

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
DARI SERANGAN EXPLOIT MENGGUNAKAN FIREWALL
FILTERING SERTA PENERAPAN MONITORING
MENGGUNAKAN CACTI**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program studi Informatika



disusun oleh

Rachmat

19.11.2638

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI
SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING
SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program studi Informatika



Disusun oleh

Rachmat

19.11.2638

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI
SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING
SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI**

yang disusun dan diajukan oleh

**Rachmat
19.11.2638**

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Februari 2023

Dosen Pembimbing,

Sudarmawan S.T, M.T

NIK. 190302035

HALAMAN PENGESAHAN
SKRIPSI

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI
SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING
SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI**

yang disusun dan diajukan oleh

Rachmat

19.11.2638

Telah dipertahankan di depan Dewan Penguji
pada tanggal 28 Februari 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Irma Rofni Wulandari, S.Pd., M.Eng
NIK. 190302329

Ahlihi Masruro, M.Kom
NIK. 190302148

Sudarmawan, S.T., M.T
NIK. 190302035

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Februari 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rachmat
NIM : 19.11.2638

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN DARI
SERANGAN EXPLOIT MENGGUNAKAN FIREWALL FILTERING
SERTA PENERAPAN MONITORING MENGGUNAKAN CACTI**

Dosen Pembimbing : Sudarmawan S.T, M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 28 Februari 2023

Yang Menyatakan,



Rachmat

PERSEMBAHAN

Alhamdulillah hirobbil ‘alamin, segala puji kepada Allah SWT berkat rahmat serta anugrah, dan karunianya sehingga skripsi ini dapat diselesaikan dengan lancar dan baik. Oleh karenanya penulis mengucapkan terimakasih kepada :

1. Ucapan rasa syukur dan terimakasih kepada Allah SWT, atas petunjuk dan diberikan kelancaran dalam proses penelitian.
2. Untuk kedua orang tua, yang telah mendoakan dan memberikan support dari materi hingga mampu menyelesaikan skripsi ini
3. Dosen Pembimbing, yang selalu memberikan arahan dan memberikan waktunya agar skripsi ini cepat terselesaikan.
4. Rasa terimakasih kepada teman-teman atas saran dan arahnya selama dalam proses pengerjaannya.

KATA PENGANTAR

Assalmu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur peneliti panjatkan kehadiran Allah SWT karena atas rahmat dan karunia-Nya, sehingga peneliti masih diberikan kesehatan dan kemudahan hingga penyusunan naskah skripsi ini dapat berjalan dengan baik dan lancar.

Skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perguruan tinggi program studi Strata 1 Informatika Universitas Amikom Yogyakarta. Dibuatnya skripsi ini salah satunya bertujuan untuk memberikan informasi dan menambah pengetahuan kepada pembaca mengenai keamanan serta monitoring jaringan.

Saya menyadari bahwa dalam proses penyusunan laporan ini tidak pernah lepas dari dorongan dan bantuan dari berbagai pihak, yang telah memberi bantuan kepada saya baik berupa pemikiran, tenaga, peran serta maupun berwujud barang dan uang. Dalam kesempatan ini saya mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan laporan diantara-Nya :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas Amikom Yogyakarta.
2. Bapak Sudarmawan S.T, M.T selaku dosen pembimbing yang telah memberikan bimbingan, saran dan masukannya dalam menyelesaikan naskah skripsi ini.
3. Hanif Al Fatta,S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Ibu Windah Mega Pradnya D,M.Kom selaku ketua Program Studi Informatika Universitas Amikom Yogyakarta.
5. Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu, dan pengalaman selama masa perkuliahan.
6. Kedua Orang tua yang telah memberikan bantuan dukungan serta doa.

