Stepping Stones Attack Simulator for TCP Connection Traceback Test

Byeong Cheol Choi*, Dong Il Seo*, Sung Won Sohn*, and Sang-Ho Lee**

* Network Security Department, ETRI, Korea
(Tel : +82-42-860-3858; E-mail: corea@etri.re.kr)
**Chung-Buk National University, Korea

Abstract: In this paper, we describe a SSAS (stepping stones attack simulator) that is automatic tool for testing and evaluation in TCP connection traceback system. The SSAS can pass multiple hosts that are included with hacker, middle-path hosts and victim's system. And SSAS can also attack through commands to exploit the victim's system. Usually, hackers do not expose their real attack positions through compromising the middle-path hosts like stepping-stones. Namely, hackers perform the stepping stones attacks in Internet. The SSAS can be utilized by developments and tests of the various countermeasure techniques of hacking. Specially, in this paper, it is used to test the performance of TCP connection traceback system.

Keywords: stepping stones attack, TCP connection traceback, hacking, SSAS

1. INTRODUCTION

1.1. Backgrounds

Recently, the focus of network security is altered passive countermeasure into active countermeasure techniques to attacks. Firewall, IDS and ESM – it's for effective management of secure nodes and countermeasure – are passive countermeasure techniques and Intrusion Traceback is new active countermeasure techniques [1-4, 7].

Intrusion traceback techniques are consisted of IP packet traceback and TCP connection traceback. In this paper, we focus on TCP connection traceback techniques and the proposed SSAS (Stepping Stones Attack Simulator) is also for testing those systems.

1.2. Trends of intrusion traceback techniques

Table 1 shows the trend of intrusion traceback techniques and the research area of this paper is to develop the automatic attacking simulator for TCP connection traceback system tests. Traceback techniques are divided into TCP connection traceback and IP packet traceback.

TCP connection traceback is for tracing the general connection-oriented hacking and IP packet traceback is for tracing the IP spoofed attacks like DoS (Denial of Service) / DDoS (Distributed DoS).

Table 1 Trends of intrusion traceback techniques

Related with DoS/DDoS	IP Traceback	Proactive Tracing	Packet Marking(PacketTraceback), Messaging(ICMP Traceback)
		Reactive Tracing	Hob-by-Hob Tracing, IPsec Authentication, etc
Related with General Hacking	Connection Traceback		Stepping Stones Attacks

Connection Traceback	Host-based		AIAA, CIS, DIDS
	Network-based	Passive	Thumb Printing, ON/OFF, Deviation, IPD-based
		Active	IDIP, SWT, ACT

1.3. Contribution of this paper

In this paper, we propose a SSAS (stepping stones attack simulator) that is automatic tool for testing and evaluation in TCP connection traceback system. The SSAS can pass multiple hosts that are included with hacker, middle-path hosts and victim's system. And SSAS can also attack through commands to exploit the victim's system. The SSAS can be utilized by developments and tests of the various countermeasure techniques of hacking. Specially, in this paper, it is used to test the performance of TCP connection traceback system.

This paper is organized as follows: The introduction is presented in Section I, the proposed system is described in Section II, experimental results can be found in Section III, and conclusions are drawn in Section IV.

2. PROPOSED SYSTEM

2.1. Design and Development

SSAS (stepping stones attack simulator) is designed and developed for testing TCP connection traceback system and performs automated remote attacks like real hackers. Fig. 1 shows the concept of SSAS (Stepping Stones Attack Simulator) and purpose of our research is to develop this concepts.

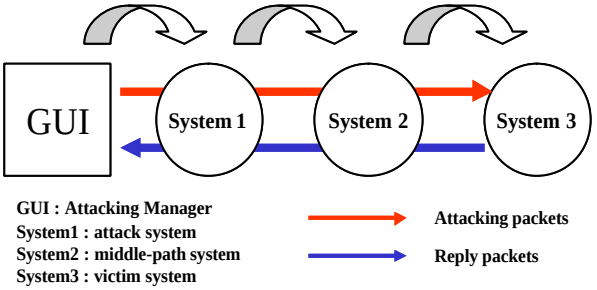

Fig. 1 Concept of SSAS (Stepping Stones Attack Simulator)

