International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2013, Vol. No. 3, Issue No. II, February **ISSN: 2231-5152**

IPV6 NETWORK SECURITY USING SNORT

Vivek Saini[1], Dr. K P Yadav[2]

[1]*Research Scholar, Dept of Computer Science & Engineering, Sai Nath University, Ranchi*
[2] *Director, MIET, Greater Noida(UP)*

ABSTRACT

IPv6 is new routing protocol. IPv6 is introduced by IETF mainly due IPv4 address exhaustion but it is also an enhanced version of IPv4. There are many changes in IPv6 header, some fields from IPv6 header has been deprecated from IPv6 and some are newly added. There is also common misconception among people that IPv6 is more secure than IPv4, which is not true. Now a day's intruders are targeting IPv6 networks as it is widely being accepted by many organization for their network. An intruder can do enough damage if it gets unauthorized access to the someone IPv6 network. So, There is need to do more research to secure IPv6 networks. Detecting an intruder in IPv6 network is hot topic among the researchers. Intrusion detection is a technique to detect the unauthorized access to the network. An intrusion-detection system (IDS) monitors system and network to detect intruders that are trying to gather information on network for which they are not authorized. IDS also alerts the administrator for misuse of network. All IDS support IPv4. But only few of them provide good support for IPv6. In this paper, Deployment of small IPv6 network and intrusion detection using Snort in the IPv6 network has been done. Mainly the focus is on intrusion detection in IPv6 network. **Keywords**: Intrusion Detection; IPv6; Snort; PCRE, IDS

INTRODUCTION

Network Intrusion detection is an approach to provide security to computer networks. Network intrusion detection is based on belief that attacker behavior will be different from the behavior of legitimate user on network. From past few years we are moving towards IPv6 networks and there is demand to secure IPv6 networks. To provide secure IPv6 network there is a need of better intrusion detection.

Currently IPv4 networks are not fully eliminated but as it is known that IPv4 address will exhaust after few years IPv6 address will come into picture so it is clear that in future a good intrusion detection technique will be required that works with IPv6 to detect intruders. IPv6 is an entirely new protocol. It is not IPv4 with larger addresses. The main motivation that gives birth to IPv6 is exhaustion of IPv4 addresses. Currently there are many tools and techniques to detect/prevent the intrusion in IPv4 but in IPv6 very few intrusion detection tools are available. As IPv6 is new protocol for communication over Internet so it is more vulnerable to attack. The next generation protocol IPv6 brings the new challenges for information security.

This paper presents the design and implementation of network-based intrusion detection system that support IPv6 protocol. Intrusion detection system architecture should focus on performance, simplicity, and scalability. Rapid development of IPv6 protocol, intrusion techniques under the IPv6 also appears accordingly, and shows a trend of fast growth. Although there are various firewalls that provide the security to the IPv6 enabled network. As IPv6 has different structure then IPv4 header so there are new complication introduced by IPv6 development. There are various types of attack that can easily bypass the firewall for example fragment overlapping [RFC5722].

Importance of firewall cannot be ignored while deployment of IPv6. Firewall must be configure properly to secure IPv6 network [3][4][6]. But relying solely on firewall might be a great risk for network. Thus, it is good to have second alternate to prevent network from various intrusions. As mentioned earlier that IPv6 is new so traditional intrusion detection system does not protect the network from intruders with the existing technology. The reason is that IPv6 is not backward compatible with IPv4. IPv6 has a new header format that is different form IPv4 header format. IDS supporting IPv6 protocol must recognize IPv6 header. For simplification IPv6 main header have extension headers. A Next Header format also allows new types of IPv6 extension headers to be defined and implemented. The IDS system must implement support for these types of headers.

There are few good tools that recognize the IPv6 header format. One of them is Snort intrusion detection system. Intrusion detection Systems and Intrusion prevention systems (IDS/ IPS) are primarily focused on identifying possible security exploit, logginginformation about security exploit, attempting to stop them, and reporting them to network administrator. Mainly intrusion detection systems are based on rule language. A rule language contains the signature of security exploit.

This paper presents the detection of intrusion trying to brute force in IPv6 network to get unauthorized access. An IPv6 network has been deployed using two virtual machines (VM) and an Ubuntu Physical system. Ubuntu is setup as router to forward packet between virtual machines. One VM used as an attacker and one is as victim. Snort is configured between the packet flow from one VM to another VM to analyze the packets and detect the intrusion.

