Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DESIGN & DEPLOYMENT OF TESTBED BASED ON ICMPv6 FLOODING ATTACK

[1,2]REDHWAN M. A. SAAD, [1]SELVAKUMAR MANICKAM, [1]ESRAA ALOMARI, [1]MOHAMMED ANBAR AND [1]PARMINDER SINGH.

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

[2]Faculty of Engineering and Architecture, University of Ibb, Ibb, Yemen

E-mail: redhwan@nav6.usm.my , selva@nav6.usm.my, esraa@nav6.usm.my, anbar@nav6.usm.my, parminder@nav6.usm.my

ABSTRACT

One of the important protocols in IPv6 implementation is ICMPv6 which is used for neighbor and router discovery. However, this protocol also could be used by attackers to deny network services like ICMPv6 flood attacks which network decreases performance.

In ICMPv6 flooding attacks detection, behavioural-based approaches, particularly suffer from the unavailability of the benchmark datasets. This can lead to the lack of precise results evaluation of ICMPv6flooding attack detection systems, comparison, and deployment, which originates from the deficiency of adequate datasets. Most of the datasets in the IPv6 field are from local environment and cannot be used on a large scale due to privacy problems and do not reflect common trends. They also lack some statistical features. Therefore, there is not any available benchmark dataset infected by ICMPv6-based foods for performing a Denial of Service (DoS) attacks against Web servers by using ICMPv6 flooding method. In addition, there is no Web access log infected by ICMPv6-based flood available for researchers.

This paper presents the ICMPv6-based flooding attacks testbed to study the behaviour of ICMPv6 flooding attack as well as evaluating different solutions proposed for detecting ICMPv6-based flood of DoS attacks by various researchers.

Keywords: *ICMPv6 flooding attacks, Denial of Service attacks, IPv6 testbed Network.*

1. INTRODUCTION

Recently, IPv6 security and its threats have been considered as one of the significant issues and, therefore, this point is still under discussion in the current research [1-4], because of IPv6 security threats during the transmission, it is essential to improve the security of data transmission [5].

Distributed Denial of Service (DDoS) attack is the main source of the threats of IPv6 security[6]. DDoS can be classified into four types including User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) flood, Transmission Control Protocol (TCP) and Smurfs[3].

The main issue for the analysis and enhancement of proper security solutions is to have test-beds that can be employed in conducting the experimental security study in a safe and reasonable manner, but the utilization of test-beds has faced some obstacles where the main obstacle is the absence of the benchmark test-bed which is infected by ICMPv6-based flood that can be employed for standardization and evaluation of different detection and mitigation systems [7].

The most ideal methodology for assessing and validating the researcher's hypothesis and systems is the deployment of these detection and mitigation systems over application traces and real network with significant set of flood and abnormal behaviour.

After the introduction in section I, the rest of this paper is organised as follows:

We describe related work in section II. Section III contains the ICMPv6 messages. Section IV shows brief comparison between IPv6 and IPv4 ICMP. Section V presents the classification of the Denial of Service attacks using ICMPv6. In section VI we briefly describe some types of ICMPv6-based flooding attack structure. Some famous tools which have been used in ICMPv6 flooding DDoS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacks are described in section VII. In section VIII we describe the technical details of the proposed testbed setup and design. Finally, we conclude our work in section IX.

2. RELATED WORKS

Until now, various types of security benchmark data sets such as KDD[8], DARPA [9, 10], LBNL [11], DEFCON [12], CAIDA [13] are available for used by the researchers. These data sets can be employed in the detection of several types of attacks and they can be used for systems assessment as well. Unfortunately, these data sets have been criticized to be used in intrusion detection in IPv4 networks as they do not include any classes of ICMPv6 flooding traces [10].

One of the important and challenging research problems in detecting DDoS attacks is extracting a sufficient and valid features such as IP sources and IP destination that can be used to build efficient models to identify a DDoS attack [14]. Recently, a latest dataset released in the intrusion detection domain named The Ark IPv6 topology dataset [13] is produced by using a scamper to perform ICMP-based traceroutes using the Paris traceroute technique. This dataset meets a lot of the researchers needs, but it has the limitation of having specific traces and it is not a comprehensive dataset of ICMPv6 floods type like DDoS. The IP source and IP destination features are deleted from the dataset due to security issues as shown in Figure 1.

