IMPLEMENTASI KEAMANAN JARINGAN BERBASIS *FIREWALL RAW* TERHADAP *BRUTE FORCE LOGIN CYBER ATTACK*

PROJEK AKHIR

OLEH:

ZUMARDI IRFAN

09040581721014

PROGRAM STUDI TEKNIK KOMPUTER

PROGRAM DIPLOMA KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

IMPLEMENTASI KEAMANAN JARINGAN BERBASIS *FIREWALL RAW* TERHADAP *BRUTE FORCE LOGIN CYBER ATTACK*

PROJEK AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Ahli Madya Komputer

OLEH:

ZUMARDI IRFAN

09040581721014

PROGRAM STUDI TEKNIK KOMPUTER

PROGRAM DIPLOMA KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

IMPLEMENTASI KEAMANAN JARINGAN BERBASIS *FIREWALL RAW* TERHADAP *BRUTE FORCE LOGIN CYBER ATTACK*

PROJEK AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Ahli Madya Komputer

Oleh:

ZUMARDI IRFAN
09040581721014

Palembang, Agustus 2020
Mengetahui,

Pembimbing	Koordinator Program Studi Teknik Komputer
Ahmad Heryanto, M.T.	**Huda Ubaya, M.T.**
NIP. 198701222015041002	**NIP. 198106162012121003**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 07 Agustus 2020

Tim Penguji :

1. Ketua : Rahmat Fadli Isnanto, S.Si., M.Sc

2. Pembimbing I : Ahmad Heryanto, M.T.

3. Penguji I : Tri Wanda Septian, S.Kom., M.Sc

4. Penguji II : Adi Hermansyah, M.T.

Mengetahui,
Koordinator Program Studi Teknik Komputer

Huda Ubaya, S.T., M.T.
NIP. 198106162012121003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Zumardi Irfan

NIM : 09040581721014

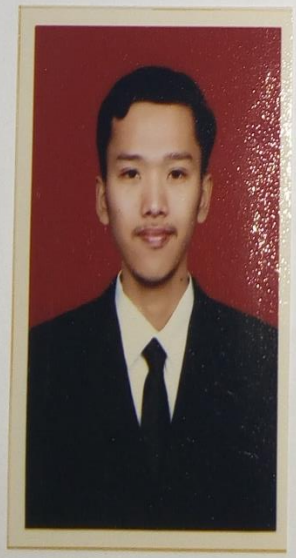
Program Studi : Teknik Komputer

Peminatan : Teknik Komputer Jaringan

Judul : Implementasi Keamanan Jaringan Berbasis *Firewall RAW* Terhadap *Brute Force Login Cyber Attack*

Menyatakan bahwa laporan projek akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan



Palembang, Agustus 2020

Zumardi Irfan

NIM. 09040581721014

HALAMAN PERSEMBAHAN

"Masa depan adalah milik mereka yang menyiapkan hari ini."

"A little progress each day in your self is ads thing up to big result."

يَا أَيُّهَا الَّذِينَ آمَنُوا اسْتَعِينُوا بِالصَّبْرِ وَالصَّلَاةِ إِنَّ اللَّهَ مَعَ الصَّابِرِينَ

Artinya : "Hai orang-orang yang beriman, jadikanlah sabar dan shalat sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar."
(QS. Al-Baqarah [2]: 153).

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk . . .

Kedua orang tua tercinta
(Bapak Syahbirin dan Ibu Martini)
Kedua adikku tercinta
(Desta Fitriani dan Arif Afriawan)
Teman-teman seperjuangan prodi,
(Teknik Komputer Jaringan 2017)
Teman-teman organisasi,
(DPM KM Fasilkom Unsri)
Almamater perjuangan
(Universitas Sriwijaya)

Agustus 2020

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat, hidayah serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan projek akhir dengan judul "**Implementasi Keamanan Jaringan Berbasis *Firewall RAW* Terhadap *Brute Force Login Cyber Attack***". Penulisan projek ahir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar Ahli Madya Komputer.