7. Teman-teman dan sahabat yang telah memberikan arahan, motivasi dan bantuan dalam pengerjaan skripsi ini.
8. Semua pihak yang telah membantu sampai selesai-Nya penyusunan skripsi .

penulis menyadari sepenuhnya, bahwa skripsi ini tidak luput dari berbagai kekurangan, baik dari segi bahasa, sistematika penulisan maupun penyajian materi. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi penulis pada khususnya dan bagi pembaca serta dapat digunakan sebagai referensi untuk penelitian.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Wonomulyo, 16 Januari 2023

Rachmat

NIM. 19.11.2638

DAFTAR ISI

HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI Error! Bookmark not defined.	
PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN.....	xvi
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Studi Literatur.....	7
2.2 Dasar Teori.....	12
2.2.1 Winbox.....	12
2.2.2 Winbox.....	12

2.2.3	Firewall.....	13
2.2.4	Virtual Private Network (VPN)	15
2.2.5	Internet Protocol Security (IPSec)	16
2.2.6	Kriptografi	17
2.2.7	Virtualisasi	18
2.2.8	Monitoring Jaringan (Cacti)	18
2.2.9	Brute force	18
2.2.10	DDOS.....	19
2.2.11	Port Scanner	19
2.2.12	Intrusion Detection System (IDS)	19
2.2.13	Port Blocking	20
2.2.14	Linux Server	20
2.2.15	Kali Linux	21
2.2.16	NDLC.....	22
BAB III METODE PENELITIAN		23
3.1	Objek Penelitian	23
3.2	Alur Penelitian	24
3.2.1	Alur Kerja Penelitian.....	24
3.2.2	Desain Topologi	26
3.2.3	Alur Kerja Sistem.....	26
3.2.4	Alur Pertahanan Serangan.....	27
3.2.5	Alur Pengujian Serangan	28
3.2.1	Konfigurasi Firewall	30
3.2.2	Penggunaan Kali Linux	32
3.3	Alat dan Bahan	33

3.3.1	Alat.....	33
BAB IV HASIL DAN PEMBAHASAN.....		39
4.1	Hasil Pengujian Serangan dengan Nmap.....	39
4.2	Hasil Pengujian Serangan dengan Hping3.....	42
4.3	Hasil Pengujian Serangan dengan Patator	46
BAB V PENUTUP.....		50
5.1	Kesimpulan	50
5.2	Saran.....	51
REFERENSI.....		52
LAMPIRAN.....		55
	Lampiran 1 Konfigurasi Dasar Mikrotik	55
	Lampiran 2 Konfigurasi VPN Server.....	57
	Lampiran 3 Konfigurasi SNMP Server	61
	Lampiran 4 Konfigurasi Logging Mikrotik	62
	Lampiran 5 Konfigurasi Firewall Mikrotik	64
	Lampiran 6 Konfigurasi VM VirtualBox	78
	Lampiran 7 Konfigurasi Cacti.....	79
	Lampiran 8 Konfigurasi Graylog (log)	84
	Lampiran 9 Serangan Menggunakan Kali Linux	88
	Lampiran 10 Konfigurasi VPN Client	91