INTRUSION DETECTION IN NETWORK

Intrusion detection (ID) is a type of security management system for computers and networks. An Intrusion detection system gathers and analyzes network traffic in a network to find out possible security exploit in network. ID uses vulnerability assessment technique to access the security of a computer system or network. It is also referred as scanning. Intrusion detection functions include [2]:

a) Monitoring and analyzing both user and system activities.
b) Analyzing system configurations and vulnerabilities.
c) Assessing system and file integrity.
d) Ability to recognize patterns typical of attacks
e) Analysis of abnormal activity patterns
f) Tracking user policy violations

Now a day's security safeguarding is become more challenging because attacker are using more sophisticated techniques for attack.

An Intrusion Detection System Model based on protocol analysis, which can rely on scanning the vulnerability from the semantics layer to choose attack signature adapted for misuse detection, and then use the network behavior to make anomaly detection. The IDS system of IPv4 might be able to run under IPv6 environment, but not capable of solving the security problem with the new characters of IPv6, such as neighbor discovery protocol (NDP), auto-configuration. For the potential security issues leaded by the changing of IPv6 protocol, some typical IPv6 network attacks are [11]:

a) Misuse of ICMPv6 and multicast- ICMPv6 can be used by attacker to get response to the fake source address by sending a packet destined to a multicast address.
b) Network reconnaissance attacks- This one is same as in IPv4, Scanning of valid host and services.
c) Fragmentation attacks- IPv6 packet having fragment less than 1280 bytes is dropped and attacker can use dropped packet to get the state of network.
d) Efficient bottleneck- In IPv6 protocol field is replaced by an optional header. Further this optional header can point to another extension header till the last. This next to next header processing have great impact on working of IDS.

According to detection strategy, There are two types of intrusion detection, misuse-based detection and anomaly-baseddetection[7]. Knowledge-based detection include a database which contains signature of known security exploit. The audit data collected by the IDS is compared with the content of the database and, if a match is found, an alert is generated. Any suspicious activity which is not detected by signatures will considered as a part of legitimate activities. Anomaly-based detection is based on behavior user/attacker. It is based on the assumption that all anomalous activities are malicious and all the attacks are subset of anomaly activities.

Many researchers used Snort intrusion detection system for intrusion detection. Snort is open source intrusion detection system. Snort uses signature based intrusion detection. Signature is a characteristic of security exploit. Signature based detection process include examining the packet passing through the network and match the signature of packet with the database of rules[8]. Every rule stored in the database represent signature of the security exploit. If signature/rule of database matched with the packet then it an alert will be generated to the administrator.

Any intrusion detection System can also comprise of misuse detection system and anomaly detection system(ADS). As anomaly based detection is based on behavior of user. A model that define legitimate behavior of users can be used for anomaly based detection and an activity that do not conform to the defined model is malicious. However, since it is impossible to describe all the activities of all users in system, it leads to relative high false positive rate.

It is not possible to develop a intrusion detection system until network traffic is analyzed. Packet sniffers are used to analyze the network traffic. Packet sniffers was first steps towards network security. Packet sniffer tools were used to find the suspicious activity from intruders[9].

Many researchers have considered Snort for their research work in the field of intrusion detection. To find a attack it necessary to understand the network traffic[12]. Snort senses network traffic and uses it's rule/signature database to match the security exploit. Introduction of IPv6 as new communication protocol adds more vulnerabilities to network and requires increased attention of developers on intrusion detection systems. IPv6 intrusion detection requires more efforts from developer because there is coexisting environment. Smart intruders can first detect some vulnerable hosts in IPv6 subnet, after all the vulnerable hosts in a subnet are infected. There are many well known scanning techniques that are being used to find out vulnerable hosts[5]. IPv6 has the key differences with IPv4 like Fixed IPv6 basic header and Simplified basic header of IPv6. IPv6 and IPv4 can also coexist in the same network. So Intrusion detection under coexisting network environments of IPv4 and IPv6 is also needed[10].

It is very difficult and costly to change an IPv4 network to fully IPv6 network. This change possible using transitional mechanism. Some attack like bad ACK-Reset and packet fragmentation attack can be detected using ip6tables and access control list in the network path[1].

