

HTTP Packet Inspection Policy for Improvising Internal Network Security

Kuldeep Tomar

Research Scholar, Department of CSE, MRIU, Faridabad, India
Email: kuldeep_karan@rediffmail.com

S.S. Tyagi

Professor and Head, Department of CSE, MRIU, Faridabad, India
Email: shyam.fet@mriu.edu.in

Abstract—Past few years the use of Internet and its applications has increased to a great extent. There is also an enormous growth in the establishment of computer networks by large, medium and small organizations, for data transfer and information exchange. Due to this huge growth, incidents of cyber-attacks and security breaches have also increased. Data on a network is transferred using protocols such as Hyper Text Transfer Protocol, which is very vulnerable. Many types of malicious contents are hidden in packets that are transferred over a network or system, which may can to get it slow, crash or buffer overflow etc. Thus it is very important to secure networks from such types of attacks. There are lots of mechanisms available but still they are not good enough because of dynamic environment. Such kind of attacks can be countered by applying appropriate policies on network edge devices like Adaptive Security Appliance, firewalls, web servers, router etc. Also the packets which are transferred between networks, they should deeply inspect for malicious or any insecure contents. In this paper firstly we would study Network security issues and available mechanism to counter them our focus would be on inspecting the HTTP packets deeply by applying policies on ASA. Finally we would use Graphical Network Simulator (GNS3) to test such a policy.

Index Terms—Security, Traffic, Policy, HTTP, ASA, GNS3.

I. INTRODUCTION

With rapid increase in the usage of computers for general and business purpose, large number of computer networks has been established leading to critical issues like Computer network security or cyber security. Network administrator can apply any type of rule or policy on incoming and outgoing packet boundary. Rule is a type of signature but whereas policy is a combination of several rules and protocol is a group of policy which is applied according to different network environment.

In computer network protocols plays an important role. Many protocols are used to transfer different type of data. But in this paper we have used Hyper Text Transfer

protocol (HTTP) that is used for web based applications and also helpful in defining how messages are transmitted or formatted. It is a web application layer protocol which also very vulnerable and many attackers can exploit http to perform security breaches. There are many types of attacks which can happen to computer network. Approx 50 percent of widely exploited vulnerabilities are caused by buffer overflow and its ratio is increasing over time [1]. One of the most famous examples in early days is the Internet worm in 1988 that makes the use of buffer overflow vulnerabilities and infected thousands of computers [2]. In today's dynamic environment there are many security enforcing mechanism available few them are discussed in this paper. By enforcing appropriate policies and rules on network edge devices like routers, ASA, state inspection firewalls and web servers etc., security can be enhanced. Basically the effectiveness of any network security mechanism depends on providing any protocol or tool that facilitate system administrator to analyze the accuracy of these policies.

Deep packet inspection (DPI) is networking technologies that facilitate to inspect data in real time on key points, devices in a network [3]. It will provide us a facility for analyzing from layer 1 to the layer 7 of the packet. DPI can scan any type of application including different protocols like HTTP, POP, SMTP, POP3 etc. There are lots of mechanisms and tools are newly applied but still we are facing much type of problems in the web world. In this paper our main focus point is to deeply inspect HTTP packet by applying policies on network edge devices.

Lots of research work is performed for securing networks by deep packet inspection, on protocols like HTTP. Antonio Liov, Cataldo Basila done analysis of packet filters using policies for application firewalls [4]. AL-Shsaer along with his other research fellows has done valuable contribution by applying policies using algorithms for next generation firewalls [5]. We have discussed contribution of few other researchers in the section II (Background and Related Work) of this paper.

