Workshop on Computer Networks

Title-A study of the Network Denial of Service Attacks

Authors- Chi-Hsing Yu (M.S.),
- Ching-Chuan Chiang (Associate Professor, Computer Science Department, Cheng Chung Institute of Technology at National Defense University Taoyuan 335, Tel: 03-3805249)

Contact: M.S. Chi-Hsing Yu, “Lenny”
4 Fl., No.65, Lane700, Jungjeng Rd., Shindian City,
Taipei, Taiwan 231, R.O.C.
Tel: 0918-757-098
lenny@ccit.edu.tw

ABSTRACT

The Internet already pervades in each corner of our society. The electronics commerce, military C^{4}ISR, and electronics services of the Government are adopting digital information and the network deeply into their operations. All these changes and facts indicate the potential problems of network denial of service which will not only influence electronics commerce, but will also include the military and political arenas.

As of today, it seems there is no detailed information for providing a big picture of network denial of service attacks. In this paper, it provides an academic research over the network denial of service. With a depth of analysis on the theory and procedures of denial of service attacks, the preliminary integrated denial of service attack platform is originated. The integrated denial of service attack platform is constructed in order to have a better understanding of the characteristics and phenomena from denial of service attacks. A major part of this study is focusing on the verification and findings from the actual experiments based upon theory of network denial of service.

Key words or phrases: Electronics Commerce (EC); Command, Control, Communications, Computers, Intelligence, Surveillance (C^{4}ISR); Denial of Service (DoS)

1. Introduction

In the global trend of information network, the Internet already pervades in each corner of our society. The electronics commerce brings an innovation on the traditional market that overrides the geography boundary limitation. Nevertheless, the Internet also enables hackers to strike the virtual world with the power of Internet. In the past, there were some Internet events that should keep us alert. For example: The attacks on the major web site began in early February 2000 with the first major attack being on Yahoo! on February 7. The surprise attack took the Yahoo! site down for more than three hours. It was based on the Smurf attack, and most likely, the Tribe Flood Network technique.

2. Flow Chart of Denial of Service Attack and Structured Framework

According to the book of “Hacking Expose: Network Security Secret and Solutions” that was written by Stuart Mcclure, Joel Scambray, George Kurrtz, the steps of a hack process are cited at the left side of figure 1. [17] There are 9 steps listed in the flow chart. The major steps processing in sequence are footprinting, scanning, enumeration, gaining access, escalating privilege, pilfering, covering tracks, creating back doors, and the denial of service. Because the main goal of this research is focused on network denial of service, the major steps of the flow chart were revised into 3 steps：footprinting, scanning, and denial of service which is shown at the right side of figure 1. There is one issue that should be noticed here. At the left side of figure 2.8, there are 2 steps （enumeration and gaining access） also included into the process of denial of service. These 2 steps even can be used, but these 2 steps are actually not necessary to be taken for DoS attack. Therefore these 2 steps are drawn in dash-line blocks to distinguish their differences on the revised flow chart. This revised flow chart has an influence on how the integrated DoS attack platform is built. The detailed information is stated in paragraph 3.1.

It seems there is no available paper which centered their discussions on the framework of integrated DoS. Most of the related papers contributed their efforts on the fracture loopholes of protocol or partial network techniques. These kinds of papers did not give a big picture for integrated attack frameworks or interface relations. The learning threshold is not easy to achieve while we try to program an integrated denial of service attack. It makes a tough way ahead of any one who had this kind of intention to fulfill the integrated framework picture. This thesis is planning to construct an integrated denial of service attack platform which is based on the network theory and protocol to include the interface requirements of flow chart. It makes the operator easy to launch various types of DoS attacks instantly. Paragraph 3 will provide more detailed information on this subject.

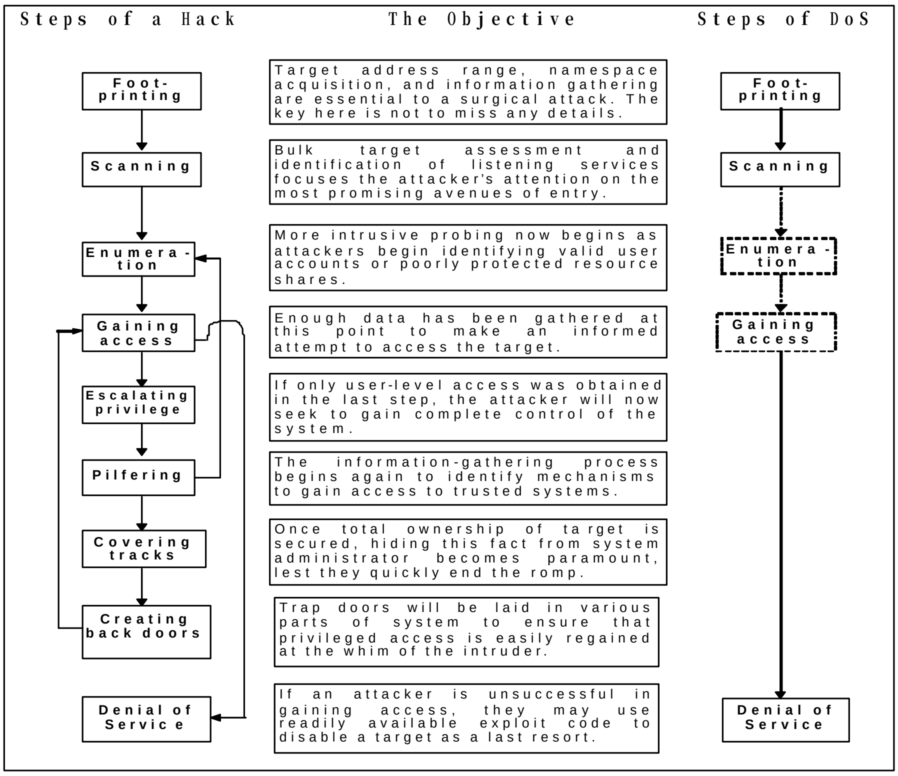

Steps of a Hack
The Objective
Steps of DoS
Foot-printing
Scanning
Enumera-tion
Gaining access
Escalating privilege
Pilfering
Covering tracks
Creating back doors
Denial of Servic e
Target address range, namespace acquisition, and information gathering are essential to a surgical attack. The key here is not to miss any details.
Bulk target assessment and identification of listening services focuses the attacker's attention on the most promising avenues of entry.
More intrusive probing now begins as attackers begin identifying valid user accounts or poorly protected resource shares.
Enough data has been gathered at this point to make an informed attempt to access the target.
If only user-level access was obtained in the last step, the attacker will now seek to gain complete control of the system.
The information-gathering process begins again to identify mechanisms to gain access to trusted systems.
Once total ownership of ta rget is secured, hiding this fact from system administrator becomes paramount, lest they quickly end the romp.
Trap doors will be laid in various parts of system to ensure that privileged access is easily regained at the whim of the intruder.
If an attacker is unsuccessful in gaining access, they may use readily available exploit code to disable a target as a last resort.
Foot-printing
Scanning
Enumera-tion
Gaining access
Denial of Service

Figure 1: The Comparison of Steps for a Hack and DOS

3. Conception of DOS Attack Platform

The conception of the integrated DoS attack platform is mainly driven from the factors of user-friendly interface, foundation theory of DoS, and the flow chart of DoS.

