MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

Implementasi Proxy dan Snort Sebagai Gateway Antivirus

[1)] Andreas Sebayang
Universitas Kristen Satya Wacana, Jl. Diponegoro 52-60 Salatiga, Jawa Tengah, Indonesia
E-Mail: 4ndreassebayang@gmail.com

[2)] Indrastanti Ratna Widiasari
Universitas Kristen Satya Wacana, Jl. Diponegoro 52-60 Salatiga, Jawa Tengah, Indonesia
E-Mail: indrastanti@uksw.edu

ABSTRACT
Technology and internet networks are two things that are always related, because in today's era the internet has become a much-needed medium for learning, communicating, exchanging data, and even playing. With the activity of using the internet network, a problem will arise, namely network security. Network security is a very important aspect as a defense in a network, to minimize the risk of data theft and unwanted access in an internet network. The purpose of this study is to implement the control and security of internet use in an agency with minimal costs. namely using the Linux operating system Ubuntu Server 18.04, Proxy Server, and Snort. The result of the system that has been created has a function to perform caching so that it can save bandwidth and can function as filtering content to minimize unwanted things on the network. In addition, the system created is very helpful for network admins to monitor the network in real-time, even can also enforce rules to protect the network.

Keyword : server, proxy, snort, system

PENDAHULUAN

Perkembangan di bidang teknologi baik di Indonesia bahkan Dunia semakin hari semakin melaju dengan sangat pesat pertumbuhannya. Dengan pertumbuhan yang sangat pesat ini kita banyak dimudahkan untuk melakukan berbagai hal. Kemajuan teknologi ini harus didukung juga dengan software dan hardware yang terbaru juga.

Teknologi dan jaringan internet adalah dua hal yang selalu berkaitan, sebab pada era sekarang ini internet menjadi media yang sangat dibutuhkan untuk menjadi media belajar, berkomunikasi dan bahkan bermain. Dengan adanya kegiatan menggunakan jaringan internet maka akan timbul sebuah masalah yaitu keamanan jaringan. Keamanan jaringan merupakan aspek yang sangat penting sebagai pertahanan suatu jaringan komputer, peran dari keamanan jaringan ini sendiri sangatlah penting untuk meminimalisirkan resiko tercurinya data maupun akses yang tidak dikehendaki dalam sebuah jaringan internet.[1]

Jaringan komputer kurang optimal ketika jaringan tersebut di serang oleh penyusup atau *hacker* dan *cracker* untuk kepentingan mencoba mendapatkan akses dari sebuah sistem keamanan, intrusi sistem yang terjadi ketika orang yang tidak berhak mencoba untuk mendapatkan akses atau mengganggu operasi normal dari sistem, (Dr. Khamitkar, 2012). Menurut data dari Badan Siber dan Sandi Negara (BSSN) Bersama dengan Indonesia Honey Project (IHP) mencatat, sepanjang 2019 total telah terjadi 98.243.890 serangan siber. Selain itu di tahun 2019 juga telah terjadi serangan malware sebanyak 22.750 kasus. Kemudian pada tahun 2020Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hamper 190 juta upaya serangan siber di Indonesia.

Maka dari itu diperlukan sebuah pengamanan pada jaringan internet dengan menggunakan gateway antivirus, dengan cara menggunakan fitur-fitur dari proxy server dan snort[1]. Proxy server digunakan sebagai alat untuk memfilter situs apa saja yang boleh diakses oleh client [2] sedangkan snort digunakan sebagai Instrusion Detection System (IDS) dalam mendeteksi serangan jaringan. Pada saat implementasinya Proxy server dan Snort akan dijalankan pada sebuah system operasi ubuntu server 18.04. [3]

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode eksperimen. Langkah-langkah atau metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi literatur
   Akan melakukan pengumpulan data, informasi, dan teori-teori mengenai Snort, IDS, Proxy server yang berasal dari karaya tulis ilmiah, buku-buku, dan jurnal yang bisa ditemukan dari internet maupun perpustakaan, dan juga apabila dirasa perlu melakukan pengumpulan data bisa ditambah dengan mewawancarai orang yang dirasa kompeten di bidang ini.
2. Analisa dan Perancangan sistem

