NETWORK TRAFFIC MONITORING DI JARINGAN INTERNET UMS MENGGUNAKAN *SURICATA* DAN *PFSENSE*

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada Jurusan Informatika Fakultas Komunikasi dan Informatika

Oleh:

NUR HASNA' SHOFIA

L 200 150 056

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2019

HALAMAN PERSETUJUAN

NETWORK TRAFFIC MONITORING* DI JARINGAN INTERNET UMS MENGGUNAKAN *SURICATA* DAN *PFSENSE

PUBLIKASI ILMIAH

oleh:

NUR HASNA' SHOFIA
L 200 150 056

Telah diperiksa dan disetujui untuk diuji oleh:

Dosen Pembimbing

Dr. Ir. Bana Handaga, M.T.
NIK.793

HALAMAN PENGESAHAN

NETWORK TRAFFIC MONITORING* DI JARINGAN INTERNET UMS MENGGUNAKAN *SURICATA* DAN *PFSENSE

OLEH

NUR HASNA' SHOFIA

L 200 150 056

Telah dipertahankan di depan Dewan Penguji

Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Pada hari Sabtu, 3 Agustus 2019

dan dinyatakan telah memenuhi syarat

Dewan Penguji:

1. Dr. Ir. Bana Handaga, M.T. (.....)
   (Ketua Dewan Penguji)
2. Fatah Yasin Al-Irsyadi, S.T, M.T. (.....)
   (Anggota I Dewan Penguji)
3. Aris Rakhmadi, S.T, M.T. (.....)
   (Anggota II Dewan Penguji)

Mengetahui,

Dekan	Ketua
Fakultas Komunikasi dan Informatika	Program Studi Informatika
Nurgiyatna, S.T., M.Sc., Ph.D	**Heru Supriyono, S.T., M.Sc., Ph.D**
NIK. 881	**NIK. 970**

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam naskah publikasi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Apabila kelak terbukti ada ketidakbenaran dalam pernyataan saya di atas, maka akan saya pertanggungjawabkan sepenuhnya.

Surakarta, Kamis 1 Agustus 2019

Penulis

NUR HASNA' SHOFIA

L 200 150 056

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl.AYaniTromolPos1PabelanKartasuraTelp.(0271)717417,719483Fax(0271)714448
Surakarta57102Indonesia.Web:http://informatika.ums.ac.id.**Email:informatika@ums.ac.id**

NETWORK TRAFFIC MONITORING* DI JARINGAN INTERNET UMS MENGGUNAKAN *SURICATA* DAN *PFSENSE

Abstrak

Universitas Muhammadiyah Surakarta memiliki jaringan kabel dan nirkabel yang terpasang di semua kampus digunakan untuk akses data & internet. Salah satu masalah jaringan di UMS saat ini adalah sering muncul captcha pada waktu-waktu tertentu ketika melakukan *browsing google search* melalui jaringan kabel. Hal ini mengurangi kecnyamanan pengguna. *Suricata* adalah sistem *open source* yang dapat digunakan untuk mendeteksi penyusupan dalam jaringan, yang dimungkinkan bisa mengidentifikasi penyebab munculnya captcha yang mengganggu. Dalam penelitian ini penulis mencoba meneliti masalah tersebut, yaitu mengidentifikasi penyebab munculnya captcha menggunakan *suricata* dan *pfsense*. Metode yang digunakan adalah dengan mengamati aliran data 2 buah *Server* di UMS dan pengujian menggunakan tool aplikasi *Selenium* dan *Hey* untuk mengetahui berapa request redundan yang menyebabkan munculnya halaman *google reCaptcha.* Dari hasil pengamatan didapatkan bahwa pengujian menggunakan *Selenium* dan *Hey* belum cukup untuk bisa mengetahui penyebab masalah yang ada. Di butuhkan monitoring jaringan UMS dengan cakupan yang lebih luas serta spesifikasi perangakat keras yang lebih tinggi.

Kata Kunci: *Suricata, pfsense, monitoring, captcha*.