3.1 Requirement of Integrated DoS Attack Platform Based on Theory, Flow Chart, and User-Friendly Interface

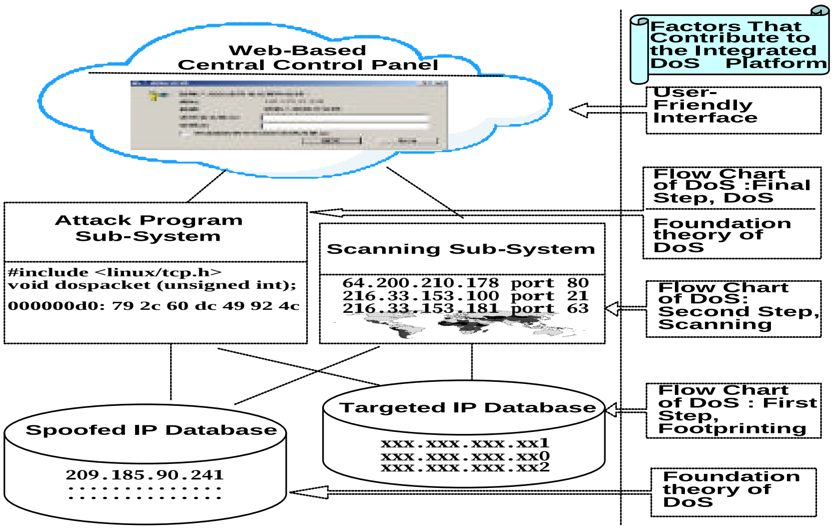
Basically, the integrated DoS attack platform is divided into five sub-systems. It includes the web-based interface central control panel, scanning sub-system, attack program sub-system, spoofed IP address database, and target IP address database.

The factor of user-friendly interface drives the web-based interface central control panel. Because the web-based interface is the trend of Internet; so the central control panel will be designed as a web-based interface for the user to launch a variety of DoS attacks.

The foundation theory of DoS factor results in the sub-system of attack programs, and the spoofed IP address database. Various foundation theories of denial of service are fully implemented by coding the software programs. It is used while the user executes the DoS attack command.

The factor of flow chart for DoS drives the scanning sub-system, and targeted IP database. Because the flow chart of the DoS attack requires a scanning process, so the scanning sub-system will be designed to meet the requirement. All the scanning data will be collected and stored into an appropriated database. There is a statement that provides a very clear meaning of spoofed IP. This statement is abstracted as follows: "The attacking host must ensure that the source IP address is spoofed to be a routable but unreachable host, as the target host will send its response to this address". According to the TCP/IP three-way handshake theory, it proves the above statement is correct while using the SYN flood attack. The only exception for the spoofed IP address is while it is being used as input data for the Fraggle attack. The Fraggle attack requires a reachable, spoofed IP address instead of an unreachable IP address. Based on the different requirements of spoofed IP addresses, there are different tables of spoofed IP addresses being established. The target IP address database will also be built up as necessary.

All these sub-systems are interactive *via* a web-based control Panel. The interaction diagram for these five sub-systems is drawn in figure 2. As to the detailed function of each sub-system, it will be described in the following paragraph.



```
#include <linux/tcp.h>
void dospacket (unsigned int);
000000d0: 79 2c 60 dc 49 92 4c
```

Figure 2: Diagram of Sub-Systems for the DoS Attack Platform and Contributed Factors

3.2 Web-Based Central Control Panel

A web-based central control panel can be accessed through the Internet. It is the control center to scan the available IP addresses from the Internet and links with the database of the spoofed source IP addresses, the targeted IP addresses, the attack programs sub-system. It simplifies the DoS attack procedure by linking the required database and the attack programs together.

Based on experience, a user-friendly interface has a huge advantage for an operator to learn from the new system. This "web-based central control panel" smoothes all the required procedures to launch any types of DoS attack. The feature of web-based homepage is not only convenient to operate, but also can reduce the total operational time for launching a DoS attack.

3.3 Scanning Sub-System

The scanning sub-system is used as the IP address and port number scanner over the Internet resource. This scanning sub-system is able to scan IP addresses through the Internet and stores the scanning results to the spoofed IP database directly without any manual data entry process. It makes the whole process of DoS attack more convenient. The user can designate the required IP range to be scanned from the scanning sub-system. The available port numbers for a specific IP address also can be scanned by this scanning sub-system. This scanning sub-system fully implements the required functions as described by the second step (scanning) in the DoS attack flow chart. The scanning process is initiated from the web-based central control panel.

3.4 Attack Programs Sub-System

Based on the theory and type of DoS, this sub-system is required to generate various TCP/IP packets and is able to control its flag, source IP address, destination IP address to include the number of packets. The default setting of the source IP address (0.0.0.0) is designated to read the data in the spoofed IP database for the attack programs sub-system. The major idea in collecting various DoS programs is to verify it and comparing with the foundation theory of DoS. This process will create the innovation way for launching a DoS attack. All the commands and related parameters that are required to make the attack programs workable have changed from the traditional line-command format to a new method of form entry *via* the web page. It is a key role to support the linking requirement from the web-based central control panel.

3.5 Spoofed IP Database

The spoofing IP is identified through the scanning process which conforms to the flow chart of denial of service. Based on the characteristic and dynamic status of the spoofed IP, all data in the database are updated whenever the scanning process is initiated. Based on the different principle of DoS attack used, there are 2 categories of spoofed IP tables made. This database records each spoofed IP during the scanning process. The final output table in the database will serve as an input of spoofed source IP for the attack programs sub-system.

3.6 Targeted IP Database

The main idea of the "targeted IP database" is that it uses the scanning process to collect all the IP addresses or the IP range for the targeted hosts. The contents in the targeted IP database are dependent on the mission requirements.

4. Construction and Laboratory Design

4.1 Construction of Attack Simulation Environment and Consideration

The DoS attack platform is built on the Linux version 7.2 operating system with an Apache server including PHP version 4.1.2 module function. This platform is also capable to link with the PostgreSQL version 7.1 database through the PHP module. The integrated DoS attack platform consists of 5 sub-systems. These sub-systems are: web-based central control panel, scanning sub-system, attack programs sub-system, spoofed IP database, and targeted IP database.

In order to measure and observe the performance of the integrated DoS attack platform, there are some nodes that are set up including targeted hosts, a mixture of Windows and Linux operating system, attack platform hosts, observing hosts with sniffer and tcpdump software function. The scenario suite to be used under this laboratory simulation environment is to implement various popular types of DoS packet attacks.

The detailed profile of a laboratory simulation environment is in figure 3.