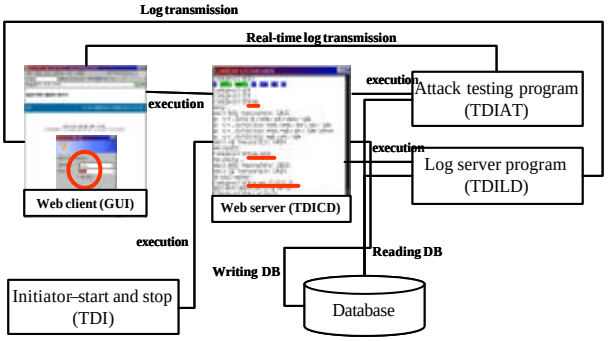

Fig. 2 Design of SSAS (Stepping Stones Attack Simulator)

Fig. 2 shows the design of SSAS (Stepping Stones Attack Simulator). SSAS is consisted of four sub-blocks as follows:

- *TDI* (Test Data Generator for SSAS: Initiator - start and stop)
- *TDICD* (Test Data Generator for SSAS: Web Server Daemon for Console)
- *TDIAT* (Test Data Generator for SSAS: Attack Testing Program)
- *TDILD* (Test Data Generator for SSAS: Log Server)

In the SSAS, TDI that is a basic initiator program performs START and STOP commands, and it does control TCICD that is a web server daemon for console. The start of SSAS is achieved by [#tdi start] command and the stop of SSAS is ended by [#tdi stop] command. After TDICD is started by [#tdi start] command, web server daemon opens the port #995. Web client uses the SSAS web GUI through connecting the web server (TDICD). In the web client, we perform the configuration of SSAS, attacking by TDIAT, and logging on database by TDILD. If we want to see the past attacking log data, we can get the log data by searching the index of the log database that is created by TDILD.

2.2. Analysis of the SSAS sub-blocks

TDI (Test Data Generator for SSAS : Initiator - start and stop)

TDI is a SSAS main block that performs starting and ending the TDICD program. TDI can execute STOP and START commands used by input factor and it shows usages when is used other factors. As TDICD is a sub-block of SSAS that is used to user interface, it is executed and stopped by TDI sub-block that is a main block of SSAS.

TDICD (Test Data Generator for SSAS : Web Server Daemon for Console)

TDICD make a connection to server through opening port #995, and it returns the web pages within the connection of permitted IP address. Web client can execute external or internal (local), and Internet Explorer, Netscape or Opera can be used. Namely, it does not constraint by OS types.
If permitted clients are to connect the server, TDICD reads request page and notifies the extension of page. If request type is GET and extension is HTML(.html), TDICD performs the function of html_response(). If extension is GIF(.gif) or CLASS(.class), TDICD performs the function of binary_response() and transmits web page to the client. If the extension is nothing, TDICD requires the authentication by decision to first connection. If request type is POST, TDICD performs the function of parse_post() and returns the web page.

TDIAT (Test Data Generator for SSAS : Attack Testing Program)

TDIAT program performs as follows:

- TDIAT opens the port #5000 for web client
- Web client's Java applet connect to this port and request/reply the messages
- Received messages is showed in the real-time data and information window of web client (SSAS Web GUI)
- TDIAT performs attacking commands through text input window of web client

TDIAT executes the TDICD using two input factors that are the name of traceback test data for first factor and the connecting IP address for second factor. TDIAT receives first factor (name of traceback test data) and loads the linked-list data of middle-path hosts to the memory for traceback path construction. TDIAT receives second factor (connecting IP address) and does setting.

The generated data by attacks of TDIAT is logged on database as to date/time/name of test-data. If the initial settings are over, TDIAT creates two threads that are the attacking thread and transmission thread. One is an attack-thread for automatic attacks, and the other is a server-thread for transmitting the send and received data of TDIAT as real-time.

Two threads work sequentially. When attack-thread and server-thread are created, attack-thread connects the first middle-path host. And then it connects next middle-path hosts and performs sequentially commands as scenario. At this time, attack-thread logs the send and received messages. Server-thread uses Java applet for transmitting the send/received messages. If the number of message exists to the message structure, server-thread transmits the message. Otherwise, it creates the message and transmits that. After all messages are sent, Java applet sends the command through data-input window and transmits commands to socket of attack-thread. If the commands is QUIT or EXIT, the end_variable is set to zero. TDIAT informs to Java applet that and all of threads are ended.

