Evaluation of network security based on next generation intrusion prevention system

Gilang Intan Permatasari Duppa[1], Nico Surantha*[2]
Computer Science Department, Binus Graduate Program–Master of Computer Science,
Bina Nusantara University, Indonesia
*Corresponding author, e-mail: gilang.duppa@binus.ac.id[1], nico.surantha@binus.ac.id[2]

Abstract

Next Generation Intrusion Prevention System (NGIPS) is a system that works to monitor network traffic, to detect suspicious activity, and to conduct early prevention toward intrusion that can cause network does not run as it supposed to be, NGIPS provides vulnerability protection broader compared to the traditional IPS, especially in the application layer that has ability to detect and learn vulnerability asset and carried out layering inspection until layer 7 packet. This paper intended to analyze and evaluate the NGIPS to protect network from penetration system that utilize the weakness from firewall, that is exploitation to HTTP port. By the existence of NGIPS, it is expected can improve the network security, also network administrator could monitor and detect the threats rapidly. Research method includes scenario and topology penetration testing plan. The result of this research is the evaluation of penetration testing that utilizes HTTP port to exploit through malicious domain. The evaluation conducted to ensure the NGIPS system can secure the network environment through penetration testing. This study can be concluded that it can become reference to optimize network security with NGIPS as network security layer.

Keywords: *firewall, intrusion prevention system, next generation penetration testing*

1. Introduction

In the survey conducted by Symantec [1] by investigating 2100 businesses and government institutions from 27 countries in the past 12 months, most businesses suffer cyber losses, both in the form of financial data theft and credit card customer data theft, 92% of the respondents claimed that cyber theft cause significant damage because of the loss of customer confidence and decreased corporate earnings, and in middle-sized company virus attack, spyware, and backdoors were found every day. Various security survey stated that some of the highest threats are virus, penetration system, Denial of Service, insider abuse, Spoofing, Laptop theft, network/data sabotage, and unauthorized insider access. Although, virus is the most significant threat, 66% of the company viewed the penetration system as the most significant. Security in data communication networks intended to protect the space that exist within a network or emerge because the lack experience from the network administrator in maintaining the security of data communication network. The space in the data communication network can be fatal because it can be used by someone who has no authority to commit a crime.

According to Stalling [2] firewall has limited prevention, that is firewall only perform security based on the IP and port packet so that it can allow malicious packet pass through the port allowed by firewall. There are many exploitation that take advantage from the firewall weakness, this often used as a way to launch an additional attack on other internal server [3, 4]. According to Stuart [5] Next Generation Intrusion Prevention System (NGIPS) can detect better in the management attack that occur in network environment. NGIPSis a network security system that work to monitor network traffic, to detect suspicious activity, and carried out early prevention toward intrusion and event that can cause network not to running well as it supposed to be. The Next Generation of IPS is not only help to manage the risk but also allow the IT security team to focus on the effort response vulnerability or attack and work more efficiently when the incidence happened [6, 7].

The problem encountered is the increasing threat of attacks that exploit the flaws of network security by inserting the malicious packet or malware through port by default open by firewall [8] that is HTTP port, the firewall weakness is widely used by the attacker, so it needs

Received March 6, 2018; Revised October 29, 2018; Accepted November 30, 2018

security system that can do the checking of payload packet as well as detect weakness or vulnerability from the running system so obtained the network security and more optimal data and layered. According to Yuan [9, 10] in his research about False positives and Negatives from real traffic with intrusion detection/prevention system in 2012 that 90% of the alert False Positive and False negative using HTTP portand 57% of FP are thought to be HTTP inspection attacks, also 93% from alert False Negative is an old type of attack that is SQL Server Attack, and worm slammer attack. Those indicate that attacker always has new variation to evade IPS detection [9], [11]. Thus, the objectives that want to be achieved in this study is to conduct evaluation and performance analysis of NGIPS in securing network environment through penetration system test by exploiting HTTP port, so it is known the performance of inspection and protection of NGIPS. The advantage of this study is that it can become reference in improving network security by using the method of NGIPS as well as obtained optimal mechanism in implementing the Next Generation Intrusion Prevention System.

2. Research Method

In this section, we discuss about the research method used in this paper. It is started from the NGIPS inspection process, flow access control policy inspection, penetration testing design, and analysis of payload packet. In following subsection, detail about every step of this research is discussed.

2.1. NGIPS Inspection Process

According to SourcefireDocument [12], the inspection process of NGIPS through three stages of inspection, namely packet decoder, preprocessor, rules engines. Those processes are shown by the Figure 1.