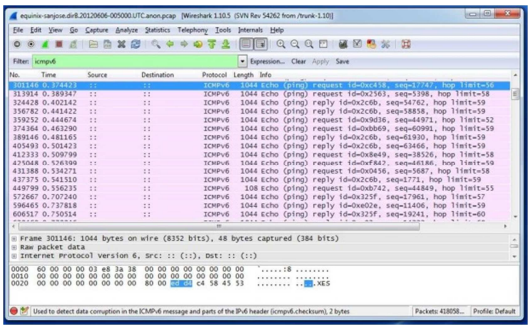

Figure 1: Snapshot from the ARK IPv6 Topology Dataset

In this paper, a complete test-bed will be illustrated in order to implement a real time ICMPv6 floods for performing DDoS attacks against Web servers by using an ICMPv6 flooding method [15]. These real time datasets can be useful to study the behaviour of ICMPv6-based flooding and to propose different solutions to detect ICMPv6-based flood for the researchers who are new in this research area.

3. ICMPv6 MESSAGES

Internet Control Message Protocol version 6 (ICMPv6) is utilized in IPv6 only [16, 17]. Its existence is an integral part of IPv6 and must be fully implemented by every Ipv6 node.

Table 1: Typical ICMPv6 Messages

Type of ICMPv6 informational message	Meaning	Type of ICMPv6 error messages	Meaning
128	Echo request	1	Destination unreachable
129	Echo reply	2	Packet to big
133	Router solicitation	3	Time exceeded
134	Router advertisement	4	Parameter problem
135	Neighhbor solicitation	100	Private experimentation
136	Neighhbor advertisement	101	Private experimentation
200	Private experimentation	107	Reserved for expansion
201	Private experimentation		
255	Reserved for expansion		

ICMPv6 messages are classified into two classes: Error Messages and Informational Messages. ICMPv6 Error Messages are known as such by having a zero in the high-order bit of their message Type field values. Thus, error messages have message Types from 0 to 127; informational messages have message Types from 128 to 255. A number of typical ICMPv6 messages are exposed in Table 1.

4. DIFFERENCES BETWEEN IPv6 AND IPv4 ICMP

IPv6 and IPv4 are very similar in terms of functionality (but not in terms of mechanisms). In Table 2 shows brief comparison between IPv6 and IPv4.

Table 2: Brief Comparisons Between IPv6 and IPv4

	IPv4	IPv6
Addressing	32 bits	128 bits
Address Resolution	ARP	ICMPv6 NS/NA
Auto-configuration	DHCP&ICMP RS/RA	ICMPv6 RS/RA & DHCPv6
Fault Isolation	ICMP	ICMPv6
IPsec support	Optional	Recommended
Fragmentation	Both in hosts and routers	Only in hosts

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ICMP specification for IPV6 has some distinctive changes than in IPV4 ICMP. Such as ND substitutes the ARP and various administrative changes in IPV6 for instance:

- Next Header Value. ICMPv6 has NH value of 58 whereas IPv4 has only 1
- Neighbor Discovery substitutes ARP. With ICMPV6 it finds the nodes by ND messages similar to the ARP mechanism in IPV4
- Increased Path Maximum Transmission Unit (PMTU).In IPV4 every node minimum capacity at least to carry 576 bytes whereas in IPv6 , it is 1500 bytes
- Multicast Listener Discovery (MLD). ICMPV6 messages are used by IPV6 replacing IGMP.

This protocol allows multicast listeners to get desirable addresses .No broadcast in IPV6 any more instead it uses multicast. Thus, with ICMPV6 it services to auto-configure, neighbour discovery the nodes [18].

