JURNAL RESISTOR
Vol. 1 No 2 – Oktober 2108
p-ISSN 2598-7542 (Print), e-ISSN 2598-9650 (Online)
Available Online at :
http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

ANALISA DAN PROBLEM SOLVING KEAMANAN ROUTER MIKROTIK RB750RA DAN RB750GR3 DENGAN METODE PENETRATION TESTING (STUDI KASUS: WARNET AULIA.NET, TANJUNG HARAPAN LAMPUNG TIMUR)

Arif Hidayat[1], Ismail Puji Saputra[2]

[1]Prodi Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro
Kota Metro, Indonesia
[2]UPT. PUSTIK, Universitas Muhammadiyah Metro
Kota Metro, Indonesia

e-mail: androidarifhidayat@gmail.com[1], ismailpujisaputra@gmail.com[2]

Received : Oktober, 2018	Accepted : Oktober, 2018	Published : Oktober, 2018

Abstract

Information and communication technology is something that is difficult to separate from human life in the present era. One example of information and communication technology is a network of proxy routers. This study uses the penetration testing method, which aims to analyze the security system of the proxy router that has been applied to Warnet Aulia.net. In analyzing network security, the Mikrotik Router is done by the method of penetration testing where the form of attacks on the network is simulated. In this study Python and Winboxpoc.py were successfully run on the Windows 10 operating system. The results of this study indicate that the network security owned by the Aulia.net cafe network still has many gaps to exploit. As for the results of some attacks, it shows serious things in terms of exploitation, such as the output of getting a proxy router password and username. Therefore, this study also provides a solution on how to prevent the mikrotik router from being exploited. Problem solving is explained using several alternative solutions, so that practitioners or network technicians are expected to be able to utilize knowledge related to the results of this study in order to secure the router.

Keywords: *security mikrotik, winbox POC, mikrotik router, hacking, penetration testing.*

Abstrak

Teknologi informasi dan komunikasi merupakan hal yang sulit terpisahkan dari kehidupan manusia di era sekarang ini. Salah satu contoh teknologi informasi dan komunikasi tersebut adalah jaringan router mikrotik. Penelitian ini menggunakan metode penetration testing, yang bertujuan melakukan analisis terhadap sistem keamanan router mikrotik yang sudah di terapkan pada Warnet Aulia.net. Dalam menganalisa keamanan jaringan Router Mikrotik dilakukan dengan metode penetration testing dimana bentuk serangan terhadap jaringan disimulasikan. Pada penelitian ini phyton dan winboxpoc.py sukses dijalankan pada sistem operasi Windows 10. Hasil penelitian ini menunjukkan keamanan jaringan yang dimiliki oleh jaringan warnet Aulia.net masih memiliki banyak celah untuk dieksploitasi. Adapun hasil beberapa serangan menunjukkan hal yang serius dalam hal eksploitasi seperti luaran mendapatkan username dan password router mikrotik. Oleh karena itu penelitian ini juga memberikan solusi bagaimana agar router mikrotik terhindar dari jenis exploitasi tersebut. Problem solving dijelaskan menggunakan beberapa alternative solusi, sehingga para praktisi atau teknisi jaringan diharapkan dapat memanfaatkan knowledge terkait hasil penelitian ini agar dapat melakukan pengamanan router.

Kata Kunci: *keamanan mikrotik, winbox POC, mikrotik router, hacking, penetration testing.*

1. PENDAHULUAN

Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resources yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri. Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri.