UNIVERSITAS MUHAMMADIYAHSURAKARTA
FAKULTAS KOMUNIKASI DANINFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl.A Yani Tromol Pos 1 Pabelan Kartasura Telp.(0271)717417 ,719483Fax (0271)714448
Surakarta 57102 Indonesia. Web : http://informatika.ums.ac.id .Email:informatika@ums.ac.id

SURAT KETERANGAN LULUSPLAGIASI
...138/A.4-II.3/INF-FKI/VIII/2019

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa:

Nama	: NUR HASNA' SHOFIA
NIM	: L200150156
Judul	: ***NETWORK TRAFFIC MONITORING*** **DI JARINGAN INTERNET UMS MENGGUNAKAN** ***SURICATA*** **DAN** ***PFSENSE***
Program Studi	: Informatika
Status	: **Lulus**

Adalah benar – benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 19 Agustus 2019
Biro Skripsi Informatika

Ihsan Cahyo Utomo, S.Kom.,M.Kom

NETWORK TRAFFIC MONITORING DI JARINGAN INTERNET UMS MENGGUNAKAN *SURICATA* DAN *PFSENSE*

Abstrak

Universitas Muhammadiyah Surakarta memiliki jaringan kabel dan nirkabel yang terpasang di semua kampus digunakan untuk akses data & internet. Salah satu masalah jaringan di UMS saat ini adalah sering muncul captcha pada waktu-waktu tertentu ketika melakukan *browsing google search* melalui jaringan kabel. Hal ini mengurangi kecnyamanan pengguna. *Suricata* adalah sistem *open source* yang dapat digunakan untuk mendeteksi penyusupan dalam jaringan, yang dimungkinkan bisa mengidentifikasi penyebab munculnya captcha yang mengganggu. Dalam penelitian ini penulis mencoba meneliti masalah tersebut, yaitu mengidentifikasi penyebab munculnya captcha menggunakan *suricata* dan *pfsense*. Metode yang digunakan adalah dengan mengamati aliran data 2 buah *Server* di UMS dan pengujian menggunakan tool aplikasi *Selenium* dan *Hey* untuk mengetahui berapa request redundan yang menyebabkan munculnya halaman *google reCaptcha.* Dari hasil pengamatan didapatkan bahwa pengujian menggunakan *Selenium* dan *Hey* belum cukup untuk bisa mengetahui penyebab masalah yang ada. Di butuhkan monitoring jaringan UMS dengan cakupan yang lebih luas serta spesifikasi perangakat keras yang lebih tinggi.

Kata Kunci: *Suricata, pfsense*, *monitoring, captcha*.

Abstract

Universitas Muhammadiyah Surakarta has wired and wireless networks installed on all campuses used for data & internet access. One of the network problems at UMS now is that captcha often appears at certain times when browsing Google Search over a cable network. This causes user inconvenience. Suricata is an open source system that can be used to detect intrusions in the network which is possible to identify the cause of the disturbing captcha. In this study the writter tried to examine the problem, namely identifying the cause of the emergence of captcha using suricata and pfsense. The methods used in this study were observing the data flow of 2 servers in UMS and testing by using Selenium and Hey application tools to find out how many redundant requests are causing the reCaptcha google page to appear. The result of this study shows that the testing using Selenium and Hey was not enough to find out the cause of the problem here. UMS network monitoring is needed with wider coverage and higher hardware specifications.

Keywords: suricata, pfsense, monitoring, captcha.

1 PENDAHULUAN

Universitas Muhammadiyah Surakarta merupakan salah satu perguruan tinggi di Surakarta pada tahun 2018 telah terakreditasi A. UMS memiliki banyak fakultas dan program studi, untuk mendukung program studi tersebut UMS menyediakan banyak gedung di beberapa tempat. Dalam rangka menunjang Visi, Misi dan melancarkan program-program akademik, UMS, membentuk sebuah Biro bernama Biro Teknologi Informasi yang bertugas untuk memberikan dukungan layanan dalam bidang teknologi informasi. Biro TI UMS terdiri dari dua divisi yaitu software dan infrastruktur, divisi infrastruktur terbagi menjadi sub divisi pemeliharaan server dan jaringan.

Meningkatnya transmisi data baik lokal maupun internet, menuntut UMS untuk terus mengembangkan infrastruktur & memperbesar bandwidth jaringan data. Pengadaan jaringan data baik kabel maupun wifi yang sudah dibangun oleh Biro TI mencakup semua gedung dimana UMS memiliki gedung yang tersebar di beberapa kampus. Terkait bandwidth, Biro TI UMS menetapkan standar untuk jalur akses sebesar 100Mbps, jalur distribusi 1000Mbps, jalur core 10Gbps, dan jalur internet yang dilanggan saat ini sebesar 1,2Gbps. Tercatat di jaringan UMS terdapat 240 buah *switch manageable*, 14 buah *router*, 250 *access point*, jumlah perangkat komputer yang tersambung jaringan secara bersamaan rata-rata 5.000 dimana 90% lebih tersambung ke *WiFi.*(Wibowo, S.H.S., *Personal Communication*. 2019, April 12)

Sejalan dengan bertambahnya pengguna & kapasitas penggunaanya, infrastruktur jaringan data selalu berkembang dengan bandwidth yang membesar pula. Hal ini mengakibatkan masalah yang semakin kompleks dalam pengelolaan jaringan data di UMS, baik masalah kontrol, monitoring maupun keamanan. Maka kemudian isu keamanan & kenyamanan layanan jaringan data turut menjadi perhatian bagi Biro TI UMS.