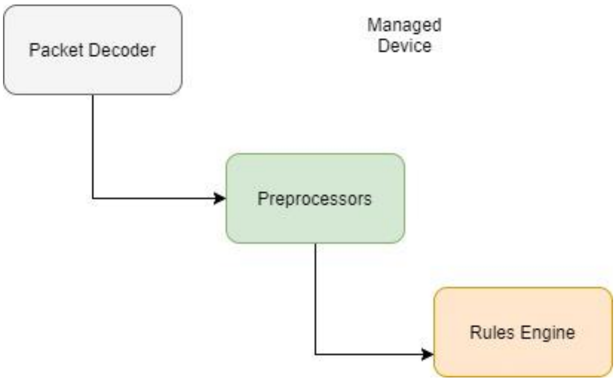


Figure 1. NGIPS inspection process

Figure 1 shows the flow about how the packet is inspected by NGIPS through the following three stages:

a) Packet decoder: Packet will be first going through decoding, packet decoder stage will convert packet header and payload become easier format to use and analyze by preprocessor and rules engines. Each packet layer will be decoded started from data link, then network layer until transport layer packet.
b) Processing packet: Then the data is sent to preprocessor for then to conduct traffic normalization on the app screen and detect anomaly protocol. After the packet going through preprocessor inspection then the package send to rules engine
c) Rules engine evaluate header packet and payload to determine whether packet that going through NGIPS match with the rules object. Rule engine using three methods of inspection namely:
    a. The Rules optimizer classified all the active rules based on the criteria such as transport layer, application protocol, traffic to or from protection network.
    b. The Multi-rule Search Engine by performing three types of searching, namely:

i. Protocol field search will search the particular field that same with apps protocol
ii. Generic content search will examine ASCII or binary byte that suitable with payload packet
iii. Packet Anomaly Search that is rule engine will examine packet header and payload which contains particular spesific content (unnormal payload package)

c. The event selector that is after multi search engine examine the packet, rule engine will trigger alert and add it into event queue.

According to Figure 2 [12, 13], event selector will select event based on queue priority and then record the event into the database event. Then the data displayed on dashboard intrusion event. Packet that pass through NGIPS will be evaluated by decoder packet, preprocessor, and rules engine. Each process can cause the system to generate intrusion event, which is indication from the packet have dangerous content as well as risking the target server or network environment both from the internal network or the external network.

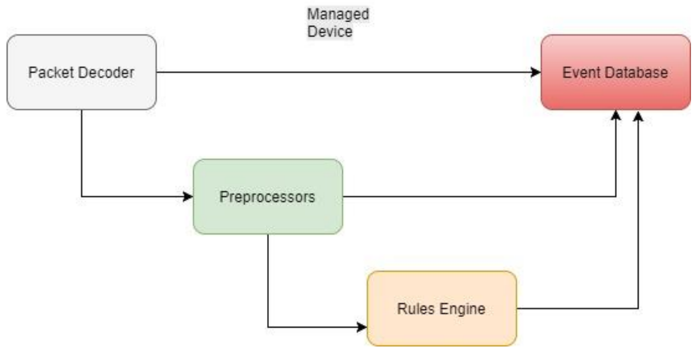


Figure 2. Event database NGIPS process

2.2. Flow Access Control Policy Inspection

Access Control Policy (ACP) will execute packet that going through NGIPS based on the given rules action configuration [13]. The following is the inspection scheme based on rules action policy. Figure 3 is a flow inspection packet carried out by access control policy. Packet will go through network policy inspection by network source and destination network validation. File policy inspection stage is analysis on file transfer, file content or URL filtering. Intrusion policy inspect payload packet to detect vulnerability, before the packet forward to the IP destination. All packet will be analyzed and fitted with the database policy and intrusion policy, if the packet match with one of the rules policy then packet will be dropped and will not forward to the IP destination. The unsuitable packet with one of the rule will be analyze by default action.

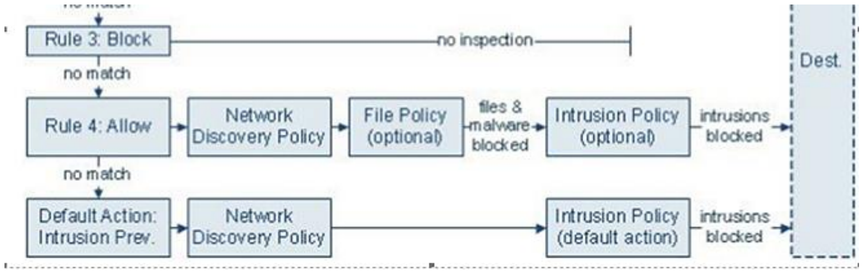


Figure 3. Access control policy process in inspecting packet [13]

2.3. Penetration Testing Design

This study will focus on penetration testing that will be conducted by the writer on local network, the following is topology penetration testing design [14, 15]. Based on Figure 4 attack will be done to Metasploitable OS. However, the attack package will first pass the Next Generation virtual IPS and will be inspected by Next Generation IPS, Next Generation IPS will determine whether packet will be dropped or forwarded, if the packet will be forwarded then it will attack the Metasploitable OS or protected server.