In the content organization of this paper, our first paragraph would be on Introduction to the concept of this paper and in our second paragraph we would discuss the work done by earlier researchers, their contribution in this

field. In the third paragraph we would focus upon types of Network Security Issues and attacks related to HTTP Protocol, in respect to the dynamic computing environment. Many types of attacks and security breaches can occur on Computer Networks, in which HTTP flooding attack is also a major threat which can lead to denial of service or network outage. In the fourth paragraph we would discuss the currently available protection mechanism and our focus would be on deep packet inspection (DPI). In the fifth paragraph we would be explaining what the main contributions of our work are, how it can be used for enhancing security. In the sixth paragraph we would explain simulation and experimentation by using advanced policy which is to be implemented on ASA using Graphical Network Simulator (GNS3). We would be showing simulated Network diagram, coding of the implemented policy, screenshots showing success results of the implemented policy. In the Last paragraph we would conclude the work of our paper including future work that can be carried out, followed by references and author Profile. In our opinion this paper can act as a base for creating awareness and enhancing Security in an Internal Network, using advanced policies or rules to be applied on Network edge devices.

II. BACKGROUND AND RELATED WORK

There are many researchers who had done lots of work on packet inspection and packet filtering, may be just even after the establishment of first Network. We have studied and get inspired by the work of many researchers, who have done valuable contribution in this area. Few papers related rules set packet filtering, policies mitigating HTTP related attacks and implementing deep packet inspection policies on firewall etc are following:

Cataldo Basile, Antonio Lioy, has done a valuable contribution in their paper [6] which extends a previous model for analysis of packet filters to the policy anomaly analysis in application firewalls. Both rule-pair and multi rule anomalies are detected, hence reducing the likelihood of conflicting and suboptimal configurations. The expressiveness of this model has been successfully tested against the features of Squid, a popular Web caching proxy offering various access control capabilities. The tool implementing this model has been tested on various scenarios and exhibits good performance.

Gouda and Liu [8,15] introduced techniques based on Firewall Decision Diagrams, in the field of rule set optimization by redundancy removal Focus on distributed Firewalls [9] and analysis of single packet filters [10] was by Al-Shaer. Their work has two main limitations: It considers only the packet filter scenario and they detect only anomalies in rule. Their classification is the starting point of several works that share the same limitations.

Anja Feldmann, Jennifer Rexford, and Ramon Caceres [12] basically focus on 3 parameter aggregation, timeout and trigger and also analyze the effect of these parameter on 3 metrics traffic percentage, setup rate, and number of shortcut.

Zhibin Zhang work on stateful packet inspection policy[14], It is a type of dynamic packet filtering firewall technology where the main focus point is to monitor the status of active user. SBI analyze packet from physical layer to application layer [20]. System administrator can fix some set of parameter based on port number range, packet length, header size etc for analysis.

Wool, A., Tel Aviv Univ., Tel Aviv, Israel [16] work on "Errors: Measuring the Holes in Swiss Cheese". In this paper a rule/signature based check point engine is used which collect full state information about packet from all layers and also store these information in a table known as dynamic state table. In check point firewall rule set an inspection module is used that scan packet and then pass through TCP/IP stack [17, 21]. If case packet get fail then either it is rejected or dropped by firewall.

In 2012 Mohamed Ibrahim AK, Lijo George, Kritika Govind, S. Selvakumar, proposed and tested an Kernel level HTTP filter based on Threshold value to allow only genuine HTTP GET request in the system leading to protection from DDoS attack [24]. Few Attackers tries to set a trap to exploit Uniform Resource Locator (URL) to generate HTTP GET flooding attack, because of existing solutions to prevent HTTP attacks are based on usage of Access Control Lists (ACL) and browser level cache maintenance. These types of techniques generally get failed when they are subjected to dynamic URL based HTP attacks. The solution proposed in their paper was tested and results shows that only genuine HTTP GET requests were allowed rest all malicious HTTP requests were filtered.

Kannaiyaraja, Babu, Senthamaraiselvan, Arulandam, in their paper [22], "Routers Sequential Comparing Two Sample Packets for Dropping Worms", performed valuable experiments to generate results to find out malicious contents by comparing first two packets leading to inspection of packets to avoid network Intrusion.

Akbaş, E., Hakem Bilisim, Istanbul [18] basically works on content filtering. In this technique a strain driver filters all incoming and outgoing packet. In case of filtering structure a policy based criteria is applied and based on this criteria at the run time black-list and white-list packets are identified for blocking or passing the packet. By using this technique packet transmission act separately.