Pada kesempatan ini, penulis menyampaikan ucapan terima kasih kepada semua pihak untuk setiap bimbingan, semangat dan doa yang diberikan kepada penulis sehingga terselesaikannya projek akhir ini. Ucapan terima kasih, penulis sampaikan kepada:

1. Allah SWT, yang telah memberikan segalanya kepada penulis berupa kesehatan, orang tua, pembimbing, teman, dll sehingga dapat menyelesaikan laporan projek akhir ini.
2. Orang-orang tercinta, Ayah, Ibu, Adik-adik, serta ponakan-ponakan tersayang, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis demi lancarnya penulisan projek akhir ini.
3. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing projek akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan projek akhir.
4. Bapak Tri Wanda Septian, S.Kom., M.Sc dan Adi Hermansyah, M.T. selaku dosen penguji sidang projek akhir yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.
5. Bapak Rendyansyah S.Kom., M.T. selaku Pembimbing Akademik, yang telah membimbing penulis dari semester satu hingga terselesainnya projek ahir ini dengan baik.

6. Bapak Huda Ubaya, S.T., M.T. selaku Koordinator Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Seluruh Dosen Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Univeristas Sriwijaya.
8. Staff di Program Studi Teknik Komputer, khususnya Mbak Faula yang telah membantu penyelesaian proses administrasi.
9. Staff di Fakultas Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
10. Seluruh petinggi atau pimpinan yang ada dilingkungan Fakultas Ilmu Komputer, Universitas Sriwijaya, yang telah membantu proses administrasi selama masa kampus.
11. Teman-teman Laboratorium Jarkom yang telah banyak membagi ceritanya Kak Ahmad Ilham Arismawan, Kak Rahman Ramadhan, dan Kak Yoggie Al Hanif, Serta semua penghuni Laboratorium Jarkom.
12. Teruntuk teman-teman satu angkatan, khususnya Teknik Komputer Jaringan 2017, Alvin Mulya Pradana, Yoga Faturahman, Kiki Arifudin, Tiara Nur Azmi, Stevanus William, M. Taufik Hidayat, Wahyu Hairullah dan Tantri Langgeng Widodo. Semoga sukses untuk kita semua.
13. Serta Organisasi di Fakultas Ilmu Komputer Universitas Sriwijaya, DPM KM (Dewan Perwakilan Mahasiswa). Terima kasih atas kesempatannya dalam menjadi keluarga besar, atas ilmu yang telah diberikan serta wadah berbagi yang hangat.
14. Serta semua pihak yang telah membatu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian projek akhir ini. Terima kasih semuanya.

Semoga dengan terselesainya projek ahir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari Implementasi Keamanan Jaringan Berbasis *Firewall RAW* Terhadap *Brute Force Login Cyber Attack*.

Dalam penulisan laporan ini, penulis menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk perbaikan laporan projek akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, Agustus 2020

Penulis

Implementation of Network Security Based on Raw Firewall Against Brute Force Login Cyber Attack

Zumardi Irfan (09040581721014)
Department of Computer Systems, Computer Engineering Study Program,
Faculty of Computer Science, Sriwijaya University
Email: zumardiirfan@gmail.com

Abstract

The focus of this research is to protect the network from brute force login cyber attacks, by implementing a raw firewall on one of the network devices, namely mikrotik. The network built in this study has four LANs where the first LAN, second LAN and third LAN are attackers while the fourth LAN is administrator or attacked using WiFi communication and UTP cable. Brute force attack is a type of attack carried out to gain access as a user with an authentication attempt. This attack is carried out by trying all the passwords until the correct one is found. In this study two test scenarios were conducted: (i) the first test carried out a brute force attack before the implementation of the raw firewall, and (ii) the second test carried out a brute force attack again after the implementation of the raw firewall. Raw firewall rules are applied as many as seven rules. The results obtained from the study in the form of logs and address lists that are applied successfully get the source of the attack and limit the attack, Filtered port services applied successfully protect the remote access login port, the use of cpu resources before the raw firewall implementation on average is 28.24% and the cpu resource after implementation raw firewall on average by 2.28% when an attack occurs, the implementation of raw firewall against cyber attack brute force login successfully protects the network.