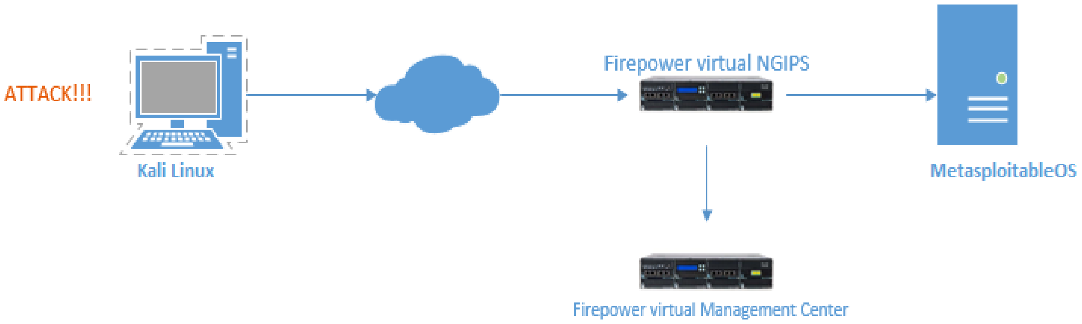


Figure 4. Topology penetration testing

The writer builds virtual Next Generation IPS as sensor that will inspect traffic that will pass through metasploitable OS, Next Generation IPS will be configured inline so that Next Generation IPS will directly take action to the packet that already inspected, each packet will be analyzed based on rule based signature, if packet found contain vulnerability then Next Generation IPS will directly perform prevention act by dropping packet [13], each alert will be logged by Firepower Management Center to be known and further analyzed by administrator. Next Generation IPS will also conduct discovery toward the protected apps [13], to find out the possibility of vulnerability owned by the app, so if there is packet that contains vulnerability, Next Generation IPS will immediately perform prevention act by dropping the packet. In this study will conduct various penetration system test. Each penetration system testing will conduct interchangeably, then will be viewed the effects resulting from the attacks performed and action performed by Next Generation IPS tested. The penetration testing method conducted can be seen in Table 1.

Table 1 is a scenario of penetration testing that will be conducted in this study, that is penetration attack that utilize SQL vulnerability toward protected asset, access to malicious site from protected asset to find out whether NGIPS can detect and protect asset from the exploitation of malicious site, and detect the security vulnerability owned by protected asset to test the
real-time contextual awareness feature.

Table 1. Scenario of Penetration System Testing that will be Conducted

Types of attack	Method of Attacks	Target of attack	Effect produced	Expectation Result	Severity	Purpose of attack
SQL Injection	Send database command to display username and password information	Metasploitable OS	Unauthorized access	NGIPS block packet	High	Testing the ability of NGIPS, protecting assest from external attack
Exploit Malicious Site	Redirection javascripttoward malicious domain inserted by malicious site	PC user	Attacker can exploit PC target and instal malware through malicious site	NGIPS drop packet	High	Testing the ability of NGIPS in protecting asset when accessing public network.

The following are the scenario penetration testing that will be done:
1. Scenario of SQL injection attacks
   a. Check the connection between kali linux and metaspoitable OS pass the NGIPS
   b. Conduct SQL injection attacks passing the kali linux tools dvwa

   c. Carry out verification whether injection succeeded on dvwa tools
   d. Carry out verification whether there is connectivity layer 3 between kali linux (attacker) to metasploitable OS (victim) on feature connection event Firesight Management Center.
   e. Conduct verification whether SQL injection packet successfully detected and dropped by NGIPS in feature intrusion event
   f. Analyze the attacks
2. Scenario of penetration testing access to Malicious site
   a. Setting and testing connectivity between PC, NGIPS, and Internet
   b. Conduct penetration experiment without NGIPS protection
   c. Conduct verification whether access to malicious site is successful
   d. Carry out penetration testing on NGIPS environment
   e. Carry out verification whether access to malicious site is successful
   f. Conduct verification in feature Intrusion Event to find out whether penetration is successfully detected by NGIPS and packet is dropped
   g. Analyze the attacks

2.4. Analysis of Payload Packet

The evaluation stage explains what the writer does to the results of penetration testing or to the features owned by Next Generation IPS that will be conducted in chapter 3. The writer conducts analysis on packets that has been inspected by NGIPS, content, signature, or what vulnerability detected on the packet. To validate the accuracy of NGIPS inspection, and verify whether packet that already detected is a malicious packet. The step analysis method used by the writer to analyze payload from package inspected by NGIPS is described as follow:

a) Verification Of Intrusion Event: The analysis is started by verification of NGIPS inspection that was shown in feature intrusion event. It is done by verifying source network and destination network from intrusion packet whether it was in accordance with network environment. Furthermore, it was conducted checking whether packet was dropped or allowed by NGIPS.
b) Analysis of Rule Engine: Analyze the rule engine to find out content that mached with NGIPS signature so that packet was detected as malicious or valnerable packet.
c) View Reference Document: After finding out vulnerable content which was detected by NGIPS, we read reference document of NGIPS related to the intrusion, to get information the impact of packet or content vulnerable.
d) Search related document: Collecting information related to vulnerable content from website journal, report, or literature study in the research that was done by individual or certain organization, such as virustotal site to search information of virus or content malware from a file and URL/domain.
e) Conclusion: Analysis result then was done by drawing the conclusion about detection result, e.g. analyzing whether there was false-positive or false negative, or NGIPS detected successfully and did onset prevention correctly

3. Result and Discussion

In this section, we discuss the result of penetration testing that we did to to the next generation IPS. As mentioned in section, we perform two kinds of penetration testing, i.e. attack of SQL injection and exploitation of malicious site. After the penetration testing, we perform payload analysis to evaluate the ability of next generation IPS in protecting network from both of attacks.