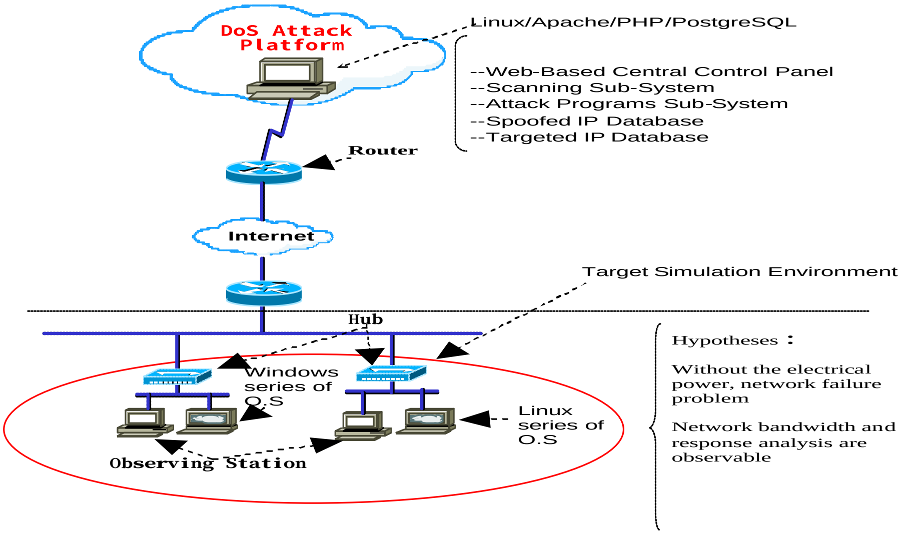

DoS Attack Platform
Linux/Apache/PHP/PostgreSQL
--Web-Based Central Control Panel
--Scanning Sub-System
--Attack Programs Sub-System
--Spoofed IP Database
--Targeted IP Database
Router
Internet
Target Simulation Environment
Hub
Windows series of O.S
Linux series of O.S
Observing Station
Hypotheses :
Without the electrical power, network failure problem
Network bandwidth and response analysis are observable

Figure 3: DoS Attack Simulation Environment Profile

4.2 The Attack System Prototype for Integrated Denial of Service

The prototype of attack platform is built on the Linux Operating system with an Apache server function that can be accessed from the any point of the Internet. The feature of this system is that it can be operated with an IE web browser without any additional software requirements. The architecture of the software package and related version that is used to build the integrated DoS attack platform is shown in figure 4.

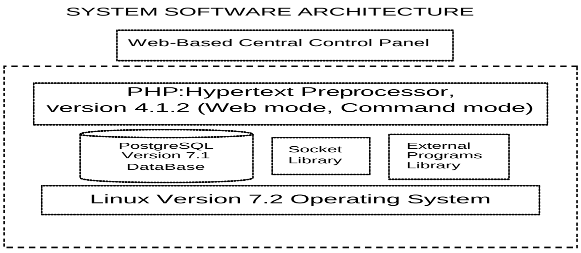

SYSTEM SOFTWARE ARCHITECTURE
Web-Based Central Control Panel
PHP:Hypertext Preprocessor, version 4.1.2 (Web mode, Command mode)
PostgreSQL Version 7.1 DataBase
Socket Library
External Programs Library
Linux Version 7.2 Operating System

Figure 4: Software Package of the DoS Attack Platform

Basically, anyone intending to connect to this attack system can type in the host name or IP of the attack system into the Uniform Resource Locator (URL). To prevent the unauthorized person to use this attack platform, there is an account and password web page shown on the screen while you visit this specific IP. The prototype of access authorization web page is shown in figure 5.

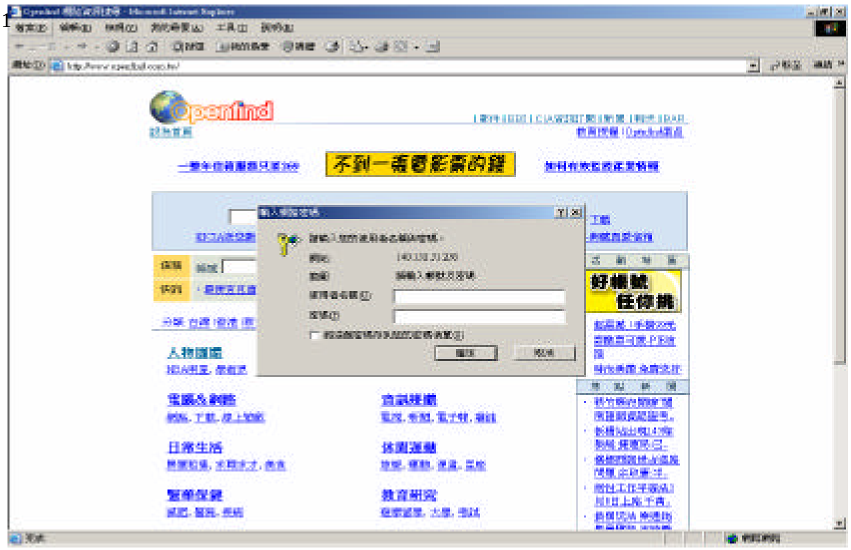
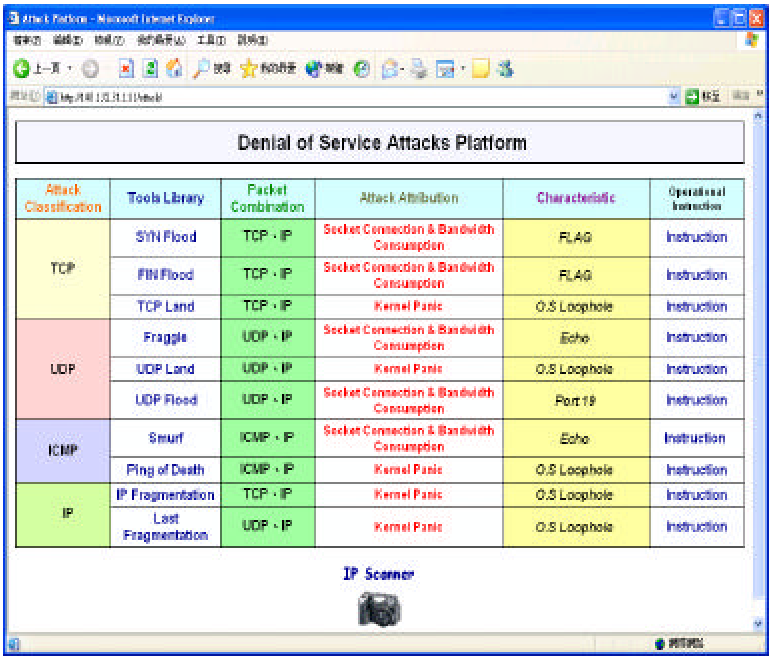


Figure 5 : Access Authorization Web Page

When the account and password are checked and correctly verified, the web page of the attack platform will show up. The DoS attack platform will provide various tools that can be used to launch a denial of service attack. These include attack classifications, packet combinations, attributions, and characteristic information available on this attack platform. There are operational instructions available for each kind of tools for the convenience of the user to understand the operational procedure. The attack platform adopts the multi-layer technique. The hyper-link function connects to other linked web pages. The attack tools and related operational instructions, for the brevity sake, will use the hyper-link function to link other web pages. The prototype of the denial of service attack platform is shown in figure 6. The scanning sub-system is illustrated in figure 7 and in figure 8.

Once the operator uses the mouse to click in the tool, the web page of the related packet generator will show on the screen. All the required operational information will be noted within the operational instructions. The example content of operational instructions is shown in figure 9. The packet generator is capable to generate the TCP, IP, UDP, ICMP packets which provide the flexibility of function to control the packets *via* the web page operational interface. The prototype of various packet generators is shown in figure 10, in figure 11, and in figure 12 respectively.