5. DENIAL OF SERVICE ATTACKS USING ICMPv6

Sending error messages and excessive numbers of ICMPv6 to destinations are examples of denial of service (DoS) that could badly interrupt and drop the established communication where ICMPv6 can be utilized to generate DoS in several ways. Moreover, in case of infiltration of spurious communication messages onto a link, the interfaces might be disabled and also the legitimate address could be disrupted and invalidated.

Data flooding is considered as one of the categories of Denial of Service Attacks (DOS) where DoS is classified into five categories in terms of attacked level. In this attack, the attacker tries to send massive quantities of data through using the bandwidth which is available to the network, host or device at its highest level. The flooding attacker can simply bombard the targeted victim with normal meaningless packets through using the spoofed source addresses on the available bandwidth like flooding pinging.

Simple data flooding is mostly seen in the form of DDoS attacks [19, 20] as demonstrated in figure 2.

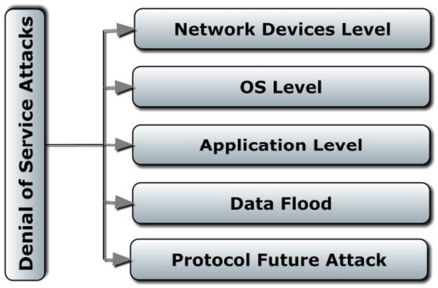

Figure 2: Classification of DoS Attacks

An ICMP flood attack is a way of denial-of-service (DoS) attack or it is known as a 'ping flood'. An ICMP flood is considered as the simplest ping-based DoS attacks in which the attacker excessively send ICMP/ping packets to the victim's system by using a technique of sending ICMP packets constantly without waiting for a reply. Thus, the victim is overloaded with a flood of packets [21, 22].

Many thousand Router Advertisements (RA) can be flooded by attackers. As a result, such attack lead to immediately freeze all Microsoft Windows computers as they are completely overloaded with that many SLAAC processes.

6. ICMPv6-BASED FLOODING ATTAK STRUCTURE

Flooding attacker is considered as the most common attack type in IPv4 networks. It operates to drowning the network device (router) or a host node with a huge amount of traffic through overloading the victim with floods. Accordingly, the targeted victim will not have the ability to process this huge amount of packets and, therefore, the targeted network device turn out to be out of service. When this device is flooded with network traffic from several hosts concurrently, the attacker can be a local or a distributed denial of service attack (DDoS). Additionally, this attacker has the ability to negatively influence the IPv6neworks since the key principles of the flooding attack is the same [23-26].

Mostly, the DDoS flooding attacks can be classified into two types including direct attacks and reflector attacks. For the direct attacks (Figure 3), the attacker uses the zombie machines in order to directly send a flood of packets to the victim. In terms of OSI layers, direct DDoS attacks can be classified into two groups: application-layer DDoS attacks and network-layer DDoS attacks.

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Application-layer DDoS attacks include: HTTPS flood, HTTP flood, FTP flood, etc. Meanwhile Network-layer DDoS attacks includes: TCP flood, UDP flood, ICMP flood and SYN flood.

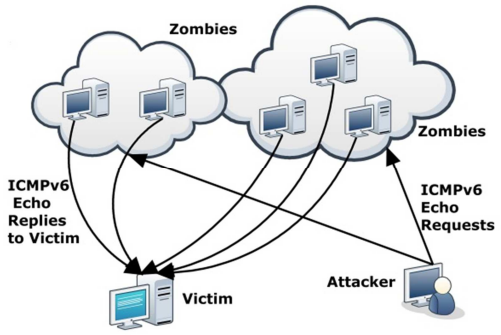

Figure 3: The Architecture of Flooding DDoS Direct Attacks

For reflector attacks (Figure 4), the attacker uses the zombie machines or spoofing the source IP address of the victim server in order to send request messages to reflector machines. Therefore, the reflector machines send their replies to the given address which, in turn, makes packet flooding at that site of the victim server. ICMP ECHO reply flood, SYN ACK (RST) flood, DNS flood, Smurf attack and Fraggle attack are considered as the most well-known reflector attacks[27].