3.1. Attack of SQL Injection

Onset penetration testing SQL Injection would be done according to topology as shown by Figure. 5. Figure 5 is penetration attack SQL injection [16] design that was done from kali linux to target server (metaploit OS), packet from attacker was continued by router then it was inspected by NGIPS, determined whether packet would be continued to protected server of dropped the packet, alert of inspection result was sent to firesight management center and showed on feature intrusion event, this research has sent sql injection to metaploitOS from kali linux using DVWA tools [14]. Penetration was done by sending SQL query to sleep the user agent for 6 seconds, so that the application will be not respond (delay) to any queries or requests for 6 seconds. the following query that has been used, "' (select * from (select (sleep (6))) a) #" query that instructs the user agent to freeze for 6 seconds and makes the application as though it is down and does not respond to the request during the periode, this attack can be dangerous in critical applications like market place or internet banking. The following display experiment exploits using SQL injection through tools dvwa.

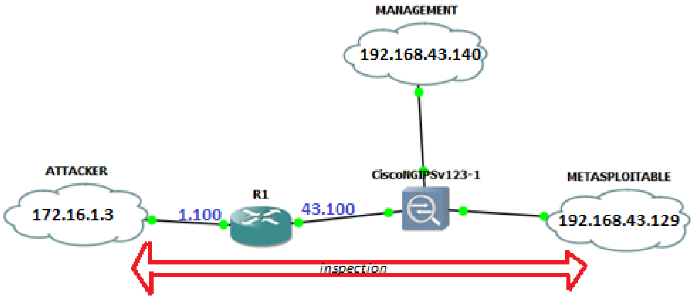
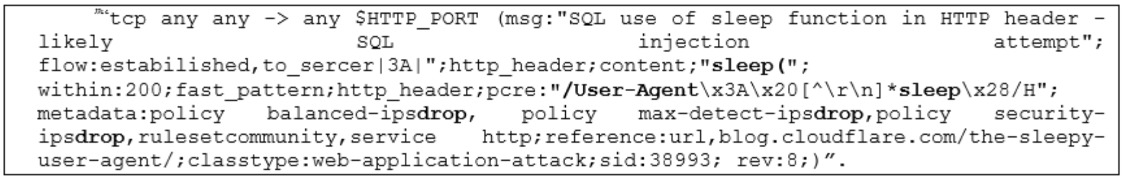


Figure 5. Topology environment penetration testing SQL injection on GNS3

Output SQL injection from kali linux was detected successfully by NGIPS and it was not continued to kali linux. NGIPS detected malicious content and took dropping action of the packet. So that packet was not continued to MetaploitableOS that caused connection timeout. Detail of injection SQL packet is "SQL use of sleep function in HTTP header-likely SQL injection attempt" that was detected successfully by NGIPS. Based on output above, it was known that rule policy of the event was as shown by Figure 6

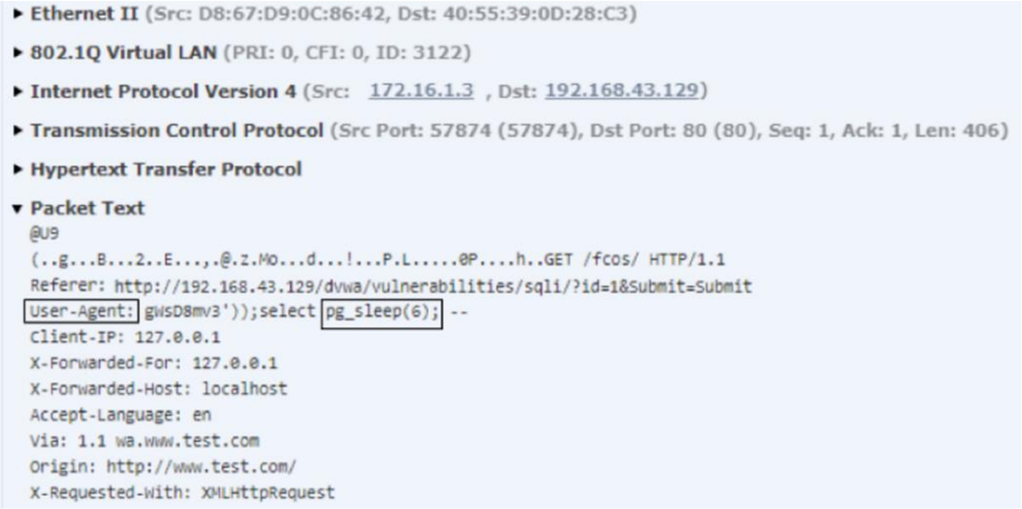


```
     ™“tcp any any -> any $HTTP_PORT (msg:"SQL use of sleep function in HTTP header -
likely                    SQL                    injection                    attempt";
flow:estabilished,to_sercer|3A|";http_header;content;"sleep(";
within:200;fast_pattern;http_header;pcre:"/User-Agent\x3A\x20[^\r\n]*sleep\x28/H";
metadata:policy   balanced-ipsdrop,   policy   max-detect-ipsdrop,policy   security-
ipsdrop,rulesetcommunity,service   http;reference:url,blog.cloudflare.com/the-sleepy-
user-agent/;classtype:web-application-attack;sid:38993; rev:8;)”.
```