Dalam hal penggunaan internet, salah satu tujuan akses pengguna internet civitas akademika UMS adalah website mesin pencari google yang alamatnya adalah google.co.id atau google.com atau aplikasi-aplikasi di bawah domain google. Penggunaan mesin pencari ini cukup dominan di UMS karena popularitas, kesederhanaan, dan kemudahannya. Masalah muncul ketika pengguna melakukan

pencarian dengannya, muncul halaman dengan captcha yang mengganggu kenyamanan pengguna yang seakan-akan menyatakan bahwa komunikasi dari sisi pengguna kurang aman dan kurang dipercaya oleh pihak google. Gejala ini muncul sekitar bulan September 2018.(Wibowo. S.H.S., *Personal Communication*. 2019, April 12)

Menanggapi masalah yang muncul tersebut, penting untuk dilakukan analisis terkait lalu lintas data dari UMS ke server Google. Penulis mencoba menganaliss menggunakan tools yaitu *suricata* & *pfsense*. Menurut Nazwita & Ramadhani (2017) *Suricata* adalah perangkat lunak *open source* yang digunakan untuk mendeteksi ancaman jaringan. *Suricata* mampu mendeteksi penyusup secara *realtime* (IDS). Mencegah penyusup (IPS) dan memantau keamanan jaringan (NSM). *Suricata* dapat dipasang diberbagai system operasi di antaranya *pfsense. Pfsense* adalah perangkat lunak *open source* turunan *FreeBSD* yang digunakan khusus sebagai *firewall* yang menawarkan berbagai fitur dapat dikonfigurasi melaui web dan tidak memerlukan pengetahuan tentang system [N Regian, S Rinaldy, P Mohamad Dawud, Kiswanto Roni , P Edi Pratama 2015].

Penelitian ini bertujuan untuk mengetahui apakah suricata bisa mendeteksi penyebab munculnya captha dan bisa menginformasikan sumbernya. Adapun manfaat penelitian ini, bisa dijadikan bahan pertimbangan manajemen BTI-UMS untuk mengambil kebijakan strategis & teknis terkait jaringan data di UMS.

