

Analysis of Dynamic Intelligent Network Security System

Adesh Kumar and Vijay Maheshawari

Abstract- Firewall and IPS (Intrusion Prevention System) do packet filtering as compare with the filtering rules that set up at security policies. This thesis presents dynamic new plans to decrease by harm malice traffic for strengthening network security. It is the ways which designed in thesis. 1) The bypass passage that, first of all, is an enemy of authenticated packet at external routing. 2) Attack detection of an external router. 3) Bandwidth expansion. 4) It is attack information delivery to connected security system. 5) A generation of a filter. 6) Filtering rules setup of IPS and Firewall 7) Dynamic update of blocking filter 8) Dynamic network security system formation.

Proposed intelligent connection of IPS watched the existing firewall and a disadvantage of an invasion detection system that was used in order to prevent an attack of a hacker, and to have seen them in order to solve a problem.

Keywords: DDoS, Firewall, Hacker Attack, IPS, Network Security

1. INTRODUCTION

What is a Hacker? Many journalists and writers have been fooled into using the word hacker to describe crackers. These are people (mainly adolescent males) who get a kick out of breaking into computers [1]. Kevin Mitnick [2] who was a hacker was arrested by 1995 FBI to suspicion to have stolen software and all kinds of data etc. from as penetrated into a computer network.

Security measures about an attack of hackers seem to be paradox of a window and a shield, and it is to develop an early security book to prevent if a form of a new attack of a hacker is grasped. An attack of the hacker who let you damage is attacking DoS(Denial of Service) Attacks using Nameservers in 2000, Code Red II, Nimda in 2001, MS SQL Server slammer in 2002, Blaster in 2003, and W32/Novarg.A, NetSky in 2004 [3] exploit for a vulnerability in phpBB's in 2005 [4]. exploitation of a vulnerability in the way Microsoft Internet Explorer in 2006 [5].

An attack of a hacker caused network traffic, and penetrated illegally into a network computer system, and to be serious over the whole worlds. There are firewall [6] and HIDS, NIDS [7] and Viruswall [8] like Fig.1. in the existing network security system. Firewall does an invasion interception as installed in gateway of an inner network. Be installed in an inner network, and HIDS, NIDS does intrusion detection. Viruswall cures computer Virus of a host and a network.

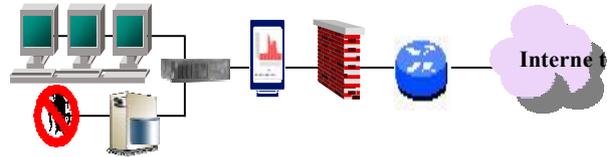


Fig.1. The existing network security system.

The existing Firewall the following disadvantage exists.

- 1) There is not a defense book about dynamic attacks such as DoS, the Worm which used large packet etc., or response is late. 2) Investigate a header of packet only, and Payload does not investigate it. 3) Proxy Service of Application Level cause bottleneck phenomenon of packets, and communication performance delay at gateway. The existing IDS the following disadvantage exists. 1) Misuse Detection is difficult about an unknown attack pattern. 2) Detection misjudgment ratio is high in case of Anomaly Detection about short length packet [9]. 3) There is a little the protective operation which is aggressive after intrusion detection.

Study of this paper will be studied Intelligent Connection of Network Security System overcoming these disadvantages. And it is composed to a boundary part of external, internal of a network and security systems for invasion prevention to be located in gateway and an internal network like IPS(Intrusion Prevention System) [10].

2. RELATED WORK

I study an attack by generations of the hacker who is the related study that cared for proposed security systems. more than. Was infringed from attacks of 5th generations of hackers at recent 6th generations, and consider it to analysis data through the results and Data Base.

A hacker makes a computer virus through a computer and networks in order to attack the target object. An attack of a hacker and a computer virus try to be divided by generations. 1th generation used Primitive Virus, 2th generation used Encryption Virus, 3th generation used Stealth Virus, 4th generation used Armour Virus.