TESTBED SIMULATION

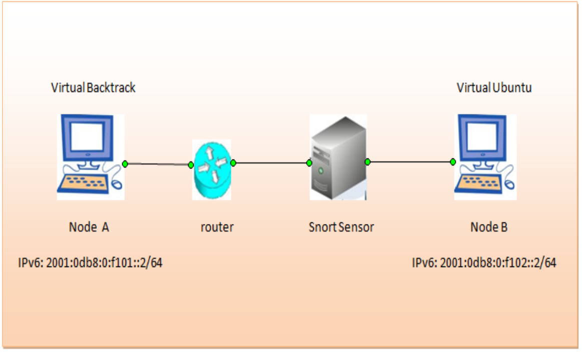
Firewalls are good option to secure a network. But sometimes intruders are manage to bypass firewall. So, it is good if there is wall behind wall that is an intrusion detection system in the network. It will lead to more secure network. Snort is an open source intrusion detection system. It has both intrusion detection and prevention capabilities in network. Snort has enriched rule database for IPv4 intrusion detection means it has many signatures for known IPv4 security exploit. But when it comes to IPv6 intrusion detection it lacks good rule database for IPv6 intrusion detection.

A. Purpose

IPv6 network has been deployed to test an attack scenario. FTP server has been configured on one virtual machine. Physical Ubuntu system configured as router between two IPv6 networks. Snort is configured on this router to counter the FTP brute force attack on FTP server machine.

B. Experimental Design

The experimental design was deployed using two virtual machines and one router. Figure 1 shows the testbed topology. Host operating system is Ubuntu 12.04 which is also acts as router between networks. Node A virtual machine operating system is Backtrack which is used for brute force attack.



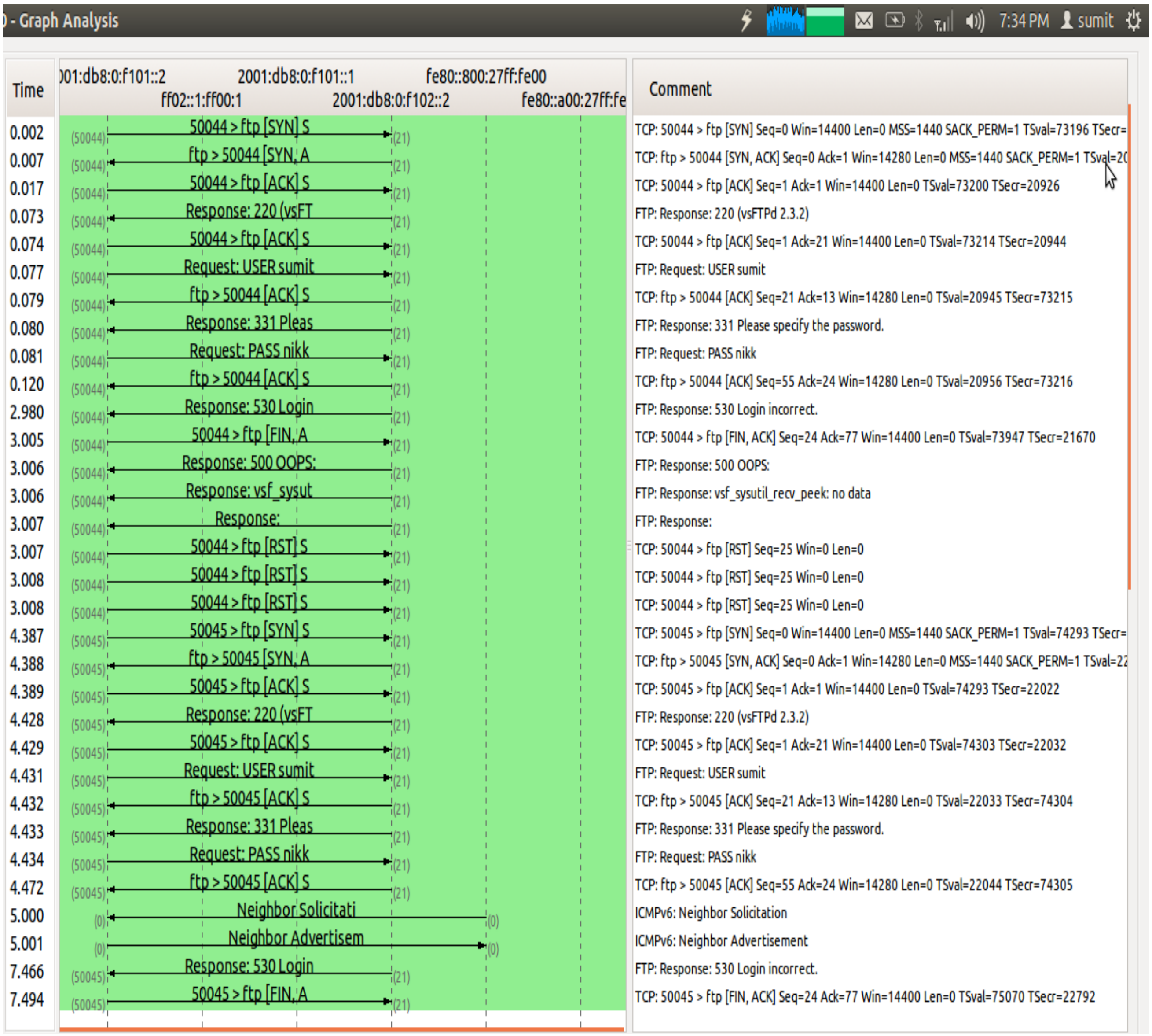
Node B virtual machine operating system is Ubuntu 11.10 which is running FTP service on port 21. Node A trying to get unauthorized access to FTP service running on Node B. Snort is configure in the network to detect brute force attack. Every packet following from Node A to Node B(or vice versa) will be analyzed by snort to find matching pattern according to written rule. Router is configured for IPv6 packet forwarding. Packet forwarding is disabled by default in Ubuntu, enable it from configuration files. Open */etc/sysctl.conf* in text editor move to line read as

```
#net.ipv6.conf.all.forwarding=0
```