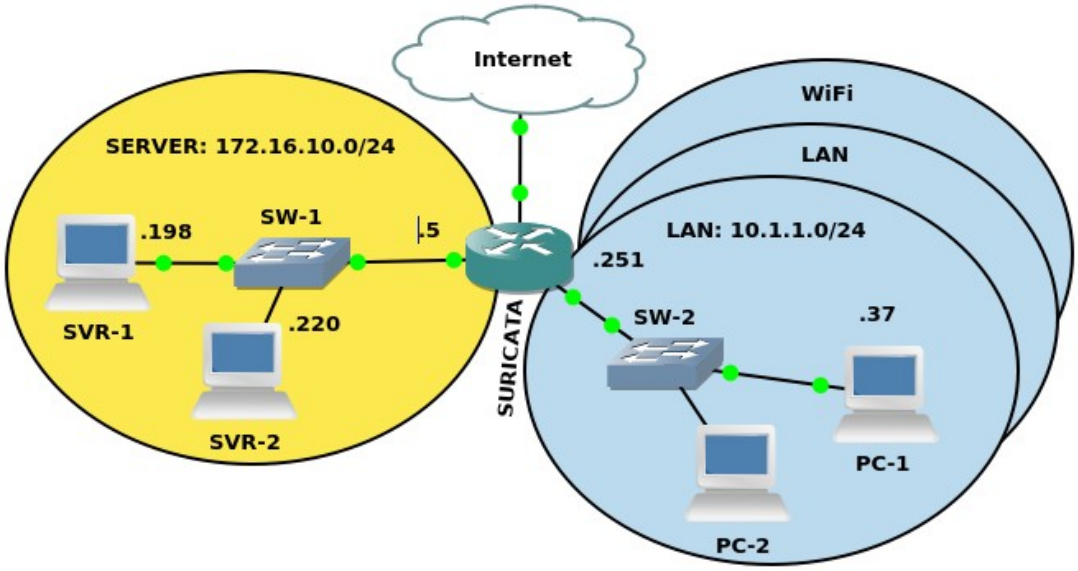
2 METODE

Di dalam penelitian ini akan disediakan perangkat *IDS* dengan *Suricata*, dilakukan monitoring terhadap beberapa perangkat dalam jangka waktu tertentu, dilakukan pengujian dengan perangkat lunak *Selenium* dan *Hey*. *Suricata* akan memberi peringatan apabila ada aliran data yang melewati perangkat *Suricata* yang mencurigakan. Peringatan ini berdasarkan *rule* yang telah ditetapkan sebelumnya. *Rule* yang dipakai dalam penelitian ini adalah *rule* bawaan *Suricata* dan *rule* berlisensi *GPL* dari *Snort*, sehingga nantinya masih banyak muncul peringatan yang sifatnya umum. *Selenium* dan *Hey* digunakan untuk memberikan aliran data secara masif ke alamat *web* tertentu, dalam hal ini adalah *Google*, dengan harapan *Suricata* dan *Google* memberikan peringatan tertentu.

2.1 Analisis Kebutuhan

2.1.1 Kebutuhan Perangkat Keras

Tujuan utama penelitian ini adalah untuk mengetahui adanya aktifitas yang mencurigakan di jaringan LAN dan server UMS. Dibutuhkan perangkat seperti router yang sekaligus dijadikan perangkat IDS, switch hub, server, desktop dan kabel LAN. Router harus terhubung ke internet, switch hub menghubungan server dan desktop ke router menggunakan kabel UTP, sehingga membentuk topologi seperti gambar 1.



Gambar 1: *Topologi*

Router menggunakan sebuah mesin *virtual* yang berjalan di *Proxmox Server*, dengan spesifikasi: processor 4 core, RAM 2 GB, hardisk 64 GB dan 3 buah v*irtual LAN card* 1 Gbps. *Switch* yang gunakan adalah *switch manageable* dengan VLAN 194 terhubung internet, VLAN 101 terhubung jaringan server dan VLAN 110 terhubung jaringan LAN. Pengujian menggunakan 2 buah server web yang diperkirakan banyak diakses dari internet dan sebuah desktop yang menjalankan request otomatis dalam jangka waktu tertentu.

2.1.2 Kebutuhan Perangkat Lunak

Perangkat lunak utama dalam penelitian ini adalah *Suricata* yang berjalan di sistem operasi *pfSense* yang dipasang di perangkat *router*. Perangkat lunak yang dibutuhkan lainnya adalah alat yang digunakan untuk menguji yaitu: *Selenium* dan *Hey*.

2.1.2.1 pfSense

pfSense adalah sebuah distribusi perangkat lunak jaringan gratis, berbasis sistem operasi *FreeBSD* [Sarifin dan Astuti 2012]. Konfigurasi *pfSense* berbasis web untuk semua komponen, sehingga untuk mengkonfigurasinya tidak diperlukan pengetahuan tentang sistem *UNIX/FreeBSD*, tidak menggunakan *command line*, dan tidak perlu mengedit berbagai konfigurasi secara manual. *pfSense* menyediakan *Package Manager* untuk memasang dan melepas paket-paket tambahan. Paket-paket ini digunakan untuk meningkatkan fungsionalitas dari *pfSense* dengan menyediakan fasilitas dan utilitas tambahan yang tidak disediakan pada instalasi *basic*.

Gambar 2: *pfSense Package Manager*

2.1.2.2 Suricata

Suricata adalah perangkat lunak *IDS*, *IPS* dan *monitoring* untuk jaringan yang berkinerja tinggi. *Suricata* adalah perangkat lunak *open source* yang dikelola yayasan non-profit, *Open Information Security Foundation* (*OISF*). *Suricata* dikembangkan oleh *OISF* dan *vendor* pendukungnya [Kuswanto 2014]. *Suricata* dapat dipasang di berbagai

sistem operasi dalam bentuk paket instalasi, termasuk di *pfSense* dapat dipasang meggunakan *Package Manager*.

Suricata memonitor lalulintas jaringan dengan memberi peringatan apabila ada lalulintas mencurigakan yang melewati suatu antar-muka jaringan. Peringatan diambil dari daftar aturan, dalam penelitian ini penulis menggunakan aturan *ETOpen* bawaan *Suricata* dan *Snort Community* yang berlisensi *GPLv2*. Daftar aturan akan lebih lengkap apabila menggunakan versi *Professional* yang berbayar.

2.1.2.2 Selenium

Selenium adalah seperangkat alat khusus yang digunakan untuk mengotomasi peramban *web* [Wang & Du 2012]. Komponen utama *Selenium* terdiri dari *WebDriver* dan *Selenium IDE*. *Selenium WebDriver* adalah kumpulan *binding* bahasa pemrograman tertentu yang digunakan untuk menjalankan peramban *web*. S*elenium IDE* adalah *ad-on* dari *Google Chrome* dan *Mozilla Firefox* yang akan melakukan pemutaran dan perekaman interaksi sederhana dengan peramban.