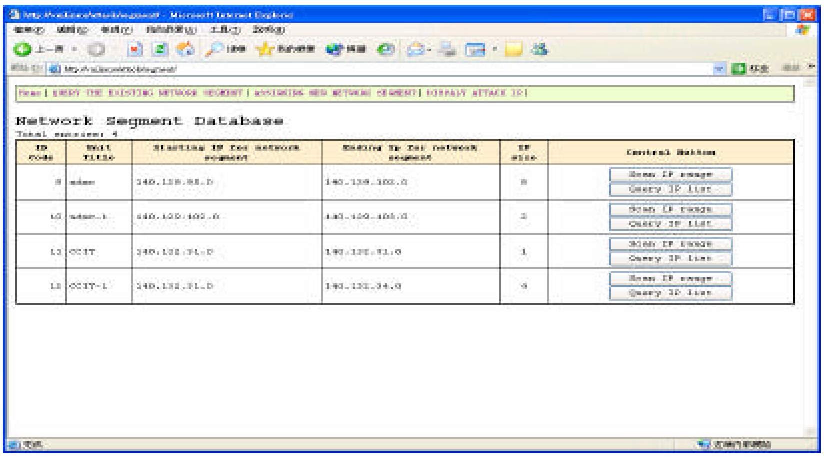


Denial of Service Attacks Platform

Attack Classification	Tools Library	Packet Combination	Attack Attribution	Characteristic	Operational Instruction
TCP	SYN Flood	TCP - IP	Socket Connection & Bandwidth Consumption	FLAG	Instruction
	FIN Flood	TCP - IP	Socket Connection & Bandwidth Consumption	FLAG	Instruction
	TCP Land	TCP - IP	Kernel Panic	O.S Loophole	Instruction
UDP	Fraggle	UDP - IP	Socket Connection & Bandwidth Consumption	Echo	Instruction
	UDP Land	UDP - IP	Kernel Panic	O.S Loophole	Instruction
	UDP Flood	UDP - IP	Socket Connection & Bandwidth Consumption	Port 19	Instruction
ICMP	Smurf	ICMP - IP	Socket Connection & Bandwidth Consumption	Echo	Instruction
	Ping of Death	ICMP - IP	Kernel Panic	O.S Loophole	Instruction
IP	IP Fragmentation	TCP - IP	Kernel Panic	O.S Loophole	Instruction
	Last Fragmentation	UDP - IP	Kernel Panic	O.S Loophole	Instruction

IP Scanner

Figure 6: Prototype of the DoS Attack Platform



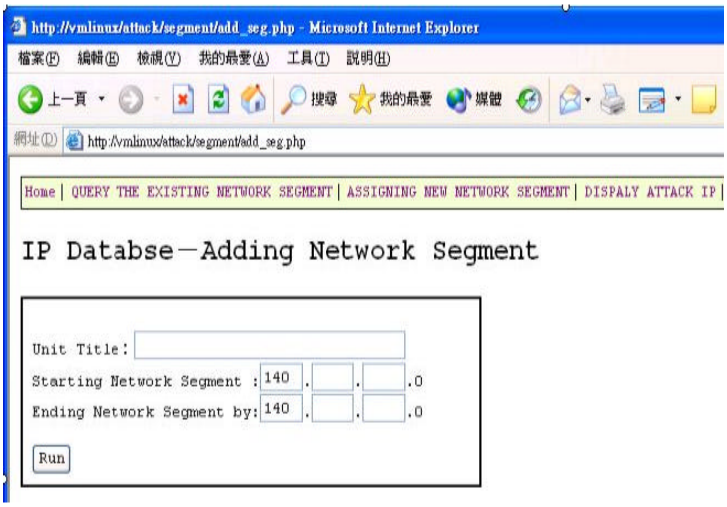
Home | QUERY THE EXISTING NETWORK SEGMENT | ASSIGNING NEW NETWORK SEGMENT | DISPLAY ATTACK IP |

Network Segment Database

Total entries: 4

ID Code	Unit Title	Starting IP for network segment	Ending Ip for network segment	IP size	Control Button
8	admin	140.128.88.0	140.128.102.0	8	Scan IP range Query IP list
10	admin-1	140.120.102.0	140.120.105.0	2	Scan IP range Query IP list
12	CCIT	140.128.31.0	140.128.31.0	1	Scan IP range Query IP list
13	CCIT-1	140.128.31.0	140.128.34.0	4	Scan IP range Query IP list

Figure 7: Main Operational Page of a Scanning Sub-System


http://vmlinux/attack/segment/add_seg.php - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D)
http://vmlinux/attack/segment/add_seg.php

Home | QUERY THE EXISTING NETWORK SEGMENT | ASSIGNING NEW NETWORK SEGMENT | DISPALY ATTACK IP |

IP Databse—Adding Network Segment

Unit Title：

Starting Network Segment ：140 . . .0

Ending Network Segment by:140 . . .0

Run

Figure 8: IP Range Assignment of a Scanning Sub-System

Scanning Operational Instructions

Step 1 : Using the left key of the mouse, click on the “IP Scanner” button which is located at the central bottom on the web-based central control panel. After this click, a new web page will show on the screen.

Step 2 : Adding a new IP range (segment) to be scanned by using the left key of the mouse, click on the “Assigning New Network Segment” button which is located at the left side of the top bar. Once you click on the “Assigning New Network Segment” button, another new web page will show on the screen.

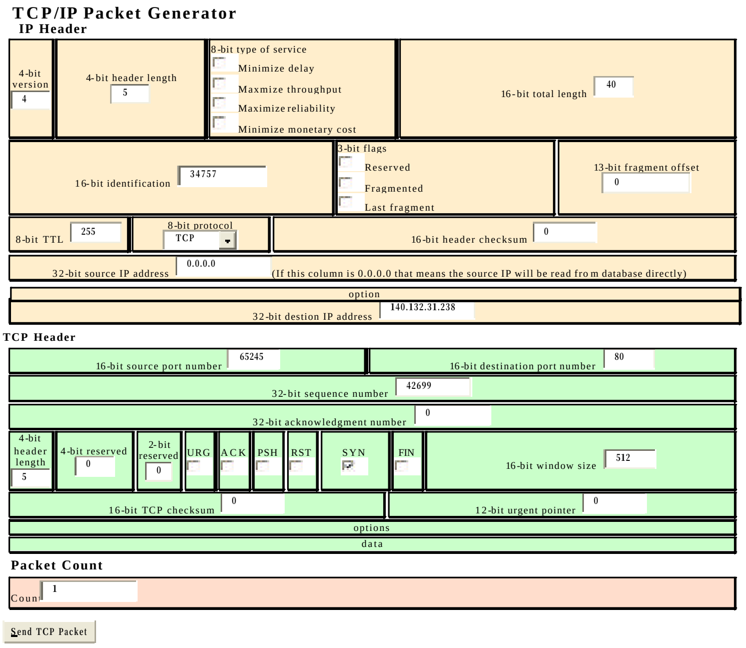
Step 3 : Key in the unit title at your convenience and key in the related IP range you want to scan for the unit title.

Step 4 : Using the left key of the mouse, click on the “Run” button to finish this process.

Step 5 : If you want to use the existing IP range listing in the “Assigning New Network Database”, you can use the left key of the mouse, click on the “Query IP list” button which is located in the “Control Button” column to display the latest IP scanning history.