Beberapa penelitian yang dilakukan mengenai analisa dan problem solving keamanan jaringan router mikrotik antara lain seperti penelitian yang dilakukan oleh (Arta.dkk, 2018) yang berjudul *"Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik"*. Hasil penelitian tersebut menyatakan bahwa 1) serangan atau penyusupan dapat dicegah dengan menerapkan Intusion Prevention System (IPS), 2) serangan terdeteksi tergantung pada pola serangan yang ada didalam ruleIPS, 3) serangan yang dilakukan dengan software brutus dalam bentuk bruteforce sudah bisa dicegah secara maksimal, 4) serangan yang dilakukan dengan Nmap pada command prompt windows 7 dalam bentuk port scanning masih belum bisa dicegah secara maksimal karena IPS masih membutuhkan beberapa kali serangan untuk bisa mendeteksi serangan dari IP yang sama, 5) log mikrotik bekerja dengan maksimal untuk mendeteksi serangan yang terjadi.

Penelitian lain yang kedua mengacu pada masalah yang diangkat oleh (Prayudi, 2018) yang berjudul *"Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksploitasi"*. Hasil dari penelitian ini yaitu mensimulasikan keamanan data dari serangan DoS (Denial of Service) didalam MetaRouter yang tereksploitasi, sehingga diharapkan akan mempermudah dalam monitoring data dan manajemen network. Selain itu dengan menggunakan Metarouter maka sebuah RouterOS dapat menjalankan beberapa RouterOS lainnya dalam bentuk virtual.

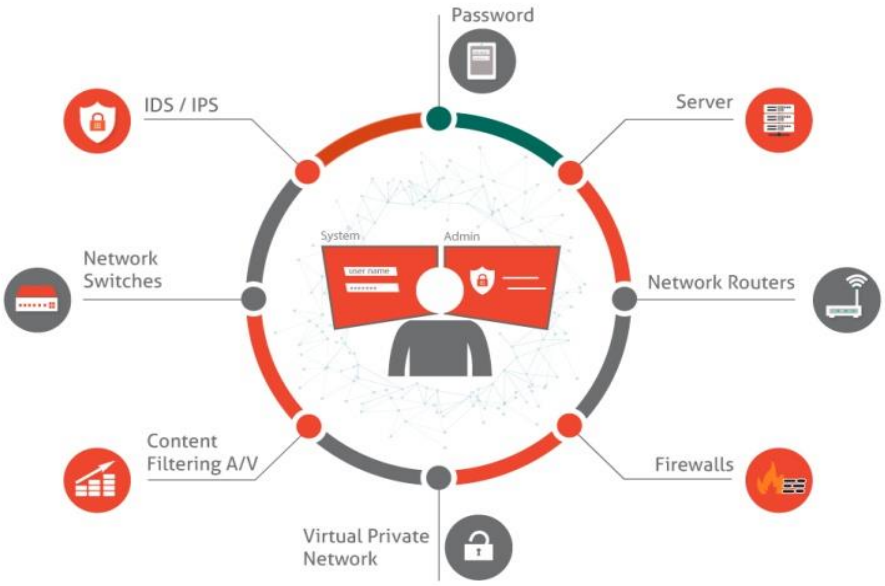
Penelitian lain yang ketiga mengacu pada masalah yang diangkat oleh (Amarudin, 2018) yang berjudul *"Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking".* Berdasarkan peneltian yang telah dilakukan bahwasanya simulator GNS3 dapat dengan mudah deterapkan dalam mendesain topologi jaringnan maupun dalam mensimulasikan pengujian keamanan jaringan khususnya pada metode keamanan Port Knocking. Selain itu hasil penelitian yang telah dilakukan dengan Metode Port Knocking dapat diterapkan untuk mengamankan Router dari akses orang lain yang tidak berhak mengaksesnya.

Penelitian lain yang keempat mengacu pada masalah yang diangkat oleh (Shaifullah, 2018) yang berjudul *"Desain Firewall Terhadap Serangan Ddos Pada Router Mikrotik"*. Hasil dari penelitian tersebut yaitu dengan adanya rancangan konfigurasi Firewall pada mikrotik Router OS maka sangat membantu dalam pertolongan pertama pada serangan Distributed Denial of Service attacks (DDOS), serta manfaat lainnya yaitu membuat jaringan internet lebih secure dan baik.

