

**PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN
HOTSPOT UNTUK SISWA MENGGUNAKAN AUTHENTICATION
LOGIN PAGE CAPTIVE PORTAL DI SMK MUHAMMADIYAH 1
PLAYEN**

SKRIPSI



Disusun oleh

Rifal Rinaldi

15.11.9082

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN
HOTSPOT UNTUK SISWA MENGGUNAKAN AUTHENTICATION
LOGIN PAGE CAPTIVE PORTAL DI SMK MUHAMMADIYAH 1
PLAYEN**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Informatika



Disusun oleh

Rifal Rinaldi

15.11.9082

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

PERSETUJUAN

SKRIPSI

PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN HOTSPOT UNTUK SISWA MENGGUNAKAN AUTHENTICATION LOGIN PAGE CAPTIVE PORTAL DI SMK MUHAMMADIYAH 1 PLAYEN

Yang dipersiapkan dan disusun oleh

Rifal Rinaldi

15.11.9082

Telah disetujui oleh Dosen Pembimbing Skripsi

Pada tanggal 20 September 2021

Dosen Pembimbing,

Yudi Sutanto, M. Kom
NIK 190302105

PENGESAHAN

SKRIPSI

**PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN HOTSPOT
UNTUK SISWA MENGGUNAKAN AUTHENTICATION LOGIN PAGE CAPTIVE
PORTAL DI SMK MUHAMMADIYAH 1 PLAYEN**

Yang disusun oleh

Rifal Rinaldi
15.11.9082

Telah dipertahankan di depn Dewan Penguji
Pada tanggal 20 September 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Yudi Sutanto, M.Kom
NIK. 190302039

Donni Prabowo, M.Kom
NIK. 190302253

Eli Pujastuti, M.Kom
NIK. 190302227

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 September 2021

**DEKAN FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

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

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah tanggung jawab saya pribadi.