Figure 6. Rule policy to SQL injection event

Based on the data, writer conducted analysis to understand how and what variable that was used by NGIP to inspect injection SQL packet [6], [12], [18], NGIPS did layering inspection from network layer with rule any [variable net] any [port] -> any [variable net] $HTTP_PORTS, it means flow traffic from variable *any net* with *"any"* port to variable *any net* port HTTP, NGIPS checking the packet header whether it was in accordance with the rule. In this research environment, variable *home_net* was 192.168.43.129 and variable external_net was (negation) *!home_net* it meant the packet matched with rule network policy which was a to home_net port 80 then intrusion policy would conduct content checking from payload packet whether payload had suitable content with signature rule policy which was " sleep(" and "user-agent". then NGIPS would check metadata rule to determine action state toward packet, if packet would be continued or dropped, in this case metadata rule policy using balance connectivity and security policy with recommendation to dropping packet, the alert was shown in intrusion event with message "SQL use of sleep function in HTTP header-likely SQL injection attempt" and it was clarified as web application attack. To validate the result of inspection NGIP, then the writer did adjustment of payload from packet text with rule engine NGIPS

Figure 7 shows detail packet of SQL Injection that was injected by NGIPS, payload that was shown by NGIPS was encoding packet to ease analysis, the sleep command is inserted in the function sleep user-agent as "pg_sleep (6);" the injection gives orders to the user-agent delay for 6 seconds, so the application will not respond to the request within the time period (application processing delay). This method of SQL injection not display data or information to the attacker but execute commands to exploit application that cannot be detected by the PHP code. Function sleep user-agent gave a big impact on the critical application that resides in transaction zone. Rule Engine NGIPS managed to detect such attacks and dropping packet with precaution so that SQL injection attacks are not forwarded toward the target server that is MetasploitableOS, NGIPS managed to do the protection from SQL injection with sleep commands user-agent attack was categorized as High Priority.

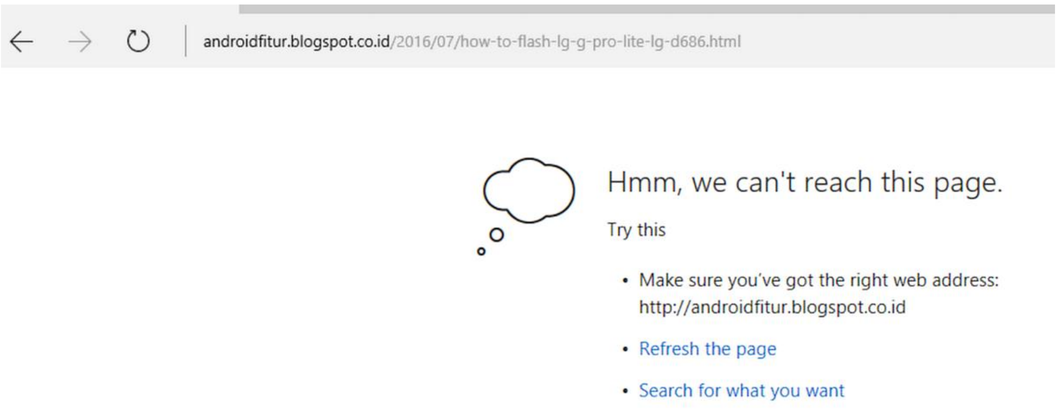


```
▸ Ethernet II (Src: D8:67:D9:0C:86:42, Dst: 40:55:39:0D:28:C3)
▸ 802.1Q Virtual LAN (PRI: 0, CFI: 0, ID: 3122)
▸ Internet Protocol Version 4 (Src:  172.16.1.3 , Dst: 192.168.43.129)
▸ Transmission Control Protocol (Src Port: 57874 (57874), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 406)
▸ Hypertext Transfer Protocol
▾ Packet Text
  @U9
  (..g...B...2..E...,.@.z.Mo...d...!...P.L.....0P....h..GET /fcos/ HTTP/1.1
  Referer: http://192.168.43.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
  User-Agent: gWsD8mv3'));select pg_sleep(6); --
  Client-IP: 127.0.0.1
  X-Forwarded-For: 127.0.0.1
  X-Forwarded-Host: localhost
  Accept-Language: en
  Via: 1.1 wa.www.test.com
  Origin: http://www.test.com/
  X-Requested-With: XMLHttpRequest
```

Figure 7. Packet text SQL injection

3.2. Malicious Domain

Penetration Testing was performed by accessing domain which was infected by malware. From the result of collecting information, it was known some malicious domain which was used by attacker to deliver malware. In this paper, we perform access to malicious domain as shown by Figure 8. It tried to access malicious domain from PC that had been protected by NGIPS. Before http packet was sent to proxy or to router internet, NGIPS first did inspection the packet, inspection process can be seen in Figure 9.



androidfitur.blogspot.co.id/2016/07/how-to-flash-lg-g-pro-lite-lg-d686.html

Hmm, we can't reach this page.