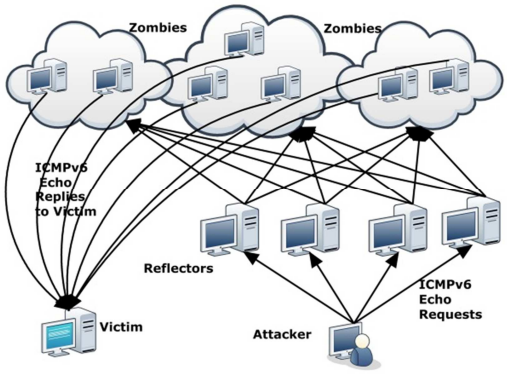

Figure 4: The Architecture of Flooding DDoS Reflector Attacks

7. TOOLS USED FOR ICMPv6 FLOODING DDOS ATTACKS

There are several security tools available to launch an ICMP flooding attacks like DoS/DDoS attack [28]. Using these tools, attacker(s) can launch a successful DoS/DDoS attack easily because these tools are easily available online and are easy to use. This section will discuss some of the famous tools used to perform ICMPv6 flooding DDoS attacks[29].

A. *THC-IPV6 Attack Toolkit:* A complete toolkit set to attack the inherent protocol weaknesses of IPv6 and ICMPv6[30]. One of the included tools is "denial6" which is used to collect denial-of-service tests against a target.

B. *SI6 Networks' IPv6 Toolkit*: The SI6 Networks' IPv6 toolkit is a set of IPv6 security/ trouble-shooting tools that can send arbitrary IPv6-based packets[31].

C. *Scapy:* To send completely crafted IPv6 packets [32].

8. PROPOSED TEST-BED SETUP AND DESIGN

8.1 Scenario-Based Setup

This section describes the methods of installation and configuration of the environment required.

To conduct our testbed to generate the ICMPv6 flood attack in IPv6 networks, we setup an IPv6 network at the National Advanced IPv6 Center – University Science Malaysia (USM). As shown in Figure 5, the following hardware and software are used in the testbed setup for the IPv6 testbed:

- Operating systems: Ubuntu 14.10, windows7.
- Networking tools: Wireshark 1.10.5.
- Attacking tools: THC-IPV6 Attack Tool 0.6
- IPv6 nettwork.

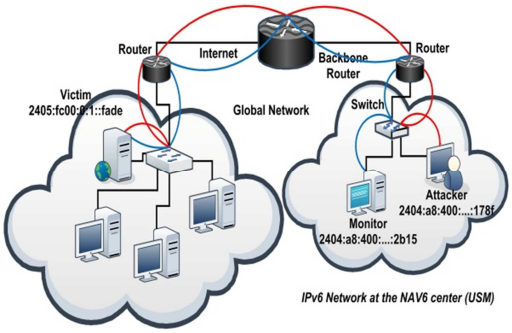

Figure 5: ICMPv6 DoS Flooding Attack Testbed Structure

Using THC-IPv6 attack tool "denial6", ICMPv6 flood attack is used to produce a threat situation on early ICMP flood attacks. The flooding packets are generated using different attack rates starting from 1000 Pings to 100000 Pings. This

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ping flood attacks are used to flood large amounts of data packets to the victim's workstation in an attempt to overload the victim.

8.2 Experimental Results

Using the ICMPv6-based flooding attack testbed, we successfully run denial-of-service experiments against Web services as shown in Figure 6.

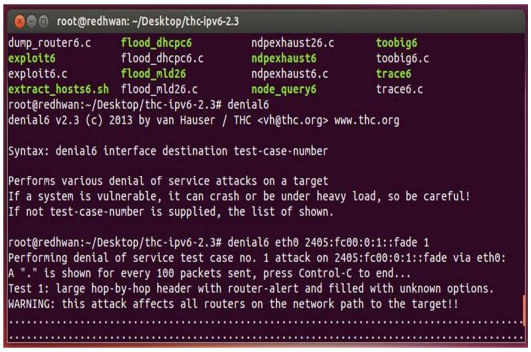

Figure 6: ICMPv6-Based Flooding Attack Against Web Services

In order to find the active global unicast IPv6 address, the best methodology is to use ping6 that sends an ICMPv6 echo request. The active IPv6 address should reply to ICMPv6 echo reply (ICMPv6 type 129) (IANA, 2011).