Yogyakarta, 28 September 2021

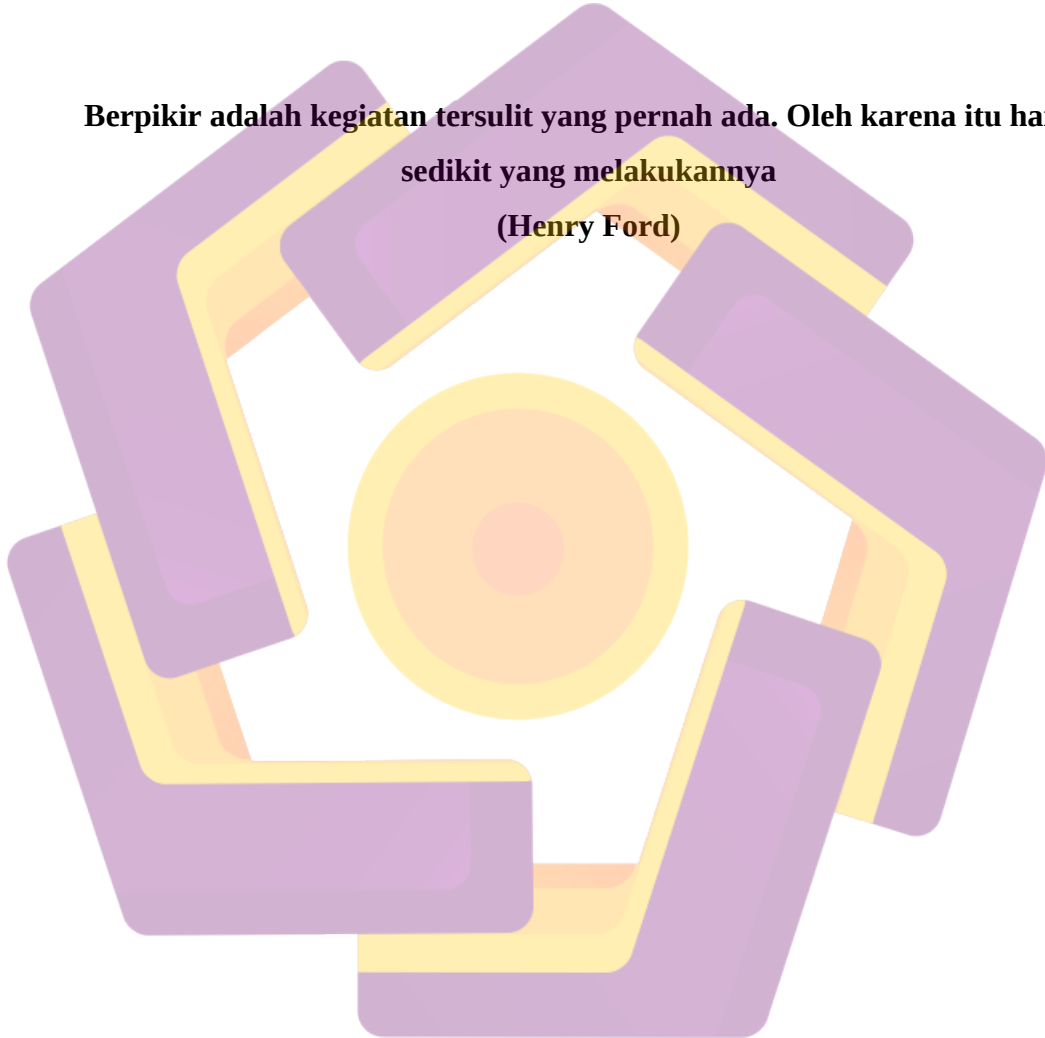


Rifal Rinaldi
NIM. 15.11.9082

MOTTO

**Pembelajaran tidak didapat dengan kebetulan. Ia harus dicari dengan semangat dan disimak dengan tekun
(Abigail Adams)**

**Berpikir adalah kegiatan tersulit yang pernah ada. Oleh karena itu hanya sedikit yang melakukannya
(Henry Ford)**



PERSEMBAHAN

Puji syukur Alhamdulillah penulis panjatkan atas kehadiran Allah SWT yang telah memberi rahmat, nikmat dan karunia-Nya sehingga penyusun skripsi ini dapat diselesaikan dengan baik. Pada kesempatan kali ini. Penulis ingin menyampaikan ucapan dan rasa terimakasih yang sebesar-besarnya kepada semua pihak yang terlibat dalam penyusunan skripsi ini. Beserta seluruh jerih payah dan tenaga yang sudah tercurahkan, Penulis mempersembahkan skripsi ini kepada :

1. Kedua orang tua dan saudara yang telah memberi dukungan, motifasi dan do'anya.
2. Bapak Yudi Sutanto, M.Kom sebagai dosen pembimbing yang telah membimbing selama pengerjaan skripsi sampai selesai.
3. Bapak/Ibu Dosen Universitas AMIKOM Yogyakarta yang telah mengajar selama perkuliahan dan terimakasih ilmunya.
4. Pihak SMK Muhammadiyah 1 Playen yang telah mengizinkan untuk menjadikan sekolah tersebut sebagai tempat observasi.
5. Teman-teman 15-S1IF-09 yang telah menemani selama kuliah di Universitas Amikom Yogyakarta.
6. Terimakasih kepada pihak-pihak yang entah dimana yang secara tidak langsung membantu skripsi ini dan tidak dapat saya sebutkan.

KATA PENGANTAR

Assalamu 'allainkum Warahmatullah Wabarakatuh

Alhamdulillah, atas izin Allah sehingga penulis dapat menyelesaikan laporan skripsi yang berjudul **“PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN HOTSPOT UNTUK SISWA MENGGUNAKAN METODE AUTHENTICATION LOGIN PAGE CAPTIVE PORTAL DI SMK MUHAMMADIYAH 1 PLAYEN “**.

Penyusunan laporan ini dimaksudkan untuk meraih gelar sarjana S1 dan menyelesaikan study pada Jurusan Informatika di Universitas AMIKOM Yogyakarta.

Proses penyusunan laporan skripsi ini tidak terlepas dari bantuan dan bimbingan dari berbagai pihak secara langsung maupun tidak langsung yang telah memberi motivasi kepada penulis. Terimakasih banyak yang sudah ikut dalam penyusunan laporan ini.

Akhirnya dengan doa kepada Allah SWT semoga laporan Skripsi ini dapat bermanfaat bagi semua pihak.

