Attacking Test and Online Forensics in IPv6 Networks

LIU Wu, DUAN Hai-xin, LIN Tao, LI Xing, WU Jian-ping

Network Research Center of Tsinghua University
Beijing, P.R. China
liuwu@cernet.edu.cn

Abstract: Although IPv6 protocol has considered and implemented more security mechanisms compared with IPv4, there are still many security threatens in IPv6 Networks. Being one of the key protocols in IPv6, the Internet Control Message Protocol (ICMPv6) suffers from severe security risks. In this paper we construct an IPv6 attacking test system ATS_ICMP_6 exploiting the ICMPv6 Unreachable Message, which shows that the security of IPv6 protocol is still very weak. In the other hand, we has designed and implemented a network forensics prototype 6Foren in IPv6 environment based on the protocol analysis technology, its functions include packet capture, data reconstruct and messages replay etc. the 6Foren can be used as the online digital forensics which support the online forensic of HTTP, FTP, SMTP and POP3 protocols.

1 Introduction

As the rapid development of Internet applications, the Internet Protocol version 4 (IPv4) [10] addresses will soon be exhausted and there are more and more applications running in the next generation Internet based on the Internet Protocol version 6 (IPv6) which boosts the deployment of IPv6 networks [5].

IPv6 protocol (RFC2460) [1] inherits all the merits from IPv4 and adds some new characters, which will greatly improve transmission efficiency. For example, IPv6 changes some fields in the IPv4 main header and extension headers. In IPv4, all nodes can fragment the packets. In the mean while IPv6 also enhanced security in IPv6.

But, as the wide deployment of Internet Protocol version 6 (IPv6) [1] networks, its vulnerabilities have become visible. IPv6 deployment raises security issues for both those not yet managing IPv6 networks as well as those who are. Network attackers have successfully used IPv6 to evade the defenses erected against undesired network traffic [2][3][4].

Recently, [11] awareness has been raised about several threats against the TCP [6] protocol in IPv6. These attacks are based on sending forged TCP segments to any of the TCP endpoints, requiring the attacker to be able to guess the four-tuple that identifies the connection to be attacked.

While these attacks were known by the research community, they were considered to be unfeasible. However, increases in bandwidth availability, and the use of larger TCP windows [12] have made these attacks feasible. Several general solutions have been proposed to either eliminate or minimize the impact of these attacks [13][14][15]. For protecting BGP sessions, specifically, a counter-measure had already been documented in [16], which defines a new TCP option that allows a sending TCP to include a MD5 [17] signature in each transmitted segment.

All these counter-measures address attacks that require an attacker to send spoofed TCP segments to the attacked host. However, there is still a possibility for performing a number of attacks against the TCP protocol, by means of ICMPv6 [7].

With the Internet Control Message Protocol (ICMPv6) [8], one could extrapolate the concept of "hard errors" [8] to ICMPv6 Type 1 (Destination Unreachable) codes 1 (communication with destination administratively prohibited) and 4 (port unreachable). Thus, any of these messages could elicit a connection abort.

For example, ICMPv6 defines the "Packet Too Big" (type 2, code 0) error message, that is analogous to the ICMP "fragmentation needed and DF bit set" (type 3, code 4) error message in IPv4. For IPv6 networks, intermediate systems do not fragment IP packets. Thus, there's an implicit "don't fragment" bit set in every IPv6 datagram sent on a network. Therefore, hosts do not treat ICMPv6 "Packet Too Big" messages as hard errors, but use them to discover the MTU of the corresponding internet path, as part of the Path MTU Discovery mechanism for IPv6 [9].

The Host Requirements RFC [3] states that a TCP instance should be notified of ICMPv6 error messages received for its corresponding connection.

In order to allow ICMPv6 messages to be demultiplexed by the receiving host, part of the original packet that elicited the message is included in the payload of the ICMPv6 error message. Thus, the receiving host can use that information to match the ICMPv6 error to the instance of the transport protocol that elicited it.

Neither the Host Requirements RFC nor the original TCP specification [6] recommends any security checks on the received ICMPv6 messages. Thus, as long as the ICMPv6 payload contains the correct four-tuple that identifies the communication instance, an attacker could send a spoofed ICMPv6 message to the attacked host, and, as long as he is able to guess the four-tuple that identifies the communication instance to be attacked, he can use ICMPv6 to perform a variety of attacks, such as DoS, DDoS, Man-In-The-Middle, Smurf, Redirect attack etc.

This paper aims to raise awareness of the use of ICMPv6 to perform a number of attacks against IPv6 networks, to show that IPv6 protocol is also not secure, to pay attention to the security problems of IPv6.

The field of computer forensics has become a critical part of legal systems throughout the world used for detecting attacks in IP networks. As early as 2002 the FBI stated that “fifty percent of the cases the FBI now opens involve a computer. However, the accuracy of the methods -- and therefore the extent to which forensic data should be admissible -- is not yet well understood. Therefore, we are not yet able to make the kinds of claims about computer forensics that can be made about other kinds of forensic evidence that has been studied more completely.