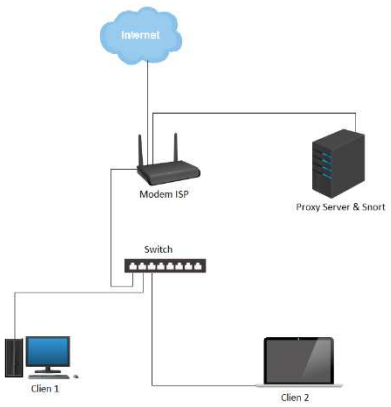
MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

Untuk dapat memahami sistem yang akan dibanngun, perlu dilakukan identifikasi terhadap kebutuhan spesifikasi sistem. Sistem yang akan dibangun adalah sistem pencegahan intrusi menggunakan snort dan penggunaan proxy untuk melakukan filtering nanntinya akan diujicobakan dengan melakukan serangan dan akses konten yang sudah diblokir pada sistem yang telah dibuat.Berdasarkan dari hasil Analisa terhadap sistem yang akan dibuat, dilakukan perancangan dengan menanamkan rules untuk mendeteksi intrusi yang sesuai. Dengan adanya pemodelan ini diharapkapkan bisa memperoleh suatu gambaran mengenai penyelesaian masalah yang telah diidentifikasi sebelumnya

3. Implementasi
   Pada tahap ini akan dilakukan implementasi sistem pendeteksi intrusi yang sesuai dengan rancangan yang telah dibuat sebelumnya
4. Pengujian sistem
   Pada tahap ini dilakukan evaluasi terhadap sistem yang telah dibangun, hal ini dibutuhkan agar apabila terjadi kesalahan pada saat perancangan bisa segera disesuaikan dengan keadaan yang ada.
5. Penulisan
   Pada tahap terakhir dalam pembuatan sistem ini dilakukan analisis dari data yang telah didapatkan dari hasil pengujian untuk membandingkan satu sama lain. Hasil analisis tersebut dituliskan dan ditarik kesimpulan dari penelitian tersebut.

PEMBAHASAN

Pada tahap proses penelitian untuk melakukan uji coba sistem yang telah dirancang menggunakan topologi sebagai berikut



Gambar 1. Topologi Jaringan

Pada tahap perancangan topologi yang digunakan seperti gambar diatas, Keberadaan server yang terletak disamping moden bertujuan dengan semua proses *traffic* data keluar dan masuk akan dialihkan terlebih dahulu menuju ke squid proxy server (*Transparent Proxy)* untuk melakukan caching dan jika data yang lewat terkena filter akan tidak diizinkan untuk masuk ke client. *Tools* yang dibutuhkan adalah :

1. VirtualBox
   Pada VirttualBox menggunakan dua *Network Adapter* yaitu NAT dan Host-only. NAT digunakan untuk server mendapat koneksi langsung ke internet, sedangkan Host-only digunakan agar server bisa terkoneksi langsung dengan host dan bisa diatur IP Address tidak satu segmen dengan jaringan lokal untuk faktor keamanan.
2. Sistem Operasi
   Sistem Operasi yang digunakan adalah Ubuntu Server 18.4
3. Package
   Untuk package yang digunakan yaitu ada dua yaitu squid, dan snort

Pada tahap selanjutnya melakukan konfigurasi Squid Proxy Server dan Snort dilakukan langsung pada Sistem Operasi Ubuntu Server 18.04 sebagai wadahnya. Langkah awal yang dilakukan adalah menginstall *package* Squid dengan perintah sudo apt install squid lalu melakukan konfigurasi pada *squid.conf.*

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
```

Gambar 2. Konfigurasi pada internal network

Pada tahap ini dihadapkan dengan konfigurasi internal network atau jaringan local, Harus menghilangkan tanda pagar pada kelima acl localnet src dengan tujuan agar jaringan lokal dapat mengakses internet.

Salah satu konfigurasi yang penting dan menjadi perhatian selanjutnya adalah pada bagian pendaftaran hak akses agar jaringan lokal bisa mengakses *cache* pada *proxy server*

