

ANALISIS SISTEM KEAMANAN WPA2 PADA JARINGAN WIRELESS MENGGUNAKAN METODE SIGNAL SCANNING DAN MAC CHANGER (STUDI KASUS DI KOS PUTRA RAHMA)

Rindi Insan Cahyadi¹, Edhy Sutanta², Joko Triyono³

¹Program Studi Informatika, Universitas AKPRIND Indonesia
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029

Abstract

Putra Rahma boarding house is on Jl. Bhinneka Tunggal Ika, Wonocatur, District. Banguntapan, Bantul Regency, Special Region of Yogyakarta 55198. In this place the boarding house residents installed wireless to meet the internet connection needs in the boarding house. The wireless internet connection installed in the boarding house is often accessed by unauthorized people, causing the wireless network to become slow.

To overcome the following problems, it is necessary to analyze the WPA2 security system on the wireless network using the Signal Scanning method and Mac Changer using netcut software to see who is accessing the wireless network in the boarding house and requires 3 tools in network testing to find out whether the wireless security system is good. or not.

Based on the results of 30 tests, it can be seen that, using the Mac Changer method, users do not have the right to know the MAC address of a wireless network with a WPA2 security system because it has not yet entered the targeted wireless network, and by using the signal scanning method, wireless network providers can detect suspicious IPs. on the WPA2 security system.

Keywords: netcut software, boarding house Wireless network, Signal Scanning Method, Mac Changer.

Abstrak

Kost Putra Rahma berada di Jalan Bhinneka Tunggal Ika, Wonocatur, Banguntapan, Bantul, Daerah Istimewa Yogyakarta. Di tempat tersebut penghuni kost memasang koneksi internet wireless untuk memenuhi kebutuhan koneksi internet penghuni kost. Koneksi internet wireless yang dipasang di kost tersebut seringkali diakses oleh orang yang tidak berhak sehingga mengakibatkan jaringan wireless menjadi lambat. Untuk mengatasi permasalahan tersebut, diperlukan analisis sistem keamanan pada jaringan wireless yang dipasang.

Dalam penelitian ini digunakan metode signal scanning dan mac changer dengan menggunakan software netcut untuk melihat siapa saja yang mengakses jaringan wireless di kost tersebut. Pengujian juga dilakukan menggunakan alat bantu berupa perangkat lunak saat pengujian sistem keamanan wireless.

Berdasarkan hasil 30 kali pengujian, diketahui bahwa dengan menggunakan metode Mac Changer, pengguna yang tidak berhak tidak dapat mengetahui alamat MAC jaringan wireless yang menerapkan sistem keamanan WPA2. Dengan menggunakan metode signal scanning, penyedia jaringan wireless dapat mendeteksi IP pengguna yang mencurigakan.

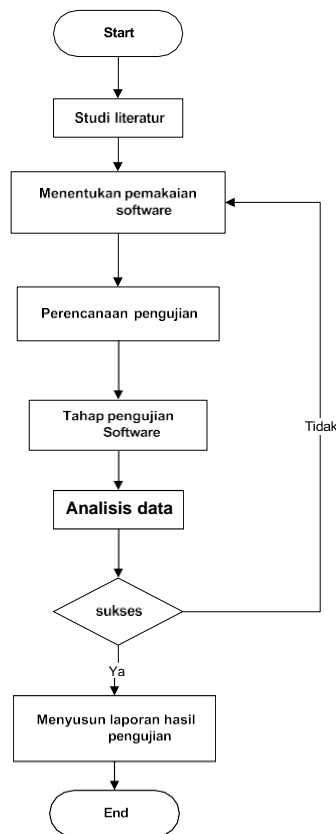
Kata kunci: netcut software, boarding house Wireless network, Signal Scanning Method, Mac Changer.

Pendahuluan

Internet merupakan sekumpulan jaringan yang saling terhubung dimana jaringan tersebut menyediakan sambungan global informasi. Internet secara harfiah ialah sistem globa dari seluruh jaringan komputer yang saling terhubung menggunakan standar Internet Protocol Suite (TCP/IP) untuk melayani miliaran pengguna di seluruh dunia [1].