Berdasarkan hasil penelitian tentang mengenai analisa dan problem solving keamanan jaringan router mikrotik yang telah dipaparkan di atas, maka dilakukan penelitian lebih lanjut dengan judul *"Analisa dan Problem Solving Keamanan Router Mikrotik RB750ra dan RB750GR3 dengan Metode Penetration Testing"*. Studi kasus dalam penelitian ini yaitu pada Warnet Aulia.net Tanjung Harapan, Lampung Timur, Indonesia. *Output* yang di hasilkan berupa hasil analisa dan problem solving keamanan router mikrotik.

Penetration testing adalah subkategori dari etchical hacking yaitu sebuah metode dan prosedur yang bertujuan untuk menguji dan melindungi keamanan informasi. Penetration testing merupakan aktifitas mengevaluasi sistem keamanan yang sudah dibuat dengan cara melakukan simulasi serangan menggunakan metode yang biasa digunakan oleh peretas. Kegiatan ini perlu mendapat persetujuan legal

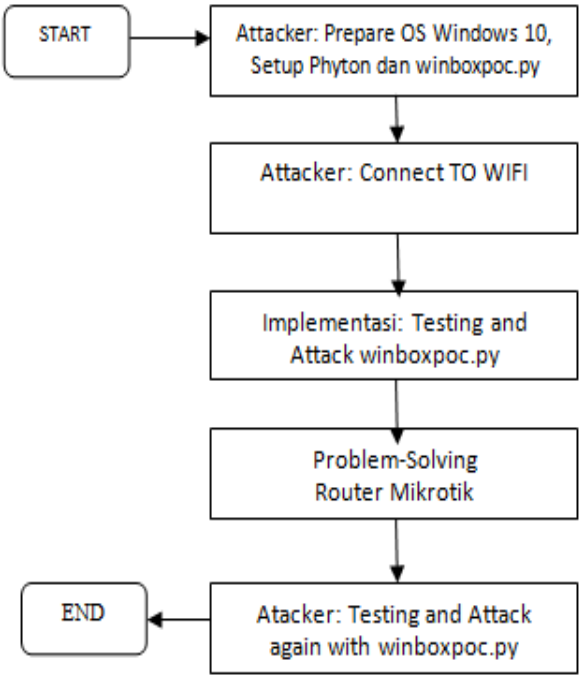
dari pemilik sistem tersebut. Gambar 1 berikut ini merupakan cakupan penetrasi testing pada lajur jaringan komputer yang didalamnya antara lain seperti; *Password, Server, Network Routers, Firewall, VPN, Content Filtering, Network Switch,* dan *IDS*. Kemudian perlu diketahui bahwasannya dalam penelitian ini penulis menyoroti tentang eksploitasi mendapatkan username dan password dalam jaringan router mikrotik.



Gambar 1. Penetration Testing dalam Jaringan

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah berfokus pada lajur *Penetration Testing*. Pada tahap ini peneliti membuat alur penelitian yag dapat dilihat pada Gambar 2.