2.1.2.3 Hey HTTP Load Generator Pengganti *ApacheBench* (*ab*)

Hey adalah program kecil yang dibuat oleh *Jaana B. Dogan* menggunakan *Golang* [Dogan 2019] yang digunakan untuk mengirim permintaan dan memberi beban terhadap aplikasi *web*, biasanya digunakan untuk membuat tolok ukur *server web*. *Hey* menjalankan sejumlah permintaan otomatis dengan tingkat konkurensi tertentu yang menghasilkan statistik, status dan pesan-pesan kesalahan.

2.2 Skenario Pengujian

2.2.1 *Intrusion Detection Server Web*

IDS dalam mendeteksi aktifitas yang mencurigakan dalam sebuah jaringan dengan melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah perangkat yang biasanya berupa *router* atau *firewall*, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan), seperti *SQL Injection* dan *XML Attack* [Prasad 2016]. menurut Gondohanindijo (2011) *Intrusion* merupakan aktivitas yang tidak sah atau tidak dinginkan yang menggangu ketersediaan dari informasi yang terdapat di sebuah sistem.

Menurut Risyad, Data dan Pramukantoro (2018) dalam penelitiannya membandingkan *Suricata* dan *Snort* menangani serangan TCP SYN *Flood,* didapatkan hasil bahwa *Snort* lebih unggul dalam kecepatan deteksi, akurasi deteksi dan efektivitas deteksi sedangkan

Penelitian ini menginspeksi jaringan server dan jaringan LAN UMS. Ada dua buah server yang dimonitor, server ini diatur sedemikian rupa agar lalulintas dari dan ke server melalui perangkat *Suricata*, sehingga apabila ada aktifitas yang mencurigakan akan dicatat oleh *Suricata*, kemudian dianalisa aktifitas apa saja yang disusupkan ke server. Objek yang dianalisa fokus pada sistem, aplikasi *web* dan *database*.

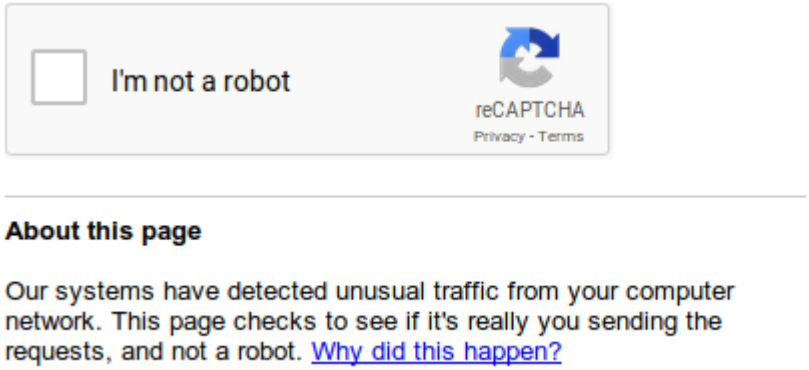
2.2.2 Masalah *Google reCAPTCHA*

Disebutkan dalam situs Bantuan *Google* [Bluequoll 2019], bahwa halaman "*Unusual traffic*" muncul ketika *Google* secara otomatis mendeteksi permintaan yang datang dari suatu jaringan komputer yang tampaknya melanggar ketentuan layanan. Kadang ditampilkan gambar *reCAPTCHA* agar pengguna dapat terus menggunakan menggunakan layanan *Google*. Permintaan yang dianggap melanggar ketentuan layanan antara lain:

1. Mengirim pencarian dari robot, program komputer, atau layanan otomatis.
2. Menggunakan perangkat lunak yang mengirimkan pencarian ke *Google* untuk melihat bagaimana peringkat situs web atau halaman web di *Google*.

3. Menggunakan aplikasi, program, atau skrip untuk melakukan sejumlah besar pencarian dalam waktu singkat.

Lalu lintas ini mungkin telah dikirim dengan sengaja menggunakan *plug-in* peramban atau skrip/program yang mengirimkan permintaan otomatis, atau oleh perangkat lunak berbahaya, atau mungkin saja oleh perangkat seperti *VPN*, *server proxy* atau *internet gateway*.