first uncomment it and change it to read as

```
net.ipv6.conf.all.forwarding=1
```

Hydra tool is used for ftp brute force attack. Wireshark is used to analyze network traffic. Figure 2 shows traffic flow in IPv6 network between node A and Node B



Time		Comment
0.002	50044 > ftp [SYN] S	TCP: 50044 > ftp [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=73196 TSecr=
0.007	ftp > 50044 [SYN, A	TCP: ftp > 50044 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=20
0.017	50044 > ftp [ACK] S	TCP: 50044 > ftp [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=73200 TSecr=20926
0.073	Response: 220 (vsFT	FTP: Response: 220 (vsFTPd 2.3.2)
0.074	50044 > ftp [ACK] S	TCP: 50044 > ftp [ACK] Seq=1 Ack=21 Win=14400 Len=0 TSval=73214 TSecr=20944
0.077	Request: USER sumit	FTP: Request: USER sumit
0.079	ftp > 50044 [ACK] S	TCP: ftp > 50044 [ACK] Seq=21 Ack=13 Win=14280 Len=0 TSval=20945 TSecr=73215
0.080	Response: 331 Pleas	FTP: Response: 331 Please specify the password.
0.081	Request: PASS nikk	FTP: Request: PASS nikk
0.120	ftp > 50044 [ACK] S	TCP: ftp > 50044 [ACK] Seq=55 Ack=24 Win=14280 Len=0 TSval=20956 TSecr=73216
2.980	Response: 530 Login	FTP: Response: 530 Login incorrect.
3.005	50044 > ftp [FIN, A	TCP: 50044 > ftp [FIN, ACK] Seq=24 Ack=77 Win=14400 Len=0 TSval=73947 TSecr=21670
3.006	Response: 500 OOPS:	FTP: Response: 500 OOPS:
3.006	Response: vsf_sysut	FTP: Response: vsf_sysutil_recv_peek: no data
3.007	Response:	FTP: Response:
3.007	50044 > ftp [RST] S	TCP: 50044 > ftp [RST] Seq=25 Win=0 Len=0
3.008	50044 > ftp [RST] S	TCP: 50044 > ftp [RST] Seq=25 Win=0 Len=0
3.008	50044 > ftp [RST] S	TCP: 50044 > ftp [RST] Seq=25 Win=0 Len=0
4.387	50045 > ftp [SYN] S	TCP: 50045 > ftp [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=74293 TSecr=
4.388	ftp > 50045 [SYN, A	TCP: ftp > 50045 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=22
4.389	50045 > ftp [ACK] S	TCP: 50045 > ftp [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=74293 TSecr=22022
4.428	Response: 220 (vsFT	FTP: Response: 220 (vsFTPd 2.3.2)
4.429	50045 > ftp [ACK] S	TCP: 50045 > ftp [ACK] Seq=1 Ack=21 Win=14400 Len=0 TSval=74303 TSecr=22032
4.431	Request: USER sumit	FTP: Request: USER sumit
4.432	ftp > 50045 [ACK] S	TCP: ftp > 50045 [ACK] Seq=21 Ack=13 Win=14280 Len=0 TSval=22033 TSecr=74304
4.433	Response: 331 Pleas	FTP: Response: 331 Please specify the password.
4.434	Request: PASS nikk	FTP: Request: PASS nikk
4.472	ftp > 50045 [ACK] S	TCP: ftp > 50045 [ACK] Seq=55 Ack=24 Win=14280 Len=0 TSval=22044 TSecr=74305
5.000	Neighbor Solicitati	ICMPv6: Neighbor Solicitation
5.001	Neighbor Advertisem	ICMPv6: Neighbor Advertisement
7.466	Response: 530 Login	FTP: Response: 530 Login incorrect.
7.494	50045 > ftp [FIN, A	TCP: 50045 > ftp [FIN, ACK] Seq=24 Ack=77 Win=14400 Len=0 TSval=75070 TSecr=22792