Step 6 :You can use the left key of the mouse to click on the “Scan IP range” button to start the scanning process. The scanning data will be stored directly into the database.

Figure 9: An Example of Operational Instructions



TCP/IP Packet Generator

IP Header

4-bit version 4

4-bit header length 5

8-bit type of service
□ Minimize delay
□ Maxmize throughput
□ Maximize reliability
□ Minimize monetary cost

16-bit total length 40

16-bit identification 34757

3-bit flags
□ Reserved
□ Fragmented
□ Last fragment

13-bit fragment offset 0

8-bit TTL 255

8-bit protocol TCP

16-bit header checksum 0

32-bit source IP address 0.0.0.0 (If this column is 0.0.0.0 that means the source IP will be read fro m database directly)

option

32-bit destion IP address 140.132.31.238

TCP Header

16-bit source port number 65245

16-bit destination port number 80

32-bit sequence number 42699

32-bit acknowledgment number 0

4-bit header length 5

4-bit reserved 0

2-bit reserved 0

URG □ ACK □ PSH □ RST □ SYN ☑ FIN □

16-bit window size 512

16-bit TCP checksum 0

12-bit urgent pointer 0

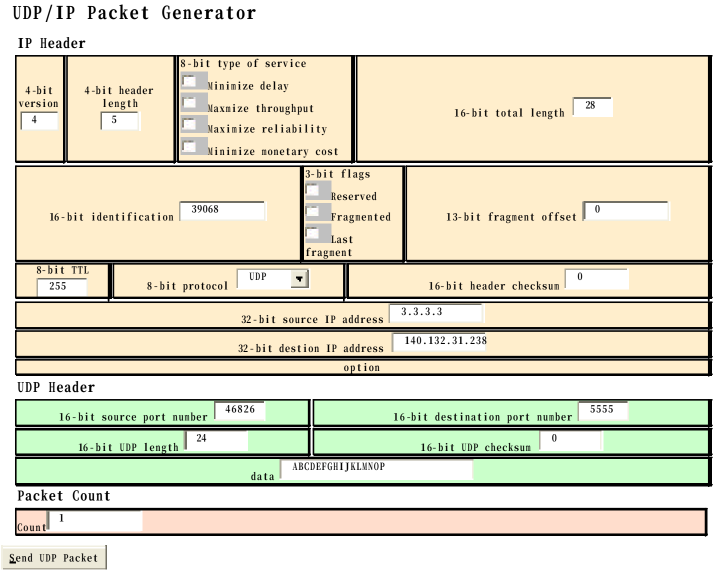
options

data

Packet Count

Count 1

Figure 10: Web Page of TCP/IP Packet Attack Tool



UDP/IP Packet Generator

IP Header

4-bit version 4

4-bit header length 5

8-bit type of service
□ Minimize delay
□ Maxmize throughput
□ Maximize reliability
□ Minimize monetary cost

16-bit total length 28

16-bit identification 39068

3-bit flags
□ Reserved
□ Fragmented
□ Last fragment

13-bit fragment offset 0

8-bit TTL 255

8-bit protocol UDP

16-bit header checksum 0

32-bit source IP address 3.3.3.3

32-bit destion IP address 140.132.31.238

option

UDP Header

16-bit source port number 46826

16-bit destination port number 5555

16-bit UDP length 24

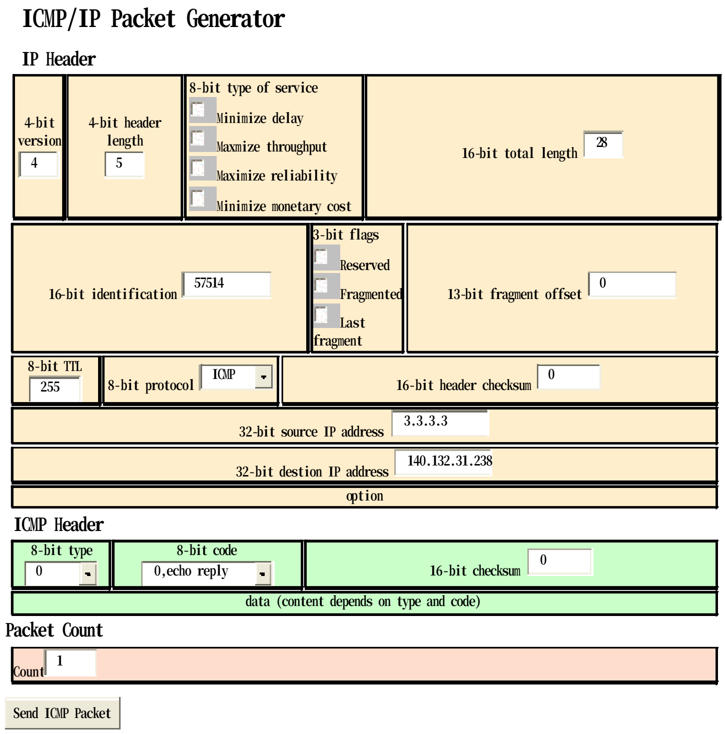
16-bit UDP checksum 0

data ABCDEFGHIJKLMNOP

Packet Count

Count 1

Figure 11: Web Page of UDP/IP Packet Attack Tool



ICMP/IP Packet Generator

IP Header

4-bit version: 4

4-bit header length: 5

8-bit type of service: □ Minimize delay □ Maxmize throughput □ Maximize reliability □ Minimize monetary cost

16-bit total length: 28

16-bit identification: 57514

3-bit flags: □ Reserved □ Fragmented □ Last fragment

13-bit fragment offset: 0

8-bit TTL: 255

8-bit protocol: ICMP

16-bit header checksum: 0

32-bit source IP address: 3.3.3.3

32-bit destion IP address: 140.132.31.238

option

ICMP Header

8-bit type: 0

8-bit code: 0,echo reply

16-bit checksum: 0

data (content depends on type and code)

Packet Count

Count: 1

Figure 12: Web Page of ICMP/IP Packet Attack Tool

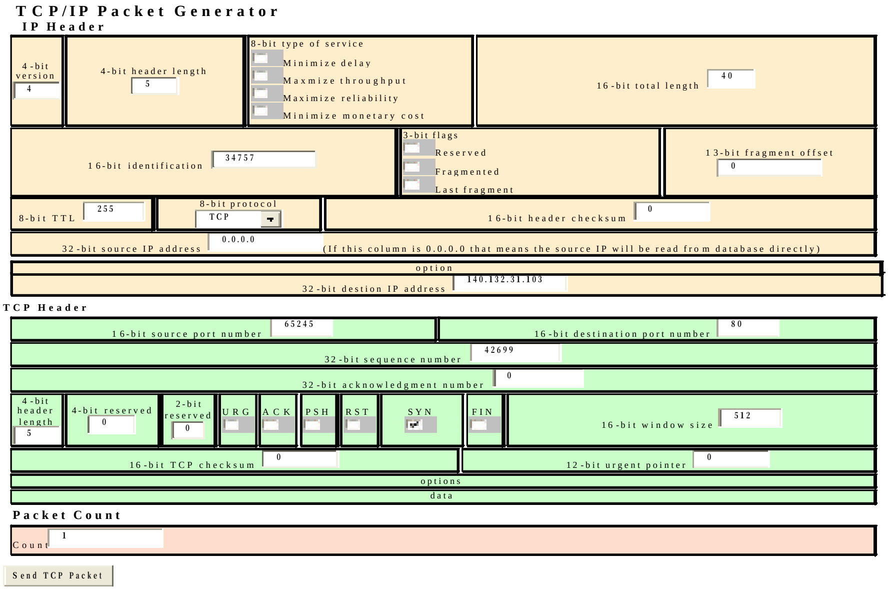
4.3 Verifications and Findings

4.3.1 Initial Verification on the Structured Framework of Integrated DoS Attack Platform

There are 3 major portions to the integrated DoS attack platform that are required to be verified: (1) reading data from input portion (2) scanning data being stored into database portion (3) database linking portion.