Kost Putra Rahma berada di Jl. Bhinneka Tunggal Ika, Wonocatur, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55198. Di tempat tersebut penghuni kost memasang wireless untuk memenuhi kebutuhan koneksi internet di dalam kost. Koneksi internet wireless yang dipasang di kost tersebut seringkali diakses oleh orang yang tidak berhak, karena sistem keamanan jaringan yang digunakan masih sebatas pengaturan modem ISP dan pengaturan router bawaan, tanpa ada keamanan tambahan.

Penelitian serupa dengan penelitian ini pernah dilakukan antara lain oleh Haerudin dan Arif Kurniadi [2], Marti Widya Sari [3], dan Inda Sari dan Muh Yamin [4]. Kesamaan penelitian ini dengan tiga penelitian sebelumnya terletak pada metodologi. Perbedaan penelitian ini dibandingkan dengan penelitian-penelitian tersebut adalah metode yang digunakan untuk analisis keamanan jaringan. Metode signal scanning telah digunakan pada penelitian-penelitian yang sudah ada namun pada dipenelitian ini menggunakan 2 metode dalam penelitian. Diagram alir proses pengerjaan penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

TINJAUAN PUSTAKA

Penelitian ini menggunakan rujukan 4 (empat) hasil penelitian sebelumnya, yang dibahas secara singkat di bagian ini. RS H.L Manambai Abdulkadir yang terletak di kota Sumbawa Provinsi Nusa Tenggara Barat, saat ini menggunakan koneksi jaringan yang terdiri dari 6 perangkat wireless untuk melayani seluruh unit di kantor, menggunakan keamanan WPA2- PSK. Wireless yang

digunakan lebih sering mengalami masalah pada sistem keamanan jaringan dibandingkan menggunakan jaringan LAN. Adapun jenis serangan yang terjadi adalah brute force seperti flooding dan illegal access yaitu metode untuk meretas password dengan cara mencoba semua kemungkinan kombinasi yang ada pada wordlist. Serangan flooding terhadap perangkat wireless yang berimbas pada PC dan mengakibatkan PC tersebut tidak dapat mengakses internet [2].

Penelitian lain tentang analisis keamanan WPA2-PSK dan Radius Server pada jaringan wireless menggunakan metode wireless penetration testing. Hasil penelitian ini menyatakan bahwa keamanan wireless yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain. Walaupun demikian, dari hasil studi pustaka diketahui bahwa sistem keamanan wireless yang benar-benar mampu memberikan tingkat keamanan yang lebih baik adalah dengan menggunakan sistem keamanan Remote Authentication Dial In User Service (RADIUS) server [3].

Penelitian lainnya mendefinisikan keamanan jaringan wireless dan mendapatkan hasil dari pemakaian IDS. Implementasi dilakukan pada sistem operasi Linux Ubuntu versi 18.04 LTS menggunakan snort dan iptables sebagai pencegah serangan. Setelah itu, digunakan wireshark untuk analisis serangan yang terjadi dalam jaringan tersebut. Metode penelitian yang digunakan adalah Security Policy Development Life Cycle (SPDLC) dengan melewati beberapa tahapan, yaitu: analysis, design, implementation, enforcement, enhancement. Hasil penelitian tersebut menyatakan bahwa serangan yang dilakukan oleh penyerang pada jaringan dapat diketahui dan ditangani sebelum kerusakan yang lebih luas terjadi, dan penggunaan wireshark dapat menganalisis serangan dengan baik melalui flow graph yang disediakan [4].