Computer forensics can be divided into two types: host based forensics and network based forensics [18]. The host based forensics is also called Software Forensics, which is mainly used to trace code to its authors [25]. Some computer scientists focus largely on the examination of file system data [20], whereas others also include the collection of data [19] [21][22][23][24] [26].

While in the other hand, there is very few forensic tools for network based forensics, especially for IPv6 networks.

As IPv6 protocol (RFC2460) header structure has changed greatly with that of IPv4 protocol, current IPv4 forensic tools could not meet the IPv6 forensic needs. So we need to design and implement forensic tools for IPv6 network security management.

This paper is organized as follows. In section 2, we describe the basic idea of ICMPv6 attack. The details on implementation of ICMPv6 attacks are described in section 3. Section 4 describes the 6Foren: Online Forensics in IPv6 Network. In section 5, we show two cases of ICMPv6 attacks and display the 6Foren system. Finally we present our conclusions in section 6.

2 IPv6 Attacking Test and Online Forensics Environment

To verify and test our IPv6 Attacking tools and Online Forensic system 6Foren, it needs a pure IPv6 network environment.

As seen in Fig. 1, the left side is the topology of the pure IPv6 attacking test bed A6TB which is an open attacking test bed. In A6TB we deploy some IPv6 attacking host and some IPv6 victim host which is used for the IPv6 attacking test. Both the attacking hosts and victim hosts are all pure IPv6 machines connected via CERNET2 which is also pure IPv6 Backbone network connecting all the Chinese educational organizations to USA, Asia and Europe IPv6 networks.

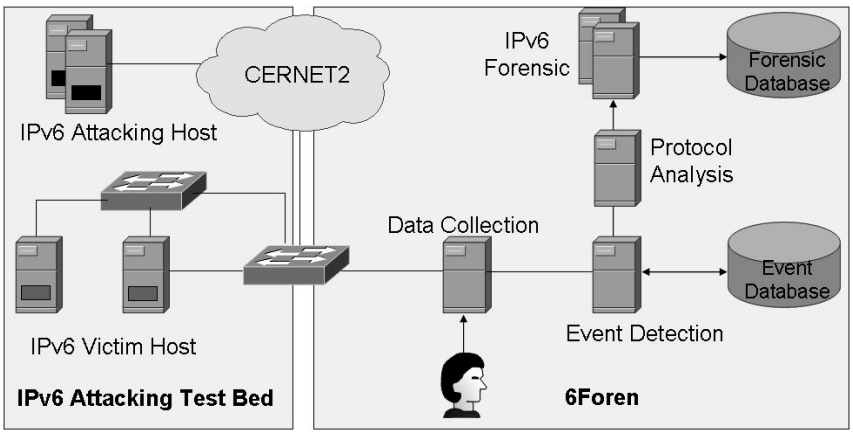

Fig. 1 The Topology of IPv6 Attacking Test Bed and 6Foren

As seen in the right of Fig.1, 6Foren is deployed near the key switch of the test bed A6TB to capture the attacking flow and then executing online forensic actions.

As seen in Fig. 2, in normal communication, when node V (Victim) want to visit node T (Target) which is out the V's LAN, packets from V to T is first delivered to the default router R1 (Router-1) in the LAN, and R1 will route V's packets to other routers and finally to T. in this case, packets from V to T are transmitted along the solid line shown in Fig. 2.

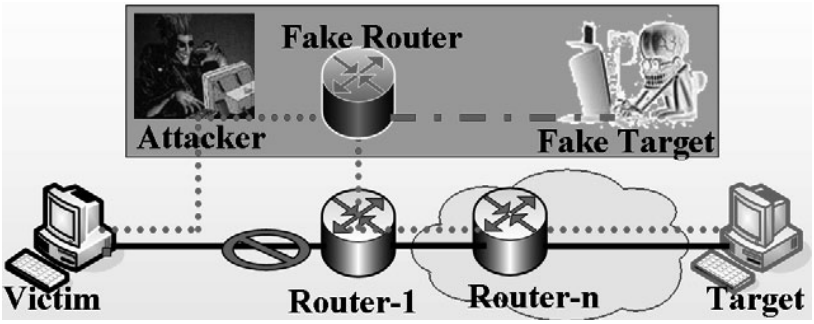

Fig.2 Basic Idea and Attacking Test Environment of ICMPv6 Attack

If A (Attacker) want to attack traffic from V to T, he will first detect the activity of V by sending an ICMPv6 Echo quest packet with bad IPv6 header parameter to T, if V is alive, A will then send an ICMPv6 Redirect Message to V which will redirect all V's packet from R1 to FR (Fake Router) which is illegally constructed by A. Finally, A can execute any attacking action to traffic from V.

In the following section, we will describe the attacking process in details.

3 IPv6 Attacking Test and Online Forensics Environment

In this section, we briefly summarize key techniques for IPv6 attacking test using ICMPv6 messages we combined for this research.