Keywords: Network security, raw firewall, brute force, cyber attack

Implementasi Keamanan Jaringan Berbasis *Firewall Raw* Terhadap *Brute Force Login Cyber Attack*

Zumardi Irfan (09040581721014)
Jurusan Sistem Komputer, Program Studi Teknik Komputer,
Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: zumardiirfan@gmail.com

Abstrak

Fokus penelitian ini adalah melindungi jaringan dari *brute force login cyber attack*, dengan implementasi *firewall raw* pada salah satu perangkat jaringan yaitu mikrotik. Jaringan yang dibangun pada penelitian ini memiliki empat *LAN* dimana *LAN* pertama, *LAN* kedua dan *LAN* ketiga sebagai *attacker* sedangkan *LAN* keempat sebagai *administrator* atau *attacked* dengan menggunakan komunikasi WiFi dan kabel *UTP*. Serangan *brute force* adalah jenis serangan yang dilakukan untuk mendapatkan akses sebagai pengguna dengan upaya autentikasi. Serangan ini dilakukan dengan mencoba semua kata sandi sampai yang benar ditemukan. Pada penelitian ini dilakukan dua skenario pengujian : (i) pengujian pertama melakukan serangan *brute force* sebelum implementasi *firewall raw*, dan (ii) pengujian kedua melakukan serangan *brute force* kembali setelah implementasi *firewall raw*. *Rule firewall raw* yang diterapkan sebanyak tujuh *rule*. Hasil yang diperoleh dari penelitian berupa *log* dan *address list* yang diterapkan berhasil mendapatkan sumber serangan dan membatasi serangan, *Filtered port services* yang diterapkan berhasil melindungi *port remote access login*, penggunaan *resource cpu* sebelum implementasi *firewall raw* rata-rata sebesar 28.24% dan *resource cpu* setelah implementasi *firewall raw* rata-rata sebesar 2.28% saat terjadi serangan, implementasi *firewall raw* terhadap *brute force login cyber attack* berhasil melindungi jaringan.

Kata Kunci: Keamanan jaringan, *firewall raw*, *brute force*, *cyber attack*

DAFTAR ISI

Halaman

BAB III METODOLOGI PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

NOMENKLATUR

GUI	=	*Graphical User Interface*
SSH	=	*Secure Shell*
Telnet	=	*Telecommunications Network Protocol*
FTP	=	*File Transfer Protocol*
Nmap	=	*Network Mapper*
HTTP	=	*Hypertext Transfer Protocol*
IMAP	=	*Internet Message Access Protocol*
POP3	=	*Post Office Protocol 3*
OSI	=	*Open System Interconnection*
IPSec	=	*IP Security*
SSL	=	*Secure Sockets Layer*
VPN	=	*Virtual Private Network*
TCP	=	*Transmission Control Protocol*
UDP	=	*User Data Protocol*
Log	=	*Logging*
OS	=	*Operating System*
IP Address	=	*Internet Protocol Address*
MPLS	=	*Multiprotocol Label Switching*
NAT	=	*Network Address Translation*
TTL	=	*Time To Live*
SrcNAT	=	*Source Network Address Translation*
DstNAT	=	*Destination Network Address Translation*
DHCP	=	*Dynamic Host Configuration Protocol*
PPPOE	=	*Point-to-Point Protocol Over Ethernet*
RAM	=	*Random Acces Memory*
PCI	=	*Peripheral Component Interconnect*
IRQ	=	*Interrupt ReQuest*
USB	=	*Universal Serial Bus*

AP	=	*Access Point*
GHz	=	*Gigahertz*
Mbps	=	*Megabits per second*
CPU	=	*Central Processing Unit*
LAN	=	*Local Area Network*
WLAN	=	*Wireless Local Area Network*
UTP	=	*Unshielded Twisted Pair*
OSPF	=	*Open Shortest Path First*
Ether	=	*Ethernet*
SSID	=	*Service Set Identifier*
Millennia	=	Jangka waktu seribu tahun
Lower Case	=	Huruf kecil
Upper Case	=	Huruf Besar
HTTPS	=	*Hypertext Transfer Protocol Secure*
ICMP	=	*Internet Control Message Protocol*
MAC Address	=	*Media Access Control Address*
SYN	=	*Synchronous*

DAFTAR LAMPIRAN

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan adalah suatu cara untuk menghindari berbagai ancaman serangan *cyber*. Ancaman dapat berasal dari internal maupun eksternal [4]. Proteksi harus diterapkan agar terhindar dari serangan tersebut. Salah satunya yaitu memanfaatkan fitur *firewall* untuk mengontrol *traffic data* yang masuk, melewati, atau keluar dari *router* [2]. *Administrator* juga bisa memanfaatkan sistem keamanan jaringan yang lain seperti *IDS (Intrusion Detection System), Intrusion Prevention System (IPS), Proxy Server*, *Layer 7 Protocol* dan sistem keamanan lainnya.