Gambar 3: *Google reCAPTCHA*

Gambar 4: *Google reCAPTCHA*

Google tidak memiliki cara untuk mengetahui berapa banyak perangkat yang berbagi alamat *IP* publik yang sama. Sebuah *internet gateway* dapat melewatkan permintaan dari banyak komputer. Pada penelitian ini, penulis akan melakukan pengujian dengan menjalankan aplikasi yang memberikan permintaaan secara otomatis ke *Google*. Hasil yang diharapkan adalah berapa jumlah permintaan dalam satu waktu yang menyebabkan munculnya halaman dengan *reCAPTCHA* dan peringatan apa saja yang muncul di *Suricata*.

1. Menjalankan skrip/aplikasi *Selenium* setiap dua menit sekali dalam jangka waktu satu hari menggunakan *Python Selenium binding*.

   Isi skrip yang dijalankan:

```
from selenium import webdriver
from selenium.webdriver.common.keys import Keys
import time
for i in range(720):
 driver = webdriver.Firefox()
 driver.implicitly_wait(30)
 driver.maximize_window()
 driver.get("http://www.google.com")
 search_field = driver.find_element_by_name("q")
 search_field.clear()
 search_field.send_keys(
         "Selenium WebDriver Interview questions"
 )
      search_field.submit()
 lists= driver.find_elements_by_class_name("r")
 print ("Found " + str(len(lists)) + " searches")
 driver.quit()
 time.sleep(120)
```

2. Menjalankan aplikasi *Hey* untuk mengakses halaman https://www.google.com/ dengan jumlah request (n) 5.000 kali, dilakukan 3 kali dengan konkurensi (c) 1.000, 2.000 dan 3.000, dengan perintah seperti berikut:

   `hey -n 5000 -c 1000 https://www.google.com/`

3 HASIL DAN PEMBAHASAN

3.1 *Intrusion Detection Server Web*

Dari pengamatan tanggal 2 April 2019 sampai dengan 5 April 2019 diperoleh bahwa percobaan serangan terbanyak dengan menyerang *form login* dari *Wordpress,* yaitu *Cleartext Wordpress Login, Wordpress Login Bruteforcing* dan *Nmap Scripting Engine User Agent,* kemudian ada serangan *Wordpress* xmlrpc.php Bruteforce yang dapat mengakibatkan CPU bekerja keras dan kekurangan memori.

Tabel 1 menunjukkan sepuluh besar serangan yang ditujukan ke server. *GNU/Linux APT User Agent Outbound* muncul karena saat pengamatan terjadi proses update sistem operasi, tidak berbahaya. Terdapat serangan terhadap website berbasis *Drupal* dengan *Drupalgeddon2* dan *remote code execution.* Ada pula serangan *SQL Injection* yang dapat memanipulasi *database*.

Tabel 1: *Sepuluh Besar Percobaan Serangan ke Web Server*

No.	*Alert*	Jumlah
1.	ET POLICY Cleartext WordPress Login	24.444
2.	ET POLICY GNU/Linux APT User Agent Outbound likely related to package management	22.714
3.	ET WEB_SERVER Wordpress Login Bruteforcing Detected	2.565
4.	ET SCAN Nmap Scripting Engine User Agent Detected (Nmap Scripting Engine)	485
5.	ET WEB_SPECIFIC_APPS Drupalgeddon2	426
6.	ET SCAN Possible WordPress xmlrpc.php BruteForce in Progress Response	366
7.	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT & SELECT FROM	242
8.	SERVER WEBAPP Drupal unsafe internal attribute remote code execution attempt	236
9.	SERVER WEBAPP Drupal 8 remote code execution attempt	194
10.	ET SCAN ZmEu Scanner User Agent Inbound	120

Website menggunakan Content Management System (CMS) seperti *Wordpress* dan *Drupal* sebaiknya menggunakan protokol *HTTPS* agar data *user* dan *password* yang dikirim terenkripsi, dan selalu diperbarui ke versi yang terbaru.