Gambar 2. Alur Penelitian

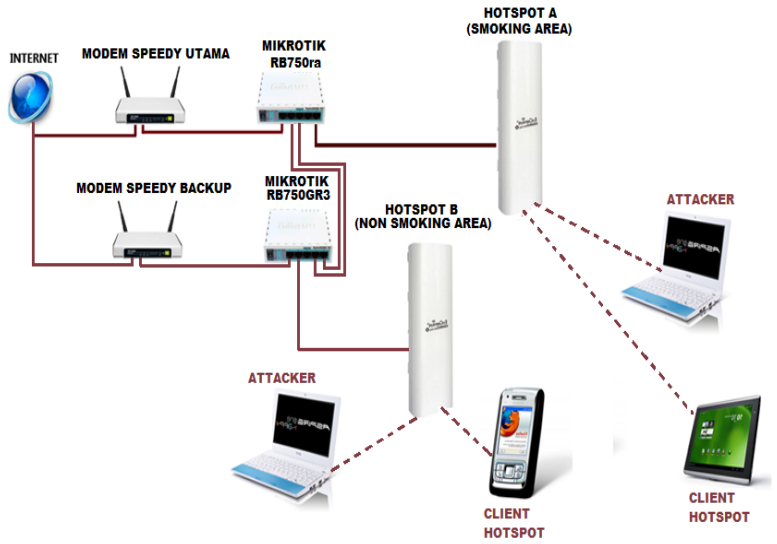
3. HASIL DAN PEMBAHASAN

Tahap Implementasi merupakan penerapan pengujian serangan ke sistem jaringan router. Selain itu juga pada tahapan ini akan dijelaskan bagaimana teknik attacking ini akan bekerja. Adapun Sistem operasi yang digunakan yaitu Windows 10. Sedangkan untuk software yang digunakan adalah *phyton* dan *winboxpoc*.

Pada penelitian ini, pengujian dilakukan menggunakan komputer attacker yang sudah dipersiapkan sebelumnya. Komputer attacker masuk/connect kedalam jaringan warnet Aulianet Tanjung Harapan Lampung Timur. Pengujian Attacking dilakukan di dua router yang berbeda versi OSnya, yaitu pada router RB750ra dan RB750GR3.

3.1 Design Topologi

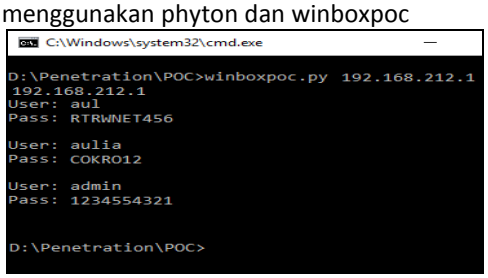
Arsitektur jaringan warnet Aulia.net Tanjung Harapan lampung Timur ini terdiri dari dua *Router Mikrotik* dan dua *Access Point*. *Router Mikrotik* bertindak sebagai server, dan *Access Point* bertindak sebagai hub atau alat penyampai hotspot ke client. Kemudian utuk design arsitektur atau topologi jaringan dalam implementasi *penetration testing* ini dapat dilihat pada pada Gambar 3.



Gambar 3. Topologi Jaringan Warnet Aulia.net

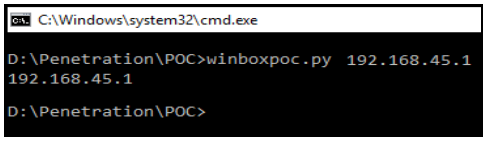
3.2 Implementasi Attacking

1) Attacking port 8291 pada **RB750ra** menggunakan phyton dan winboxpoc



Gambar 4. Hasil Sukses Eksploitasi *Router Mikrotik* ada *OS Versi 6.38.7*

2) Attacking port 8291 pada **RB750GR3** menggunakan phyton dan winboxpoc



Gambar 5. Hasil Gagal Eksploitasi *Router Mikrotik* pada *OS versi 6.42.3*

3) Kemudian pada Tabel 1. Berikut ini merupakan hasil uji *Penetration Testing* pada warnet Aulia.net

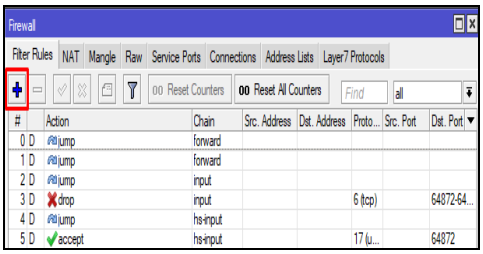
Tabel 1. Hasil *Penetration Testing*

Jenis Serangan	Informasi yang dibutuhkan	Status Serangan	Hasil Serangan
Attacking port 8291 pada **RB750ra** menggunakan *phyton* dan *winboxpoc*	Attacker harus berada dalam jaringan WLAN Aulia.net	Berhasil	**Sukses** menampilkan Username dan Password Router Mikrotik *DENGAN OS Versi* 6.38.7
Attacking port 8291 pada **RB750GR3** menggunakan *phyton* dan *winboxpoc*	Attacker harus berada dalam jaringan WLAN Aulia.net	Gagal	**Gagal** Menampilkan Username dan Password Router Mikrotik dengan *OS Versi 6.42.3*

