PENGAMANAN MIKROTIK ROUTERBOARD DARI SERANGAN KEAMANAN DENGAN NOTIFIKASI BOT TELEGRAM

Mufria J Purba✉, Arif Gunawan Putra Simanjuntak
Universitas Methodist Indonesia, Medan, Indonesia
Email: jonatan.purba@gmail.com

DOI: https://doi.org/10.46880/methoda.Vol11No3.pp241-246

ABSTRACT

The task of the network administrator is also not easy, this is because an admin must secure his network from an attack that can cause the network router to go down until it is damaged. There are so many ways to prevent a person/company from being able to provide optimal service, one of which is to attack the router using a DDoS attack type. Therefore, a network security is needed with the Intrusion Detection System (IDS) method. Intrusion Detection System (IDS) is a method used to detect suspicious activity in a system or network. In this study, IDS is used as a deterrent and sends notifications of DDoS attacks on Mikrotik routers via Telegram bots. The process of testing DDoS attacks in the form of ping flood, SYN Flood and UDP Flood, telegram bot notifications were successfully implemented quite well, where IDS sent notifications via network admin telegram bots.
Keyword: *Mikrotik, IDS, DDoS, Telegram Bot.*

ABSTRAK

Tugas administrator jaringan juga tidak mudah, hal ini dikarenakan seorang admin harus mengamankan jaringannya dari serangan yang dapat menyebabkan router jaringan down hingga rusak. Banyak sekali cara yang dapat dilakukan untuk mencegah seseorang/perusahaan untuk dapat memberikan layanan yang optimal, salah satunya adalah dengan menyerang router menggunakan tipe serangan DDoS. Oleh karena itu diperlukan suatu keamanan jaringan dengan metode Intrusion Detection System (IDS). Intrusion Detection System (IDS) adalah metode yang digunakan untuk mendeteksi aktivitas mencurigakan dalam suatu sistem atau jaringan. Pada penelitian ini, IDS digunakan sebagai pencegah dan mengirimkan notifikasi serangan DDoS pada router Mikrotik melalui bot Telegram. Proses pengujian serangan DDoS berupa ping flood, SYN Flood dan UDP Flood, notifikasi bot telegram berhasil diimplementasikan dengan cukup baik, dimana IDS mengirimkan notifikasi melalui bot telegram admin jaringan.
Kata Kunci: *Mikrotik, IDS, DDoS, Telegram Bot.*

PENDAHULUAN

Router merupakan suatu alat yang digunakan untuk mengirimkan paket data melalui sebuah jaringan. Akan tetapi tidak semua perusahaan yang memiliki sebuah jaringan diatur menggunakan mikrotik router. Salah satunya adalah Balai Pengelola Transportasi Darat (BPTD) kota Medan. Pada Balai Pengelola Transportasi Darat (BPTD) koneksi internet pada client masih disalurkan langsung dari modem internet melalui switch antar ruangan. Pada penggunaan internet dengan akses client yang cukup banyak, tentu dengan hanya mengandalkan modem bukan pilihan yang tepat. Oleh sebab itu dibutuhkanya penambahan router pada manajemen jaringan serta untuk menambah keamanan jaringan.

Router yang dapat digunakan untuk mengelola jaringan adalah mikrotik router. Pengelolaan mikrotik router tersebut tentu

dilakukan oleh seorang administrator jaringan. Tugas administrator jaringan juga tidak dapat dikatakan mudah, hal ini dikarenakan seorang admin harus mengamankan jaringanya dari suatu serangan yang dapat mengakibatkan router jaringan down hingga rusak. Masalah keamanan jaringan komputer merupakan faktor yang sangat penting diperhatikan dan dikelola oleh seorang admin jaringan.