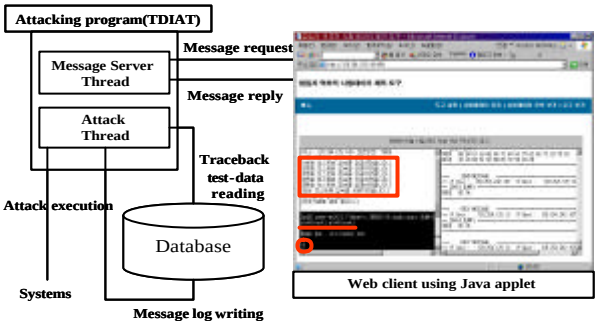

Fig. 3 TDIAT (Test Data Generator for SSAS: Attack Testing Program)

TDILD (Test Data Generator for SSAS: Log Server)

TDILD permits connection to the web client of Java applet by opening the port #7000 and it is designed to show the received messages in real-time data and information windows. TDILD is executed by TDICD and uses two factors that are log name and connecting IP address. TDILD opens the server by port #7000 and sends the next-number message of log-file that received from Java applet. If TDILD informs the all messages to Java applet of web-client, the end variable (m_break) is set to zero. TDILD informs the end of transmission to Java applet and program is ended. If TDILD sends the message of END, the Java applet is ended and TDILD is also done.

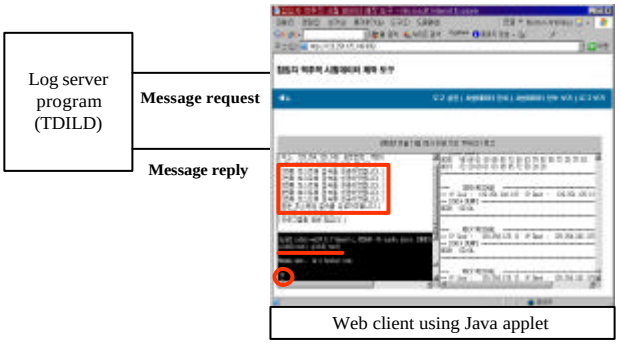

Fig. 4 TDILD (Test Data Generator for SSAS: Log Server)

3. Experimental Results

We develop the SSAS that use C language in Linux-based OS. It is offered to web server for user interface environment and can be used regardless of OS platforms. Java applet is used and GDBM that offered by basic package in Linux released-version is also used.

In this research, we develop a SSAS (stepping stones attack simulator) that is automatic tool for testing and evaluating the TCP connection traceback system. The SSAS can pass multiple hosts that are included with hacker, middle-path hosts and victim's system. And SSAS can also attack through commands to exploit the victim's system.

The SSAS can be utilized by developments and tests of the various countermeasure techniques of hacking. Specially, in this research, it is used to test the performance of TCP connection traceback system.

In the real-time viewer of SSAS, the left-upper widow shows messages of attacking information as real-time, and the left-lower window shows the send/received data, and the right-side window shows the captured dump-data. When all connections are completed, the down-side text window can send input-data. Therefore, we cannot use before completed all connections. Real-time viewer of SSAS is developed by Java applet and consists of data from TDIAT (attacking program). TDIAT (attacking program) opens the port #5000 and send data.

The web client of Java applet connects the same port and receives data from the server. After all connections are completed, web client commands the scenario and press the "ENTER" key. Therefore, we can make the attacking flow to simulate the stepping stones attack. We can use both general character-command-sets and HEX values. If we want to input by HEX value, it must be started '[' character and ended ']' character in the data flow. Also, it must be written two characters even if HEX value can be expressed by one character.

Example 1: ls –aF ➔ [6C 73 20 2D 61 46]

We can see the results of send/receive data that are transmitted in text-input window through the real-time dump and data window. And also, we can see the lists of registered test-data sets from 'See the Test Data Information' menu.