Al-Shaer, E.S., Hamed, H.H. have done valuable contribution in their paper [19] which enhance the correctness of next generation firewall rule policies. In this paper a firewall policy advisor tool is used to written algorithm for creating error free rule-generation, rule-modification and rule-deletion. A basic formalization structure of firewall rule relation for the all possible relation is created. Each and every rule is passed through this algorithm.

III. NETWORK SECURITY ISSUES

In today's dynamic computing environment attacks on

computer networks are increasing day by day. There are many issues, few of the security issues or major attacks [4] which occur on computer networks are discussed below:

- Manipulation with router updates can cause traffic to flow to unauthorized destinations. These kinds of attacks are sometimes called “route injection” attacks.
- When an attacker manipulates IP packets to falsify IP addresses then masquerading attack takes place. Masquerades can be used to inject false data into a network or gain unauthorized access.
- Poor configuration, deployment of appropriate security detection, prevention mechanisms and tools in a network can also create serious problems.
- Users form a network access such websites from which malicious programs can be injected to internal network by which secret information can be compromised or get manipulated.
- In the case of land attack router receives packet with matching / same IP address at the both destination and source address fields, and with the similar port number in the destination port and source port fields. It may cause denial of service or degrade the performance of the router.
- TCP SYN Attack involves many uncompleted transmitted connections on the destination. By this attack the genuine TCP user connection queues are filled up and thus services are denied to them. It has been shown that more than 90% of the DOS attacks use protocols [5]. The TCP SYN flooding is the most commonly-used attack. It consists of a stream of spoofed TCP SYN packets directed to a listening TCP port of the victim. Not only the Web servers but also any system connected to the Internet providing TCP-based network services, such as FTP servers or Mail servers.
- DOS attacks: Denial of service attacks is one of the most dangerous attacks and a major threat to small & large organizations networks, systems, users etc. By increased usages of internet there is high increase in denial of service (DOS) attacks [6] [23]. The main aim of this attack is the denial of services by attempting to bound access to a service or machine. According to recent surveys DoS attacks are a major threat, leading to Cyber attacks. DOS attacker consumes a large set of memory area of the target machine or devices so that it cannot be compatible to provide services to the users, or it may be able to reboot, system crash or denying services to legitimate users. Just about one or other server or host may experience DOS attacks at any time.

Some common DOS attacks are:

Death of Ping request: enormous ICMP packet create a sequence of fragmented packet with same offset value. That’s why system will create

different type of problem like rebooting, crashing etc [7].

Flood of ICMP Packet: Attacker can send thousands of fake requests to a particular system so that system cannot longer work properly.

- HTTP GET flooding attack: The attacker sends an overwhelming number of HTTP GET or HTTP POST requests to the targeted HTTP server, depleting the victim’s resources. The requests have legitimate contents and they originate over valid TCP connections. By serving those requests as normal requests, the server ends up exhausting its resources.

Organizations must deploy a comprehensive detection system to constantly map and monitor activities to prevent hackers from slipping anything past their networks’ defenses. It’s the role of network administrator to deploy an efficient mechanism for Identification, authorization and to keep track of activities being logged and looked upon.

IV. PROTECTION MECHANISM

There are many mechanisms available to counter Network Security breaches few of them are discussed briefly below:

- IDS/IPS: Also known as IDPS (Intrusion detection and prevention system). It detects the intrusion & then protects our network from application level attack. Mainly IDS/IPS is used to identify malicious activity and attempts to provide an alert or block/stop it. For providing higher level security we can use DPI (Deep Packet Inspection) in place of simple IDS.
- ISP edge Router: This edge device can accept traffic with source address that belongs to the customer network & in other side same customer network can also accept traffic with source address.
- Reactive Mechanism: These mechanisms reduce the impact of attack on the victim. These mechanisms are also called as early working systems which respond to an attack immediately when the attack is detected.
- Firewall: Firewall is a type of security mechanism system that controls the intrusion or say virus packet by analyzing incoming and outgoing packet at network. Basically firewalls are categorized as Hardware and Software firewalls. Generally routers are treated as hardware firewalls and Operating Systems of next generation has inbuilt firewall which restricts internal networks are called as software
- firewalls. Based on communication state, firewalls can be categorized as Packet filters, Application Layer Firewalls, Proxy Servers and Network Address firewalls.