During the experiments, access to the target Web server is impossible as a huge amount of ICMPv6 packets are sent. This means the services are denied wherever the experiment is conducted.

The Wireshark program is used to assist in monitoring the network traffic, i.e., to provide more validity regarding the sending and receiving the packets from the source to the destination side (see Figure 7).

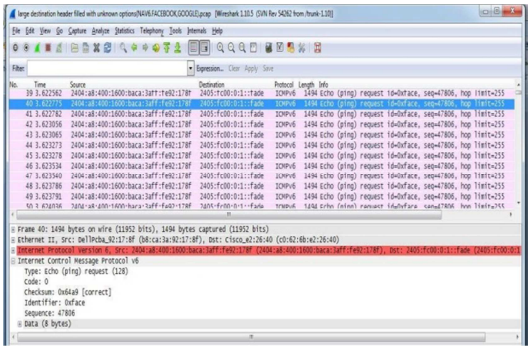

Fig. 7. Wireshark Snapshot of Monitoring Network Traffic

In the network security field, the researchers need malicious trace files for evaluation and validation of their system. Thus, we present sample results which are generated from ICMPv6-based flood test-bed when launching ICMPv6-based flooding Denial of Service attacks as shown in Figure 8.

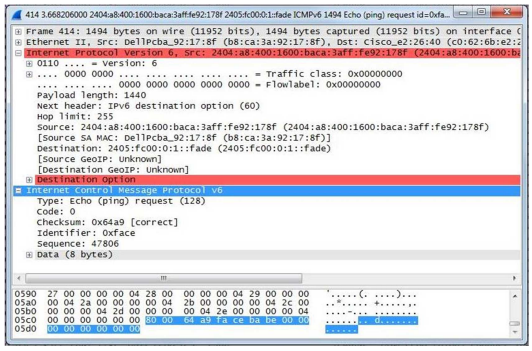

Figure 8: Sample ICMPv6 Packet Captured

9. CONCLUSION

The purpose of this study is to propose a real time test-bed for ICMPv6 flood researchers, especially on the IPv6 network. Moreover, it attempts to suggest proper solutions for the shortcomings of the current test-beds environment where ICMPv6-flood are configured and utilized in order to conduct ICMPv6 flood DoS attacks against the targeted network server. Consequently, we have reviewed the various challenges and drawbacks of the current test-beds and datasets available to study the behaviour of ICMPv6-based flood and to evaluate various solutions proposed to detect ICMPv6-based flood by various researchers.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper and to thank the National Advanced IPv6 Center, Universiti Sains Malaysia for providing facilities and support to setup the testbed. This original research was proudly supported by the RUT grant of University Science Malaysia (USM) (Grant No. 1001/PANY/857001).

REFERENCES:

[1] V. Alangar and A. Swaminathan, "Ipv6 Security: Issue Of Anonymity," *International Journal Of Engineering And Computer Science,* vol. 2, p. 7, 2013.

[2] E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia - Social and Behavioral Sciences,* vol. 2, pp. 5285-5291, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Y. Xinyu, M. Ting, and S. Yi, "Typical DoS/DDoS threats under IPv6," *Computing in the Global Information Technology,* pp. 55-61, 2007.

[4] R. Saad, S. Manickam, and S. Ramadass, "Utilizing Data Mining Approches in the Detection of Intrusion in IPv6 Network: Review & Analysis," *International Journal of Network Security (2152-5064),* vol. 4, 2013.

[5] D. Zagar and K. Grgic, "IPv6 security threats and possible solutions," in *Automation Congress, 2006. WAC'06. World*, 2006, pp. 1-7.

[6] E. Alomari, B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *International Journal of Computer Applications,* vol. 50, 2012.