```
# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
http_access allow localnet
```

Gambar 3. Konfigurasi pendaftaran hak akses

Gambar 3 bertujuan untuk mendaftarkan konfigurasi berdasarkan tahap sebelumnya, Harus menambahkan http_access allow localnet agar sistem mengizinkan jaringan lokal untuk mengakses internet.

Konfigurasi Firewall yang digunakan pada penelitian ini adalah untuk *trasnparant proxy* yang bertujuan setiap data yang keluar dan masuk dari jaringan akan dialihkan untuk melewati Squid Proxy Server terlebih dahulu untuk melakukan fungsi cache dan menjalankan filter blokir terhadap acl yang sudah dibuat.

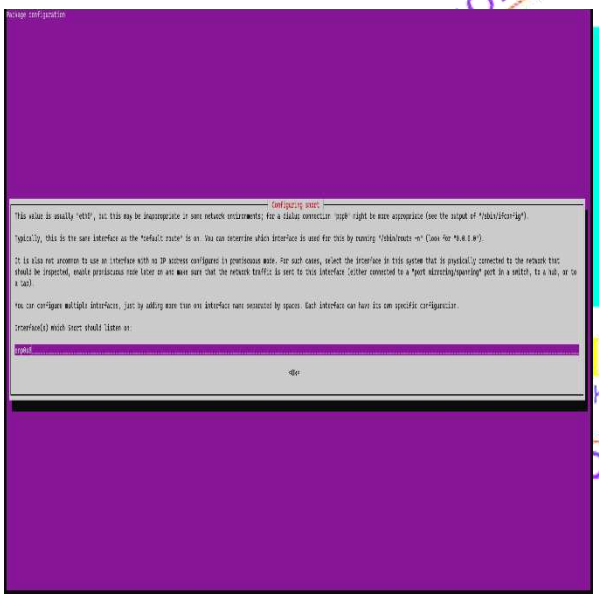
MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

Tabel 1. Transparent Proxy

```
iptables -t nat -A PREROUTING -s 192.168.6.66
-p tcp --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport
80 -j REDIRECT --to-port 3128
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -t mangle -A PREROUTING -p tcp --
dport 3128 -j DROP
```

Tabel 1 merupakan sebuah transparent proxy yang digunakan sebagai pengalihan lalu lintas jaringan menuju ke squid proxy server. Baris pertama dan kedua pada kode program merupakan perintah untuk merouting jalur menuju ke IP proxy server akan diterima melalui *port* 80 lalu di *redirect* ke *port* 3128 yang merupakan *port* dari squid proxy server.

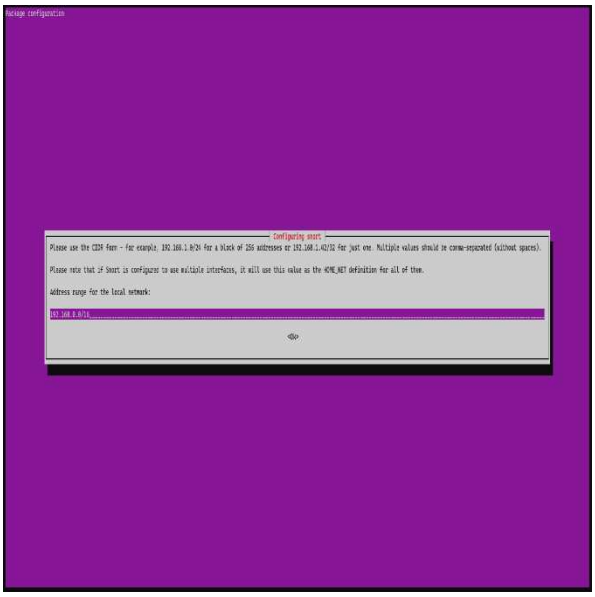
Selanjutnya melakukan penginstallan package snort dengan perintah apt install oinkmaster snort snort-common snort-rules-default snort-doc. Tahapan konfigurasi pada penginstallan *snort* wajib memeriksa interface atau port yang aktif pada sistem seperti berikut



Gambar 4. Konfigurasi adapter interface

Gambar 4 Menjelaskan untuk mengisi bagian ini, perlu melakukan pengecekan adapter interfaces yang digunakan pada sisttem operasi dengan perintah *ifconfig.* Diharapkan megisi sesuai adapter yang aktif. Snort akan melakukan scan terhadap adapter tersebut.

Setelah mendaftarkan *interface* atau *port* yang digunakan sebagai jalur lalu lintas jaringan untuk mengamankan jaringan, maka perlu juga dilakukan konfigurasi pendaftaran *range IP* yang akan diamati oleh *snort* sebagi berikut



Gambar 5. Konfigurasi Range IP

Gambar 5 Pada tahap ini harus mengisi range IP, Harap amati IP pada jaringan sehingga dapat menentukan prefix subnet yang sesuai.

PENGUJIAN SISTEM

Setelah melakukan tahap konfigurasi maka pada sub bab ini akan dilanjutkan dengan membahas tahap pengujian sistem yang telah dibuat, Admin jaringan bisa memantau *traffic request* data dari client yang sudah *diredirect* terlebih dahulu menuju ke squid proxy server

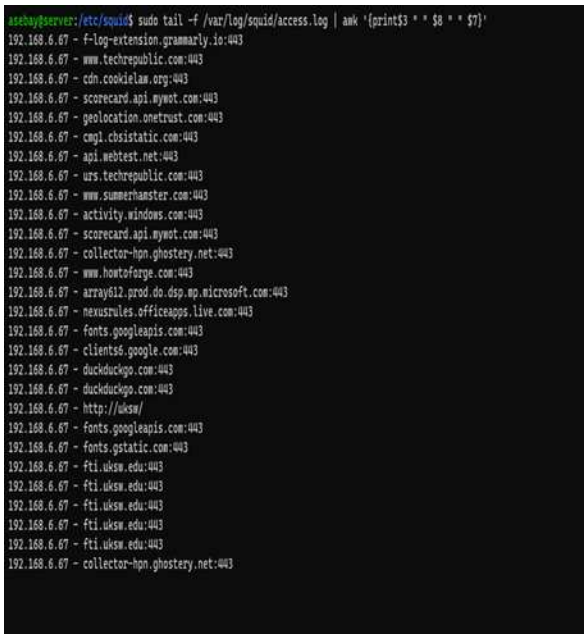
Tabel 2. Perintah Monitoring Traffic Real time