- Deep Packet Inspection: DPI [13] is a networking technology that ISP uses to monitor what applications are receiving and releasing traffic on the network. As we know that data on the internet flows in the form of packets with the help of protocols like TCP/IP, HTTP etc. These packets are made of two main elements: payloads and headers. Header role is to provide destination address and the payload contains data. Using DPI packet are more deeply analyzed and examine the content of communications and based on certain set of user defined or privately defined policies can accelerate or decelerating the packets or can drop them.

There are many mechanisms available to enforce security in a network or edge devices, still they are not enough as newer networks are being established day by day also the technologies are changing rapidly. In this paper our approach is to apply some policy to counter HTTP packet flood attack on network edge devices like ASA (Adaptive security appliance) or firewall and we would simulate them using GNS3 network simulator.

V. MAIN CONTRIBUTIONS OF OUR WORK

- Studying different types of Network security issues or attacks.
- Analyzing the importance of HTTP Deep Packet Inspection.
- Applying a Policy to enhance Network Security on Edge devices.
- Testing the policy using GNS3 network simulator to protect our network from attacks like HTTP GET flooding attack.

VI. SIMULATION AND EXPERIMENTATION

In our work, Attackers flood to the target system with connection requests from outside network to internal network. We have developed a simulated environment using Graphical Network Simulator (GNS3) which is a open source Cisco software that simulates complex networks while being as close as possible from the way the real network perform, all of this without having dedicated network hardware such as switches, routers, ASA etc. Here in the Fig. 1, below we have an internal network which contains few systems, connected to a switch connected to a web server/ router, connected to an ASA as network edge device. The Ethernet switch hypervisor runs on 127.0.0.1:7200, Port 1 is in access mode, with native VLAN1, is connected to router / web server Fast Ethernet 0/1. Router / web server is dynamic emulated Cisco 3725 with 256 MB RAM, Router hypervisor runs on 127.0.0.1:7200, console is port 2102. Fast Ethernet 0/0 is connected to emulate device ASA1 Ethernet1. Hardware is genu-emulated Cisco ASA 5520 with 256 MB RAM. ASA firewall wrapper runs on 127.0.0.1: 10525, console is on port3001. Attacker device

hardware is dynamics emulated Cisco 3275 with 256 MB RAM. We simulate that the attacker attacks from outside the internal network and tries to flood the target system by HTTP flood messages. Large number and different large size HTTP packets are being sent to the victim.

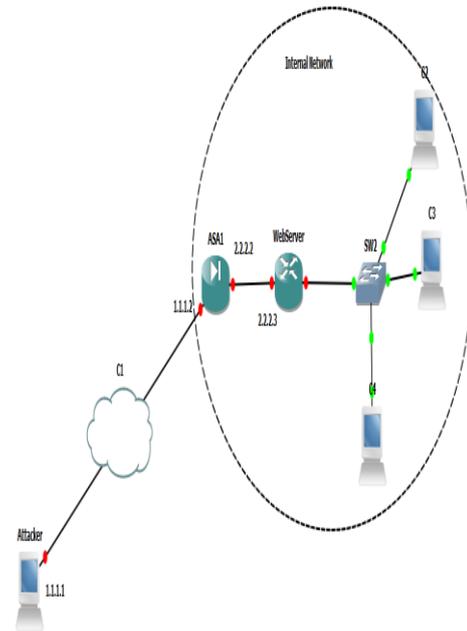


Fig. 1: Network Diagram of Simulated Environment

In this the attacker attempts to crash the system of the target system by sending many packets, so that the victim gets flooded with packets reducing the data sending capacity for normal traffic. Attacker sends many HTTP GET or HTTP POST requests to victims system or network. Those requests have legitimate content and shows to originate on valid connections. By those requests malicious content is also introduced to the victim network or system ending up in network outage. So as to protect our internal network from this attack we apply a policy on edge device. This policy can protect our internal network from following:

- Inspecting the http packet for any content mismatch.
- Deep packet inspection by checking http header.