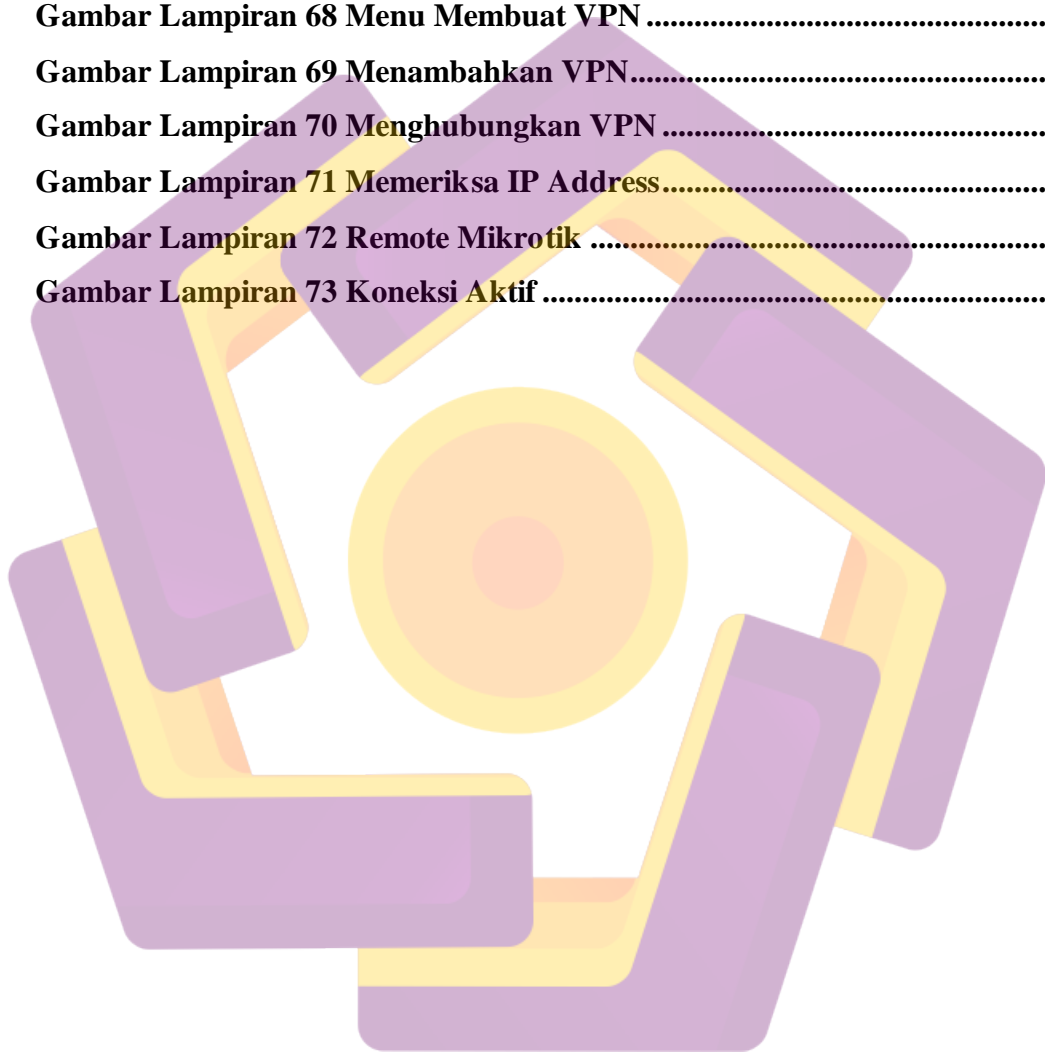
DAFTAR GAMBAR

Gambar 3. 1 Alur Kerja Penelitian	25
Gambar 3. 2 Gambar Desain Topologi	27
Gambar 3. 3 Alur Kerja Sistem Keamanan dan Monitoring	26
Gambar 3. 4 Alur Pertahanan	27
Gambar 3. 5 Gambaran Umum Serangan Exploit	28
Gambar 3. 6 Detail Serangan Port Scanner	29
Gambar 3. 7 Detail Serangan DDOS	29
Gambar 3. 8 Konfigurasi Pencegahan Port Scanning	30
Gambar 3. 9 Konfigurasi Pencegahan DDOS	31
Gambar 3. 10 Konfigurasi Port Mengarah Ke IP Tertentu	31
Gambar 3. 11 Konfigurasi Pencegahan Bruteforce	31
Gambar 3. 12 Username untuk penelitian	32
Gambar 3. 13 Password untuk penelitian	32
Gambar 3. 14 Router Mikrotik RB941-2nD	33
Gambar 3. 15 Laptop Asus X441UV	35
Gambar 3. 16 Laptop Acer Aspire 5 A514-52G-59RA	36
Gambar 4. 1 Grafik penggunaan CPU	41
Gambar 4. 2 Detail trafik interface ether 1	41
Gambar 4. 3 Grafik log pada monitoring	41
Gambar 4. 4 Grafik penggunaan CPU	44
Gambar 4. 5 Grafik penggunaan memori	44
Gambar 4. 6 Detail trafik interface ether 1	45
Gambar 4. 7 Grafik ping ke ether 1	45
Gambar 4. 8 Grafik log pada monitoring	46
Gambar 4. 9 Grafik penggunaan CPU	48
Gambar 4. 10 Detail trafik interface ether 1	49
Gambar 4. 11 Grafik log pada monitoring	49