As seen in Fig. 3, the IPv6 Attacking Test System using ICMPv6 Messages (which is called ATS_ICMP_6) is mainly distributed in two logical hosts (Attacker and Fake Router), and consists of the following 6 functional modules:

Initialization: this module is mainly used to load some initial information used for ATS_ICMP_6, which include:

(1) Interface: network card used for the attacking system ATS_ICMP_6

(2) IPv6 Addresses of current legal default router, which includes both of the global IPv6 address and the link local IPv6 address

(3) MAC Address of current legal default router

(4) IPv6 Addresses of Attacker himself, which includes both of the global IPv6 address and the link local IPv6 address

(5) MAC Address of Attacker himself

(6) IPv6 Addresses of Fake Router, which includes both of the global IPv6 address and the link local IPv6 address

(7) MAC Address of Fake Router

Alive Detection: this module is used to detect whether the specific victim is now active in the network. In addition, it can also return the list of active hosts in the LAN.

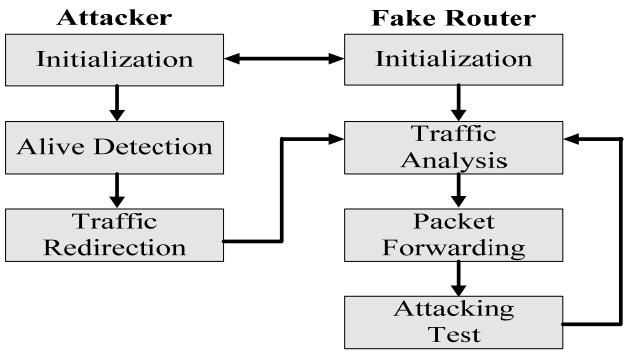

Fig.3 Structure and Functional Module of ATS_ICMP_6

Traffic Redirection: this module is used to change traffic from legal default router to the Fake Router further traffic analysis and attacking test. This module takes the key role in ATS_ICMP_6.

Traffic Analysis: When Fake Router starts working, this module is listening all traffic redirected from victims, used to change traffic from legal default router to the Fake Router further traffic analysis and attacking test. This module takes the key role in ATS_ICMP_6.

Packet Forwarding: This module is used to modify, drop or relay specific traffic according to the requirement of specific Attacking Test module.

Attacking Test: Based on the modules described above, this module is used to test some specific type of IPv6 attacking. Before test, this module will send the attacking policy such as attacking Type, Code and other parameters which is used for IPv6 attacking test.

Note: we must state that, in most cases the logical hosts Attacker and Fake Router can be deployed in one physical machine.

In the following sub sections, we will introduce some of the key modules used in this system.

3.1 Alive Host Detection

Before attacking, the attacker must first detect the activity of the victim host in the network.

To do this, the attacker can send an ICMPv6 message with bad parameter to the victim, when receiving this bad message, the victim will send back a Parameter Problem message to the attacker, according to which, the attacker knows that the victim is now "alive". Fig. 4 shows the Alive Host Detection algorithm.

Process Alive_Host_Detection

INPUT: V -- IPv6 Address of Victim, if V=NULL, then V="FF02::1", the multicast address

OUTPUT: The alive host list AHL: if V=NULL, AHL include all the active host in the LAN

BEGIN

Construct an ICMPv6 Ping Request message MS (Type=128, Code=0) with bad parameter

Send MS to V

Start the Packet Filter Process and set the filter="ip6 and dst V" to capture packets return from V with Parameter Problem Messages

If return TRUE, then V is alive

Else V is not alive

END

Fig.4 The algorithm of Alive Host Detection

3.2 Start the Packet Forwarding Function

Before attacking, especially the traffic redirection attacking, the attacker must start the packet forwarding function in the fake router to forward the redirected traffic to where the attacker wants it to be.

```
int Start_Packet_Forwarding(char* interface, char * policy)
{
        sprintf(cmd,"echo 1 > /proc/sys/net/ipv6/conf/%s/forwarding",interface);
        system(cmd);
        system("echo 1 > /proc/sys/net/ipv6/conf/default/forwarding");
        system("echo 1 > /proc/sys/net/ipv6/conf/all/forwarding");
        Forwarding_traffic(policy);
        return 0;
}
```

Fig.5 Packet Forwarding Function

Fig. 5 shows the packet forwarding function which can relay the traffic from victims to the “right” place after being redirected from default router to the fake router.

The first four lines in Start_Packet_Forwarding is used to open the packet forwarding function in the kernel of the Fake Router to forwarding all traffic flowing across it.

The function Forwarding_traffic will relay, modify or drop specific traffic according to the policies defined by the parameter “policy” which is transmitted by specific attacking test module.

3.3 Traffic Redirection

After the detection of alive host, now the attacker can use ICMPV6 Route Redirect Message to redirect the V’s traffic to FR which is the faked router constructed by the attack for further attacking actions.

The algorithm is shown in Fig. 6.