PEMBAHASAN

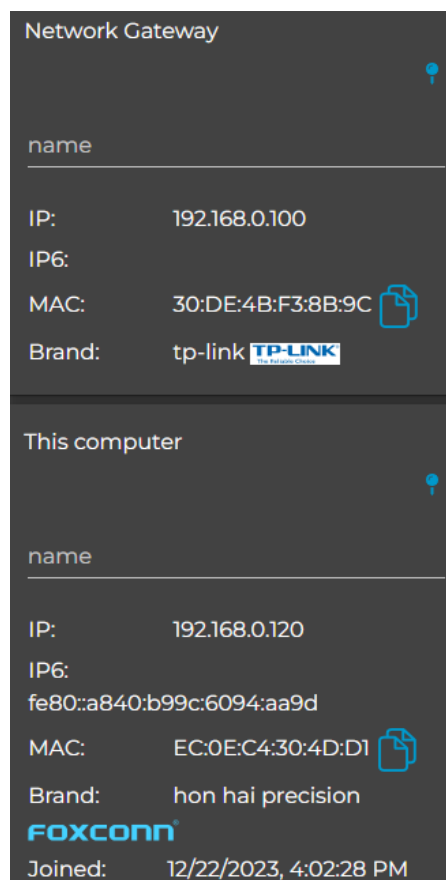
Netcut adalah tool pengelola jaringan yang dikembangkan oleh Arcai pada tahun 2001. Arcai sendiri merupakan komunitas yang secara aktif mengembangkan berbagai jenis aplikasi sejak tahun 1999. Archai meluncurkan aplikasi ini dengan memanfaatkan kelemahan Address Resolution Protocol (ARP) Selain itu, Netcut sering digunakan oleh orang tak bertanggung jawab untuk menyusup dan mencuri koneksi internet dari sebuah jaringan. dalam pemakaiannya Netcut tidak mengharuskan penggunaanya untuk memiliki akses sebagai administrator. Bagi seorang user biasa, dengan memakai Netcut bisa bertindak layaknya seorang administrator jaringan. *Software* tersebut dapat melacak dan menampilkan daftar pengguna ketika terhubung dalam koneksi yang sama. *Software* ini bekerja dengan cara mengidentifikasi IP address yang digunakan. Netcut sebagai jaringan pengelola yang tidak lepas dari fungsi utama yang bisa dimanfaatkan dari netcut berikut ini:

1. Memantau perangkat yang terhubung dengan jaringan
Pada fungsi pertama dari aplikasi Netcut untuk memantau jaringan komputer. Dengan menggunakan aplikasi ini, pengguna dapat melihat perangkat-perangkat yang terhubung di dalam jaringan. Dengan berdasarkan informasi ini, pengguna bisa mengetahui ada tidak penyusup di jaringan.
2. Mengontrol pengguna *bandwidth* internet
Pengertian Netcut sebagai aplikasi pengelola jaringan juga bisa didapatkan dari kemampuannya untuk mengontrol penggunaan bandwidth internet dalam jaringan. Fitur ini dapat memanfaatkan jika mendapati perangkat yang menyedot bandwidth dalam jumlah besar dan kemudian membuat akses perangkat lain lambat.
3. Mengelola akses internet perangkat dalam jaringan
Menggunakan aplikasi Netcut tidak hanya berguna untuk membatasi pemakaian bandwidth. Pengguna juga bisa mengizinkan atau menolak koneksi internet dari sebuah perangkat. Jika, ingin dapat memakai Netcut untuk mematikan koneksi internet secara total.
4. Mengetahui MAC Address setiap perangkat dalam jaringan dengan aplikasi Netcut juga memungkinkan pengguna untuk mengetahui MAC address dari semua perangkat dalam jaringan. Bukan hanya itu, Netcut juga memberi pengguna akses untuk melakukan clone MAC address dari sebuah perangkat apa pun yang terhubung.

5. Melindungi komputer dari serangan ARP Spoof

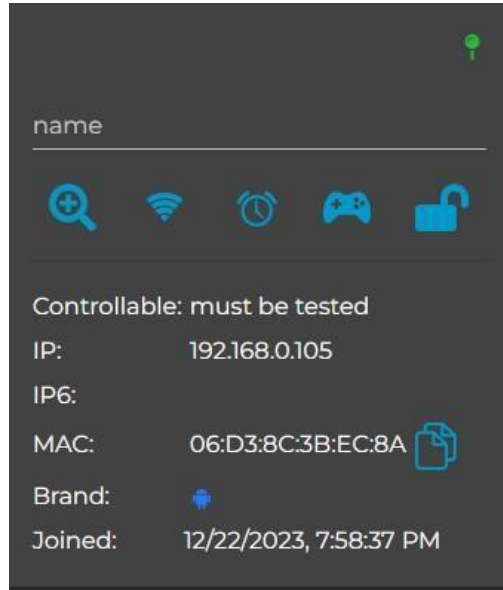
Netcut juga memiliki fungsi untuk melindungi komputer dari serangan cyber, khususnya serangan yang memakai teknik ARP spoof. Cara Netcut menangkal ARP spoof dilakukan dengan memperbaiki ARP mapping. Terdapat fitur Protect My PC pada Netcut yang memungkinkan pengguna memperoleh fungsi ini.