```
tail -f /var/log/squid/access.log |
awk '{print$3 " " $8 " " $7}'
```

Tabel 2 Merupakan sebuah baris perintah yang bertugas untuk menampilkan bagian terakhir dari data yang lewat atau alamat dari data tersebut, semua informasi diakses dari direktori */var/log/squid/access.log* secara *real time* dan akan dikombinasikan dengan baris perintah selanjutnya yaitu untuk memindai pola Bahasa pemrosesan seperti mencocok pola dalam program dan nama jalur data yang berisi input untuk dibaca atau ditampilkan.

Dari baris perintah yang telah dijalankan seperti pada Kode Program 2 akan menghasilkan hasil pemantauan *traffic* pada jaringan sebagai berikut

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089



Gambar 6. Hasil monitoring Traffic Real Time

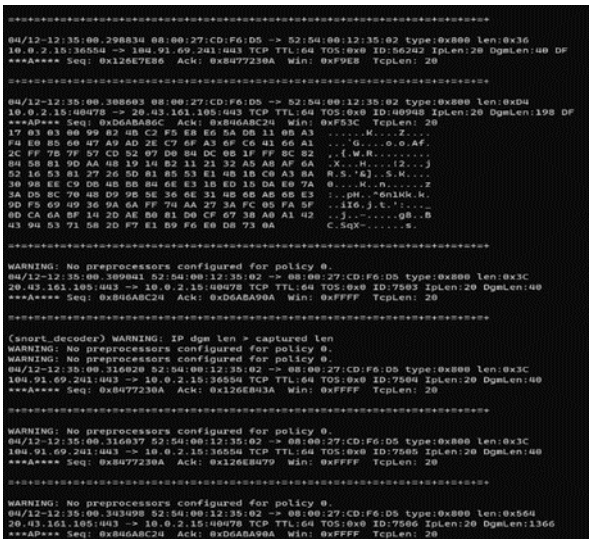
Gambar 6 Berdasarkan gambar diatas dapat dilihat *traffic* jaringan yang dialihkan yang melalui server dan admin bisa secara langsung melakukan *tracer* pada alamat data yang diinginkan dengan melakukan menetekan *ctrl + klik pada alamat domain yang ingin dituju.*

Selain itu juga terdapat fungsi snort yang digunakan sebagai *Sniffer*
Untuk membaca dan menganalisa setiap protocol yang melewati server. Perintah untuk menjalankan mode *sniffer* dapat dimodifikasi dengan baris perintah sebagai berikut:

Tabel 3. Perintah Menjalankan Mode Sniffer