While 5th generations circulate it so that use Worm Virus, and viral oneself is duplicated through other network and systems large by intention of an invader did it so as to attack it. This attack is a Code Red v.2 attack like a DoS attack. Propagation of Code-Red Worm used weakness point of Windows index server, and scattered. Buffer overflow of Remote existed in a Microsoft IIS web server version, and was known at that time. Hacker generated Code-Red Worm, and used this weakness point. 2001 years started an attack, and international server more than 359,000 was infected by attacks through 2001. July 19. Code-Red II. Worm through July 12. Code-Red I. Worm. Therefore caused economic assumed loss more than 2,600 million dollars, and avoid same with star

Adesh Kumar and Vijay Maheshawari are with Shobhit University, Meerut (India), Corresponding Author : adesh.mtech56@gmail.com

statistics national ten high ranks [11]. The A which is a hacker is control to Master through attack commands, adjust Agents, and adjust Reflectors, and attack the target server which becomes to a short time, and the back jockey agents do it according to commands. Cause explosive increase traffic, and attack target server is hard to be equal to traffic, and network service makes discontinuance it like these results.

Let hacker come off an answer to be delivered to hosts to attack as deal with an answer about an accessed connection SYN request from attack object server, and the DDoS attack server of a dependency host attacks a departure of network traffic. And attack it of the N:N which an invader is not exposed to even if I chase it.

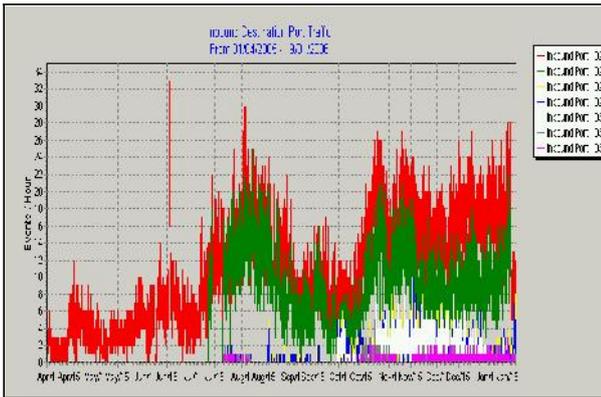


Fig.2. Traffic ratio

Fig.2. showed network traffic by ports from 01/04/2005 to 19/01/2006. The section which was above displayed of a graph is network traffic along an attack. An attack of the current hacker will be made progress to 6th generations at 5th generations. Also, use a low-ranking infection system in the state that expose status of an invader, and do not get through a Command union and hacking by hacking Programming, and attack target. A hacking technique is converted in automation ways at manual operation ways, and is mobilizing the way how explosive increases expansion and harmful traffic by a threat about Internet network serviceability.

3. INTELLIGENT CONNECTION OF NETWORK SECURITY

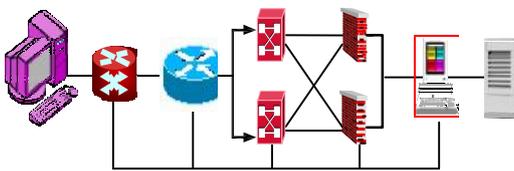


Fig.3. Structure of intelligent connection of network security systems

Fig.3. assumed the network simulation model that network traffic joined an experiment network to have appeared through 1Gbps router the front of internal network and 10 Gbps router which were external router and internal server were connected of 1Gbps router. The external network system that was used so as to verify

intelligent connection IPS generates three 2.5 Gbps phosphorus 7.5 Gbps background traffic and 2.5 Gbps traffic getting a SYN flooding attack and DDoS attacks and infection of a Slammer computer virus done to normal MPEG stream.

Evaluated residual bandwidth of an experiment network as analyzed the performance experiment results. Were proposed, and before start of intelligent connection IPS minimized an influence to reach to the experiment results as reset a firewall system for a test.

A host assumes with one state during permission, infection, 3 state of a movement in simulation experiment. Get infection done for the first time, and the start steps other hosts are all converted with permission state as they select voluntarily a host of external. Copy a computer virus on other host whom an address was generated voluntarily, and a infected host transmits it by a speed of a total circuit.

The results of an experiment network show to a chart between time and packet process ratios as analyze relationship.

4. PERFORMANCE AND EVALUATION EXPERMENT

4.1 Invasion Prevention Experiment about an Attack of a Hacker

A hacker executes it at arbitrary hosts of external for SYN flooding attacks to have been made as use an address to have been forged. SYN flooding attack used The Regents of the University of California [13]. Send the IP address packet which deceive a client, and was forged to a network. Network Neighborhood executed it for experiment through direct communication lines.