To redirection of the victim, the attacker must first construct some type of ICMPv6 Messages:

(1) ICMPv6 Neighbor Advertisement Message NAM (Type=136, Code=0)

(2) ICMPv6 Router Advertisement Message RAM (Type=134, Code=0)

(3) ICMPv6 Router Redirection Message RRM (Type=137, Code=0)

Second, these messages must be sent to the LAN in a proper period to notify the victim that the default router has been changed to the fake router.

To ensure the successful attack, the broadcast period is key factor.

Note: if V=NULL, the fake default route information will be planted in every hosts in the LAN, which means that all the Traffic in the LAN will be first redirected to the fake router.

```
Process Redirect_Traffic_Static_IPv6
INPUT: V -- IPv6 Address of Victim, if V=NULL, then V="FF02::1", the multicast address
OUTPUT: The alive host list AHL: if V=NULL, AHL include all the active host in the LAN
BEGIN
  Initial: routerip =get_default_router();// get current default router's IPv6 address
   victimmac =get_mac(V);// get V's MAC address
  Start_Packet_Forwarding();//start the packet forwarding function
  Construct an ICMPv6 Neighbor Advertisement Message NAM (Type=136, Code=0)
  Construct an ICMPv6 Router Advertisement Message RAM (Type=134, Code=0)
  Construct an ICMPv6 Router Redirection Message RRM (Type=137, Code=0)
  while (1) {
        Send NAM to V
        Send RAM to V
        Send RAM to V
        Sleep(period)
  }
END
```

Fig.6 Redirect Traffic for Host with Static IPv6 Address

We can see from Fig. 7 that, seconds after starting Redirect_Traffic_Static_IPv6, one more router information:

"2001:da8:200:9002:21d:9ff:fe1c:9bff dev eth0 lladdr 00:1d:09:1c:9b:ff router REACHABLE"

has been planted in the victim's router table, which shows that now the default router is "2001:da8:200:9002:21d:9ff:fe1c:9bff" that is the fake router's IPv6 address constructed by the attacker.

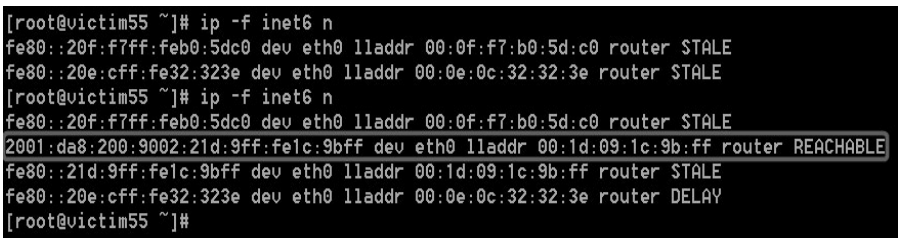

Fig. 7 Route Information Before Traffic Redirection v.s Route Information After Traffic Redirection in Victim

3.4 Attacking Test

Actually, this module includes two parts: the server side and client side.

The server side is deployed in the fake router, its main function is receiving and process attacking parameters and policy, then sends them to the Traffic Analysis module.

The client side is deployed in another machine, it is mainly used for attacker(s) to:

(1) fill in the attacking command and relative parameters

(2) control the attacking process

(3) adjust attacking parameters while attacking

(4) stop the attacking process

(5) display the attacking results

4 6Foren: Online Forensics in IPv6 Network Environment

Fig. 8 shows the basic structure and main modules for IPv6 network based forensics which we called it 6Foren. 6Foren mainly includes the following modules: Data Collector, TCP Stream Classification, TCP Message Reconstruction, Application Protocol Parser Manager and Online Evidence Display. We will describe these modules in detail.

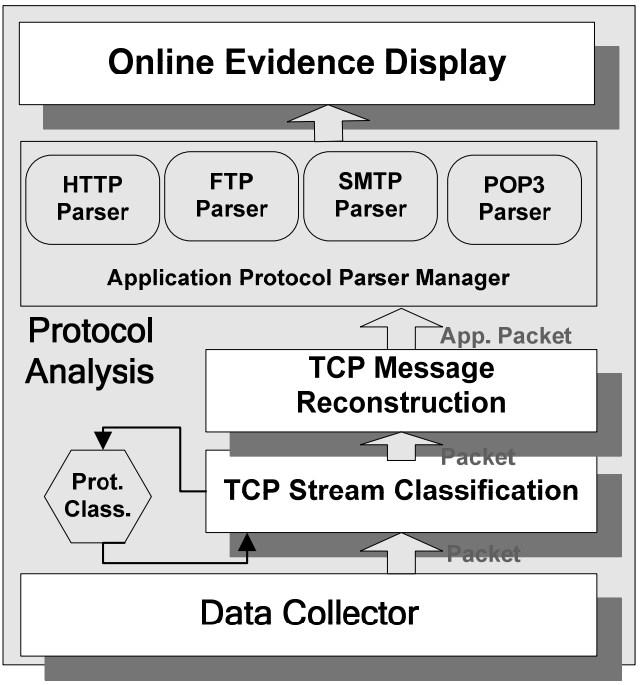

Fig.8 Structure and Main Module of 6Foren

4.1 Data Collector

To obtain accurate online forensic analysis result, we must first capture proper packets in which the attacking flow is transmitted.