4.3.1.1 Reading Data From Input Portion

The integrated DoS attack platform has been tested to find out whether the attack program is able to read the data and parameters correctly from the input of the web page through the web-based central panel. The sniffer software is used to monitor the results. The final results indicate that the input data and parameters conform to the commands being executed by the attack program. The required data are entry into the columns of the packet generator which is shown in figure 13. The final output data is shown in figure 15. The related data in figure 13 are match to the data in figure 15.



TCP/IP Packet Generator

IP Header

4-bit version: 4
4-bit header length: 5
8-bit type of service: □ Minimize delay □ Maxmize throughput □ Maximize reliability □ Minimize monetary cost
16-bit total length: 40
16-bit identification: 34757
3-bit flags: □ Reserved □ Fragmented □ Last fragment
13-bit fragment offset: 0
8-bit TTL: 255
8-bit protocol: TCP
16-bit header checksum: 0
32-bit source IP address: 0.0.0.0 (If this column is 0.0.0.0 that means the source IP will be read from database directly)
option
32-bit destion IP address: 140.132.31.103

TCP Header

16-bit source port number: 65245
16-bit destination port number: 80
32-bit sequence number: 42699
32-bit acknowledgment number: 0
4-bit header length: 5
4-bit reserved: 0
2-bit reserved: 0
URG □ ACK □ PSH □ RST □ SYN ☑ FIN □
16-bit window size: 512
16-bit TCP checksum: 0
12-bit urgent pointer: 0
options
data

Packet Count

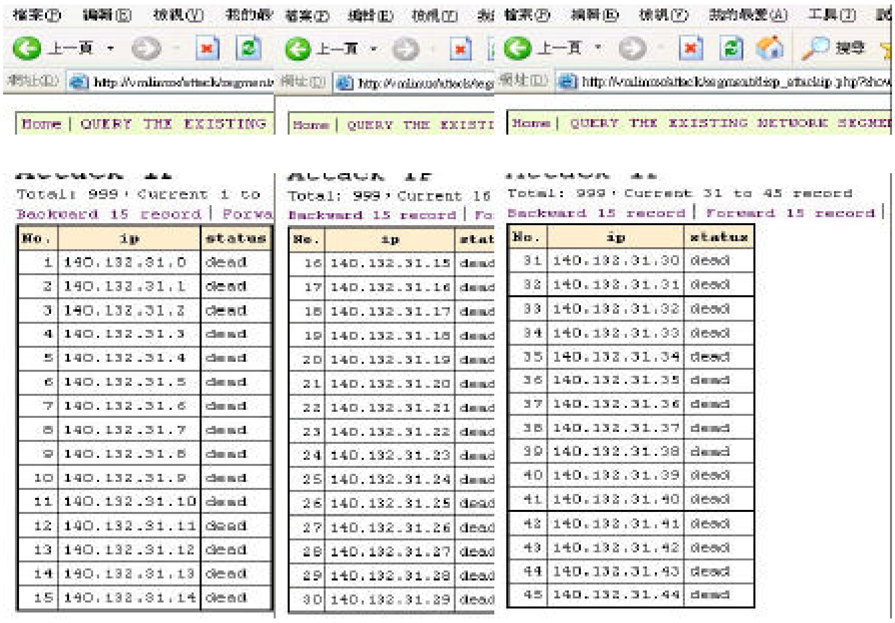
Count: 1

Send TCP Packet

Figure 13: An Example of Reading Data From Input

4.3.1.2 Scanning Data be Stored Into Database Portion

The scanning of the IP address by the scanning sub-system has been checked and conforms to the IP data in the database. The SQL command is used to verify the contents in the related table as a separate way for checking to find out if the data is correct. The results were correct. One example of scanning results is shown in figure 14. After the scanning process was finished, the IP addresses in the database are shown in figure 15. The IP addresses in the database prove that match to the results of IP scanning.



http://vnlinux/attack/segment/ip_attackip.php?show

Home | QUERY THE EXISTING NETWORK SEGMENT

Total: 999，Current 1 to
Backward 15 record | Forwa

No.	ip	status
1	140.132.31.0	dead
2	140.132.31.1	dead
3	140.132.31.2	dead
4	140.132.31.3	dead
5	140.132.31.4	dead
6	140.132.31.5	dead
7	140.132.31.6	dead
8	140.132.31.7	dead
9	140.132.31.8	dead
10	140.132.31.9	dead
11	140.132.31.10	dead
12	140.132.31.11	dead
13	140.132.31.12	dead
14	140.132.31.13	dead
15	140.132.31.14	dead

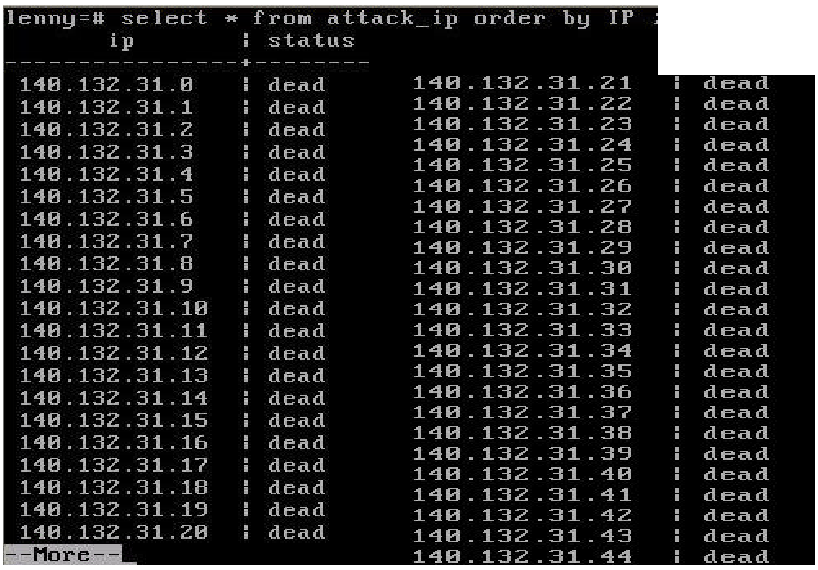
Total: 999，Current 16
Backward 15 record | Fo

No.	ip	stat
16	140.132.31.15	dead
17	140.132.31.16	dead
18	140.132.31.17	dead
19	140.132.31.18	dead
20	140.132.31.19	dead
21	140.132.31.20	dead
22	140.132.31.21	dead
23	140.132.31.22	dead
24	140.132.31.23	dead
25	140.132.31.24	dead
26	140.132.31.25	dead
27	140.132.31.26	dead
28	140.132.31.27	dead
29	140.132.31.28	dead
30	140.132.31.29	dead