Wassalamu 'allaikum Warahmatullahi Wabarakatuh

Yogyakarta, September 2021

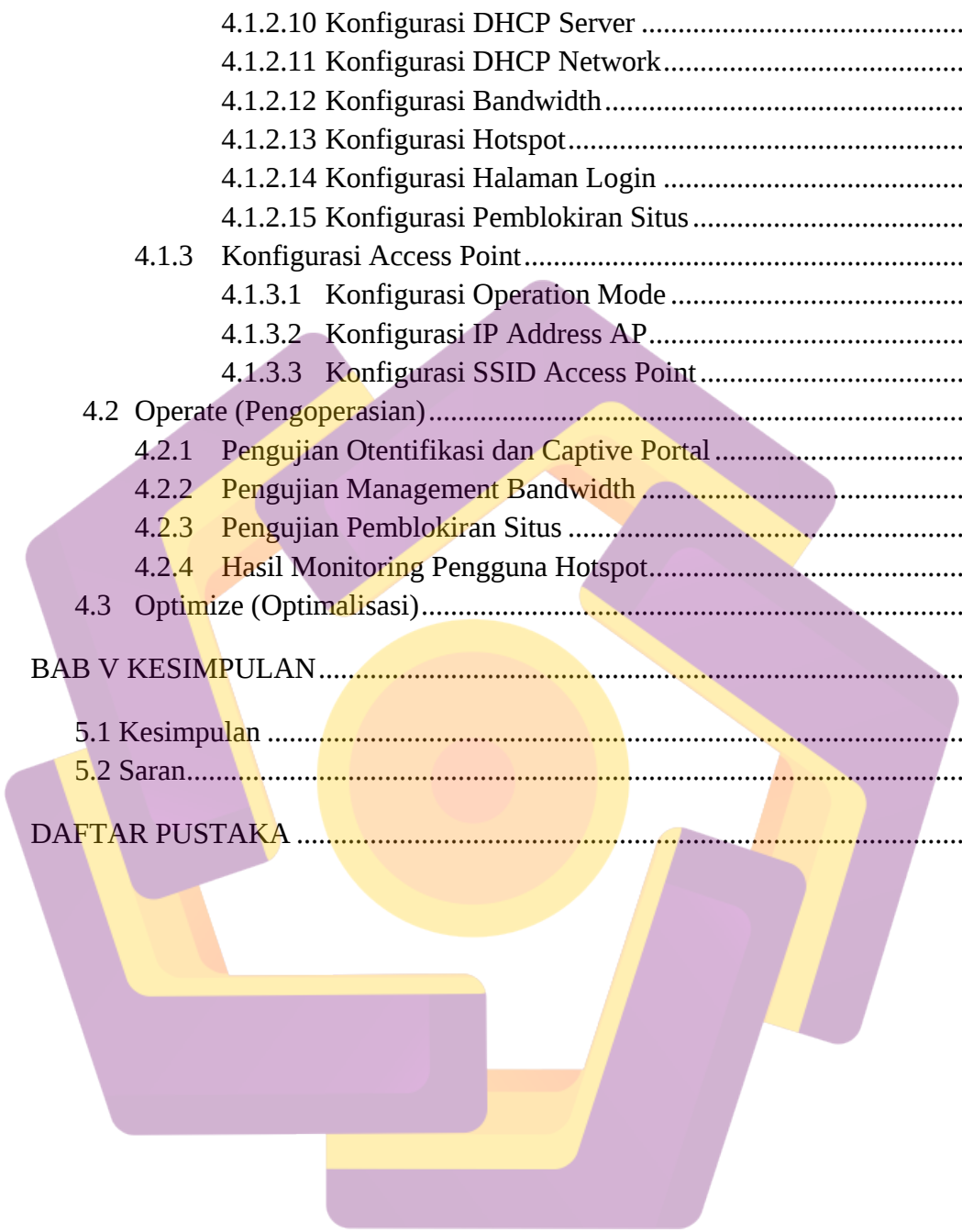
Penyusun

DAFTAR ISI

COVER	i
HALAMAN JUDUL.....	ii
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN.....	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvi
ABSTRACT	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penelitian	4
1.4.1 Tujuan Penelitian	4
1.4.2 Manfaat penelitian	4
1.4.2.1 Bagi Penulis	4
1.4.2.2 Bagi Objek.....	4
1.4.2.3 Bagi Akademik	5
1.5 Metode Penelitian	5
1.5.1 Metode Pengumpulan Data.....	5
1.5.2 Metode Analisa	5
1.5.3 Metode Perancangan	6
1.5.4 Metode Pengembangan	6