Figure 2: Network Traffic Flow

PATTERN MATCHING

Snort uses a simple, lightweight rules description language that is flexible and quite powerful. Snort rule describe a attack pattern that is being used by intruders to penetrate network. When Snort encounter a packet than match it with the rule database if pattern matched it generate an alert to system administrator. Below is the rule for FTP bruteforce attack.

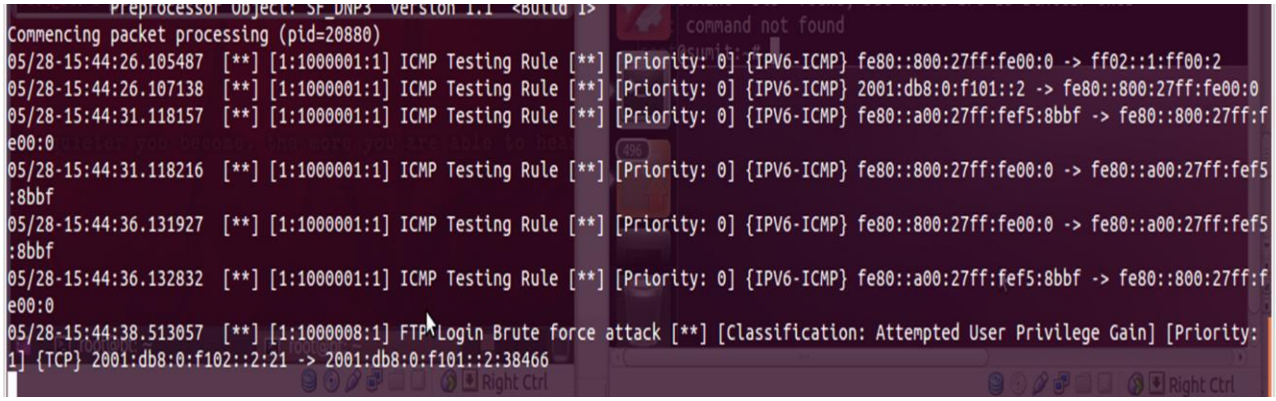
```
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any  (    msg:"FTP    Login
    Brute        force"; content:"530";pcre:"/^530\s+(Login)/smi";
detection_filter:track by_src, count 5, seconds 60; classtype:attempted-user;
sid:1000008; rev:1; )
```

Alert is action that alert to system administrator about the attack and log attack information to Snort log directory. TCP is protocol.

HOME_NET and EXTERNAL_NET are defined in Snort's configuration file. Home network is 2001:0db8:0:f102::0/64 with port number 21 that is traffic generated from network 2001:0db8:0:f102 prefix to any outside external network. Port number 21 is responsible for generating FTP traffic. Normally one can use content rule option for pattern matching but it is not much accurate. PCRE(Perl Compatible regular expression) is robust rule option to detect an attack. PCRE rule option is more accurate than content and reduce false positives. When attacker try to brute force a password of FTP service running on victim computer, each time FTP server reply with message “530 Login Incorrect”. Snort use this message to get attacker information and block the further access to home network after five times in 60 seconds.