In our 6Foren, we will take two different data collecting mechanisms to ensure the accurate data collection.

In normal condition, if we can control the entire network flow which means that the attacking flow can be "seen" by us, we can just mirror the network flow containing the attacking packets to a specific interface where we can easily collect the data.

But sometimes, we are not the administrator of the network and do not have the right get the network flow. In this case, we can redirect the network flow first to our data collector using the Traffic Redirection module described in § 3.3

4.2 TCP Stream Classification

When packet is captured, it must first be classified according to its TCP attribution, and the system needs to maintain a table to save the classification information of the TCP stream.

The TCP Stream Classification module must consider the following problems:

(1) The TCP stream table must save application layer information for this connection for further handling.

(2) The TCP Stream Classification should accurately recognize the begin and end of the TCP connection

(3) During the system running, the TCP stream table should be kept smaller

4.3 TCP Message Reconstruction

The main functions of the TCP Message Reconstruction module include:

(1) Reconstruct the IP packet with error arrival order

(2) Reproduce the session process of the communication sides

4.4 Application Protocol Parser Manager

To distinguish classify different kinds of application protocols, the Protocol Classification module of 6Foren inspects all captured packets and judge that whether it belongs to some protocol when transmitting. By adding and deleting elements of the TCP stream table, 6Foren dynamically obtain data in some TCP connection and then classify and reconstruct TCP packets to entirely save all the application protocol data. 6Foren will also parse file name, file type and contents etc. according to different protocol signatures. Fig. 6 shows the Flow Chart of Protocol Classification module in 6Foren.

(1) HTTP Protocol

In HTTP protocol, the client start to transmit session through the GET request packet in TCP connection, in the meanwhile the contents of the file will be sent to the client from the server side. 6Foren judge the start of the HTTP file transmission mainly by the GET signature in the traffic header (seen in Fig. 6), and then add the reverse TCP stream to the monitored TCP classification list, if the reverse TCP data has the “HTTP/*.* 200” header, then the TCP Packet Reconstruction module will save all the reverse TCP data.

(2) FTP Protocol

FTP protocol has two modes (seen in Fig. 6): PORT and PASV, which possess the signature PORT and PASV respectively in the starting of the FTP stream. As the FTP protocol negotiate data connection IP address and port number in the session, we must continuously listening the controlling connection for some times to get sufficient information, and also the FTP data can either be upload or download, so the implementation of FTP Forensic is very difficult.

In PORT mode, the data connection address and port can be directly gotten because they exist in the PORT command itself, while the RETR or STOR command exist in the next session of the same direction.

While in PASV mode, the data connection address and port exist in the 227 response packet, and RETR or STOR command is executed by client, so it needs multiple listening.

(3) SMTP and POP3 Protocol

POP3 packets and SMTP packets are similar. The POP3 packets begin with "Received", while the SMTP packets begin with "DATA" (in Outlook Express and Outlook) or "Data" (in Foxmail). The text and attachment of email will be transmitted in the same direction of the same TCP connection, so it can be easily captured.

4.5 Online Evidence Display

While the attacking event is detected, it will be recorded in the Attack Event Database for attack event replay in the law court.

In the mean while, the detected attacking event can be displayed in a new webpage for the online forensic.

5 Experimental Results

5.1 Start the IPv6 Attacking System ATS_ICMP_6

The IPv6 Attacking System ATS_ICMP_6 is implemented in Linux system with kernel version over 2.4. To simplify the operation of administrator and other tester, the server side has been registered as a Linux service, which will be started automatically when the operating system starting. When ATS_ICMP_6 starts, it will listen on port 8899 (which can be specified as other port).

The client side is implemented via web page. All the attacking test cases can be operated in browser anytime and anywhere.

In the following sub section, we will take two attacking cases as examples.

5.2 Case 1 ICMPv6 Error Message for DoS attack

As seen in Fig. 9, to start the Redirection Attack, the attacker execute the following steps:

(1) fills in the following items:

a) Redirection Source: the source that the packets will be illegally redirected

b) Redirection Target: the target that the packets will illegally redirected

c) Older Router: the current legal default router, which in normal case will forwarding traffic to legal target

d) New Router: the fake router which will execute the redirection attack

(2) click the “Start Attack” button

In this case, packets from victim54.vhost.edu.cn to www.cernet2.edu.cn via the default router router6.vhost.edu.cn will be first redirected to the fake router fakerouter6.vhost.edu.cn and then be leading to a fake target which is seen in Fig. 2.