1.5.5	Metode Testing	6
1.5.6	Metode Implementasi.....	6
1.6	Sistematika Penulisan	6
BAB II LANDASAN TEORI		8
2.1	Tinjauan Pustaka.....	8
2.2	Dasar Teori.....	12
2.2.1	Pengertian Jaringan Komputer	12
2.2.2	Topologi Jaringan Komputer	12
2.2.3	Keamanan Jaringan Komputer	13
2.2.4	Jaringan Hotspot	15
2.2.4.1	Access Point	15
2.2.4.2	Internet.....	16
2.2.4.3	Winbox	17
2.2.5	Teknologi Pengamanan Wireless.....	18
2.2.5.1	Enkripsi WEP	18
2.2.5.2	Enkripsi WPA.....	18
2.2.5.3	Enkripsi WPA 2.....	19
2.2.5.4	Captive Portal	19
2.2.6	Standarisasi Wireless LAN (IEEE).....	20
2.2.6.1	IEEE 802.11.....	20
2.2.6.2	IEEE 802.11a.....	21
2.2.6.3	IEEE 802.11b.....	21
2.2.6.4	IEEE 802.11g.....	21
2.2.6.5	IEEE 802.11n.....	22
2.2.7	Mikrotik	22
2.2.7.1	Penjelasan Mikrotik.....	22
2.2.7.2	Jenis-Jenis Mikrotik	23
2.2.7.2.1	Mikrotik RouterOS.....	23
2.2.7.2.2	Mikrotik RouterBoard	24
2.2.7.3	Mikrotik RB750.....	25
2.2.8	PPDIOO	25
2.2.8.1	Prepare (Persiapan).....	25
2.2.8.2	Plan (Perancangan).....	26
2.2.8.3	Design (Desain)	26
2.2.8.4	Implement (Implementasi)	26
2.2.8.5	Operate (Operasional).....	27
2.2.8.6	Optimize (Optimalisasi)	27
BAB III ANALISIS DAN PERENCANAAN.....		28

3.1 Tinjauan Umum Objek Penelitian	28
3.1.1 Gambaran Umum SMK Muhammadiyah 1 Playen	28
3.1.2 Visi dan Misi	29
3.1.3 Struktur Organisasi	30
3.1.4 Gambar Lokasi	30
3.2 Prepare (Persiapan)	30
3.2.1 Analisis Kondisi Daerah Lokasi	30
3.2.2 Analisis Kondisi Topologi Jaringan	31
3.2.3 Pengumpulan Data	32
3.2.4 Identifikasi Masalah	32
3.3 Plan (Perencanaan)	33
3.3.1 Kebutuhan Fungsional	33
3.3.2 Kebutuhan Non-fungsional	34
3.3.2.1 Kebutuhan Perangkat Keras (Hardware)	34
3.3.2.2 Kebutuhan Perangkat Lunak (Software)	38
3.3.3 Kebutuhan Sumber Daya Manusia	39
3.4 Design (Desain)	39
3.4.1 Sistem Yang Direncanakan	39
3.4.2 Rancangan Topologi Jaringan	40
3.4.3 Cara Kerja Sistem	40
3.4.4 Perancangan Konfigurasi Interface	41
3.4.5 Perancangan Konfigurasi IP Address	42
3.4.6 Perancangan Interface Login Page Captive Portal	42
3.4.7 Perancangan Username dan Password	43
3.4.8 Perancangan Manajemen Bandwidth	43
3.4.9 Perancangan Pemblokiran Situs	43
BAB IV IMPLEMENTASI DAN PEMBAHASAN	44
4.1 Implement (Implementasi)	44
4.1.1 Login Winbox	44
4.1.2 Konfigurasi Mikrotik	45
4.1.2.1 Konfigurasi Administrator	45
4.1.2.2 Konfigurasi Waktu	46
4.1.2.3 Konfigurasi Interface	47
4.1.2.4 Konfigurasi IP Address	48
4.1.2.5 Konfigurasi Route	49
4.1.2.6 Konfigurasi DNS	50
4.1.2.7 Konfigurasi Firewall NAT	51
4.1.2.8 Konfigurasi IP POOL	51
4.1.2.9 Konfigurasi DHCP Client	53