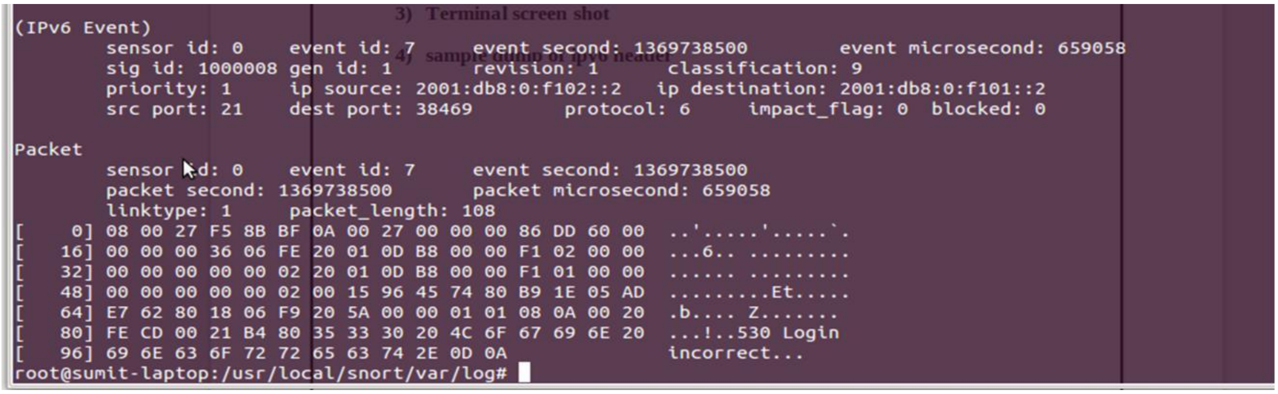
RESULTS

When Snort encounter a pattern matching in a packet, it's output plug-in shows the brief results and send detailed report to a log directory. U2spewfoo is a tool to view detailed report form logs. It also shows the payload of a packet. Figure 3 shows brute force attack displaying attack message “FTP Login Brute force attack”. It also displaying attack source and target with port numbers in the last. Figure 4 shows detailed report about the attack event. Snort manages events details very precisely. It shows the signature id that causes to generate alert and it also shows generated event time with respect to unix epoch time. So that administrator can investigate further about the attack.



```
         Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=20880)
05/28-15:44:26.105487  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} fe80::800:27ff:fe00:0 -> ff02::1:ff00:2
05/28-15:44:26.107138  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} 2001:db8:0:f101::2 -> fe80::800:27ff:fe00:0
05/28-15:44:31.118157  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} fe80::a00:27ff:fef5:8bbf -> fe80::800:27ff:f
e00:0
05/28-15:44:31.118216  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} fe80::800:27ff:fe00:0 -> fe80::a00:27ff:fef5
:8bbf
05/28-15:44:36.131927  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} fe80::800:27ff:fe00:0 -> fe80::a00:27ff:fef5
:8bbf
05/28-15:44:36.132832  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0] {IPV6-ICMP} fe80::a00:27ff:fef5:8bbf -> fe80::800:27ff:f
e00:0
05/28-15:44:38.513057  [**] [1:1000008:1] FTP Login Brute force attack [**] [Classification: Attempted User Privilege Gain] [Priority:
1] {TCP} 2001:db8:0:f102::2:21 -> 2001:db8:0:f101::2:38466
```

Figure: 3 Console output



```
(IPv6 Event)
        sensor id: 0    event id: 7     event second: 1369738500        event microsecond: 659058
        sig id: 1000008 gen id: 1       revision: 1      classification: 9
        priority: 1     ip source: 2001:db8:0:f102::2   ip destination: 2001:db8:0:f101::2
        src port: 21    dest port: 38469        protocol: 6     impact_flag: 0  blocked: 0

Packet
        sensor id: 0    event id: 7     event second: 1369738500
        packet second: 1369738500       packet microsecond: 659058
        linktype: 1     packet_length: 108
[    0] 08 00 27 F5 8B BF 0A 00 27 00 00 00 86 DD 60 00  ..'.....'.....`.
[   16] 00 00 00 36 06 FE 20 01 0D B8 00 00 F1 02 00 00  ...6.. .........
[   32] 00 00 00 00 00 02 20 01 0D B8 00 00 F1 01 00 00  ...... .........
[   48] 00 00 00 00 00 02 00 15 96 45 74 80 B9 1E 05 AD  .........Et.....
[   64] E7 62 80 18 06 F9 20 5A 00 00 01 01 08 0A 00 20  .b.... Z.......
[   80] FE CD 00 21 B4 80 35 33 30 20 4C 6F 67 69 6E 20  ...!..530 Login
[   96] 69 6E 63 6F 72 72 65 63 74 2E 0D 0A              incorrect...
root@sumit-laptop:/usr/local/snort/var/log#
```