Sistem keamanan jaringan komputer bisa jadi secara fisik maupun secara non fisik. Secara fisik adalah sistem keamanan server beserta perangkat pendukungnya dari pencurian, bencana alam dan kerusakan akibat kesalahan manusia. Sedangkan secara non fisik adalah berupa kerusakan sistem operasi server, kerusakan pada program aplikasi ataupun terhadap gangguan dari luar sistem seperti serangan hacker, virus, trojan dan lain sebagainya (Sutarti, Pancaro, & Saputra, 2018). Banyak sekali cara yang ditempuh untuk menghalangi seseorang/perusahaan untuk dapat memberikan layanan yang optimal.

Namun seringnya jaringan server mengalami gangguan karena diserang yang disebabkan oleh serangan jenis DDoS, gangguan tersebut bisa berupa kegagalan sistem, halt, error request bahkan kerusakan hardware server. Serangan Distributed denial-of-service (DDoS) merupakan jenis serangan yang telah ada. sejak tahun 1990, dimana volume dan intensitas DDoS terus meningkat. Pada akhir tahun 2014, dilaporkan bahwa serangan DDoS merupakan teknik serangan yang paling populer. Dengan demikian, DDoS merupakan salah satu ancaman utama dunia maya dan menjadi masalah utama keamanan cyber (Gong et al., 2019).

Dalam penelitian menyatakan bahwa DDoS berhasil menyerang jaringan dengan tingkat 90%, sehingga dibutuhkanya sebuah sistem pendeteksi terhadap router ketika terjadinya sebuah serangan DDoS. Pendeteksi serangan tersebut bertujuan untuk mengamankan router dari pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkanya sebuah keamanan jaringan dengan metode Intrusion Detection System (IDS) (Ginting, Napitupulu, & Jamaluddin, 2015). Intrusion Detection System (IDS) adalah metode yang digunakan untuk mendeteksi sebuah aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Metode ini memberikan peringatan kepada admin bahwasanya terjadi suatu serangan dan menutup serangan tersebut. Sehingga serangan DDoS tidak sempat masuk kedalam sebuah router yang dapat menyebabkan router down.

Untuk menambah keamanan, maka digunakan fitur notifikasi untuk memberikan peringatan kepada admin jaringan ketika adanya serangan DDoS. Peringatan notifikasi serangan DDoS dapat dilakukan dengan konfigurasi alert bot telegram pada jaringan mikrotik. Penggunaan notifikasi bot telegram sangat berguna bagi seorang administrator jaringan dalam rangkan memberikan peringatan ketika adanya serangan DDoS, hal ini dikarenakan bot telegram mampu memberikan informasi berupa data penyerangan pada jaringan mikrotik. Sehingga monitoring jaringan dari tindakan yang dapat merugikan pengguna yang dilakukan secara realtime oleh notifikasi bot telegram.

Beradasarkan pada latar belakang masalah di atas dan kesimpulan dari penelitian sebelumnya, maka pada penelitian ini akan menambahkan sebuah router serta mengamankan router jaringan mikrotik dari sebuah serangan DDoS dengan IDS dan notifikasi bot telegram dengan riset jaringan pada Balai Pengelola Transportasi Darat (BPTD).

LANDASAN TEORI

Setiap jaringan komputer pasti memiliki celah keamanan. Ada beberapa jenis serangan yang terdapat pada jaringan *wireless* yang perlu diketahui, beberapa jenis serangan yang umum digunakan para penyerang adalah *spoofing,* DDOS, *sniffer, DNS poisoning, ping of death,* dan *brute force* (Sada, 2019).

Spoofing

Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya (Ketaren, 2016).

DDoS (*Distributed Denial of Service*)

Serangan DOS *(Denial-Of-Service attacks*) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut (Pradipta, 2017).

Sniffer

Sniffer paket atau penganalisa paket yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer (Pradipta, 2017).

DNS Poisoning

DNS Poisoning merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi IP *Address* yang salah mengenai sebuah *host*, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya (Hendarsyah, 2012).

Ping Of Death

Penyerang mengirimkan serangkaian paket data ke target yang tidak sesuai ketentuan aturan jaringan. Jika secara terus menerus bisa mengakibatkan jalur koneksi penuh dan berakibat *drop*nya server karena tidak bisa menampung kebutuhan tersebut (Sada, 2019).