Pada Gambar 2 ditampilkan kinerja Netcut, perangkat lunak Netcut ini menggunakan protokol ARP untuk melacak dan menampilkan daftar pengguna yang terhubung ke koneksi yang sama dengan mengidentifikasi alamat IP yang digunakan perangkat lunak ini. perangkat lunak Netcut ini menggunakan protokol ARP untuk melacak dan menampilkan daftar pengguna yang terhubung ke koneksi yang sama dengan mengidentifikasi alamat IP yang digunakan perangkat lunak ini. Saat dijalankan, Netcut pertama-tama memindai alamat IP pengguna, kemudian mengubah komputer pengguna menjadi gateway, memantau semua perangkat yang terhubung dan memungkinkan pengguna untuk mengkonfigurasi pengaturan jaringan untuk area tersebut. pengguna dapat memutuskan sambungan perangkat dengan memilih alamat IP yang ditampilkan dan memilih Putus. Setelah itu akan muncul informasi "In Testing" sebagai pengguna bahwa software tersebut bekerja. pengguna harus tahu bahwa pengguna tidak boleh memotong dua alamat IP: alamat IP server dan alamat IP komputer pengguna.

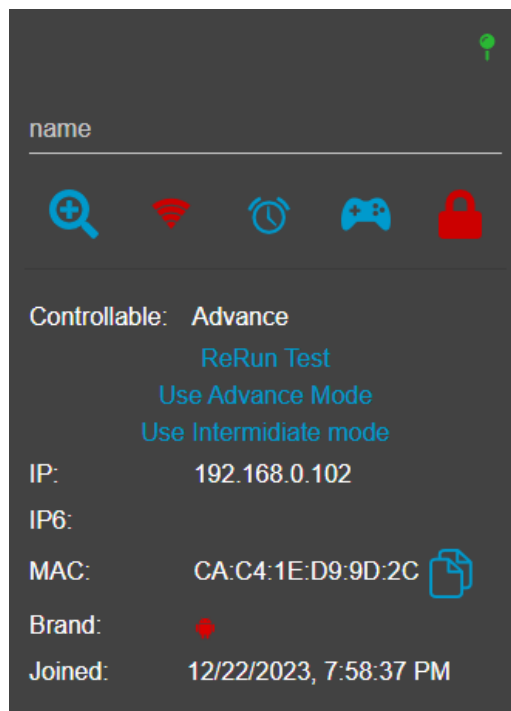


Gambar 2 IP Pengguna Serta IP Router

Berikutnya menampilkan perangkat yang terhubung dan memungkinkan pengguna untuk mengkonfigurasi pengaturan jaringan untuk area tersebut pengguna dapat memutuskan sambungan perangkat dengan memilih alamat IP yang ditampilkan dan memilih putus dapat dilihat pada Gambar 3 Dan Gambar 4.



Gambar 3 Perangkat Terhubung Ke Jaringan yang Sama



Gambar 4 Kondisi Perangkat Diputuskan Dari Jaringan yang Sama

Pengujian keamanan Wireless ini akan dilakukan dengan 3 tool untuk mencoba masuk ke dalam jaringan Wireless yang digunakan apakah keamanan jaringan ini kualitasnya bagus atau tidak dalam pengujian keamanan jaringan yang dipakai.