Figure: 4 Detailed attack Report

CONCLUSION

Growing network sizes would result in transition from IPv4 to IPv6 networks. As it is a new routing and intruders are more interested in finding security exploit in the network. Thus, arises the need to have secure IPv6 networks. Brute force attacks are frequent attack that is being utilized by intruders to get unauthorized access and it is advantage to intruders that they may go undetected because there is lack of IPv6 rule database. In this paper, a test scenario has shown to detect an brute force attack using Snort's PCRE rule. This helps to network administrator to secure their network from various attacks. Rule authors should write rules carefully so that rule do not generate false positives. A PCRE rule could impose extra overhead in the system by inspecting every packet in the flow. It will be costly in terms of resource to process every packet in the network. So, future work include writing rules for more known IPv6 attacks and use rule option available in Snort's rule language that reduce system overhead and false positives.

ACKNOWLEDMENT

The efforts, contributed by research students, associated with this work, are highly acknowledged with great thanks.

REFERENCES

[1] Wan Nor Ashiqin Wan Ali, Abidah Hj Mat Taib, Naimah Mohd Hussin and Jamal Othman, "IPv6 Attack Scenarios Testbed",IEEE Symposium on Humanities, Science and Engineering Research, Kuala Lumpur, pp. 927-932, 2012.

[2] Asmaa Shaker Ashoor and Sharad Gore, "Intrusion Detection System (IDS) &Intrusion Prevention System (IPS): Case Study", International Journal of Scientific & Engineering Research, vol. 2, pp. 1-3, 2011.

[3] D. Barrera and P. C. Van Oorschot, "Security visualization tools and IPv6 addresses in Visualization for Cyber Security", 6th International Workshop on Visualization for Cyber Security, Atlantic City, NJ, pp. 21-26, 2009.

[4] F. Beck, O. Festor, I. Chrisment and R. Droms, "Automated and secure IPv6 configuration in enterprise networks", InternationalConference on Network and Service Management (CNSM), Niagara Falls, ON, pp. 64-71, 2010.

[5] Z. Chen and C. Ji, "A Self-Learning Worm using Importance Scanning", Proc. 3rd ACM CCS WORM '05, New York, USA , pp. 26-29, 2005.

[6] A. R. Choudhary and A. Sekelsky, "Securing IPv6 network infrastructure: A new security model", IEEE International Conference on Technologies for Homeland Security, Waltham,MA, pp. 500-506, 2010.

[7] Yu-Xin Ding, Min Xiao and Ai-Wu Liu, "Research Implement on Snort-Based Hybrid Intrusion Detection System", IEEE Eighth International Conference on Machine Learning and Cybernetics, Boading, vol. 3, pp. 1414- 1418, 2009.

[8] Kedar Namjoshi and Girija Narlikar, "Robust and Fast Pattern Matching for Intrusion Detection", In the proceedings of IEEE INFOCOM, San Diego, CA, pp. 1- 9, 2010.

[9] Mohammed Abdul Qadeer, Arshad Iqbal, Mohammad Zahid and Misbahur Rahman Siddiqui, "Network Traffic Analysis and Intrusion

Detection using Packet Sniffer", Second International Conference on Communication Software and Networks, Singapore, pp. 313-317, 2010.

[10] Zhang Yu, "Study on intrusion IPv6 Detection System on Linux", Second Asia-Pecififc conference on Computational Intelligence and Industrial Applications, Wuhan, vol. 2, pp. 5-8, 2009.

[11] Zheng Zeng, "Intrusion Detection System of IPv6 Based on Protocol Analysis", International Conference on Multimedia Technology (ICMT), Ningbo, pp. 1-4, 2010.

[12] Zhou Zhimin, Chen Zhongwen, Zhou Ti Echeng and Guan Xiaohui, "The Study on Network Intrusion Detection System of Snort", International Conference on Networking and Digital Society, Wenzhou, vol. 2, pp. 194-196, 2010.