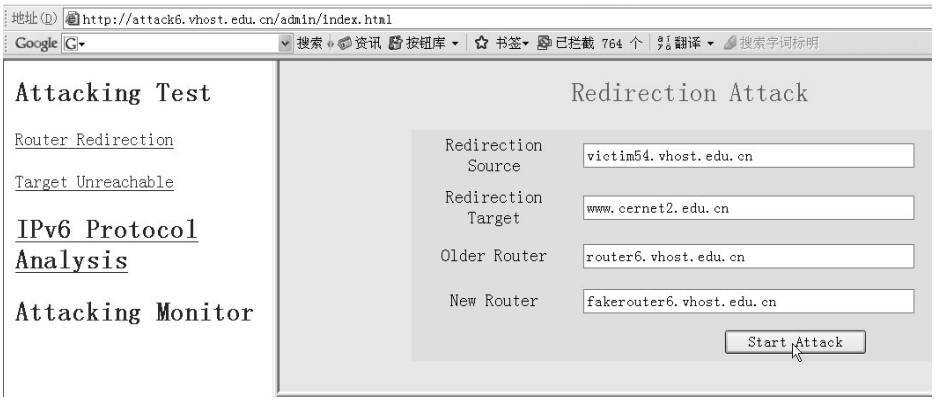

Fig. 9 The Redirection Attack

5.3 Case 2 ICMPv6 Destination Unreachable Attack

As seen in Fig. 10, to start the Destination Unreachable Attack, the attacker execute the following steps:

(1) fills in the following items:

a) Victim: the IPv6 address or DNS name of the attacked host

b) Target: the IPv6 address or DNS name that the victim will visit

c) Unreachable Type: an integer between 0 and 4 (seen in table 1) which will be used for the attack experiment

d) Unreachable Target Port: an integer which represents the target's port that the victim will connected to in the attack experiment

(2) click the "Start Attack" button

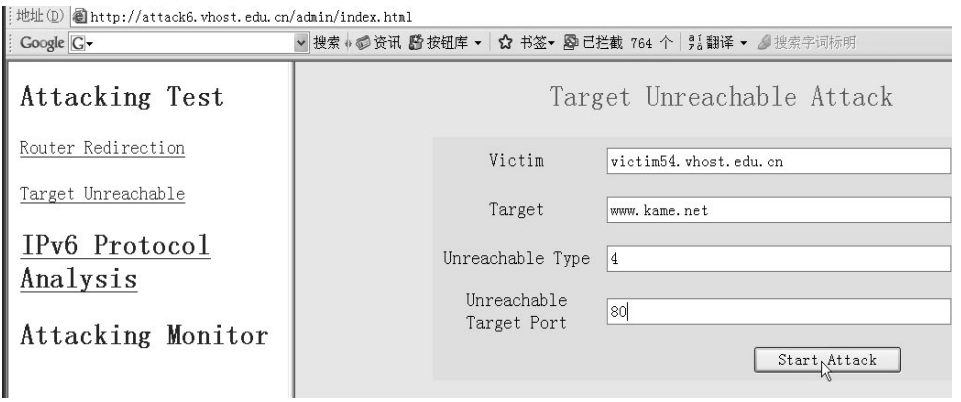

Fig. 10 The Target Unreachable Attack

In this case, before the attack, a user can visit any port of any host from victim54.vhost.edu.cn. But, after the attack, he will not visit the web service (port 80) in www.kame.net, but he can visit any other ports of this host and can visit any other hosts from victim54.vhost.edu.cn

In addition, either Victim or Target can be NULL if the Victim is NULL, it will attack all the hosts in the LAN, and if the Target is NULL, the Victim can not visit any other machine in the Internet.

5.4 Online Forensic for HTTP Protocol

As an example seen in Fig. 11, to take the online digital evidence by 6Foren, it should pass through the following 3 steps:

(3) We first send and IPv6 Route Deceive Attack by executing the following steps via HTTP protocol:

a) Redirection Source: the source that the packets will be illegally redirected

b) Redirection Target: the target that the packets will illegally redirected

c) Older Router: the current legal default router, which in normal case will forwarding traffic to legal target

d) New Router: the fake router which will execute the redirection attack

After clicking the "Start Attack" button, packets from victim54.vhost.edu.cn to www.cernet2.edu.cn via the default router router6.vhost.edu.cn will be first redirected to the fake router fakerouter6.vhost.edu.cn and then be leading to a fake target

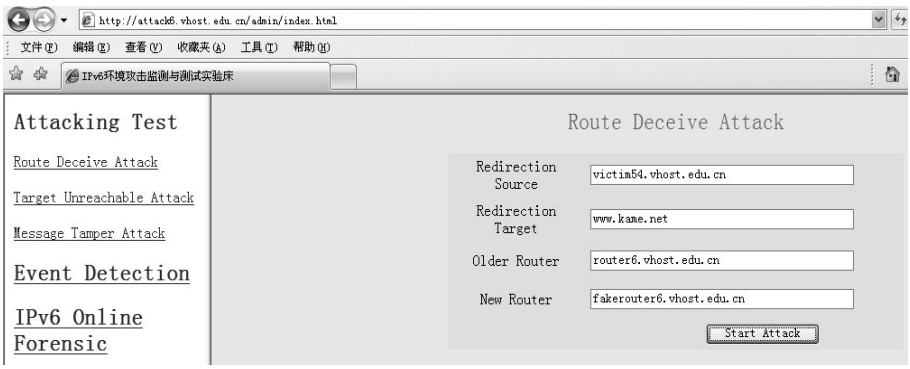

Fig. 11 Launch a Route Deceive Attack

(4) Attack Detection

Before the attacking is launched, the Event Detection daemon has been started to detect any attacks. As seen in Fig. 12, if click the "Event Detection" in the 6Foren system, it will link to the Event Detection webpage which displays the attacking event detected by 6Foren.