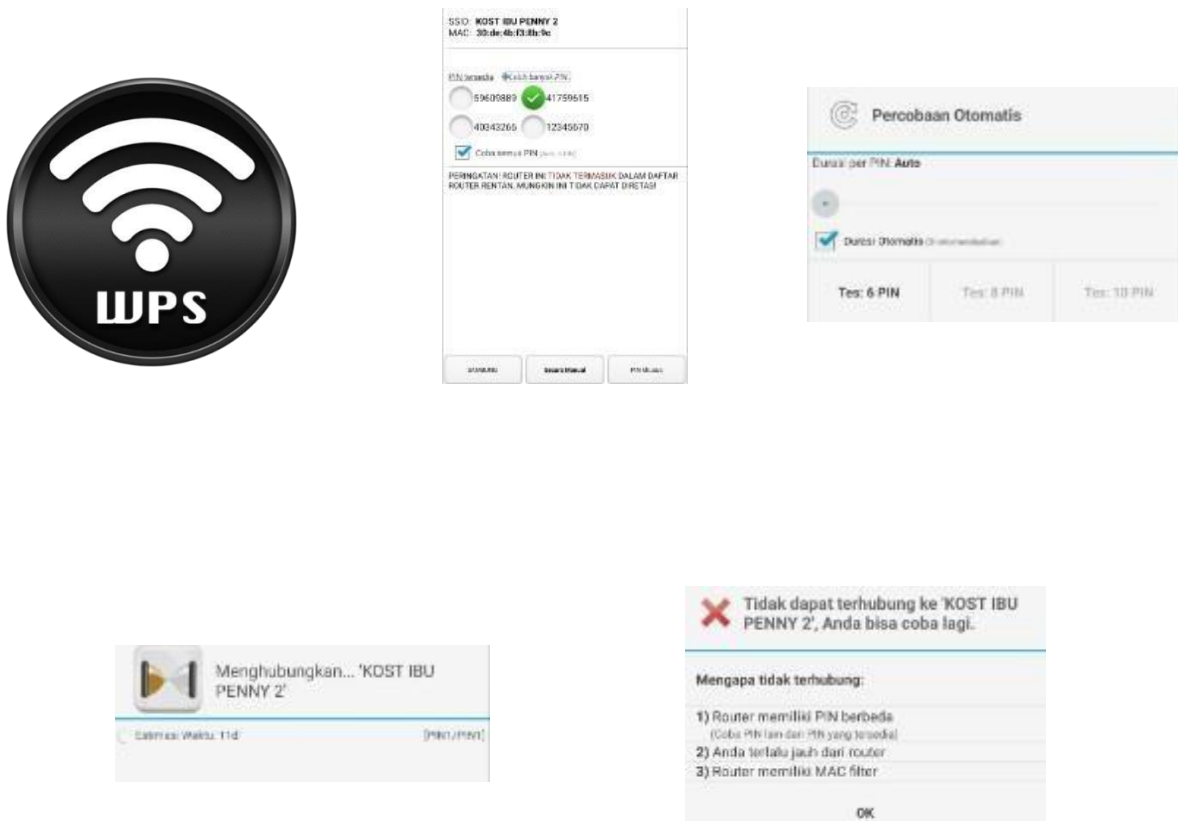
WPS WPA Tester

Dengan aplikasi ini, pengguna bisa coba mengkoneksikan perangkat ke Wireless menggunakan WPS PIN yang dihitung dengan menggunakan algoritma khusus. Tujuan utama dari aplikasi ini adalah mencari celah dari jaringan yang kita miliki, sehingga kita bisa melakukan antisipasi agar tidak dibobol oleh orang-orang yang tidak bertanggung jawab. Aplikasi ini juga mampu menembus password wireless yang tidak diketahui. Hanya saja, pengguna harus melakukan *rooting* terlebih dahulu proses tester (Gambar 5).