Gambar Lampiran 1 DHCP Client	55
Gambar Lampiran 2 DNS Setting	56
Gambar Lampiran 3 Firewall NAT	56
Gambar Lampiran 4 Firewall NAT	56
Gambar Lampiran 5 Mengaktifkan L2TP Server.....	57
Gambar Lampiran 6 IP Pool.....	58
Gambar Lampiran 7 PPP Profiles.....	59
Gambar Lampiran 8 PPP Secret.....	60
Gambar Lampiran 9 SNMP Community	61
Gambar Lampiran 10 SNMP Setting.....	61
Gambar Lampiran 11 Action Setting.....	62
Gambar Lampiran 12 Rules Setting.....	63
Gambar Lampiran 13 Rules Setting.....	63
Gambar Lampiran 14 Rule Port Scanning General.....	64
Gambar Lampiran 15 Rule Port Scanning Extra	64
Gambar Lampiran 16 Rule Port Scanning Action	65
Gambar Lampiran 17 Rule Port Scanning General.....	66
Gambar Lampiran 18 Rule Port Scanning Action	66
Gambar Lampiran 19 Rule DDOS General.....	67
Gambar Lampiran 20 Rule DDOS Extra	67
Gambar Lampiran 21 Rule DDOS Action.....	68
Gambar Lampiran 22 Rule DDOS General.....	69
Gambar Lampiran 23 Rule DDOS Extra	69
Gambar Lampiran 24 Rule DDOS Action.....	70
Gambar Lampiran 25 Rule DDOS General.....	70
Gambar Lampiran 26 Rule DDOS Action.....	71
Gambar Lampiran 27 Rule DDOS General.....	71
Gambar Lampiran 28 Rule DDOS Action.....	72
Gambar Lampiran 29 Rule VPN General.....	72
Gambar Lampiran 30 VPN Tab Action.....	73
Gambar Lampiran 31 Rule Brute Force General.....	74