3.3 Problem Solving

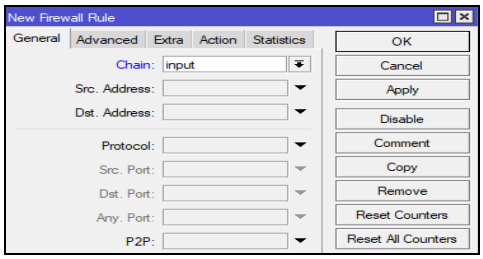
Untuk membentengi eksploitasi pencurian *password* pada router mikrotik RB750ra seperti menggunakan *winboxpoc.py*, maka penulis melakukan *reject* terhadap request *user.dat*, karena perlu di ketahui tujuan attacker mengexploitasi router tersebut hanya satu yaitu mengambil "user.dat". Adapun tahapan langkah untuk pengamanan sekaligus problem solving masalah diatas yaitu sebagai berikut:

1) Lakukan remote mikrotik via winbox kemudian Buka IP → Firewall



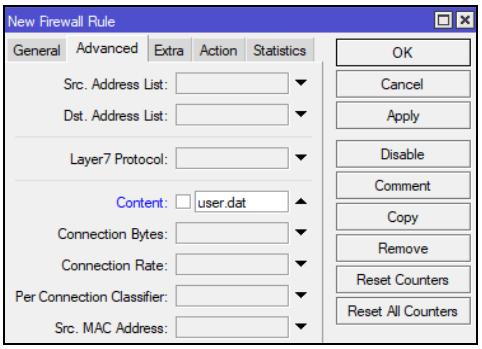
Gambar 6. Jendela *Filter Rules*

2) Kemudian pada jendela *New Firewall Rule* masuk ke tab *General* pada field *Chain* pilih *input*.



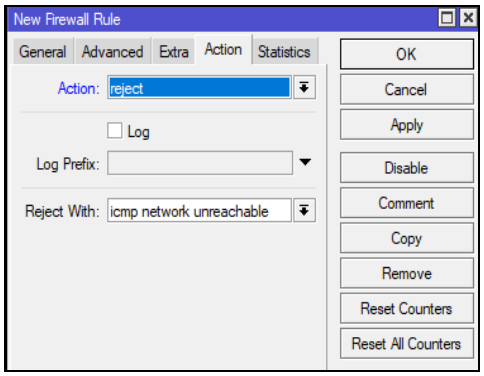
Gambar 7. Tampilan *New Firewall Rule*

Dilanjutkan masuk tab *Advanced* dan pada field *Content* isikan *user.dat*. di dalam file inilah username dan password disimpan, oleh karena itu pada tahapan ini merupakan proses bloking akses request *user.dat* oleh *attacker*.



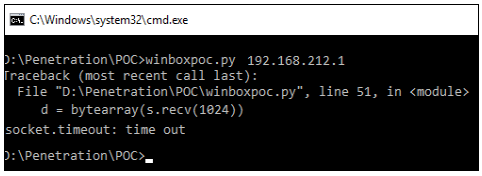
Gambar 8. Pemilihan Konten yang Ingin di *Reject*

3) Terakhir ditab Action dan pada field Action isikan reject untuk mengeblok akses ke user.dat serta pada *field Reject with* isikan *icmp network unreachable*.