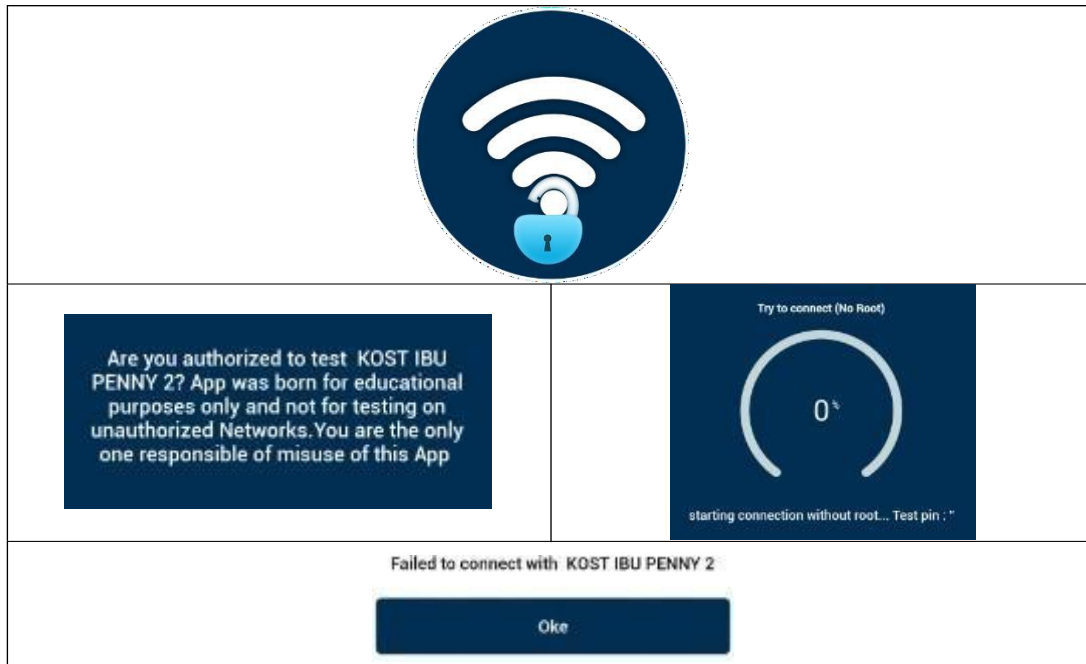
Gambar 5 Tool WPS WPA Tester

WiFi WPS Plus adalah aplikasi seluler berkualitas tinggi yang memungkinkan pengguna terhubung ke jaringan Wi-Fi di mana protokol WPS telah diaktifkan. Program ini dibuat terutama untuk menunjukkan kemampuan gadget modern berbasis sistem operasi android. Tugas utama diselesaikan dengan menggunakan perangkat lunak ini adalah untuk memeriksa router pengguna sendiri untuk ketidakberdayaan. Jika pengguna menduga ada kesalahan pada sistem titik koneksi jaringan nirkabel pengguna, program ini akan membantu pengguna menemukannya dapat dilihat pada Gambar 6.



Gambar 6 Tool Wifi Wps Plus

WPS Dumper adalah alat yang memungkinkan pengguna terhubung ke jaringan WiFi yang memiliki protokol WPS diaktifkan. WPS Dumper difokuskan untuk memverifikasi jika router pengguna rentan terhadap PIN default. Banyak router yang perusahaan instal kerentanannya sendiri dalam aspek ini. Dengan aplikasi ini pengguna dapat memeriksa apakah router, pengguna rentan atau tidak dan bertindak sesuai dapat dilihat pada Gambar 7.



Gambar 7 Tool Wps Dumper

KESIMPULAN

1. Netcut memudahkan pengguna untuk memantau aktivitas jaringan serta bisa menjadi administrator dalam mengatur jaringan untuk pengguna lain yang terhubung ke jaringan yang sama.
2. Diperlukan netcut berbayar untuk kinerja lebih stabil.
3. Berdasarkan hasil 30 kali pengujian dapat diketahui bahwa, menggunakan metode Mac Changer pengguna tidak berhak dapat mengetahui alamat MAC jaringan wireless dengan sistem keamanan WPA2 karena belum masuk pada jaringan wireless yang dituju, dan dengan menggunakan menggunakan metode signal scanning penyedia jaringan wireless dapat mendeteksi IP yang mencurigakan pada sistem keamanan WPA2.

DAFTAR PUSTAKA

- [1] B. Muslim dan I. Dayana, "sistem informasi peraturan daerah (perda) kota pagar alam berbasis web," jurnal ilmiah betrik , vol. 07, no.01, p. 4, 2016.
- [2] Y. Mulyanto, herfdani dan r. . C. Kirana, "analisis keamanan wireless local area network (wlan) terhadap serangan brute force dengan metode penetration testing (studi kasus:rs h.lmanambai abdukkadir)," jinteks, vol. 4, no. Issn 2686-3359, p. 1, 2022.
- [3] Wahyudi dan erfani, "analisis keamanan wpa2-psk dan radius server pada jaringan nirkabel menggunakan metode wireless penetration testing," penetration testing, vol. 6, p. 1, 2018.
- [4] M. Jufri dan h. , "peningkatan keamanan jaringan wireless dengan menerapkan security policy pada firewall," joisie, vol. 5, no. E-issn: 2527-3116, p. 1, 2021.

BIODATA PENULIS

Rindi Insan Cahyadi, lahir di Pagar Bunga pada tanggal 02-09-1998, dengan alamat tinggal Jalan Manyar Sewu Baturetno Banguntapan Bantul Yogyakarta, dapat dihubungi melalui email rendiinsan18@gmail.com atau telepon 085764458284. Saat ini tercatat sebagai mahasiswa Jenjang Sarjana Program Studi Informatika, Jurusan Informatika, Fakultas Teknologi Informasi dan Bisnis, IST AKPRIND Yogyakarta dengan bidang minat *computer security*.