Total: 999，Current 31 to 45 record
Backward 15 record | Forward 15 record |

No.	ip	status
31	140.132.31.30	dead
32	140.132.31.31	dead
33	140.132.31.32	dead
34	140.132.31.33	dead
35	140.132.31.34	dead
36	140.132.31.35	dead
37	140.132.31.36	dead
38	140.132.31.37	dead
39	140.132.31.38	dead
40	140.132.31.39	dead
41	140.132.31.40	dead
42	140.132.31.41	dead
43	140.132.31.42	dead
44	140.132.31.43	dead
45	140.132.31.44	dead

Figure 14: An Example of a Scanning Result



```
lenny=# select * from attack_ip order by IP ;
       ip        | status
-----------------+--------
 140.132.31.0    | dead       140.132.31.21   | dead
 140.132.31.1    | dead       140.132.31.22   | dead
 140.132.31.2    | dead       140.132.31.23   | dead
 140.132.31.3    | dead       140.132.31.24   | dead
 140.132.31.4    | dead       140.132.31.25   | dead
 140.132.31.5    | dead       140.132.31.26   | dead
 140.132.31.6    | dead       140.132.31.27   | dead
 140.132.31.7    | dead       140.132.31.28   | dead
 140.132.31.8    | dead       140.132.31.29   | dead
 140.132.31.9    | dead       140.132.31.30   | dead
 140.132.31.10   | dead       140.132.31.31   | dead
 140.132.31.11   | dead       140.132.31.32   | dead
 140.132.31.12   | dead       140.132.31.33   | dead
 140.132.31.13   | dead       140.132.31.34   | dead
 140.132.31.14   | dead       140.132.31.35   | dead
 140.132.31.15   | dead       140.132.31.36   | dead
 140.132.31.16   | dead       140.132.31.37   | dead
 140.132.31.17   | dead       140.132.31.38   | dead
 140.132.31.18   | dead       140.132.31.39   | dead
 140.132.31.19   | dead       140.132.31.40   | dead
 140.132.31.20   | dead       140.132.31.41   | dead
--More--                      140.132.31.42   | dead
                              140.132.31.43   | dead
                              140.132.31.44   | dead
```

Figure 15: An Example of Verification on the Scanning Data Being Stored Into the Database

4.3.1.3 Database Linking Portion

The integrated DoS attack platform also has been verified to find out if the attack program is able to get data from the database correctly. The contents in the database have been checked and were found to be consistent with the data be used by the attack programs. One example of the database linking test is shown in figure 16. The source IP addresses in figure 16 are match to the IP addresses in figure 15. This result proves that the database link with the attack programs sub-system is workable.

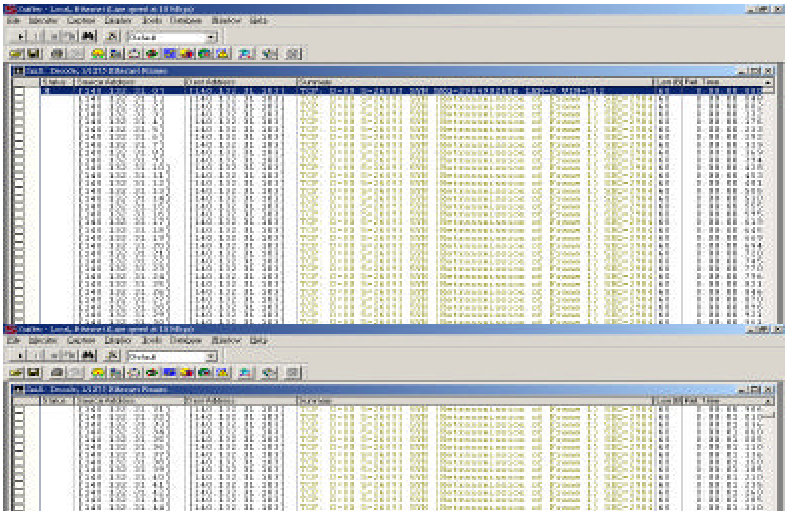


Figure 16: An Example of Verification on Database Linking and Reading Data From the Input

4.3.2 Verification and Findings From Theory of Network DoS

According to the RFC, implementation from the operating system, some loopholes already were used for different purposes. As the experimental verification process goes on, there are several loopholes that should be carefully checked. These loopholes are highlighted here. During this verification process, new types of loophole can also be found. All these loopholes are categorized, verified and summarized as follows:

● TCP/IP Three Way Handshake Category:

1. SYN Flood: The SYN flood theory was successfully implemented as tool for the DoS attack platform. It is also found that the different source IP will make a different effect to the target host. If the source IP that filled with spoofed packet that is live which means the IP is used by some other host on-line, this live IP will send a packet with an RST flag to the targeted host immediately. This action will terminate the holding process from the target host. So the SYN flood attack will not take advantage on this situation unless the source IP on the spoofed packet is a legitimate IP but its host is not on-line or dead. In this situation, the target host will not terminate this handshake process until it reaches the timeout setting. One other finding is to use the private IP address as the spoofed source IP. It is found these kind of spoofed packets do not have any impact on the targeted host. This phenomenon is caused by the current router does not relay any spoofed packet which using a private IP as the source IP address. One major challenge countered during the implementation phase is how to spoof the source IP and to predict the correct checksum for filling into the spoofed packet. Based on the RAW Socket, the spoofed source IP and checksum can be programmed directly by the coding. Each SYN packet that is sent out will make the target host response to it but must wait for a while before the spoofed packet can be dropped. Once the number of spoofed SYN packets reaches a certain level in a short time, it will create a DoS effect. The probability of success to take down a target system will depend on the queue size and timeout setting from the targeted operating system. The characteristics of the source IP being live or dead causes a different effect when launching the SYN flood attack.
2. FIN Flood：This is a brand new innovation to be developed as one kind of tool for the DoS attacks. It seems that no paper has mentioned this before, but it can be proven to be effective. This assumption is based on the theory in figure 2.3. This innovation was successfully implemented as one tool that can be used from the

integrated denial of service platform. The characteristics of the source IP being live or dead causes a different effect when launching the FIN flood attack. The performance of the FIN flood attack is less than the SYN flood attack, but it will be a useful tool while the firewall setting the rule to reject the unknown SYN connection.

- Spoofed Broadcast Category:

  1. Smurf: Usually the broadcasts are typically used for network diagnostic purposes. If the broadcast address is used as a destination IP, the source IP be filled with the target host for the spoofed ICMP packet. It will have a great impact for the target host. The Smurf is successfully implemented as a tool for the integrated DoS platform. It was found the method of broadcasting was bounded to number of hosts in the subnet. This result is caused by the most current router which does not support transmitting any broadcast addresses for another subnet. A better method was developed and will be addressed in paragraph 4.4.
  2. Fraggle: The Fraggle is also taking the advantage of broadcast address. The major difference between the Smurf and Fraggle is that the Fraggle uses UDP protocol instead of ICMP protocol. It was found the method of broadcasting was bounded to number of hosts in the subnet. This result is caused by the most current router which does not support transmitting any broadcast addresses for another subnet. A better method was developed and will be addressed in paragraph 4.4.