Try this

- Make sure you've got the right web address: http://androidfitur.blogspot.co.id
- Refresh the page
- Search for what you want

Figure 8. User access malicious domain

Data packet was through NGIPS then the packet was decoded in each layar, which was in data link layer decoder and IP decoder, then decode process was continued until application layer the same as HTTP inspection preprocessor, then inspection packet was continued to adjust signature in rule engine if packet match was with certain signature, rule engine would read action state to packet wheter packet was blocked or continued to destination IP, inspection result would be stored in database event then it was saved and shown into management device to be able to read by the administrator. NGIPS dropped the packet, the request was not continued to destination IP thus, user could not access the malicious website.

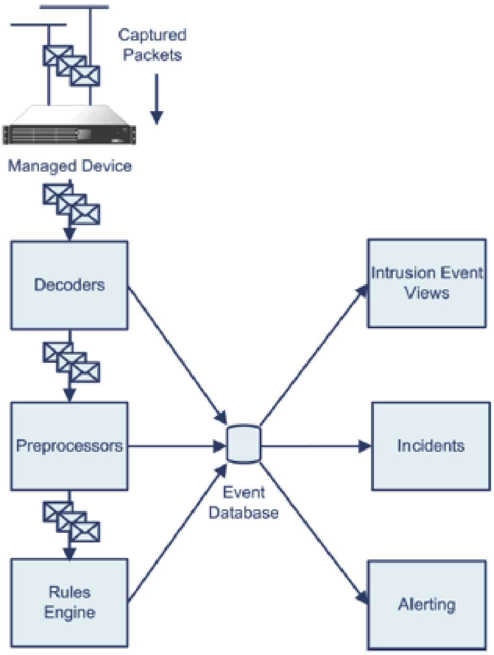
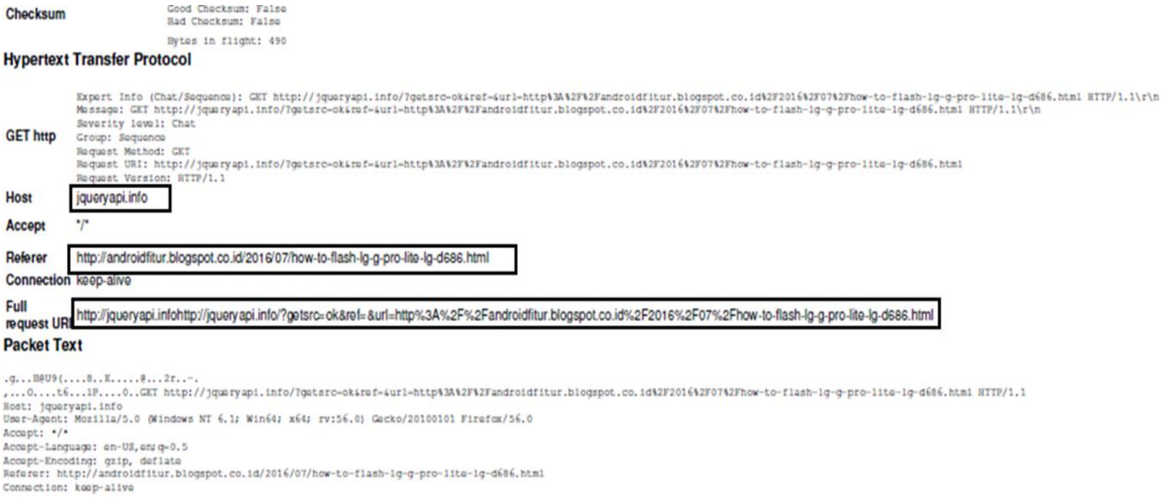


Figure 9. NGIPS inspection process

Figure 10 shows the output from view packet that converted report of detail packet that had been inspected by NGIPS. Based on packet text, it could be known that accessed URL by user redirect to exploit-kit jpueryapi.info. To get information related to jqueryapi.info, it was done by analysis the URL using website malware analyser "virustotal.com" [19] as shown by Figure 11.