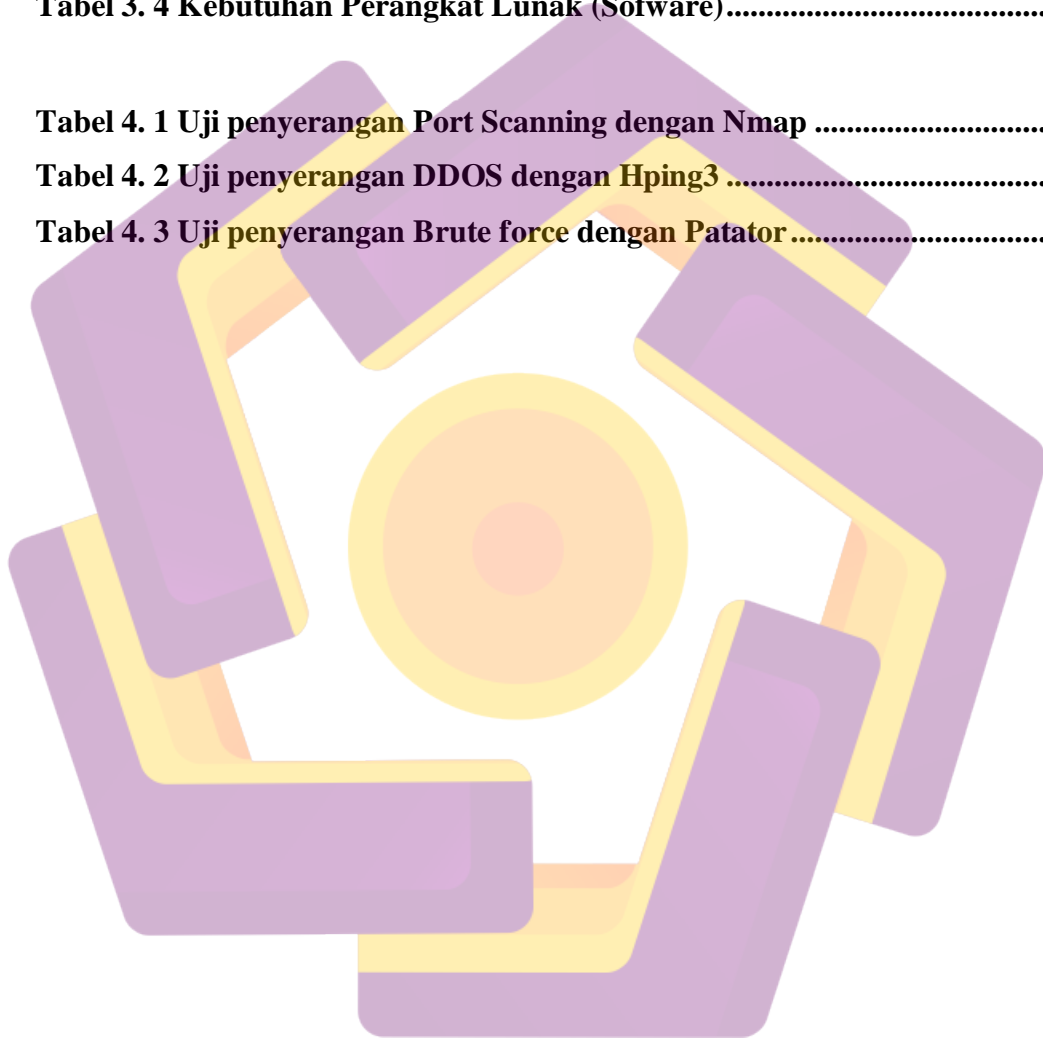
Gambar Lampiran 32 Rule Brute Force Extra	74
Gambar Lampiran 33 Rule Brute Force Action	75
Gambar Lampiran 34 Rule Brute Force General	75
Gambar Lampiran 35 Rule Brute force Extra	76
Gambar Lampiran 36 Rule Brute Force Action	76
Gambar Lampiran 37 Rule Brute Force General	77
Gambar Lampiran 38 Rule Brute Force Action	77
Gambar Lampiran 39 Konfigurasi Network VM	78
Gambar Lampiran 40 Ip Address Ubuntu	78
Gambar Lampiran 41 Login Cacti	79
Gambar Lampiran 42 Dashboard Cacti	79
Gambar Lampiran 43 Menambahkan Device	80
Gambar Lampiran 44 Menambahkan Device	80
Gambar Lampiran 45 Menambahkan Device	81
Gambar Lampiran 46 Menambahkan Device	81
Gambar Lampiran 47 Menambahkan Device	82
Gambar Lampiran 48 Menambahkan Device	82
Gambar Lampiran 49 Menambahkan Device	82
Gambar Lampiran 50 Menambahkan Device	83
Gambar Lampiran 51 Tampilan Graph	83
Gambar Lampiran 52 Tampilan Graph	84
Gambar Lampiran 53 Login Graylog	84
Gambar Lampiran 54 Menambahkan Input	85
Gambar Lampiran 55 Menambahkan Input	85
Gambar Lampiran 56 Menambahkan Input	86
Gambar Lampiran 57 Menambahkan Input	86
Gambar Lampiran 58 Menambahkan Input	87
Gambar Lampiran 59 Tampilan Log	87
Gambar Lampiran 60 Tampilan Log	88
Gambar Lampiran 61 Serangan Nmap	88
Gambar Lampiran 62 Address List	89

Gambar Lampiran 63 Serangan Hping 3	89
Gambar Lampiran 64 Address List	89
Gambar Lampiran 65 Serangan Patator	90
Gambar Lampiran 66 Address List	90
Gambar Lampiran 67 Menu Network & Internet	91
Gambar Lampiran 68 Menu Membuat VPN	91
Gambar Lampiran 69 Menambahkan VPN.....	92
Gambar Lampiran 70 Menghubungkan VPN	93
Gambar Lampiran 71 Memeriksa IP Address.....	94
Gambar Lampiran 72 Remote Mikrotik	95
Gambar Lampiran 73 Koneksi Aktif	95