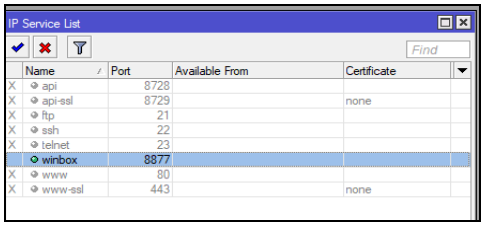
Gambar 9. Mengaktifkan Action *Reject*

4) Kemudian apabila sudah menutup request user.dat sesuai langkah diatas, maka lakukan uji coba kembali untuk melakukan POC terhadap IP Address 192.168.212.1. Dapat dipastikan tidak akan bisa memunculkan kembali username dan password pada router mikrotik dengan *OS Versi 6.38.7* tersebut, dikarenakan request sudah ditutup.



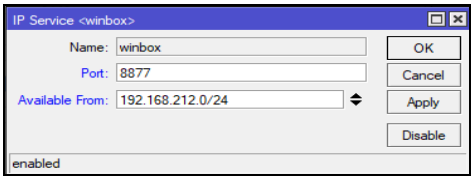
Gambar 10. Tampilan Attacker gagal mendapatkan username password dikarenakan Router mikrotik sudah dibentengi atau sudah ditutup *Request* user.dat

5) Gambar 10 diatas merupakan tampilan sukses mencegah serangan exploitasi dengan *Winboxpoc.py* pada router mikrotik yang OSnya dibawah 6.42.3.
6) Solusi yang kedua untuk mengatasi masalah winboxpoc yaitu merubah port winbox. Adapun langkahnya, Klik IP → Service kemudian rubahlah port 8291 menjadi 8877 (bebas/ sesuai keinginan).



Gambar 11. Merubah *Port Default Winbox*

7) Solusi gambar 11 diatas sangat mungkin hanya aman sementara, tidak menutup kemungkinan *attacker* melakukan scanning port di router mikrotik. Misalkan menggunakan aplikasi *Zenmap*, *Simple Post Tester*, dan *Port Scanner.*
8) Solusi berikutnya adalah dengan mengatur *permission*, dimana hanya mengizinkan IP Address tertentu yang dapat mengakses Router Mikrotik. Adapun langkahnya klik *IP* → *Service* kemudian pada field *Available From* isikan Network IP Address yang diizinkan untuk mengakses winbox.



Gambar 12. *Permission Router Access*

9) Dengan melalukan seting seperti Gambar 12 diatas, maka hanya Network dengan IP Address 192.168.212.0/24 yang dapat melakukan remot via winbox ke router mikrotik. Perlu diketahui seandainya attacker mengetahui *password* mikrotik dapat dipastikan attacker tetap tidak dapat masuk selama *attacker* tidak berada di jaringan local. Sebaiknya gunakanlah *subnet* yang sangat sempit misalkan /30 yang hanya menyisakan 2 IP Address yaitu IP Gateway dan IP Pengelola Router Mikrotik.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan diatas dapat di ambil kesimpulan, antara lain:

1. Dari penelitian dihasilkan sebuah Analisa dan Problem Solving Keamanan Router Mikrotik RB750ra dengan Metode *Penetration Testing* (Studi Kasus pada Warnet Aulia.net Tanjung Harapan Lampung Timur, Indonesia)
2. Hasil penelitian ini menunjukkan keamanan jaringan yang dimiliki oleh jaringan warnet Aulia.net masih memiliki banyak celah untuk dieksploitasi. Adapun hasil beberapa serangan menunjukkan hal yang serius dalam hal eksploitasi mikrotik seperti luaran mendapatkan *username* dan *password* router mikrotik. Hal ini sangat crusial dan berbahaya apabila juga terjadi pada jaringan instansi yang bersekala besar seperti perusahaan dan pendidikan,
3. Penelitian ini juga memberikan solusi bagaimana agar router mikrotik terhindar dari jenis exploitasi tersebut. Jawaban permasalahan diatas sudah dijelaskan dengan menggunakan alternative solusi, sehingga para praktisi atau teknisi jaringan diharapkan dapat memanfaatkan knowledge terkait hasil penelitian ini agar dapat melakukan proteksi atau mengamankan router dari pihak pihak luar yang tidak bertanggung jawab.