Brute Force

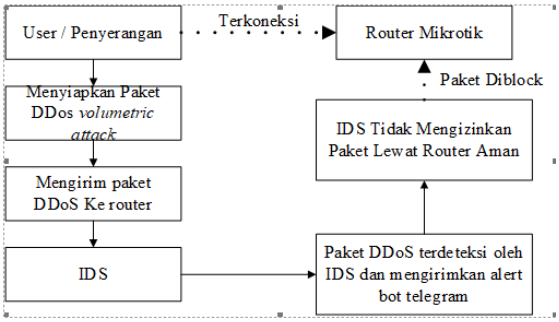
Serangan brutal (bahasa Inggris: *Brute-force attack*) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin (Purba & Efendi, 2021).

ANALISA DAN PERANCANGAN SISTEM

Pada penelitian ini, serangan DDoS yang diterapkan adalah serangan DDoS *volumetric attack* dengan jenis *ping flood, SYN flood, UDP flood* dan *TCP flood*. Serangan DDoS *ping flood* adalah serangan yang membanjiri ping ICMP atau *request* dari *client* ke router secara brutal, sehingga mengakibatkan cpu router menjadi *overload* dan *down*. Sedangkan serangan *SYN flood* dan *UDP flood* dilakukan dengan konsep yang sama, akan tetapi dengan protokol yag berbeda.

Adapun konsep dari salah satu serangan DDoS *ping flood* adalah *user* yang akan menyerangan terlebih dahulu sudah terhubung kejaringan router, hal ini bertujuan untuk mengetahui ip router yang sedang berjalan. Kemudian menyiapkan *ping flood* sebanyak mungkin untuk dilakukan ping massal yang ditujukan ke ip router, jika router tidak memiliki keamanan yang cukup, maka router akan menerima paket *ping* yang *overload* serta mengakibatkan router menjadi *down* hingga rusak. Untuk mengatasi hal tersebut maka diperlukanya metode yang dapat mendeteksi dan mencegah serangan DDoS.

Metode yang diterapkan adalah IDS (*Intrusion Detection System*), yang medeteksi dan menolak serangan DDoS *ping flood*, *SYN flood* dan *UDP flood* secara massal dengan membatasi paket yang dikirim dari klient kepada router. Sedangkan fitur notifikasi yang digunakan adalah bot telegram yang bertujuan untuk memberikan *alert* (peringatan) pada admin jaringan. Adapun skema diagram dari penyerangan DDoS *volumetric attack* dengan keamanan IDS terhadap router dapat dilihat pada gambar di bawah



Gambar 1. Skema Penyerangan

Berdasarkan pada gambar di atas, proses serangan dapat terjadi apabila suatu *user* telah terhubung dengan jaringan router, baik melalui media kabel atau nirkabel. Kemudian *user* menyediakan sebuah *tools* penyerangan DDoS *volumetric attack* yang dapat dikonfigurasi untuk mengirimkan paket serangan DDoS

volumetric attack dengan jenis *ping flood, SYN flood* dan *UDP flood* mengarah ke IP router, router yang memiliki keamanan IDS akan mendeteksi permintaan *user* yang dianggap berlebihan, sehingga IDS tidak akan mengizinkan paket serangan lewat untuk mengenai router, kemudian router mengirimkan pesan peringatan melalui bot telegram kepada *admin* jaringan.

Sebelum melakukan pengujian serangan serangan DDoS *volumetric attack* dengan jenis *ping flood, SYN flood* dan *UDP flood* menggunakan metode IDS pada router mikrotik, terlebih dahulu membangun jaringan LAN mikrotik yang menghubungkan router mikrotik terhadap komputer klient dan langkah awal adalah dibutuhkannya koneksi internet yang didapatkan dari *Internet Service Provider* (ISP). Selanjutnya konfigurasi *network ip address, routing network address, firewall NAT, Firewall IDS* yang berfungsi untuk medeteksi dan mencegah serangan DDoS

Analisa Kebutuhan Sistem

Adapun kebutuhan sistem untuk menerapkan pengamanan jaringan router dari serangan DDoS terdiri dari kebutuhan perangkat keras dan kebutuhan perangkat lunak.