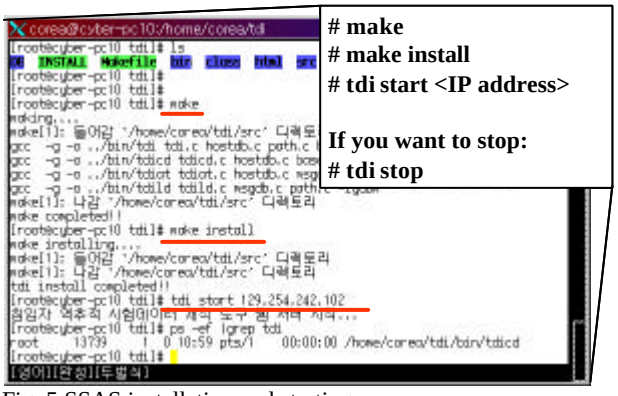

Fig. 5 SSAS installation and starting

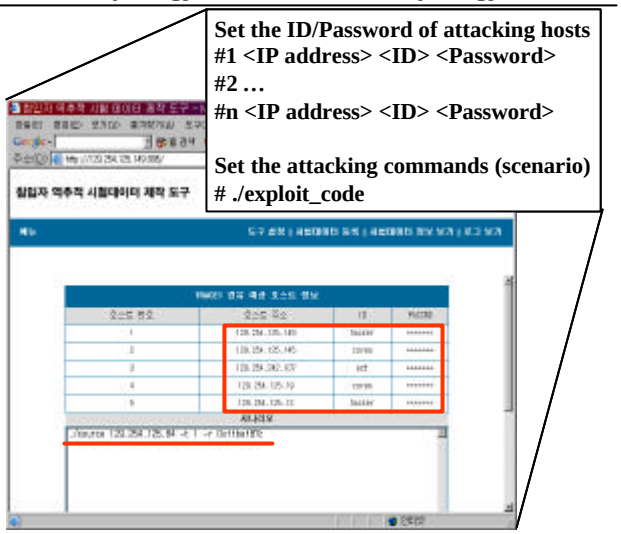

Fig. 6 Configuration of the middle-path hosts and attacking scenario

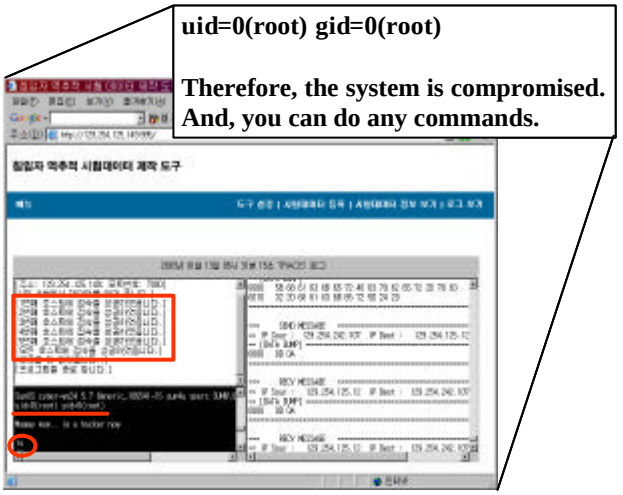

Fig. 7 Attack results (eluding path, exploiting and executing the commands)

4. CONCLUSIONS

In this research, we developed a SSAS (stepping stones attack simulator) that is automatic tool for testing and evaluation in TCP connection traceback system. The SSAS can pass multiple hosts that are included with hacker, middle-path hosts and victim's system. And SSAS can also attack through commands to exploit the victim's system.

SSAS is consisted of four sub-blocks that are TDI(Test Data Generator for SSAS: Initiator - start and stop), TDICD(Test Data Generator for SSAS: Web Server Daemon for Console), TDIAT(Test Data Generator for SSAS: Attack Testing Program), and TDILD(Test Data Generator for SSAS: Log Server).

Usually, hackers do not expose their real attack positions through compromising the middle-path hosts like stepping-stones. Namely, hackers perform the stepping stones attacks in Internet. The SSAS can be utilized by developments and tests of the various countermeasure techniques of hacking. Specially, in this paper, it is used to test the performance of TCP connection traceback system. Moreover, SSAS (Stepping Stones Attack Simulator) offers Web GUI and does not be constraints by OS (operating system).

REFERENCES

[1] T. Baba and S. Matsuda, "Attacks to Their Sources", pp20-26, IEEE INTERNET COMPUTING, March-April 2002.

[2] Dawn X. Song and Adrian Perrig,"Advanced and Authenticated Marking Schemes for IP Traceback", Proceedings of InfoCom 2001.

[3] X. Wang, D. Reeves, S. F. Wu, and J. Yuill, "Sleepy Watermark Tracing: An Active Network- Based Intrusion Response Framework", Proceedings of IFIP Conference on Security, Mar. 2001.

[4] Y. Zhang and V. Paxson, "Detecting Stepping Stones", Proceedings of 9th USENIX Security Symposium, August 2000.

[5] W. R. Stevens, "Unix Network Programming - Networking APIs", 1998 Prentice-Hall PTR.

[6] W.R Stevens, "Advanced Programming in the Unix Environment", 1997 Addison-Wesley.

[7] S. Northcutt and J. Novak, "Network Intrusion Detection an Analyst's Handbook", 2001 New Riders.