```
snort -vde
```

Tabel 3 Berfungsi untuk menjalankan mode *sniffer* secara *real time* dengan perintah tambahan untuk menampilkan MAC Address sumber, IP Address sumber, Semua parameter TCP dan juga data yang di bawa.
Baris perintah tersebut digunakan untuk mengetahui detail informasi pada packet berupa informasi *Mac Address* tujuan dan asal packet, detail informasi



Gambar 7. Tangkapan layer ketika mode sniffer dijalankan

Gambar 7 Dari hasil tangkapan layar terlihat dengan menjalan kan kode program mode *sniffer* tersebut snort dapat menampilkan MAC Address antara sumber dan tujuan, lalu IP Address sumber dan tujuan serta protocol yang digunakan.

Selain membuat mode *sniffer* pada sistem yang dibangun juga membuat mode IDS atau *Intrsion Detection System* yang berfungsi untuk mendeteksi serangan yang menuju ke server yang dibangun.

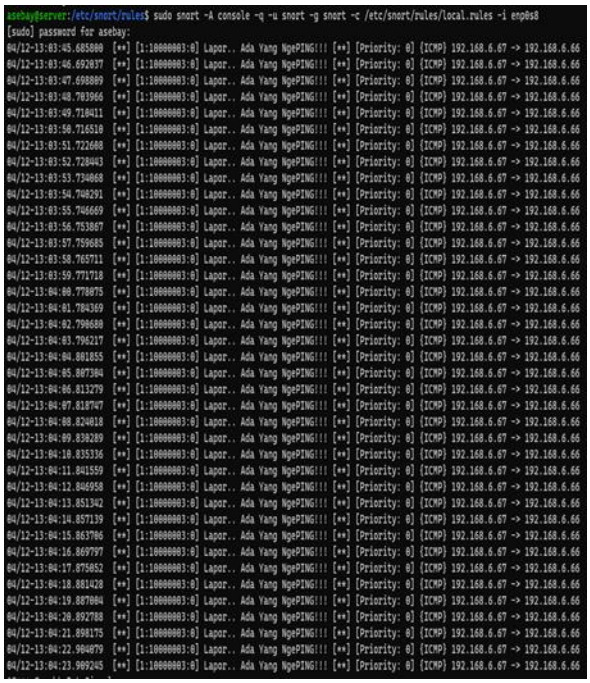
Tabel 4. Rules

```
Alert tcp any any -> 192.168.6.66 23
(msg: "Ada yang TELNET ke mesin!!!";
sid:1000001;)
Alert tcp any any -> 192.168.6.66 any
(msg: Lapor.. Ada Yang NgePING!!!";
sid:1000003;)
```

Tabel 4 Kode program ini dibuat pada direktori */etc/snort/rules/local.rules* dengan tujuan ketika admin hanya ingin menjalankan rules yang telah dibuat oleh maka ketika ada terdeteksi serangan seperti pada kode program yaitu Sistema akan menampilkan pesan ketika ada yang ingin melakukan telnet ke sistem atau ada yang melakukan ping terhadap sistem.

Pada direktori *rules* admin jaringan dapat membuat sebuah *rules* sesuai keinginan dengan mendaftarkan *rules* tersebut pada direktori yang bernama *local rules* seperti gambar dibawah ini, Snort juga sudah menyediakan sangat banyak contoh *rules* yang terletak pada direktori rules yang dapat digunakan juga dan dapat dimodifikasi menjadi sesuai keinginan dari admin jaringan.

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089



Gambar 8. Ketika Mode IDS dijalankan

Gambar 4.8 Pada proses ini perintah mode IDS telah dijalankan dan sistem coba diping dan secara langsung sistem akan menampilkan pesan seperti Digambar, *rules* yang dijalankan hanya *rules* local atau yang dibuat sendiri.

Tabel 5. Perintah menjalankan mode IDS