4.1.2.10 Konfigurasi DHCP Server	53
4.1.2.11 Konfigurasi DHCP Network.....	55
4.1.2.12 Konfigurasi Bandwidth.....	56
4.1.2.13 Konfigurasi Hotspot.....	59
4.1.2.14 Konfigurasi Halaman Login	63
4.1.2.15 Konfigurasi Pemblokiran Situs	64
4.1.3 Konfigurasi Access Point.....	66
4.1.3.1 Konfigurasi Operation Mode	66
4.1.3.2 Konfigurasi IP Address AP.....	66
4.1.3.3 Konfigurasi SSID Access Point.....	67
4.2 Operate (Pengoperasian).....	67
4.2.1 Pengujian Otentifikasi dan Captive Portal	67
4.2.2 Pengujian Management Bandwidth	70
4.2.3 Pengujian Pemblokiran Situs	72
4.2.4 Hasil Monitoring Pengguna Hotspot.....	72
4.3 Optimize (Optimalisasi).....	73
BAB V KESIMPULAN.....	74
5.1 Kesimpulan	74
5.2 Saran.....	75
DAFTAR PUSTAKA	76

DAFTAR TABEL

Tabel 2.1 Matrik Literature Review	9
Tabel 3.1 Spesifikasi RB750.....	35
Tabel 3.2 Spesifikasi TP-Link TL-WR840N	36
Tabel 3.3 Spesifikasi Leptop Lenovo G40-30	37
Tabel 4.1 IP Address	48
Tabel 4.2 IP Range.....	52
Tabel 4.3 DHCP Server	54
Tabel 4.4 DHCP Network.....	55
Tabel 4.5 Pengujian Otentikasi Login Case Cencitive.....	68
Tabel 4.6 Pengujian Otentikasi Login Ganda	69

DAFTAR GAMBAR

Gambar 2.1	Hotspot	15
Gambar 2.2	Access Point	15
Gambar 2.3	Winbox	17
Gambar 2.4	Mikrotik RB750.....	25
Gambar 3.1	Struktur Organisasi.....	30
Gambar 3.2	Denah Lokasi SMK Muammadiyah 1 Playen.....	30
Gambar 3.3	Denah Lokasi.....	30
Gambar 3.4	Denah Jaringan	31
Gambar 3.5	Topologi Jaringan.....	31
Gambar 3.6	Routerboard Mikrotik RB750.....	34
Gambar 3.7	Access Point TP-LINK TL-WR840N	36
Gambar 3.8	Leptop Lenovo G40-30	37
Gambar 3.9	Alur Flow diagram penelitian.....	40
Gambar 3.10	Perancangan Topologi Jaringan	40
Gambar 3.11	Alur Sistem Login	41
Gambar 3.12	Rancangan Tampilan Login Captive Portal	43
Gambar 4.1	Login Interface Winbox	44
Gambar 4.2	Halaman Winbox.....	44
Gambar 4.3	Konfigurasi Identitas router.....	45
Gambar 4.4	Konfigurasi Username dan Password.....	46
Gambar 4.5	Konfigurasi Waktu	46
Gambar 4.6	Konfigurasi Interface.....	47
Gambar 4.7	Konfigurasi IP Address	48
Gambar 4.8	Konfigurasi Route	49
Gambar 4.9	Konfigurasi DNS	50
Gambar 4.10	Konfigurasi NAT	51
Gambar 4.11	Konfigurasi IP POOL	52
Gambar 4.12	Konfigurasi DHCP Client.....	53