[7] J. Calvet, C. R. Davis, J. M. Fernandez, W. Guizani, M. Kaczmarek, J.-Y. Marion, and P.-L. St-Onge, "Isolated virtualised clusters: testbeds for high-risk security experimentation and training," in *Proceedings of the 3rd international conference on Cyber security experimentation and test (Berkeley, CA, USA, 2010), CSET*, 2010, pp. 1-8.

[8] K. Cup. (2014). *Data, Information and Computer Science, University of California, Irvine*. Available: https://www.Iittp_7/kdd.ics.uci.edddatabases/lcddcup99/kddcup99.html

[9] L. L. MIT. (2014). *DARPA intrusion detection evaluation.* Available: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/

[10] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," *ACM transactions on Information and system Security,* vol. 3, pp. 262-294, 2000.

[11] L. B. N. Laboratory and ICSI. (2014). *LBNL/ICSI enterprise tracing project*. Available: http://www.icir.org/enterprise-tracing/

[12] T. S. Group. (2014). *Defcon*. Available: http://cctf.shmoo.com/data/

[13] CAIDA, "The cooperative association for internet data analysis," 2014.

[14] S. Raghavan and E. Dawson, *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks*: Springer India, 2011.

[15] I. S. C. o. Excellence. (2014). *UNB ISCX Intrusion Detection Evaluation DataSet*. Available: http://iscx.ca/datasets

[16] A. Conta and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," *R December,* vol. RFC: 2463, Internet Engineering Task Force., 1998.

[17] L. Wu, D. Hai-xin, L. Tao, L. Xing, and W. Jian-ping, "H6Proxy: ICMPv6 weakness analysis and implementation of IPv6 attacking test proxy," in *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on*, 2009, pp. 519-524.

[18] S. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the secure deployment of IPv6," *NIST Special Publication,* vol. 800, p. 119, 2010.

[19] L. D. Stein and J. Stewart, *World Wide Web Security FAQ* vol. 3.1.2: Lincoln D. Stein., 2002.

[20] H. Safa, M. Chouman, H. Artail, and M. Karam, "A collaborative defense mechanism against SYN flooding attacks in IP networks," *Journal of Network and Computer Applications,* vol. 31, pp. 509-534, 2008.

[21] P. Shanmugaraja and S. Chandrasekar, "Accessible Methods to Mitigate Security Attacks on IPv4 to IPv6 Transitions," *European Journal of Scientific Research,* vol. 77, pp. 165-173, 2012.

[22] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa, and J. Lloret, "Denial of service mitigation approach for IPv6-enabled smart object networks," *Concurrency and Computation: Practice and Experience,* pp. n/a-n/a, 2012.

[23] D. Zagar and K. Grgic, "IPv6 security threats and possible solutions," 2006, pp. 1-7.

[24] R. Radhakrishnan, M. Jamil, and S. Mehfuz, "Security issues in IPv6," 2007, pp. 110-110.

[25] X. Yang, T. Ma, and Y. Shi, "Typical DoS/DDoS Threats under IPv6," 2007, pp. 55-55.

[26] A. R. Choudhary, "In-depth analysis of IPv6 security posture," 2009, pp. 1-7.

[27] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Computer Communications,* vol. 35, pp. 1312-1332, 2012.

[28] M. Glenn, "A summary of dos/ddos prevention, monitoring and mitigation techniques in a service provider

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

environment," *SANS Institute, Aug,* vol. 21, p. 34, 2003.

[29] R. M. Saad, S. Ramadass, and S. Manickam, "A Study on Detecting ICMPv6 Flooding Attack based on IDS," *Australian Journal of Basic and Applied Sciences,* vol. 7, pp. 175-181, 2013.

[30] THC. (2013). *THC-IPv6 Attack Toolkit*. Available: https://www.thc.org/thc-ipv6/

[31] F. Gont, "Security Assessment of Neighbor Discovery (ND) for IPv6," *IETF Internet-Draft,* 2013.

[32] P. Biondi. (2014). *Scapy*. Available: http://www.secdev.org/projects/scapy/