Fig.12 Route Deceive Attack Detection in 6Foren

(5) Online Evidence Display

When the the Event Detection module detect the attacking event, it will automatically open the Online Evidence Display webpage and open the original webpage that the attacker opened to launch the attacking, which can be seen in Fig. 13.

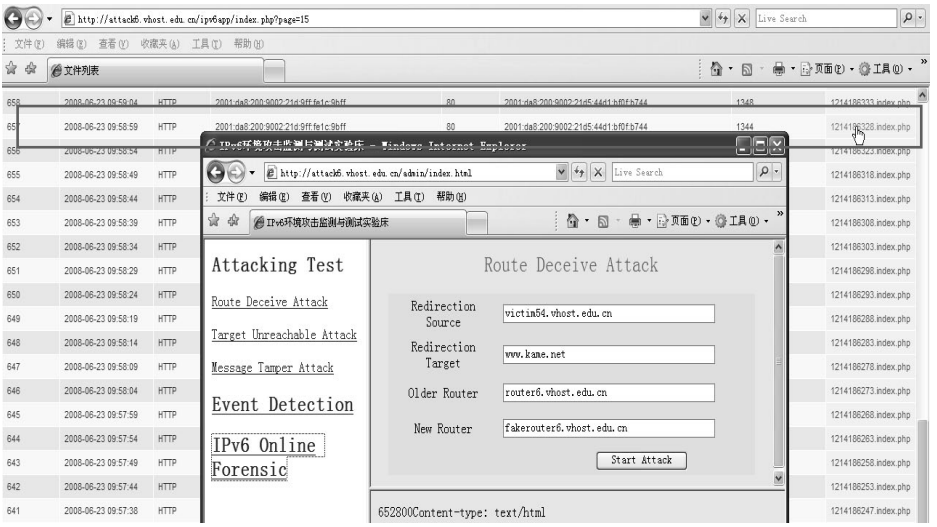

Fig.13 6Foren for HTTP protocol

As seen in Fig. 10, all the attacking events are logged into the IPv6 Forensic Database for Event Replay in courtroom, on the other hand (seen in the bottom webpage of Fig. 5), while the attack event is going on, the webpage will be displayed synchronized for Online Evidence Display (seen in the front webpage of Fig. 5).

5.5 Online Forensic for FTP Protocol

(1) Sending message with attacking signature via FTP protocol

As shown in Fig. 14, we send a PDF file named 6Foren_ftp.pdf with some attacking signature in the Attack Database

Fig. 14 FTP attacking

(2) Detect and Online Display the Attacking Evidence in Webpage

While the transmission of the attacking file, the Event Detection module successfully detected this malicious file and start the Online Forensic module to record and display the this attacking event, which can be seen in Fig. 15

Fig.15 6Foren for FTP protocol

5.6 Online Forensic for SMTP and POP3 Protocol

As seen in Fig. 16, we sent some malicious email via IPv6 SMTP email system Mail6 we specially developed for this project and then receive emails with Mail6.

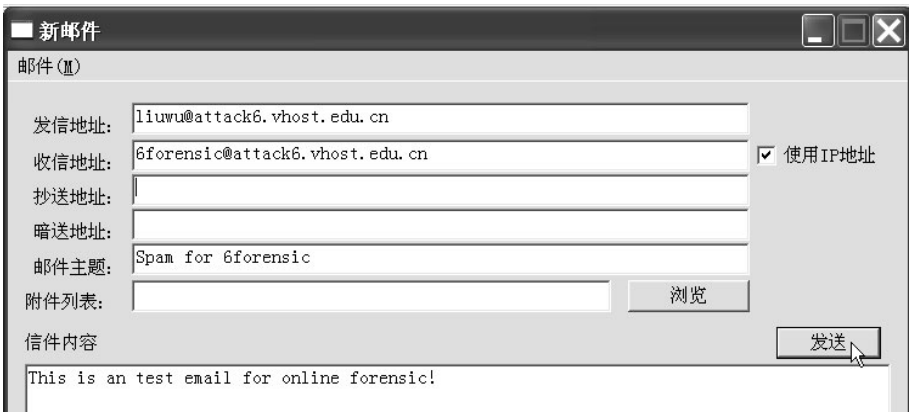

Fig. 16 Sending Malicious Email via IPv6 SMTP Email System

Seen from Fig. 17, while the attacker is sending and/or receiving emails, 6Foren will detect corresponding actions and start the Online Forensic module to record and display the original email that is being sent and received.