Hacker used Stacheldraht Tool in order to attack DDos. Also, a hacker brings down a command to Master, and induction gets in a moment the server which target becomes to 1 Gbps packet traffic through Agents and Reflectors attacked it.

A Figure 4 is the attack packets which analyzed to the Network Protocol Analyzer Etheral version0.99.0.[14]

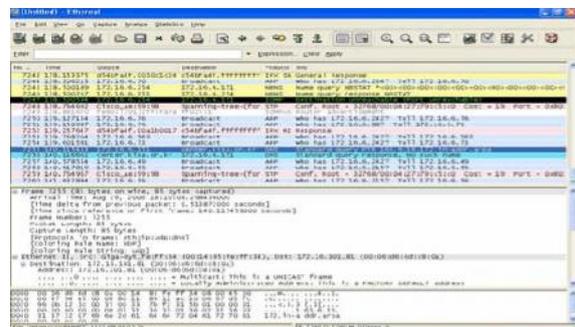


Fig 4. attack packets analyzed to the Etheral version0.99.0

Packet size viral Slammer Worm did it with 376 bytes. Infection delay time did it so as to transmit it after reproductions toward a secondary infection host as played assumption by 0.1 second the beginning [15]. If reinfection by other computer viruses reproduced works, infected host should not exchange an infection action. A traffic generator sends Slammer packet to a traffic analyzer about Slammer computer viruses in order to evaluate efficiency.

A generator sends it to the destination address which was selected voluntarily. Assumed increase about radio waves of a Slammer computer virus according to medical charge time of infected hosts in order to analyze the attack detection, analyses and security policy renewal, an influence of invasion prevention. And were independent, and selected voluntarily the non infected host, and faced the host selected each time of infection process particularly whether or not were by infection tested it.

Fig.5. appeared to what an attack began, and was proposed through SYN flooding within two seconds, and an attack by systems was cut off. Caused a DDoS attack, and in 13 seconds sections of a hacker Fig.4. got you through explosive increasing traffic of 1Gbs about target server of internal.

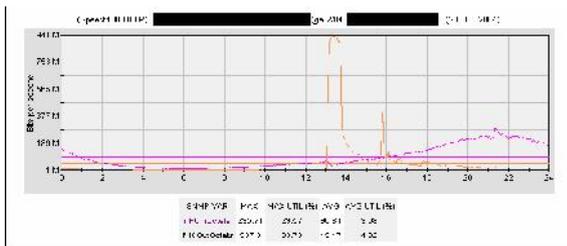


Fig 5. Protective graphs at intelligent connection of network security system

But invasion prevention system to be connected to router, firewall to IPS showed the results that had prevented an attack of DDoS, and 14 seconds sections cut off malicious traffic, and prevented an invasion. Also, the results value graph dynamically normalization got traffic of a network done like the output ratio that used a Slammer computer virus.

Fig.6. were proposed, and a continuous 4th line shows residual bandwidth in internal networks of intelligent connection of IPS. That is, attacked it, and detected it as grasped actively an attack of a hacker, and publicized to intelligent connection system. The traffic which was a computer virus by invasion blocking and invasion prevention was done away with an interception, and appeared to what can preserve the majority of bandwidth permitted through algorithm of an invasion prevention security rule.

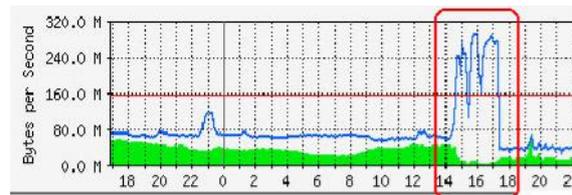


Fig.-6 Protective operation about a Slammer virus attack.

5. CONCLUSION

I studied it with an attack of 5 households and 6 households that was an attack tendency of a recent hacker and investigation about the damage at thesis. Proposed intelligent connection of IPS at papers watched the existing firewall and a disadvantage of an invasion detection system that was used in order to prevent an attack of a hacker, and to have seen them in order to solve a problem.