We apply a policy called KUL_HTTP for HTTP protocol which will work on parameters like get, regex, header length, content type, connection log etc.

Policy

```
class-map type regex match-any GET
class-map type inspect http match-any KUL_HTTP
description "WE have applied a policy named
KUL_HTTP which will inspect http protocol for web
server"
```

- match request header length gt 32
- match req-resp content-type mismatch
- match request method get
- match request body
- regex class GET
- policy-map type inspect http KUL_HTTP
- parameters
- class KUL_HTTP
- drop-connection log
- policy-map global_policy
- class inspection_default
- inspect esmtp
- inspect ftp inspect rsh
- inspect rtsp
- inspect dns preset_dns_map
- inspect skinny
- inspect h323 h225
- inspect sqlnet inspect xdmcp
- inspect netbios
- inspect sunrpc inspect tftp
- inspect h323 ras
- inspect sip
- inspect http KUL_HTTP

Here Fig. 2, displays syntax to remove policy. If we remove KUL_HTTP policy from HTTP packet injection then HTTP cannot perform any type of inspection.

Screen Shot:

```

ciscoasa# conf t
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect HTTP KUL_HTTP
ciscoasa(config-pmap-c)# end
ciscoasa# sh service-policy

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
Inspect: ftp, packet 0, drop 0, reset-drop 0
Inspect: h323 h225 default: h323_map, packet 0, drop 0, reset-drop 0
Inspect: h323 ras default: h323_map, packet 0, drop 0, reset-drop 0
Inspect: netbios, packet 0, drop 0, reset-drop 0
Inspect: rsh, packet 0, drop 0, reset-drop 0
Inspect: rtsp, packet 0, drop 0, reset-drop 0
Inspect: skinny, packet 0, drop 0, reset-drop 0
Inspect: esmtp_default: esmtp_map, packet 0, drop 0, reset-drop 0
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
Inspect: tftp, packet 0, drop 0, reset-drop 0
Inspect: sip, packet 0, drop 0, reset-drop 0
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
ciscoasa#
    
```

Fig. 2: Syntax to Remove Policy

Fig. 3 shows that without the policy there is no inspection for http packets and few parameters like message length, preset_dns_map etc are set. Since there nothing for the inspection of HTTP it means anyone can exploit it.

Screen Shot:

Fig.3: Showing Results without Policy

Now we present a Fig. 4, in which we have shown that how we can add policy from HTTP packet injection. The policy is implemented on Hardware is genu-emulated Cisco ASA 5520 with 256 MB RAM. ASA firewall wrapper runs on 127.0.0.1: 10525, console is on port3001. The policy is implemented by writing on ASA console terminal conf t, policy map global policy, class inspection default then inspect the policy KUL_HTTP by inspect KUL_HTTP and finally writing end. The command sh service-policy shows the status of policy on the ASA console. Here the last line in the screen shot shows the policy is active and lines in the mid show the map name http KUL_HTTP.

Screen Shot:

Fig. 4: Screening the Applied Policy

Fig. 5 and 6, present the status of packet inspection after applying policy. In the simulated scenario attacker tries to send packets to the victim device with IP address 2.2.2.3. From the attacker console we type telnet 2.2.2.3 80 and then the connection is open and then we send some data to internal network the ASA deployed in between with the inspection policy does packet inspection and the packet / header are deeply inspected and if contains any content mismatch or say larger size malicious packets they would be dropped.