Serangan *cyber* dilakukan oleh individu atau kelompok untuk mendapatkan informasi dan data yang penting. Ini terjadi karena semakin terbukanya dalam pengetahuan *hacking* dan *cracking*, *attacker* juga didukung dengan banyaknya *tools* yang bersifat *free*, hal ini mempermudah melakukan aksi serangan [25],[1]. Terutama melalui *router* yang terhubung langsung ke jaringan publik [8]. Salah satu serangan yang ditujukan kepada *router* adalah serangan *brute force.*

Bisnis di kawasan Eropa, Timur Tengah dan Afrika (EMEA) tahun 2018 paling sering menjadi sasaran serangan *brute force* dengan persentase sebesar 43,5 persen. *Attacker* sebagian besar menargetkan organisasi di sektor layanan publik, layanan keuangan, kesehatan, pendidikan dan layanan *provider* (Sead Fadilpašić, 2019).

Pada pertengahan Oktober hingga November 2015 telah terjadi serangan *brute force* secara besar-besaran terhadap sebuah situs *e-commerce* dari Alibaba yaitu TaoBao, serangan berhasil mendapatkan hampir 21 juta akun pengguna pada situs tersebut (Tara Seals, 2016).

Serangan *brute force* adalah jenis serangan yang dilakukan untuk mendapatkan akses sebagai pengguna dengan upaya autentikasi. Serangan ini dilakukan dengan mencoba semua kata sandi sampai yang benar ditemukan. Serangan jenis ini akan cepat berhasil apabila pilihan kata sandi lemah, sederhana,

mudah diingat, serta tidak mengubah kata sandi *default* dari sistem [19]. Serangan *brute force* sering terjadi pada akun media sosial, email, perangkat jaringan, perangkat *server* ataupun *cloud server*.

Salah satu cara untuk mengatasi hal tersebut adalah dengan menerapkan *firewall* pada salah satu perangkat jaringan. Berdasarkan *packet flow chains*, *firewall* ini melakukan proses yang lebih pendek dari pada *firewall* jenis lain. Sehingga tidak menggunakan *resource cpu* terlalu banyak karena tidak melakukan *connection tracking* [12]. *Firewall* yang dimaksud yaitu *firewall raw*.

Pada penelitian [1],[5] memanfaatkan *firewall filter rules* dan *address list* untuk mengatasi serangan *brute force* pada perangkat *router*. Pada penelitian ini *router* berhasil terlindungi dari serangan tersebut.

Berdasarkan latar belakang diatas maka penulis mengambil judul "**Implementasi Keamanan Jaringan Berbasis *Firewall RAW* Terhadap *Brute Force Login Cyber Attack***".

1.2 Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian projek akhir ini adalah sebagai berikut :

1. Melindungi jaringan dari *brute force login cyber attack.*
2. Melakukan *filtered port services.*
3. Menerapkan *log* dan *address list*.

1.3 Manfaat

Adapun manfaat yang diharapkan dari hasil penyusunan projek akhir ini adalah sebagai berikut:

1. Memberikan keamanan terhadap *brute force login cyber attack.*
2. Melindungi *port remote access login*.
3. Mengetahui sumber serangan dan membatasi serangan.
4. Menghemat penggunaan *resource cpu* pada *router*.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka didapatkan perumusan masalah pada penelitian ini yaitu :

1. Bagaimana simulasi serangan *brute force login cyber attack* pada *router*.
2. Bagaimana implementasi *firewall raw* untuk mengatasi serangan *brute force login cyber attack* pada *router*.

1.5 Batasan Masalah

Dari rumusan masalah dan latar belakang penelitian, berikut batasan masalah pada projek akhir ini adalah sebagai berikut :

1. Proses konfigurasi *firewall raw*.
2. Perangkat dan protokol komunikasi jaringan yang digunakan pada topologi yaitu *router*, *access point*, switch, komputer, laptop, kabel *UTP* jenis *straight* dan *crossover* serta *wifi*.
3. Simulasi serangan dilakukan pada telnet sedangkan untuk *remote access login* pada *SSH* dan *winbox*.
4. *Tools* serangan menggunakan *software* nmap, brutus dan putty.
5. Keluaran yang dihasilkan yaitu menghentikan serangan *brute force login* dan mengetahui sumber serangan.
6. Pengujian sistem dilakukan secara *real time* dan *online*.