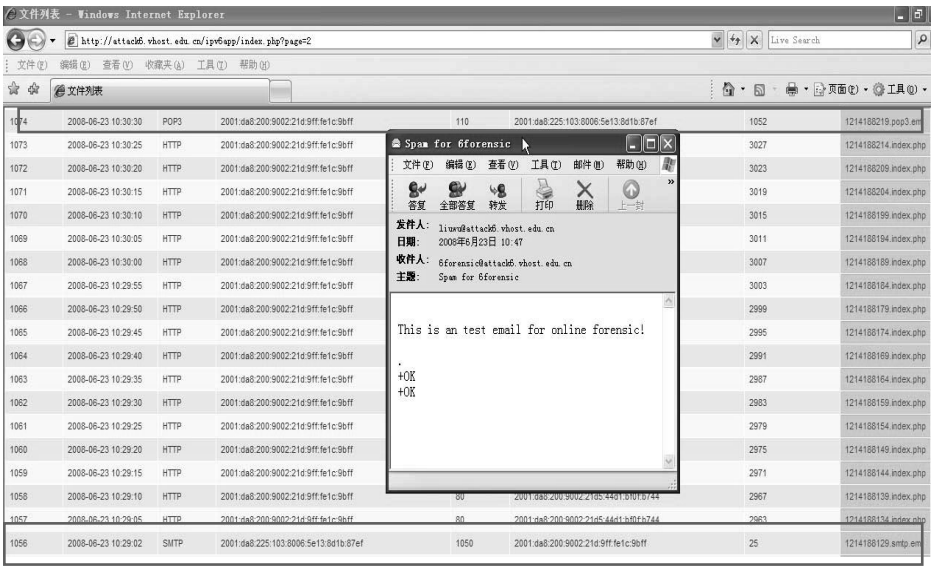

Fig.17 6Foren for SMTP and POP3 protocol

6 Conclusion

In this paper, we designed and implemented IPv6 attacking test system ATS_ICMP_6, which can execute IPv6 attacking experiments via ICMPv6 Messages. In the other hand, we designed and implemented a network forensics prototype 6Foren in IPv6 environment based on the protocol analysis technology, its functions include packet capture, data reconstruct and messages replay etc. the 6Foren can be used as the online digital forensics which support the online forensic of HTTP, FTP, SMTP and POP3 protocols.

Bibliography

[1] S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC2460, Internet Engineering Task Force, December 1998.

[2] T. Narten, E. Nordmark and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC2641, IETF, December 1998.

[3] S. Thomson and T. Narten, IPv6 Stateless Address Autoconfiguration, RFC2462, Internet Engineering Task Force, December 1998.

[4] T. Narten, E. Nordmark and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC2641, IETF, December 1998.

[5] Wu Liu, Study on Intrusion Detection Technology with Traceback and Isolation of Attacking Sources, PhD Thesis, 2004.

[6] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[7] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[8] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[9] McCann, J., Deering, S. and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[10] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[11] Watson, P., "Slipping in the Window: TCP Reset Attacks", 2004 CanSecWest Conference , 2004.

[12] Jacobson, V., Braden, B. and D. Borman, "TCP Extensions for High Performance", RFC 1323, May 1992.

[13] Stewart, R., "Transmission Control Protocol security considerations", draft-ietf-tcpm-tcpsecure-02 (work in progress), November 2004.

[14] Touch, J., "ANONsec: Anonymous IPsec to Defend Against Spoofing Attacks", draft-touch-anonsec-00 (work in progress), May 2004.

[15] Poon, K., "Use of TCP timestamp option to defend against blind spoofing attack", draft-poon-tcp-tstamp-mod-01 (work in progress), October 2004.

[16] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[17] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[18] Wu Liu, Hai-xin Duan, and Jian-ping Wu, An Authorship Analysis Model MBSFAM in Software Forensics, J. of Computer Research and Application, 2005 Vol.11(5):121-128

[19] F. Buchholz. Pervasive Binding of Labels to System Processes. PhD thesis, Purdue University, 2005.

[20] B. Carrier. File System Forensic Analysis. Addison Wesley Professional, 2005.

[21] B. D. Carrier. A Hypothesis-Based Approach to Digital Forensic Investigations. PhD thesis, Purdue University, 2006.

[22] D. Farmer and W. Venema. Forensic Discovery. Addison Wesley Professional, 2004.

[23] B. A. Kuperman. A Categorization of Computer Security Monitoring Systems and the Impact on the Design of Audit Sources. PhD thesis, Purdue University, 2004.

[24] U. Lindqvist and P. A. Porras. eXpert-BSM: A Host-Based Intrusion Detection System for Sun Solaris. In Proceedings of the 17th Annual Computer Secrity Applications Conference (ACSAC), pages 240{251.IEEE Computer Society, December 10{14 2001.

[25] E. H. Spaord and S. A. Weeber. Software forensics: Can we track code to its authors? Technical Report CSD-TR 92-010, Department of Computer Science, Purdue University, 1992.

[26] T. Stallard and K. Levitt. Automated Analysis for Digital Forensic Science: Semantic Integrity Checking. In Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC), December 8-12 2003.