Dalam melakukan penerapan dan konfigurasi sistem keamanan jaringan dibutuhkan perangkat keras yang berfungsi untuk menopang jalanya sistem keamanan jaringan agar sesuai dengan kebutuhan. Pada penelitian ini kebutuhan perangkat keras sebagai berikut:

- Router Miktrotik RB951-2^{nD}
- *Swicht*/*Hub* 4 *Port*
- Kabel UTP dengan konektor RJ45
- Laptop

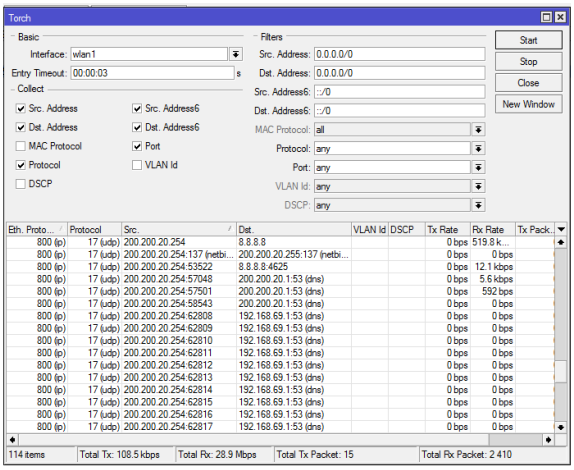
Perangkat lunak dibutuhkan untuk melakukan pengujian dan konfigurasi mikrotik. Adapun perangkat lunak yang dibutuhkan adalah sebagai berikut:

- *Winbox*
- CMD
- *Notepad*
- Aplikasi *Browser* (*Mozilla Firefox* atau *Google Crome*)

IMPLEMENTASI DAN PENGUJIAN JARINGAN

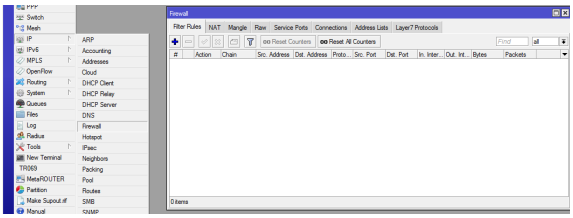
Konfigurasi Firewall UDP Flood

UDP Flood attack digunakan untuk memperlambat koneksi *Client* dikarenakan adanya lonjakan *upload* yang sangat besar yang telah dilakukan oleh Penyerang. Untuk itu konfigurasi ini akan mengatasi kondisi *UDP Flood* menggunakan *filter rule*. Untuk mengetahui kondisi bahwa mikrotik diserang *UDP Flood* bisa lihat dan melakukan cek melalui menu *torch* pada mikrotik. Hal ini bertujuan untuk menemukan *IP address* yang melakukan *UDP Flood* pada jaringan mikrotik. Adpaun menu *torch* dapat ditemukan di *Tools*>*Torch*>lalu centang "*protocol*" dan Klik "*Start*" seperti gambar di bawah ini:



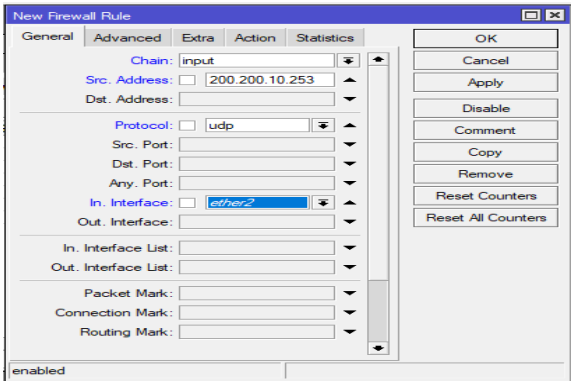
Gambar 2. Proses *Scanner Torch*

Berdasarkan pada hasil *torch* pada gambar di atas, maka diketahui bahwa *ip address* yang melakukan *flood* UDP adalah 200.200.10.253 yang menyebabkan lonjakan *upload* yang sangat besar. Selanjutnya adalah menambahkan *firewall filter rules* dengan cara klik IP>*Firewal*>*Filter Rules*, dan klik (+) untuk menambahkan *filter rule* baru:



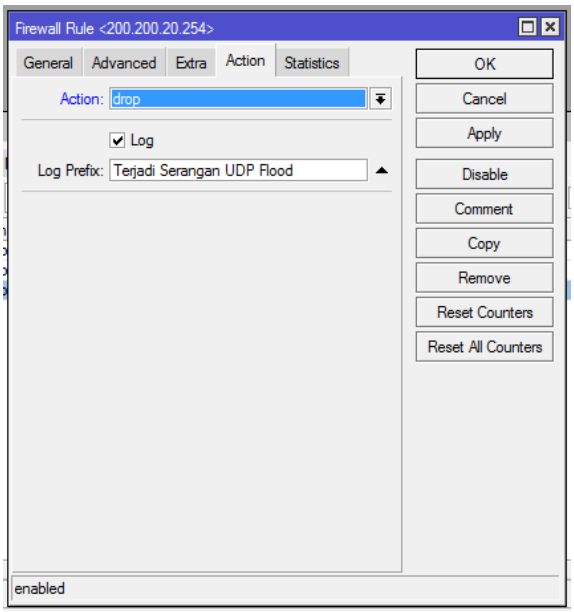
Gambar 3. Menu *Firewall Filter Rules UDP Flood*

Berdasarkan pada gambar di atas, berikut adalah konfigurasi pada tab general:



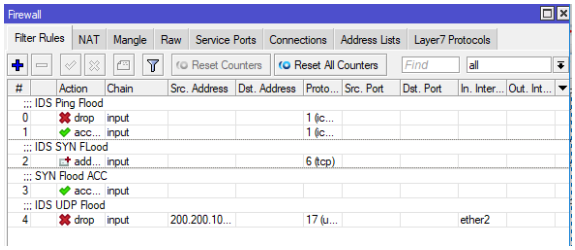
Gambar 4. Konfigurasi *Filter Rule UDP Flood* Tab *General*

Berdasarkan pada gambar di atas, pada tab *general Chain = input Src. Address = 200.200.20.254 Protocol = udp In.Interface = wlan1*. Berikut adalah konfigurasi pada tab action:



Gambar 5. Konfigurasi *Filter Rule UDP Flood* Tab *Action*

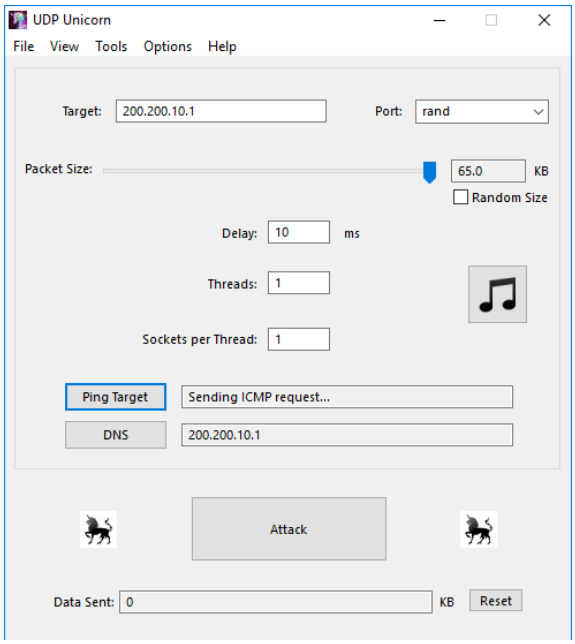
Berdasarkan pada gambar di atas, pada tab *action Action = drop*, Centang *Log, Log prefix =* Terjadi serangan *UDP FloodI.* Berikut adalah hasil penambahan filter rules serangan UDP Flood:



Gambar 6. Hasil Konfigurasi *Filter Rule UDP Flood*

Pengujian Serangan DDoS UDP Flood dan Notifikasi Serangan

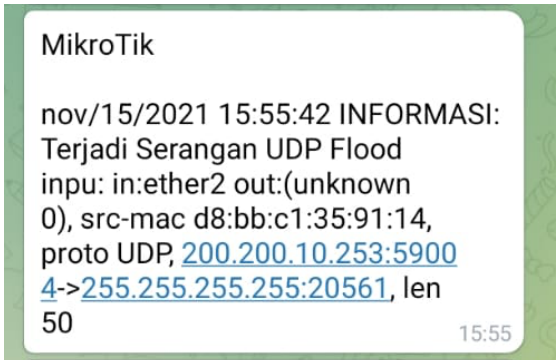
Untuk melakukan pengujian *UDP Flood* pada penelitian ini, menggunakan aplikasi yang bernama *UDP Unicorn*. Pertama buka aplikasi *UDP Unicorn* yang telah diinstall sebelumnya, selanjutnya isi IP *Target* yang akan dijadikan *Target*, IP DNS dari Google akan menjadi target yang akan di serang menggunakan UDP, lalu atur *Packet size* sampai dengan maksimum, Klik "*Ping Target*" dan "DNS" dan terakhir klik "*Attack*" lalu *UDP Unicorn* akan langsung melakukan *UDP Flooding* pada Target melalui jaringan Mikrotik. Berikut adalah tampilanya:



Gambar 7. Tampilan Menu Utama *UDP Unicorn*

Setelah dilakukan serangan *UDP Flood*, maka pada sistem mikrotik diketahui bahwa *ip address* yang melakukan *flood UDP* adalah 200.200.10.253 yang menyebabkan lonjakan *upload* yang sangat besar. Selanjutnya ketika

terjadi serangan *UDP Flood* pada mikrotik, *script scheduler* yang ada dimikrotik akan mengirimkan notifikasi informasi berupa pemberitahuan telah terjadi Serangan *SYN Flood* pada Mikrotik seperti pada gambar di bawah ini:



Gambar 8. Notifikasi Serangan DDoS *UDP Flood*

KESIMPULAN

Setelah dilakukannya pengujian jaringan serangan DDoS, maka penulis dapat menarik kesimpulan sebagai berikut:

1. Optimalisasi keamanan mikrotik *routerboard* berhasil dilakukan dengan metode IDS dan fokus pada *firewall* dan *script*.
2. Adanya IDS tersebut memberi dampak antara lain, mampu mendeteksi serangan DDOS dan memberikan notifikasi kepada administrator berupa bot telegram.

DAFTAR PUSTAKA

Ginting, A. L. T., Napitupulu, J., & Jamaluddin. (2015). Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia. *Seminar Nasional Teknologi Informasi & Komunikasi (SNASTIKOM) 2015*, 83–87. Universitas Harapan Medan.

Gong, D., Tran, M., Shinde, S., Jin, H., Sekar, V., Saxena, P., & Kang, M. S. (2019). Practical verifiable in-network filtering for DDoS defense. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 1161–1174. https://doi.org/10.1109/ICDCS.2019.00118

Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *1*(1), 12–33. https://doi.org/10.46367/iqtishaduna.v1i1.2

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35–42.

Pradipta, Y. W. (2017). Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IP Tables Berbasis Linux. *Jurnal Manajemen Informatika*, *7*(1).

Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI*, *17*(2), 143–158. https://doi.org/10.24246/aiti.v17i2.143-158

Sada, A. (2019). *Notifikasi Keamanan Layanan SSH pada Mikrotik Menggunakan SMS*. Universitas Mercu Buana.

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). Implementasi IDS (Intrusion Detection System) pada Sistem Keamanan Jaringan Sman 1 Cikeusal. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *5*(1), 1–8.