Gambar 4.13	Konfigurasi Server.....	54
Gambar 4.14	Konfigurasi DHCP Network	55
Gambar 4.15	Halaman Queue Type	56
Gambar 4.16	Konfigurasi PCQ Uploud	57
Gambar 4.17	Konfigurasi PCQ Download.....	57
Gambar 4.18	Konfigurasi PCQ	57
Gambar 4.19	Konfigurasi Simple Queues.....	58
Gambar 4.20	Konfigurasi Hotspot Server Profile	59
Gambar 4.21	Konfigurasi Server Hotspot.....	60
Gambar 4.22	Konfigurasi User Profile.....	61
Gambar 4.23	Data Username dan Password dihalaman excel	62
Gambar 4.24	Input Username dan Password	62
Gambar 4.25	Daftar User	62
Gambar 4.26	Koding HTML Halaman Login	63
Gambar 4.27	Uploud File HTML Halaman Login.....	63
Gambar 4.28	Konfigurasi HTML Directory	64
Gambar 4.29	Konfigurasi NAT.....	64
Gambar 4.30	Konfigurasi WebProxy	65
Gambar 4.31	Konfigurasi Pemblokiran Situs.....	65
Gambar 4.32	Konfigurasi Operation Mode.....	66
Gambar 4.33	Konfigurasi IP Address AP	66
Gambar 4.34	Konfigurasi nama SSID Wifi	67
Gambar 4.35	Login Berhasil	70
Gambar 4.36	Login Gagal	70
Gambar 4.37	Test Bandwidth 1 Perangkat.....	71
Gambar 4.38	Test Bandwidth 2 Perangkat di PC dan Smartpone.....	71
Gambar 4.39	Hasil Pemblokiran Situs Youtube	72
Gambar 4.40	Monitoring Pengguna Hotspot	72

INTISARI

Perkembangan teknologi yang semakin pesat, informasi semakin mudah didapat dengan adanya internet. Kebutuhan akan internet sudah di rasakan semua masyarakat terutama siswa siswi sebagai media belajar. Dengan fasilitas yang diberikan oleh pihak sekolahan sebagai jaringan nirkabel untuk siswa yang seharusnya dipergunakan sebaik mungkin. Jaringan nirkabel harus dikelola dengan baik, dijaga kerahasiaannya, integritas dan keamanannya agar akses data tidak dapat di akses oleh pihak yang tidak berkepentingan. Jenis pengamanan jaringan nirkabel menggunakan otentikasi WPA-PSK, namun *password* yang digunakan mudah tersebar ke pihak lain, bahkan dari pihak luar sekolah pun bisa tersambung.

Jaringan nirkabel tidak memberikan jaminan keamanan secara penuh, dari beberapa masalah yang timbul seperti adanya user ilegal perlu dibuat metode pengamanan jaringan nirkabel agar lebih aman dan termonitor. Teknik pengamanan jaringan dapat dilakukan dengan membuat autentikasi *captive portal*. *Captive portal* merupakan salah satu tehnik pengamanan jaringan nirkabel melalui web browser di sisi client menggunakan *username* dan *password*. Selain dapat digunakan sebagai otentikasi client juga dapat digunakan untuk manajemen *bandwidth* dan memonitoring pengguna.

SMK Muhammadiyah 1 Playen menggunakan keamanan jaringan dengan WPA-PSK, sehingga pihak lain di luar SMK Muhammadiyah 1 Playen bisa menggunakan *hotspot* sekolahan tersebut. Maka dibutuhkan keamanan jaringan yang lebih spesifik menggunakan *captive portal*. Dengan *captive portal* maka setiap siswa maupun guru memiliki username dan password sendiri-sendiri. Jadi setiap siswa maupun guru yang ingin menggunakan fasilitas hotspot sekolahan harus memiliki data *username* dan *password* di database jaringan SMK Muhammadiyah 1 Playen.

Keywords: Hotspot, Keamanan Jaringan, Captive Portal, Bandwidth.

ABSTRACT

Development of technology is the rapid, information is easier to obtain with the internet. The need for the internet has been felt by all people, especially students as a learning medium. With the facilities provided by the school as a wireless network for students that should be used as well as possible. Wireless networks must be managed properly, kept confidential, integrity and security so that data access cannot be accessed by unauthorized parties. This type of wireless network security uses WPA-PSK authentication, but the password used is easy to spread to other parties, even parties outside the school can connect.

Wireless networks do not provide full security guarantees, from several problems that arise such as illegal users, it is necessary to create a wireless network security method to make it more secure and monitored. Network security techniques can be done by creating a captive portal authentication. Captive portal is a wireless network security technique through a web browser on the client side using a username and password. Besides being able to be used as client authentication, it can also be used for management bandwidth and user monitoring.

SMK Muhammadiyah 1 Playen uses network security with WPA-PSK, so that other parties outside SMK Muhammadiyah 1 Playen can use the school's hotspot. So a more specific network security is needed using a captive portal. With a captive portal, each student and teacher has their own username and password. So every student or teacher who wants to use the school hotspot facility must have username and password data in the network database of SMK Muhammadiyah 1 Playen.

Keywords: Hotspot, Network Security, Captive Portal, Bandwidth