Screen Shot:

```

ciscoasa(config)# sh ser
ciscoasa(config)# sh service-policy

global policy:
  service-policy: global_policy
  class-map: inspection_default
  Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
  Inspect: ftp packet 0, drop 0, reset-drop 0
  Inspect: h323 h225_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: h323 ras_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: netbios, packet 0, drop 0, reset-drop 0
  Inspect: rsh, packet 0, drop 0, reset-drop 0
  Inspect: rtsp, packet 0, drop 0, reset-drop 0
  Inspect: skinny, packet 0, drop 0, reset-drop 0
  Inspect: esmtp_default_esmtp_map, packet 0, drop 0, reset-drop 0
  Inspect: sqlnet, packet 0, drop 0, reset-drop 0
  Inspect: suwpc, packet 0, drop 0, reset-drop 0
  Inspect: tftp, packet 0, drop 0, reset-drop 0
  Inspect: sip, packet 0, drop 0, reset-drop 0
  Inspect: xmcp, packet 0, drop 0, reset-drop 0
  Inspect: http, packet 0, drop 0, reset-drop 0

ciscoasa(config)# sh service-policy

global policy:
  service-policy: global_policy
  class-map: inspection_default
  Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
  Inspect: ftp packet 0, drop 0, reset-drop 0
  Inspect: h323 h225_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: h323 ras_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: netbios, packet 0, drop 0, reset-drop 0
  Inspect: rsh, packet 0, drop 0, reset-drop 0
  Inspect: rtsp, packet 0, drop 0, reset-drop 0
  Inspect: skinny, packet 0, drop 0, reset-drop 0
  Inspect: esmtp_default_esmtp_map, packet 0, drop 0, reset-drop 0
  Inspect: sqlnet, packet 0, drop 0, reset-drop 0
  Inspect: suwpc, packet 0, drop 0, reset-drop 0
  Inspect: tftp, packet 0, drop 0, reset-drop 0
  Inspect: sip, packet 0, drop 0, reset-drop 0
  Inspect: xmcp, packet 0, drop 0, reset-drop 0
  Inspect: http, packet 131, drop 0, reset-drop 0

ciscoasa(config)#
  
```

Fig. 5: Status of Packets Inspected and Policy Applied

Screen Shot:

```

ASA#
Class-map: inspection default
  Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
  Inspect: ftp, packet 0, drop 0, reset-drop 0
  Inspect: h323 h225_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: h323 ras_default_h323_map, packet 0, drop 0, reset-drop 0
  Inspect: netbios, packet 0, drop 0, reset-drop 0
  Inspect: rsh, packet 0, drop 0, reset-drop 0
  Inspect: rtsp, packet 0, drop 0, reset-drop 0
  Inspect: skinny, packet 0, drop 0, reset-drop 0
  Inspect: esmtp_default_esmtp_map, packet 0, drop 0, reset-drop 0
  Inspect: sqlnet, packet 0, drop 0, reset-drop 0
  Inspect: suwpc, packet 0, drop 0, reset-drop 0
  Inspect: tftp, packet 0, drop 0, reset-drop 0
  Inspect: sip, packet 0, drop 0, reset-drop 0
  Inspect: xmcp, packet 0, drop 0, reset-drop 0
  Inspect: http NUL HTTP, packet 161, drop 0, reset-drop 0

ciscoasa# en
  
```

Fig. 6: Status of Packets Inspected

VII. CONCLUSION AND FUTURE WORK

With rapid usage of computers attacks on networks is increasing day by day. While advanced techniques have been continuously developing for several years, it is very important to protect our office and business networks from new evolved attacks. Recent surveys have clearly revealed that attacks on smaller organizations has increased to a great extent. Many Attackers like to exploit protocols for sending malicious contents. Thus there is a great need of more awareness among users and the development of advanced security policies, rules, devices to protect networks form security breaches. In this paper network security issues are discussed. There are many mechanisms available to counter these types of attacks but for small organizations or small networks it is very hard to implement, configure or purchase mechanisms. Internal networks of small organizations can be well protected by applying improvised policies on edge devices like routers, ASA, web servers, firewalls etc. Our simulation using GNS3 shows that policy inspection success rate becomes very high and the packets were inspected. Further work is needed to investigate high level of monitoring is required for knowing attack categories their signatures and there is a great need to develop more efficient rules or policies which can be implemented on edge devices to counter maximum types of attacks with higher success rate and efficiency.