DAFTAR PUSTAKA

[1] Satwika, I. K. S., & Sukafona, I. M. (2018). Analisis Coverage Dan Quality Of Service Jaringan WiFi 2, 4 GHz Di STMIK STIKOM Indonesia. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *1*(1), 1-7.

[2] Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *IT JOURNAL RESEARCH AND DEVELOPMENT*, *3*(1), 94-104.

[3] Prayudi, Y., Si, S., & Kom, M. (2018). *SIMULASI UNTUK PENINGKATAN*

KEAMANAN DATA PADA METAROUTER YANG SUDAH TEREKSPLOITASI (Master's thesis, Universitas Islam Indonesia).

[4] Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 35-38.

[5] Shaifullah, S. M. (2018). *DESAIN FIREWALL TERHADAP SERANGAN DDOS PADA ROUTER MIKROTIK* (Doctoral dissertation, Universitas Mercu Buana Yogyakarta).

[6] Kustanto, D., & Daniel, S. (2008). Membangun Server Internet Dengan Mikrotik OS. *Yogyakarta: Gava Media Yogyakarta*.

[7] Hidayat, A. (2017). BUILDING A EXPERT SYSTEM APPLICATION FOR HELP PROBLEM SOLVING NETWORK ON MIKROTIK ROUTER. *MIKROTIK: Jurnal Manajemen Informatika*, *6*(1).

[8] Komputer, Wahana, (2009). Administrasi Jaringan dengan Ubuntu 9, Andi Offset, Yogyakarta.

[9] Lukas, Jonathan. (2006). Jaringan Komputer, Graha Ilmu, Jakarta.

[10] Hidayat, A. (2016). Panduan Belajar Mandiri Administrasi Server Jaringan Menggunakan Linux Ubuntu. *Laduni Alifatama*. Lampung (ISBN: 978-602-1397-56-5)

[11] Winarno dan Smitdev, (2014). Membuat Jaringan Komputer di Windows dan Linux, PT. Elex Media Komputindo, Jakarta.

[12] Hidayat, A. (2016). Implementasi Control Panel Hosting dengan VestaCP pada Server Intranet LAB Multimedia D-III Manajemen Informatika UM Metro. *MIKROTIK: Jurnal Manajemen Informatika*, *6*(2).

[13] Norton Peters. (1999). *Complete Guide to Networking. Sams*, India.

[14] Sinarmata, Janner, (2006). Teknologi Komputer dan Informasi, Andi Offset, Yogyakarta.

[15] Hidayat, A. (2018). SISTEM PROTEKSI FAIL OVER DENGAN RSTP PADA SERVER ROUTER INTERNET FIKOM UM METRO BERBASIS MIKROTIK. SEMNASTEKNOMEDIA ONLINE, 6(1), 1-1.

[16] Sugeng, Winarno, (2015). Jaringan Komputer dengan TCP/IP, Modula.

[17] Hidayat, A. (2017). Konfigurasi Server Cloud Storage pada Jaringan LAN pada LAB Diploma III Manajemen Informatika UM Metro. *MIKROTIK: Jurnal Manajemen Informatika*, *7*(1).

[18] Komputer, Wahana, (2013). Internet Aman & Sehat, Andi Offset, Yogyakarta.

[19] Hidayat, A., & Saputra, I. P. (2018). IMPLEMENTATION VOICE OVER INTERNET PROTOCOL (VOIP) AS A COMMUNICATION MEDIA BETWEEN UNIT AT UNIVERSITY MUHAMMADIYAH METRO. IJISCS (International Journal Of Information System and Computer Science), 2(2), 59-66.

[20] Sutanta, Edy, (2005). Komunikasi Data dan Jaringan, Graha Ilmu, Yogyakarta.