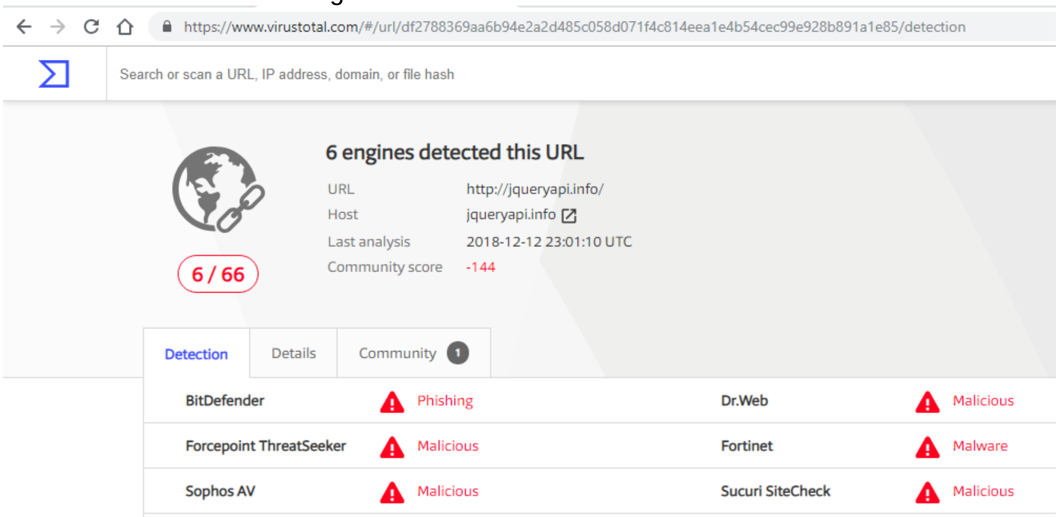
```
Checksum                 Good Checksum: False
                         Bad Checksum: False

                         Bytes in flight: 490
Hypertext Transfer Protocol

            Expert Info (Chat/Sequence): GET http://jqueryapi.info/?getsrc=ok&ref=&url=http%3A%2F%2Fandroidfitur.blogspot.co.id%2F2016%2F07%2Fhow-to-flash-lg-g-pro-lite-lg-d686.html HTTP/1.1\r\n
            Message: GET http://jqueryapi.info/?getsrc=ok&ref=&url=http%3A%2F%2Fandroidfitur.blogspot.co.id%2F2016%2F07%2Fhow-to-flash-lg-g-pro-lite-lg-d686.html HTTP/1.1\r\n
            Severity level: Chat
GET http    Group: Sequence
            Request Method: GET
            Request URI: http://jqueryapi.info/?getsrc=ok&ref=&url=http%3A%2F%2Fandroidfitur.blogspot.co.id%2F2016%2F07%2Fhow-to-flash-lg-g-pro-lite-lg-d686.html
            Request Version: HTTP/1.1
Host        jqueryapi.info
Accept      */*
Referer     http://androidfitur.blogspot.co.id/2016/07/how-to-flash-lg-g-pro-lite-lg-d686.html
Connection  keep-alive
Full
request URI http://jqueryapi.infohttp://jqueryapi.info/?getsrc=ok&ref=&url=http%3A%2F%2Fandroidfitur.blogspot.co.id%2F2016%2F07%2Fhow-to-flash-lg-g-pro-lite-lg-d686.html
Packet Text

.g...B@U9(....8..E.....@...2r..-.
,...0....t6...1P....0..GET http://jqueryapi.info/?getsrc=ok&ref=&url=http%3A%2F%2Fandroidfitur.blogspot.co.id%2F2016%2F07%2Fhow-to-flash-lg-g-pro-lite-lg-d686.html HTTP/1.1
Host: jqueryapi.info
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://androidfitur.blogspot.co.id/2016/07/how-to-flash-lg-g-pro-lite-lg-d686.html
Connection: keep-alive
```

Figure 10. Packet text from intrusion event



https://www.virustotal.com/#/url/df2788369aa6b94e2a2d485c058d071f4c814eea1e4b54cec99e928b891a1e85/detection

Search or scan a URL, IP address, domain, or file hash

6 / 66

6 engines detected this URL

URL	http://jqueryapi.info/
Host	jqueryapi.info
Last analysis	2018-12-12 23:01:10 UTC
Community score	-144

Detection Details Community 1

BitDefender	Phishing	Dr.Web	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Sophos AV	Malicious	Sucuri SiteCheck	Malicious

Figure 11. Analysis result of URL from website virustotal

3.3. Comparison of NGIPS and Traditional Firewall

From the results above performed evaluation of NGIPS experiment results versus firewall analysis capability, the comparison result of NGIPS testing versus traditional firewall capability inspection shows on Table 2. Table 2 indicates that the firewall cannot detect interruption of blind SQL injection with sleep user-agent function it is caused due to firewalls have limited inspection against HTTP Packet. The firewall cannot analyze and detecting content of http packet because by default the http inspection feature on traditional firewalls are disabled, HTTP inspection and URL filtering license needed. While in evaluation using NGIPS showed that NGIPS successfully detect SQL injection function sleep user-agent because NGIPS have a content analysis feature that can analyze the content of the payload http thus, NGIPS can dropped the injection packet through protected server.

Table 2. Result of Comparison Evaluation of NGIPS Testing Versus Firewall Capability Inspection

	Traditional FIREWALL	NGIPS
SQL injection function sleep user agent	HTTP inspection disabled; firewall cannot detect blind SQL injection content inserted in the user-agent	Inspection Enabled; NGIPS have a content analysis feature thus can detect blind SQL injection.
Exploit-Kit Attack	Inspection disabled (bypass); standard Firewalls cannot assess the domain reputation (malicious domain/URL) and detecting exploit-kit attack in the HTTP payload packet.	Inspection Enabled; NGIPS Have a Security Inteligency and behavior of compromise feature that can analyzes the reputation of the site and detecting the malicious site.