REFERENCES

- [1] Zili Shao, Chun Xue, Qingfeng Zhuge, Meikang Qiu, Bin Xiao, Edwin H.-M. Sha, "Security Protection and Checking for Embedded System Integration against Buffer Overflow Attacks via Hardware/Software", IEEE Transactions on Computers, Vol. 55, NO. 4, April 2006.
- [2] E.H. Spafford, "The Internet Worm Program: An Analysis," Technical Report TR823, Purdue Univ., 1988.
- [3] Ralf Bendrath, European Parliament, Milton Mueller, "Deep Packet Inspection and Internet Governance".
- [4] A white paper on "Stateful Inspection Firewalls" by Chris Roeckl Director, Corporate Marketing.
- [5] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, "Conflict classification and analysis of distributed firewall policies," IEEE J. Sel. Areas Commun., vol. 23, no. 10, pp. 2069–2084, Oct. 2005.
- [6] Cataldo Basile, Antonio Liroy, "Analysis of Application-Layer Filtering Policies With Application to HTTP", IEEE/ ACM Transactions on Networking, 1063-6692, 2013 IEEE.
- [7] Akbaş, E., Hakem Bilisim, Istanbul, "Next generation filtering: Offline filtering enhanced proxy architecture for web content filtering", Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium.
- [8] A. X. Liu, M. G. Gouda, "Complete redundancy detection in firewalls," in Proc. IFIP Data Appl. Security Conf., Storrs, CT, USA, Aug. 7–10, 2005, pp. 193–206.
- [9] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, "Conflict classification and analysis of distributed firewall policies," IEEE J. Sel. Areas Commun., vol. 23, no. 10, pp. 2069–2084, Oct. 2005.
- [10] Anja Feldmann, Jennifer Rexford, and Ramon Caceres, "Efficient Policies for Carrying Web Traffic Over Flow-Switched Networks", IEEE/ACM transactions on networking, vol. 6, no. 6, December 1998.

- [11] Zhibin Zhang, Yanjun Zhang, Li Guo, Binxing Fang, "LASF: A Flow Scheduling Policy in Stateful Packet Inspection Systems", Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium.
- [12] A. Mayer, A. Wool and E. Ziskind. "Fang: A Firewall Analysis Engine." Proceedings of 2000 IEEE Symposium on Security and Privacy, May 2000.
- [13] Wool, A. ;Tel Aviv Univ., Tel Aviv, Israel, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese" Internet Computing, IEEE (Volume:14 , Issue: 4).
- [14] Check Point FireWall-1, version 3.0. White paper, June 1997. <http://www.checkpoint.com/products/whitepapers/wp30.pdf>.
- [15] Mohamed Ibrahim AK, Lijo George, Kritika Govind, S. Selvakumar, "Threshold Based Kernel Level HTTP Filter (TBHF) for DDoS Mitigation", I. J. Computer Network and Information Security, 2012, 12, 31-39 Published Online November 2012 in MECS.
- [16] Kannaiyara, Babu, Senthamaraiselvan, Arulandam, "Routers Sequential Comparing Two Sample Packets for Dropping Worms", I. J. Computer Network and Information Security, 2012, 9, 38-46, Published Online August 2012 in MECS.
- [17] Akbaş, E., Hakem Bilisim, Istanbul, "Next generation filtering: Offline filtering enhanced proxy architecture for web content filtering", Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium.
- [18] Al-Shaer, E.S., Hamed, H.H., "Firewall policy advisor for anomaly discovery and rule editing", Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium.
- [19] Harshita B, N Ramesh, "A Survey of Different Types of Network Security Threats and its Countermeasures", International Conference on Electrical, Electronics and Computer Engineering, May 2013. Mysore, ISBN: 978-81-927147-3-8.
- [20] D. Moore, G. Voelker and S. Savage, "Inferring Internet Denial of Service Activity", Proceedings of UNIX Security Symposium' 2001, August 2001.
- [21] D. Moore, G. Voelker, and S. Savage, "Inferring internet denial-of-service activity, Technical report, DTIC Document", 2001.
- [22] Mitko Bogdanoski, Tomislav Shuminoski, Aleksandar Risteski, "Analysis of the SYN Flood DoS Attack", I. J. Computer Network and Information Security, 2013, 8, 1-11 Published Online June 2013 in MECS.
- [23] A white paper on "Stateful Inspection Firewalls" by Chris Roeckl Director, Corporate Marketing.
- [24] Christopher Parsons, "Literature Review of Deep Packet Inspection," Prepared for the New Transparency Project's Cyber- Surveillance Workshop, Version 4.1: March 6, 2011.