1.6 Metodologi Penelitian

Agar tujuan penelitian ini dapat tercapai, Metodologi yang di gunakan melalui beberapa tahapan, diantaranya adalah sebagai berikut :

1. Tahap Pertama (Studi Pustaka)

Tahap ini dilakukan dengan cara mengkaji dan mempelajari literatur dan referensi berupa naskah ilmiah seperti jurnal, *paper*, artikel dan internet yang berhubungan langsung dengan projek akhir ini.

2. Tahap Kedua (Perancangan Sistem)

Tahap ini merupakan tahap dimana menentukan topologi jaringan yang sesuai, menentukan perangkat keras maupun perangkat lunak yang *suitable*, media protokol komunikasi jaringan, metode serangan serta metode keamanan jaringan yang digunakan untuk merancang dan di implementasikan.

3. Tahap Ketiga (Pengujian)

Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan. Dengan melakukan pengujian berdasarkan metodologi penelitian sehingga didapatkan data hasil pengujian yang sesuai dengan batasan masalah dan parameter pengujian yang telah ditentukan untuk medapatkan hasil yang optimal.

4. Tahap Keempat (Pembahasan)

Pada tahap ini akan dilakukan pembahasan dari hasil yang didapatkan pengujian pada tahapan sebelumnya kemudian dianalisa untuk mengetahui kekurangan pada hasil perancangan serta faktor penyebabnya sehingga didapatkan data objektif dari analisis hasil pengujian dan dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Tahap Kelima (Kesimpulan dan Saran)

Tahap terakhir adalah membuat kesimpulaan dari permasalahan, studi pustaka, metodologi, dan pembahasan hasil pengujian. Kemudian beberapa saran yang dapat dijadikan landasan untuk penelitian lanjutan.

1.7 Sistematika Penulisan

Untuk memudahkan dalam proses penyusunan projek akhir dan memperjelas konten dari setiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini merupakan penjelasan mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan teori yang berkaitan dengan permasalahan yang pernah digunakan dalam penelitian ini berdasarakan sumber penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan sistematis, mengenai bagaimana penelitian dilakukan. Penjelasan pada bab ini tentang tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelasakan tentang hasil pengujian yang dilakukan serta pembahasan dari data yang didapat dari hasil pengujian. Pembahasan data akan dilakukan berdasarkan parameter yang telah ditentukan sebelumnya.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang hasil pengujian yang telah dilakukan, apakah hasilnya sesuai yang diharapakan pada BAB I, serta berisi saran-saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 104–114, Aug. 2018.

[2] L. O. H. S. S. Ayu Abrianingsih, LM.Fid Aksara, "Rancang Bangun Aplikasi Untuk Mempermudah Konfigurasi Port Knocking Dalam Mikrotik," *semanTIK*, vol. 3, no. 1, pp. 107–114, 2017.

[3] S. Dandamudi and T. Eltaeib, "Firewalls Implementation in Computer Networks and Their Role in Network Security," *J. Multidiscip. Eng. Sci. Technol.*, vol. 2, no. 3, pp. 3159–3199, 2015.

[4] T. M. Diansyah, "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark," *J. TIMES*, vol. IV, no. 2, pp. 20–23, 2015.

[5] S. Dwiyatno, G. W. Putra, and E. Krisnaningsih, "Penerapan Ospf Routing, De-Militarized Zone, Dan Firewall Pada Mikrotik Routerboardtm Dinas Komunikasi Dan Informatika Depok," *J. Sist. Inf.*, vol. 2, pp. 59–67, 2015.

[6] W. A. H. M. Ghanem and B. Belaton, "Improving accuracy of applications fingerprinting on local networks using NMAP-AMAP-ETTERCAP as a hybrid framework," *Proc. - 2013 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2013*, pp. 403–407, 2013.

[7] K. Golnabi, R. K. Min, L. Khan, and E. Al-Shaer, "Analysis of firewall policy rules using data mining techniques," *IEEE Symp. Rec. Netw. Oper. Manag. Symp.*, pp. 305–315, 2006.

