P. (2006). Managing Honeypot. Retrieved from http://oreilly.com/pub/a/sysadmin/2006/09/28/honeypots.html.

Sutton, R.E. How to build and use a Honeypot. InfoSec Sec Writers. http://www.infosecwriters.com/text_resources/pdf/build_and_use_honeypot.pdf.

Zhang, F., Zhou, S., Qin, Z. and Liu, J. (2003). Honeypot: a Supplemented Active Defense System for Network Security. *PDCAT'2003. Proceedings of the Fourth International Conference.* Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1236295

Wikipedia. Batch file. Retrieved from http://en.wikipedia.org/wiki/Batch_file.

Wikipedia *Honeypot (computing)*. Retrieved from http://en.wikipedia.org/wiki/Honeypot_(computing).