Authors' Profiles



Dr. S. S. Tyagi is presently working as a Professor and Head of the Department of Computer Science and Engineering in Manav Rachna International University, Faridabad born on 8th February 1970. He completed his Ph.D in Computer Engineering from Kurukshetra University, Kurukshetra in the year 2010. He did his M.E in software

systems from BITS Pilani in the year 2002 and B.Tech in Computer Engineering from Nagpur University, Nagpur in 1992. He is having an experience of 22 years including 4 years of industrial and 18 years of teaching experience. He has been holding various academic and administrative positions during his career. He is having a vast experience of teaching B.Tech, M.Tech, MCA and Ph.D Students. Presently he is a Professor and Head of the Department of Computer science and Engineering and also of the Department of Information Technology. He has been consultant to some software development companies. He has been an examiner and evaluator for M.Tech thesis and Ph.D thesis. He has been a reviewer for books and research papers for some renowned and reputed journals. He is guiding 07 Ph.D. Scholars in the field of Ad hoc networks, Cloud Computing, Wireless Security etc. There are around 40 publications to his credit published in reputed International Journals, National Journals and in the proceedings of International and National Conferences and contributing to the research for the benefit of mankind and society at large. His knowledge covers all major areas of Computer Science and Engineering. Currently his areas of research interest are Wireless Communication, Mobile Ad hoc Networks, Cloud Computing and Network Security.

Dr. S. S. Tyagi, Professor in Computer Science and Engineering Department, MRIU is member of various professional bodies like IEEE, CSI, QCI, ASQ etc. Complete details are as under

Membership of Professional Bodies / Institutions

Member of IEEE, Membership No.: 90841287.

Member Quality Council of India, Member No. ORG/CM/NR/213.

Member of Academic Council at Manav Rachna International University.

Chairman of Board of Studies (CSE & IT) at FET, Manav Rachna International University.

Member of BOF (Board of Faculty) at Manav Rachna International University.

Member of DRC (Departmental Research Committee) at Manav Rachna International University.

Member of American Society of Quality (ASQ).

Member of Computer Society of India (CSI) Mem no : N1217461.

Dr. S. S. Tyagi has worked for the academic and overall development of the Department of Computer Science and Engineering at MRIU for its academic excellence and he has been organizing International Conferences, National Workshops, Faculty Development Programmes and expert lectures on regular basis and contributing a lot for academic learning and overall development of faculty members and the students. He is also used to deliver expert lectures for the students and faculty members and professionals. He has been achieving good placement records for his students every year.



Kuldeep Tomar is a Research Scholar in the Department of CSE, MRIU, Faridabad, 121001, India. He is currently working as Associate Professor and Head of the Department of CSE in NGFCET, Palwal, Faridabad, and Haryana. He was born in Sonapat, Haryana on 2nd Oct, 1978. He has done M.E/ M.Tech in Computer Science and

Engineering from C.I.T.M., Faridabad, India.

He has a total experience of 12 years in different organizations. He is currently working as Associate Professor in NGF College of Engineering & Technology, Palwal, Faridabad,

Haryana. He also has worked as Assistant. Professor in Skyline Institute of Engineering & Technology, Gr. Noida; as Senior Lecturer in B.S.A.I.T.M., Faridabad; as Technical Head/Manager at SSI (Software Solutions Integrated Ltd. and as Sr. Faculty at Hartron Workstation (Haryana Govt. Undertaking).

He has published more than 12 papers in International/National Journals and conferences etc. Has is also written a book. He also is a member of Computer Society of India, Membership No:N1039627.

How to cite this paper: Kuldeep Tomar, S.S. Tyagi, "HTTP Packet Inspection Policy for Improvising Internal Network Security", IJCNIS, vol.6, no.11, pp.35-42, 2014. DOI: 10.5815/ijcnis.2014.11.05