[8] A. Harbani and M. Apriani, "Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode Port Knocking," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 8, no. 2, pp. 25–36, 2019.

[9] J. Wack, K. Cutler, and J. Pole, "Guidelines on Firewalls and Firewall Policy," Nist Spec. Publ., vol. 800, no. 41, pp. 1–74, 2002.

[10] mikrotik.co.id, "Penggunaan Custom Chain pada Firewall MikroTik," *www.mikrotik.co.id*.[Online].Available:http://www.mikrotik.co.id/artikel_li

hat.php?id=146#:~:text=Pada RouterOS MikroTik terdapat sebuah,yang melewati router (Mangle). [Accessed: 06-Mar-2020].

[11] mikrotik.co.id, "Fitur Logging Pada Mikrotik," *www.mikrotik.co.id*. [Online]. Available: http://www.mikrotik.co.id/artikel_lihat.php?id=50. [Accessed: 06-Mar-2020].

[12] mikrotik.com, "Manual:IP/Firewall/Raw," *www.mikrotik.com*, 2019. [Online].Available:https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Raw. [Accessed: 02-Mar-2020].

[13] mikrotik.com, "Manual:Packet Flow," *www.mikrotik.com*, 2019. [Online]. Available:https://wiki.mikrotik.com/wiki/Manual:Packet_Flow. [Accessed: 05-Mar-2020].

[14] mikrotik.com, "Manual:IP/Firewall/Filter," *www.mikrotik.com*, 2020. [Online].Available:https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter. [Accessed: 05-Mar-2020].

[15] mikrotik.com, "Manual:IP/Firewall/NAT," *www.mikrotik.com*, 2020. [Online].Available:https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT. [Accessed: 05-Mar-2020].

[16] mikrotik.com, "Manual:IP/Firewall/Mangle," *www.mikrotik.com*, 2020. [Online].Available:https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Mangle. [Accessed: 06-Mar-2020].

[17] mikrotik.com, "Manual:IP/Firewall/Address list," *www.mikrotik.com*, 2019.[Online].Available:https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Address_list. [Accessed: 06-Mar-2020].

[18] mikrotik.com, "Manual:System/Resource," *www.mikrotik.com*, 2019. [Online].Available:https://wiki.mikrotik.com/wiki/Manual:System/Resource. [Accessed: 06-Mar-2020].

[19] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, "Detection of SSH brute force attacks using aggregated netflow data," *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 283–288, 2016.

[20] F. E. Nugroho and T. Brotoharsono, "Analisis Perbandingan Performansi Deep Packet Inspection Firewall Antara L7-Filter dan nDPI Prodi S1

Teknik Informatika , Fakultas Informatika , Universitas Telkom," vol. 08, no. 1, pp. 1–9, 2014.

[21] C. A. Pamungkas, "Manajemen bandwith menggunakan mikrotik routerboard di politeknik indonusa surakarta," *Inf. Politek. Indonusa Surakarta*, vol. 1, pp. 3–8, 2016.

[22] K. E. Pramudita, "Brute Force Attack dan Penerapannya pada Password Cracking," *Makal. IF3051 Strateg. Algoritm. – Sem. I Tahun 2010/2011*, vol. I, no. 2011, 2011.

[23] B. Sakti, A. Aziz, and A. Doewes, "Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing," *J. Teknol. Inf. ITSmart*, vol. 2, no. 1, p. 44, 2016.

[24] R. Sharma and P. Chandresh, "Firewalls : A Study and Its Classification," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 1979–1983, 2017.

[25] - Syaifuddin, D. Risqiwati, and E. A. Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," *Techno.Com*, vol. 17, no. 4, pp. 347–354, 2018.

[26] F. Thernelius, "SIP, NAT, and Firewalls," *Development*, no. May, pp. 1–69, 2000.

[27] S. Thomason, "Improving Network Security : Next Generation Devices," *Glob. J. Comput. Sci. Technol.*, vol. 12, no. 13, pp. 47–50, 2012.

[28] W. Wilman, I. Fitri, and N. D. Nathasia, "Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 3, no. 1, pp. 27–33, 2018.

[29] Valens Riyadi, "Router Optimation with Firewall/Raw," *www.mum.mikrotik.com*, 2017. [Online]. Available: https://mum.mikrotik.com/presentations/ID17/presentation_4778_1509410534.pdf. [Accessed: 06-Mar-2020].