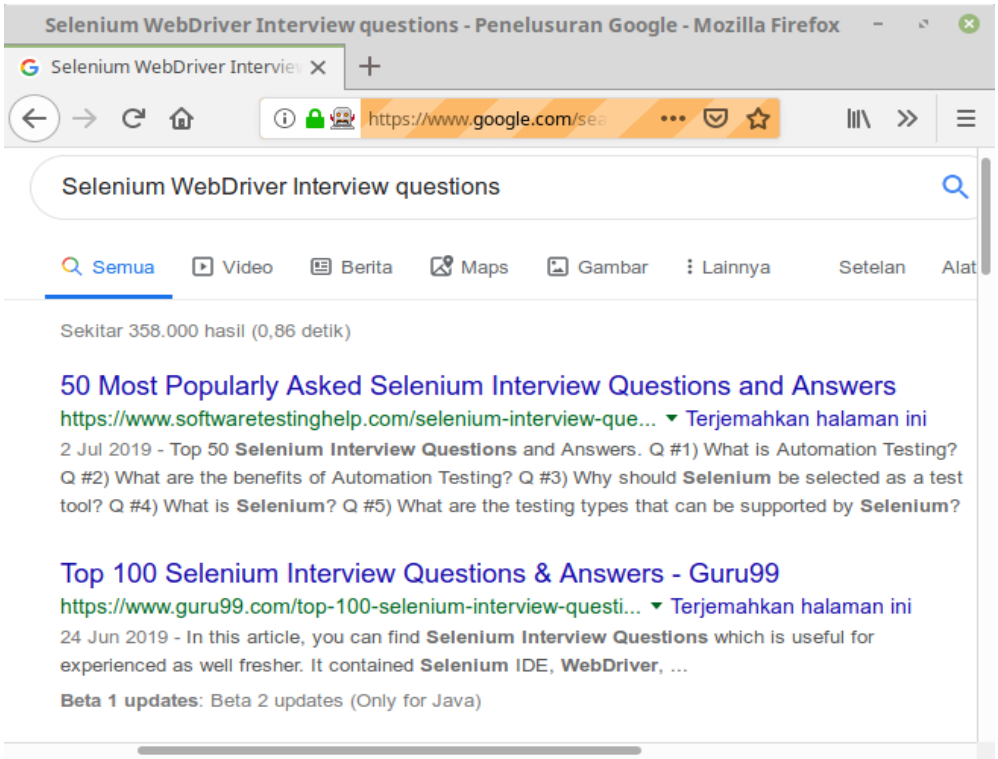
Suricata IPS dapat diaktifkan dengan automatis melakukan *block* pada alamat *IP* komputer yang menyebabkan peringatan(*alert*). Perlu berhati-hati dalam memilih aturan peringatan, karena bisa menyebabkan jaringan menjadi lumpuh, perangkat jaringan tidak bisa mengakses *internet* dan *server* tidak bisa diakses dari *internet* juga.

Suricata Vs Snort

3.2 *Masalah Google reCAPTCHA*

3.2.1 Pengujian dengan *Selenium*

Hasil eksekusi skrip *Selenium* yang menelusur kata "S*elenium WebDriver Interview questions*" di mesin pencari *Google* setiap 2 menit sekali hingga 720 kali, menunjukkan bahwa *Google reCAPTCHA* tidak muncul hingga akhir eksekusi sebagaimana terlihat pada gambar 4.



Gambar 5: *Hasil skrip selenium*

3.2.2 Pengujian dengan *Hey*

Pengujian tanggal 1 Juli 2019 dilakukan dengan *Linux Desktop* dengan pengaturan Perangakat *Suricata* hanya diakses oleh satu komputer saja, diperoleh hasil sebagai berikut:

1. n = 5.000, c = 1.000

   Error: -

   Suricata alert: SURICATA Applayer Wrong direction first Data

2. n = 5.000, c = 2000

   Error:

   a) *Get https://www.google.com/: dial tcp 216.239.38.120:443: socket: too many open files*

   Suricata alert: SURICATA Applayer Wrong direction first Data

3. n = 5.000, c = 3.000

   Error:

   a) *Get https://www.google.com/: dial tcp 216.239.38.120:443: socket: too many open files*
   b) *Get https://www.google.com/sorry/index?continue=https://www.google.com/&q=EgRn4q6-GIHh5egFIhkA8aeDS_1ez9O3vqwMv4Mi-49G5Qa6dAtzMgFy: dial tcp: lookup www.google.com on 8.8.8.8:53: dial udp 8.8.8.8:53: socket: too many open files*

   Suricata alert:

   c) *SURICATA Applayer Wrong direction first Data*
   d) *SURICATA TLS invalid handshake message*
   e) *SURICATA TLS invalid record/traffic*

Request dengan n = 5.000 dan c = 3.000 menimbulkan peringatan dari *Google* yaitu https://www.google.com/sorry/index seperti peringatan pada *Google reCAPTCHA*.

Berdasarkan pengujian menggunakan skrip *Selenium* dan *hey*, terlihat bahwa *Google* tidak benar-benar mengetahui penggunaan perangkat lunak yang melakukan pencarian otomatis, tetapi untuk pencarian otomatis dengan tingkat konkurensi tertentu, dapat dinyatakan melanggar ketentuan *Google* dengan munculnya halaman https://www.google.com/sorry/index. Pengujian ini belum menampakkan peran nyata dari *Suricata* dalam mengatasi munculnya halaman *Google reCAPTCHA*. Perlu dilakukan pengujian dengan target seluruh komputer yang ada di *UMS*, *Suricata* perlu dipasang pada perangkat keras dengan spesifikasi tinggi.