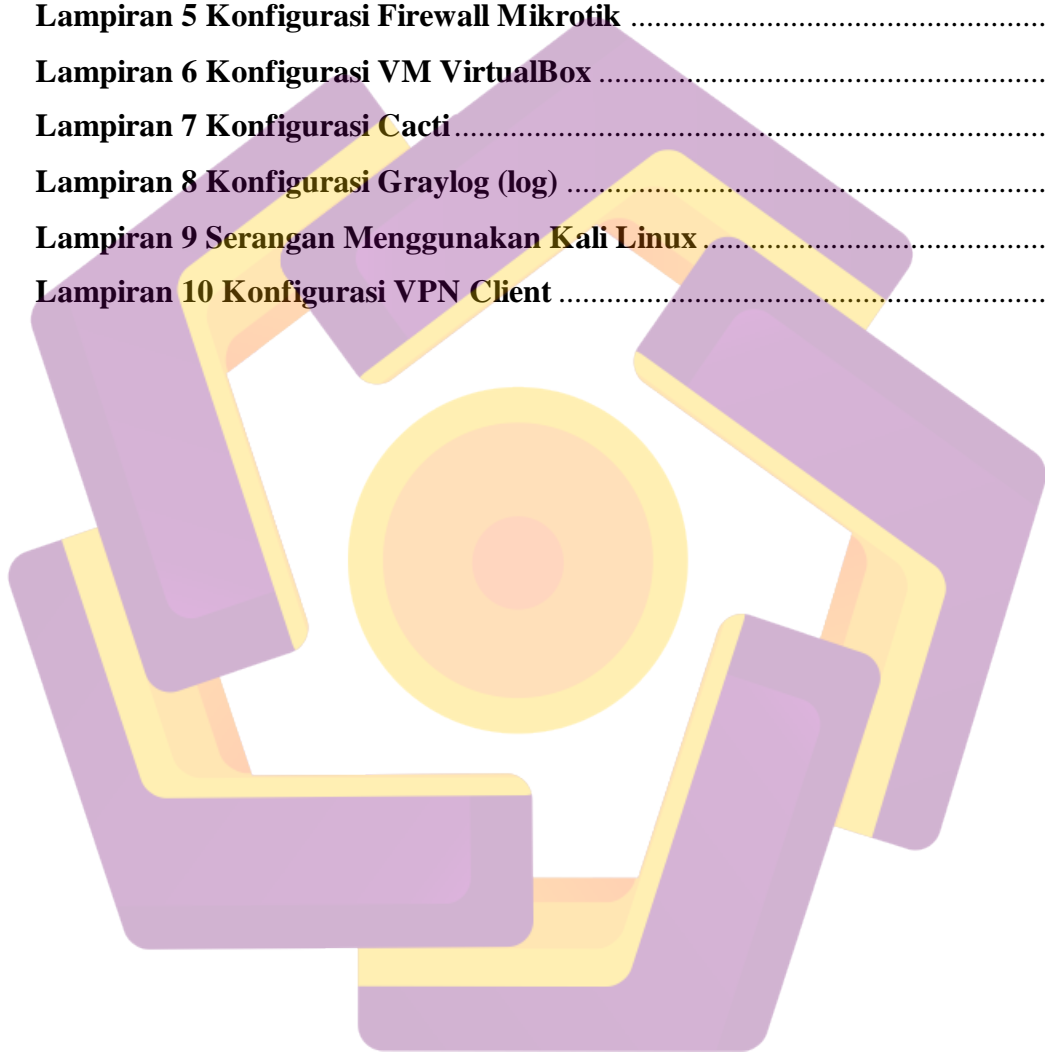
DAFTAR TABEL

Tabel 3. 1 Spesifikasi Router Mikrotik RB941-2nD	34
Tabel 3. 2 Spesifikasi Laptop Asus VivoBook X441UV.....	35
Tabel 3. 3 Spesifikasi Laptop Acer Aspire 5 A514-52G-59RA	37
Tabel 3. 4 Kebutuhan Perangkat Lunak (Software).....	38
Tabel 4. 1 Uji penyerangan Port Scanning dengan Nmap	39
Tabel 4. 2 Uji penyerangan DDOS dengan Hping3	42
Tabel 4. 3 Uji penyerangan Brute force dengan Patator	47



DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi Dasar Mikrotik	55
Lampiran 2 Konfigurasi VPN Server.....	57
Lampiran 3 Konfigurasi SNMP Server	61
Lampiran 4 Konfigurasi Logging Mikrotik	62
Lampiran 5 Konfigurasi Firewall Mikrotik	64
Lampiran 6 Konfigurasi VM VirtualBox	78
Lampiran 7 Konfigurasi Cacti.....	79
Lampiran 8 Konfigurasi Graylog (log)	84
Lampiran 9 Serangan Menggunakan Kali Linux	88
Lampiran 10 Konfigurasi VPN Client	91



INTISARI

Pada era seperti sekarang ini kebutuhan akan akses internet semakin dibutuhkan. Seiring berkembangnya waktu keamanan dunia internet juga perlu diperhatikan karena dapat mengancam keamanan pada jaringan tersebut. Router berperan penting terutama untuk menghubungkan ke jaringan internet. Sering kali router dijadikan target serangan yang dilancarkan guna mencari celah keamanan didalamnya. Router yang terhubung langsung ke ip publik lebih rentan terkena serangan karena langsung dapat diakses di jaringan internet. Serangan yang paling banyak merupakan *exploit* yaitu mencari kelemahan pada router dengan memanfaatkan port yang terbuka dan kelemahan pada *firewall* sehingga seseorang dapat lebih mudah masuk ke sistem. Agar dapat mengamankan router bisa menggunakan rule pada *firewall*.

Penggunaan *Instrusion Detection System (IDS)* dan *Port Blocking* biasa digunakan untuk mengamankan router dari serangan orang tidak bertanggung jawab yang memanfaatkan kerentanan pada router. *Instrusion Detection System (IDS)* digunakan untuk mendeteksi jika terdapat serangan pada perangkat sedangkan *Port Blocking* digunakan untuk memblokir serangan tersebut serta membantu mengizinkan perangkat diakses oleh jaringan tertentu. Terdapat juga monitoring pada router yang dapat digunakan untuk memantau jika ada problem dari router tersebut baik dari trafik yang digunakan maupun terdapat serangan bisa langsung dilihat dari aplikasi monitoring tersebut.

Hasil dari penelitian ini adalah untuk membuat keamanan dan perlindungan router dari serangan *exploit* yang memanfaatkan port terbuka terutama dari pihak luar yang ingin mengakses router, sehingga memproteksi router dari ancaman seperti *port scanning*, *DDOS*, dan *brute force*. Serta menerapkan monitoring server yang digunakan untuk memantau kondisi jaringan. Setelah *firewall* diterapkan tingkat keberhasilan melakukan *port scanning*, *ddos*, dan *brute force* adalah 0.

Kata Kunci : *Exploit, firewall, Instrusion Detection System (IDS), Port Blocking, port scanning, DDOS, brute force.*

ABSTRACT

In the current era the need for internet access is increasingly needed. As the development of the security time of the internet also needs to be considered because it can threaten security on the network. The router plays an important role especially to connect to the Internet Network. Often routers are targeted by attacks launched to find security gaps in it. Routers that are connected directly to the public IP are more vulnerable to attack because they can be directly accessed on the internet network. The most attack is an exploit that is looking for weaknesses in the router by utilizing open ports and weaknesses in the firewall so that someone can more easily enter the system. In order to secure the router, you can use a rule on the firewall.

The use of the Intrusion Detection System (IDS) and Port Blocking is commonly used to secure the router from irresponsible attacks that utilize vulnerability to the router. Intrusion Detection System (IDS) is used to detect if there is an attack on the device while the blocking port is used to block the attack and helps allow the device to be accessed by certain networks. There is also a monitoring on a router that can be used to monitor if there is a problem from the router both from the traffic used and there is an attack can be directly seen from the monitoring application.

The results of this study were to create security and protection of routers from exploit attacks that utilize open ports, especially from outsiders who want to access routers, thus protecting routers from threats such as port scanning, DDOS, and Brute Force. And implement server monitoring used to monitor network conditions. After the firewall is applied to the level of success in doing port scanning, ddos, and brute force ports are 0

Keywords : *Exploit, firewall, Intrusion Detection System (IDS), Port Blocking, port scanning, DDOS, brute force*