From the results of Exploit Kit Attack is the firewall allowing access to the malicious site. The standard firewall cannot analyze the reputation domain or detect malicious URLs. However the evaluation with NGIPS shows the NGIPS successfully detect exploit kit attack from malicious domain by using website reputation checking detects redirection towards malware domains and then againts the attacks by dropping the packet. From these two experiments using a traditional firewall and NGIPS showed that NGIPS managed to detect attacks and conducting prevention with dropped the attacks but the traditional firewalls not.

Based on the report of penetration testing above, it proves that NGIPS could save the attack that utilizes vulnerability from port HTTP but it has still needed further some compliance and development, as long as the development of attack models[16], [19].The most important is the need of trial development of penetration testing with other scenario and technology so it can be done the comparison and evaluation toward various attack by using the method from different technology.

4. Conclusion

The results of penetration testing are NGIPS successfully detects exploit that utilizes port 8080 (HTTP) and attack that exploit vulnerability MySQL through SQL injection and detection exploitation malicious domain that couldn’t be done by traditional firewall. Next Generation IPS conducts inspection until layer 7 (application layer) that will increase network security. It can be concluded that NGIPS can give better vulnerability protection than traditional firewall. It is not only can analysis based on head packet that is through it but Next Generation IPS can also analyze payload packet so that it can become solution of saving network from attack of penetration system that utilizes the weakness of firewall. Other than that, NGIPS can give better vulnerability protection. The suggestions that can give from the result is implementation NGIPS in enterprise environment should be installed after firewall so there is saving layering process and also to lighten inspection process from NGIPS, packet which is through NGIPS is packet that has been filtered by firewall. And also enable feature rule recommendation to ensure NGIPS does discovery toward vulnerability application as prevention action toward packets that can exploit the application.

Reference

[1] Fossi M, Turner D, Johnson E, Mack T, Adams T, Blackbird J, et al. Symantec Internet Security Threat Report-trends for 2009. 2010;XV(April).

[2] Stallings W. Cryptography and Network Security: Principles and Practices. *Cryptography and Network Security*. 2005. 592.

[3] Presekal A, Sari RF. Performance Comparison of Host Identity Protocol and TCP/IP with Firewall against Denial of Services. *Indonesian Journal Electrical Engineering Computer Science.* 2014; 12(12): 8335–8343.

[4] Kahtan Mohammed R, Yoichiro U. An FPGA-based Network Firewall with Expandable Rule Description. *Indonesian Journal Electrical Engineering Computer Science.* 2018;10(3): 1310–1318.

[5] Stuart D, Beaver K. Next-Generation IPS For Dummies®. Sourcefire Edition. Zhurnal Eksperimental’noi i Teoreticheskoi Fiziki. 2013: 69.

[6] Pirc J. The Evolution of Intrusion Detection_Prevention_ Then, Now and the Future _ Secureworks. 2017.

[7] Sekhar R, Perumal K, Rani SV. Analysis of Next Generation Intrusion Prevention System Using Sensor Fusion and Fuzzy Logic. *International Journal of Scientific Research Engineering & Technology (IJSRET)*. 2015; 4(9): 936–8.

[8] Kamara S, Fahmy S, Schultz E, Kerschbaum F, Frantzen M. Analysis of vulnerabilities in internet firewalls. *Comput Secur*. 2003; 22(3): 214–32.

[9] Ho C-Y, Lin Y-D, Lai Y-C, Chen I-W, Wang F-Y, Tai W-H. False positives and negatives from real traffic with intrusion detection/prevention systems. *Int J Futur Comput Commun*. 2012; 1(2): 87.

[10] Ho CY, Lai YC, Chen IW, Wang FY, Tai WH. Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems. *IEEE Commun Mag*. 2012; 50(3): 146–54.

[11] Stiawan D, Abdullah AH, Idris MY. Characterizing Network Intrusion Prevention System. *Int J Comput Appl*. 2011; 14(1): 975–8887.

[12] Sourcefire. Sourcefire 3D System User Guide. Simulation. 2014; 1–280.

[13] Cisco System. FireSIGHT System User Guide Creating Traffic Profiles. Simulation. 2015;

[14] Software Testing. Penetration Testing - Complete Guide with Penetration Testing Sample Test Cases Software Testing Help. 2017.

[15] Lakshmi DR, Mallika SS. A Review on Web Application Testing and its Current Research Directions. *International Journal Electrical Computer Engineering*. 2017; 7(4): 2132.

[16] Clarke J, Alvarez RM. SQL Injection Attacks and Defense. 2009: 494.

[17] Shinde G, Waghere SS. Analysis of SQL Injection Using DVWA Tool. 2017; 10: 107–10.

[18] Cannady JD. *Next generation intrusion detection: Autonomous reinforcement learning of network attacks*. Proc 23rd Natl Inf Syst Secur Conf. 2000; 1–12.

[19] Boonen R. FuzzySecurity_Game Over_Dolo Malo-JavaScript Adware Exposed. 2014.