```
snort -A console -q -u snort -g
snort -c
/etc/snort/rules/local.rules -I
enp0s8
```

Tabel 5 Baris kode program ini digunakan untuk menjalankan mode IDS dengan penjelasan mesin akan menjalankan snort dengan mode *alert mode* dan hanya menampilkan isi pesan, IP address sumber dan IP address target, rules yang dijalankan dari direktori yang sudah ditentukan yaitu */etc/snort/rules/local.rules* dengan network adapter yang menjadi target adalah enp0s8. Selain menggunakan rules yang telah dibuat sendiri, snort juga sudah menyediakan berbagai macam jenis deteksi serangan, Jika ingin menjalan perintah pendeteksi yang sudah disediakan oleh snort dapat merubah direktorinya menjadi snort.conf. Maka sistem akan mendeteksi jenis serangan berdasarkan klasifikasi yang sudah dibuat oleh snort.

KESIMPULAN

Berdasarkan dari pembahasan diatas dapat ditarik kesimpulan bahwa dunia teknologi informasi yang semakin berkembang secara pesat dan diikuti dengan meningkatnya pengguna internet. Dengan semakin meningkatnya pengguna internet maka tuntutan akan kecepatan akses internet dan keamanan pada jaringan sudah menjadi hal umum, untuk menjawab permasalahan tersebut maka diusulkan untuk melakukan pengimplementasian squid proxy server dan snort pada ubuntu server 18.04 yang bertujuan untuk meningkatkan kecepatan akses internet, memantau seluruh *traffic* paket data yang diarahkan menuju ke proxy server dan bisa secara langsung juga mentrace apa yang dibukan oleh client, Selain itu juga kegunaan snort dapat digunakan dalam tiga mode yaitu *sniffer, logging*. Dan *IDS.* Untuk menampilkan hasil perintah kode program membutuhkan banyak referensi seperti membaca document dari squid dan snort, melihat berbagai macam daftar perintah diinternet untuk mengoperasikan squid dan snort lalu melakukan modifikasi terhadap kode program sehingga menemukan kombinasi sendiri. Sistem yang dibagun dapat dipantau secara realtime tanpa harus menggunakan fitur tambahan dari aplikasi lain. Dapat ditarik kesimpulan juga banyak admin jaringan yang menggunakan aplikasi pihak ketiga yang sudah menggabungkan fungsi squid dan snort pada sistem aplikasi mereka buat dengan kemudahan dalam penggunaannya. Namun untuk bisa menggunakan aplikasi pihak ketiga pasti akan membutuhkan biaya untuk mendapatkannya. Kelemahan dari menggunakan aplikasi pihak ketiga yaitu admin tidak bisa memodifikasi fitur yang mereka inginkan karena keterbatasan terhadapat aplikasi tersebut. Untuk pengembangan selanjutnya sistem akan dikembangkan dan dapat digunakan secara web dengan fitur tambahan lainnya yang sudah direncanakan.

DAFTAR PUSTAKA

[1] A. P. Wicaksono, “Sistem Deteksi Intrusi dengan Snort,” p. 4, 2014.
[2] W. Wahyudi, “Membangun Proxy Server Cv Global Max Menggunakan Sistem Operasi Linux Blankon 6.0 Ombilin Sebagai Manajemen Akses Jaringan,” *Edik Inform.*, vol. 1, no. 1, pp. 63–71, Feb. 2017, doi: 10.22202/ei.2014.v1i1.1441.
[3] P. Panggabean, S. Kom, and M. Kom, “ANALISIS NETWORK SECURITY SNORT MENGGUNAKAN METODE INTRUSION DETECTION SYSTEM (IDS) UNTUK OPTIMASI KEAMANAN JARINGAN KOMPUTER,” vol. 6, no. 1, p. 12, 2018.
[4] E. R. Nainggolan, “IMPLEMENTASI PENGATURAN PROXY SERVER MENGGUNAKAN SERVICE SQUID PADA SISTEM OPERASI LINUX,” no. 2, p. 6, 2015.
[5] R. Mentang, A. A. E. Sinsuw, and X. B. N. Najoan, “Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System,” vol. 5, no. 7, p. 10, 2015.

[6] M. Ulfa, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) DI JARINGAN UNIVERSITAS BINA DARMA," p. 14.
[7] P. P. Putra, "Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap," vol. 2, no. 1, p. 7, 2016.
[8] D. T. Atmaja, E. B. Prasetya, and P. E. Kresnha, "NOTIFIKASI ADANYA SERANGAN PADA JARINGAN KOMPUTER DENGAN MENGIRIM PESAN MELALUI APLIKASI TELEGRAM DAN KONTROL SERVER," p. 8.
[9] S. Suhartono and Abd. R. Patta, "SISTEM PENGAMANAN JARINGAN ADMIN SERVER DENGAN METODE INTRUSION DETECTION SYSTEM (IDS) SNORT MENGGUNAKAN SISTEM OPERASI CLEAROS," *J. Teknol. Elekterika*, vol. 14, no. 2, p. 145, Nov. 2017, doi: 10.31963/elekterika.v14i2.1220.
[10] R. F. Olanrewaju *et al.*, "Snort-based Smart and Swift Intrusion Detection System," *Indian J. Sci. Technol.*, vol. 11, no. 4, pp. 1–9, Jan. 2018, doi: 10.17485/ijst/2018/v11i4/120917.