It is the ways which designed at these papers. 1) The bypass passage that, first of all, is an enemy of authenticated packet at external routing. 2) Attack detection of an external router. 3) Bandwidth expansion. 4) It is attack information delivery to connected security system. 5) A generation of a filter. 6) Filtering rules setup of IPS and Firewall 7) Dynamic update of blocking filter 8) Dynamic network security system formation. Were designed as proposed, and reset used a possible process, and imposed firewall of external and internal router and switching devices and gateway, and intelligent connection of IPS detected attack packet and service, and installed blocking filter and the IPS which prevented in an internal network.

Executed a SYN flooding attack and a DDoS attack and a Slammer attack to attack traffic of 1 Gbs in speeds wire 10Gbs in performance experiment. Cut off a SYN flooding attack, and the results that they attacked it, and they executed, the security system that proposed it DDoS attack and Slammer attack did a blocking.

If an attack was detected, these results enlarged bandwidth through reset of L4, L7 switching devices at router. Public information about attack information was performed dynamically, and generated a filter of intelligent filtering algorithm, and dynamic renewal and Up-date were executed.

As a result, packet by attacks of a hacker was drop, and traffic was decreased, and ensured the residual bandwidth which was normal of internal and traffic of an external network besides normal packet. Improved a traffic delay, and therefore intelligent connection of IPS appeared as improved the existing invasion blocking and a disadvantage of an invasion detection system.

6. REFERENCES

- [1] Eric S. Raymond. (Editor): <http://www.catb.org/~esr/faqs/hacker-howto.html>. 7 Mar 2006
- [2] Kevin Mitnick.: <http://www.webster.edu/~kmitnick/courses/frosh/dairy/mitnick.htm>
- [3] CERT/CC Incident Notes.: <http://www.cert.org/> incident notes
- [4] Exploit for a vulnerability in phpBB's.: August 01, 2005-Current Activity. <http://www.us-cert.gov/current/archive/2005/08/01/archive.html>
- [5] Exploitation of a vulnerability in the way Microsoft Internet Explorer.: <http://www.us-cert.gov/current/archive/2006/04/03/archive.html#iememfail>
- [6] Ray Hunt, Theuns Verwoerd.: Reactive firewalls a new technique. Computer communication 26. (2003) 1302-1317
- [7] Dreger H, Kreibich C, Paxson V, Sommer R.: Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context. Lecture Notes in Computer Science, Vol. 3548 (2005) 206-221
- [8] TREND MICRO White Papers.: The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast (2006)
- [9] JensTolle, Marko Jahnke, Michael Bussmann, SvenHenkel.: Meta IDS Environments: An Event Message Anomaly Detection Approach. Proceedings of the Third IEEE International Workshop on Information Assurance (2005)
- [10] McAfee.: White Paper_Host and Network Intrusion Prevention. http://www.mcafee.com/us/local_content/white_papers/wp_host_nip.pdf, (2005)
- [11] David Moore, Colleen Shannon, Jeffery Brown.: Code-Red: a case study on the spread and victims of an Internet Worm. Internet Measurement Workshop (2002)
- [12] Masaru KATAYAMA, Hidenori KAI, Junichi YOSHIDA, Hiroki YAMADA, Kohei SHIOMOTO, and Naoaki YAMANAKA.: A 10Gb/s Firewall System for Network Security in Photonic Era. IEICE TRANS. Vol. E88-B, No. 5, (2005)
- [13] Vulnerability Note VU#596827.: <http://www.kb.cert.org/vuls/id/596827> FedCIRC Advisory FA- 000-01 Denial-of-Service Developments.: <http://www.uscert.gov/federal/archive/advisories/FA-2000-01.html>
- [14] Etheral version0.99.0. <http://www.ethereal.com/download.html> (2006)
- [15] David Moore, Vern Paxson.: Inside the slammer worm. IEEE COMPUTER SOCIETY, (2003)
- [16] MRTG -2.14.6. <http://oss.oetiker.ch/mrtg/> (2006) computer and networks, Mobile Communication, Ubiquitous Information Security.



Adesh Kumar is pursuing M.Tech. at Shobhit University, Meerut. His research areas are Network Security, SAP, digital communication etc.



Vijay Maheshwari did his M.Tech. from Shobhit University, Meerut. He is also an Assistant Professor in Shobhit University, Meerut. His research interest includes Genetic Algorithms & Neural Network Design.