- Kernel Resource Category:

  1. Land: The land attack is basically to use the same IP address and port number for both of source and destination target host. This tool is successfully implemented. In this way, the target host will have kernel panic. During the verification process, it is found that the current operating systems have solved this kind of problem. The only operating system that still can be impacted by this attack is the Windows 95 operating system without patch or an early Windows version.
  2. Ping of Death: The ping of death utilizes large data in the oversized 65530 bytes datagram to launch the DoS attack. This tool is successfully implemented. The testing results indicate that the ping of death is a useful tool to freeze the Windows 2000 operating system without patch or an early Windows version.

4.4 Revision of Integrated DoS Attack Platform

4.4.1 Issues Statement

There are two issues that were noticed during the implementation of the prototype on the integrated denial of service attack platform. These issues are listed as follow:

The dead IP to be used as the spoofed source IP is dynamically changed and is not in a static status. This situation is based on the dead IP that will change into a live status when the computer which has the legitimated IP is connected to the Internet. Another issue is the method of broadcasting was bounded to number of hosts in the subnet. This result is caused by the most current router which does not support transmitting any broadcast addresses for another subnet.

4.4.2 Revision

The revised integrated denial of service platform is to enhance this issue. Here is the resolution that be proposed.

The resolution is based on the IP data from the history of the IP scanning process. If the scanning sub-system is used to scan the latest IP status before launch the DoS attack, it may not absolutely solve this problem, will make the spoofed source IP more reliable.

As stated in the previous paragraph, the broadcast of Smurf is bounded to the number of hosts in the subnet. The new method is to use the live spoofed IP instead of using the broadcast IP. With this change on the spoofed IP, the effect of DoS attack will be enhanced by controlling the number of hosts. The integrated DoS attack platform has improved these 2 issues by adding a new operational procedure and changing the way to launch the Smurf, Fraggle attacks.

5. Conclusions and Recommendations

5.1 Conclusions and Contributions

This paper shows how to build an integrated denial of service platform starting with a depth of study on the network theory loopholes. There are many DoS software tools being tested and modified as necessary. It also goes through the verification process that makes sure the concept of structured framework for the integrated DoS platform is constructed correctly. The framework for an integrated DoS platform is not only proposed, but successfully implemented in study process. Based on the prototype of DoS attack platform, the evaluation of tools has been accomplished. It provides a more flexible and effective way to control the contents of network packets. The primary know-how to build this integrated DoS platform is to combine the techniques of database, web page, and network programs into a linking format of different types of packet generators for launching a variety of DoS attacks. The final product of integrated DoS attack platform creates a tremendous advantage for the network administrator to better know the characteristics of DoS.

The major contributions of this thesis are summarized in the following points:

- Constructing a web-based DoS attack platform for the network administrator to implement the denial of service as part of network safety testing.
- To study various DoS theories and associated tools, process the verifications to develop a new way of network DoS attack.
- Providing the DoS attack platform model to use as a reference usage in the information force.

5.2 Recommendations and Future Work

Network security has become a serious issue because of the computers being in every corner of our society. Based on past experience, the general computer user is not familiar with the network security problem. After a depth of academic research on the network security arena, computer users should be very concern with this issue. In order to enhance network security, a full function network attack platform should be developed and used to test any weak points existing in computer systems when connected to the Internet. The recommendation in this thesis is to use the integrated DoS attack platform for further extending development for better understanding the network security issue. This recommendation drives the direction for future work using this paper. The future work of this paper is stated as follows:

Although the integrated DoS attack platform is capable to launch various types of DoS attacks in the format of TCP, UDP, IP, ICMP packets, there are still other types of packet being used by the router, the gateway, …etc. In theory, if there are more packet generators available, the more new types of network attack can be implemented. The denial of service attack platform is built upon the packet generator basis. Therefore, this integrated DoS attack platform can be used as a foundation layer to extend developing further research in the network testing arena. On the other hand, the wireless network is now popular within our society. To extend the integrated DoS attack platform into the wireless network will also be a fertile field to discover. The future works can be focused on these 2 subjects for further research.

BIBLIOGRAPHY

[1] Andrew S.T., Computer Networks, 3 rd Ed, Prentice-Hall, 1996.

[2] Computer Coordination Center., "CERT Advisory CA-96-26 Denial- of-Service Attack via pings", http://www.cert.org/advisories /CA-1996 -26 .html", Dec. 1996. - visited 20.5.2001.

[3] Computer Coordination Center, "CERT Advisory CA-97-28 IP Denial- of-Service Attacks, http://www.cert.org/advisories/CA-1997-28.html", Dec. 1997. - visited 20.5.2001.

[4] Computer Coordination Center, "CERT Advisory CA-2000-01 Denial- of-Service Developments, http://www.cert.org/advisories/CA-2000- 01.html", Jan. 2000. - visited 20.5.2001.

[5] Computer Coordination Center, "CERT Advisory CA-1998-13 Vulnerability in Certain TCP/IP Implementations http://www.cert. org/ advisories/CA-1998-13.html", Dec. 1998. - visited 20.5.2001.

[6] Chen Y.W., "Study on the prevention of SYN flooding by using traffic policing", IEEE/IFIP NOMS, pp. 593 -604, 2000.

[7] Elliot J., "Distributed denial of service attacks and the zombie ant effect", IT Professional, pp. 55-57, Mar./Apr. 2000.

[8] Ferguson P., Senie D., "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Jan. 1998.

[9] Frank Kargl, Joern Maier, Michael Weber, "Protecting Web Servers from Distributed Denial of Service Attacks", The Tenth International World Wide Web Conference, ACM, May 2001.

[10] Fulp E., Zhi Fu, Reeves D.S., Wu S.F., Xiaobing Zhang, "Preventing denial of service attacks on quality of service", DARPA Information Survivability Conference & Exposition II, pp. 159 -172, 2001

[11] Gregg D. M., Blackert W. J., Heinbuch D.V., Furnanage D., "Assessing and quantifying denial of service attacks", IEEE MILCOM: Communications for Network-Centric Operations, pp. 76-80, 2001.

[12] Harris B., Hunt R., "TCP/IP security threats and attack methods", ELSEVIER Computer Communications, Feb. 1999.

[13] Lau F., Rubin S. H., Smith M. H., Trajkovic L., "Distributed Denial of Service Attacks", IEEE International Conference on System, Man, and Cybernetic, 2000.

[14] Momjian B., PostgreSQL Introduction and Concepts. Addison—Wesley., Nov. 2000.

[15] Roger M. N., "Denial of Service", Communications of the ACM, ACM, Nov. 1994.

[16] SecurityFocus Corporation Site, http://www.securityfocus.com - visited 25.3.2001.

[17] Stuart Mcclure, Joel Scambray, George Kurrt, Hacking Exposed: Network Security Secrets and Solutions, Third Edition, Osborne/McGraw-Hill, Apr. 2001.

[18] Stevens W. R., Advanced Programming in the Unix Environment, Addison—Wesley., Sep. 2000.

[19] Stevens W. R., TCP/IP Illustrated, Volume 1 The Protocols, Addison—Wesley, Oct. 1999.

[20] Stevens W. R., TCP/IP Illustrated, Volume 3 TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison—Wesley, Jan. 1996.

[21] Stevens W. R., Unix Network Programming Volume 1, Prentice-Hall, Jul. 1998.

[22] Stevens W. R., Unix Network Programming Volume 2, Prentice-Hall, Jul. 1998.