Rekomendasi yang diusulkan untuk mengatasi munculnya *Google reCAPTCHA* adalah meminimalisir jumlah perangkat yang berbagi satu alamat *IP* publik dengan membuat *Internet Gateway Load Balancing* yang *IP* publiknya lebih dari satu yang bekerja secara bergantian.

4 PENUTUP

4.1 Kesimpulan

Hasil penelitian tentang *Network Monitoring* di jaringan internet UMS menggunakan *Suricata* dan *pfSense* dapat disimpulkan sebagai berikut:

1. *Suricata* dapat mendeteksi dan memberi peringatan adanya upaya penyusupan ke *server*, di antaranya: upaya *login* terus menerus ke *website* berbasis *Wordpress* dan *Drupal* dengan *bruteforcing* dan upaya penyusup melakukan *SQL Injection*.
2. *Suricata* dapat melakukan *block* terhadap alamat *IP* yang menyebabkan peringatan, namun perlu selektif dalam melakukan *blocking*, karena dapat menyebabkan jaringan menjadi lumpuh.
3. *Google* tidak benar-benar mengetahui penggunaan perangkat lunak yang melanggar ketentuan *Google*, tetapi akses pada tingkat konkurensi tertentu dapat menyebabkan munculnya halaman *reCAPTCHA*, walaupun tidak menggunakan perangkat lunak yang melanggar ketentuan *Google*.
4. Penulis merekomendasikan untuk dibuat *Internet Gateway Load-balancing* untuk mengatasi munculnya halaman *Google reCAPTCHA*.

4.2 Saran

Setelah penelitian selesai, penulis memberikan saran dan pertimbangan untuk penelitian selanjutnya di UMS berkenanaan dengan *Network Monitoring* sebagai berikut:

1. Meneliti lebih detail tentang *IPS* terutama hal-hal yang harus dilakukan *blocking* dan yang tidak.
2. Melakukan *monitoring* jaringan di UMS yang lebih luas dengan spesifikasi perangkat keras yang lebih tinggi.

DAFTAR PUSTAKA

N. Regian Andi, S. Rinaldy Fadillah, P. Mohamad Dawud, Kriswanto. Roni, P. Edi Pratama (2015). *Impelementasi Monitoring Jaringan VPN pada Web dan Mail Server*.e-Proceeding of Applied Science : Vol.1, No.1, Hal 85-91.

Nazwita, Ramadhani. Siti (2017). *Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata*. Seminar Nasional Teknologi Informasi, Komunikasi dan Industri (SNTIKI) 9 Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau Pekanbaru, 18-19 Mei 2017, ISSN (Online) : 2579-5406, Hal 30-317.

Bluequoll (2019). *"Unusual traffic" blocks searching or requires reCAPTCHA*, Google Help Center, url: https://support.google.com/websearch/thread/2596872, di akses tanggal 31 Juli 2019.

Dogan, Jaana B. (2019). *Hey*, url: https://github.com/rakyll/hey, di akses tanggal 31 Juli 2019.

F. Wang dan W. Du (2012). *A Test Automation Framework Based on WEB*. IEEE/ACIS 11th International Conference on Computer and Information Science, Shanghai, 2012, pp. 683-687, doi: 10.1109/ICIS.2012.21.

Prasad, Prakhar (2016). *Mastering Modern Web Penetration Testing*, Birmingham – Mumbai: Pakt Publishing, hal. 101-195.

Gondohanindijo, Jutono (2011). *Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System).* Majalah Ilmiah INFORMATIKA Vol. 2 No. 2 Mei 2011, Hal 47-54.

Risyad, Emir. Data, Mahendra, P. Eko Sakti (2018). *Perbandingana Performa Intrusion Detection System (IDS) Snort dan Suricata dalam Mendeteksi Serangan TCP SYN Flood*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol.2, No.9, September 2018 Hal 2615-2624.

Sarifin, Agus dan Astuti, B.R.T.(2012). *Penerapan Router pfSense Berbasis FreeBSD di Warnet Emax Sragen*, IJNS Vol. 1 No. 1 November 2012, Hal 61-66.

Kuswanto, Dwi (2014). *Unjuk Kerja Intrusion Prevention Sistem(IPS) berbasis Suricata pada Jaringan Local Area Network Laboratorium TIA+ Tehnik Informatikan Universitas Trunojoyo,* NERO Vo.1 No.2, Hal 73-81.