ANALISIS DAN IMPLEMENTASI KEAMANAN WIRELESS MENGGUNAKAN METODE AUTHENTICATION CAPTIVE PORTAL DI MAPAN COFFEE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Informatika

disusun oleh
YUSUF ARIANTO
16.11.0842

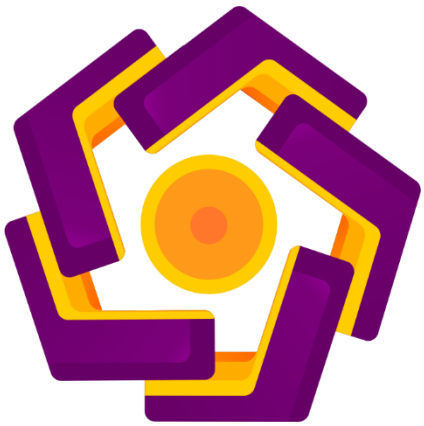
Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

ANALISIS DAN IMPLEMENTASI KEAMANAN WIRELESS MENGGUNAKAN METODE AUTHENTICATION CAPTIVE PORTAL DI MAPAN COFFEE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi S1 Informatika



disusun oleh
YUSUF ARIANTO
16.11.0842

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI KEAMANAN WIRELESS MENGGUNAKAN METODE AUTHENTICATION CAPTIVE PORTAL DI MAPAN COFFEE

yang disusun dan diajukan oleh

Yusuf Arianto
16.11.0842

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Januari 2023

Dosen Pembimbing,

Arief Setyanto, S.Si., MT, Ph.D
NIK. 190302036

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI KEAMANAN WIRELESS MENGGUNAKAN METODE AUTHENTICATION CAPTIVE PORTAL DI MAPAN COFFEE

yang disusun dan diajukan oleh

Yusuf Arianto
16.11.0842
Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Januari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Arifiyanto Hadinegoro, S.Kom, MT **NIK. 190302289**	
Mei P Kurniawan, M.Kom **NIK. 190302187**	
Arief Setyanto, S.Si., MT, Ph.D **NIK. 190302036**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Januari 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 : Yusuf Arianto
NIM : 16.11.0842

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAN IMPLEMENTASI KEAMANAN WIRELESS MENGGUNAKAN METODE AUTHENTICATION CAPTIVE PORTAL DI MAPAN COFFEE

Dosen Pembimbing : Arief Setyanto, S.Si., MT, Ph.D

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, 19 Januari 2023

Yang Menyatakan,

Yusuf Arianto

HALAMAN PERSEMBAHAN

Puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, saya ucapkan rasa syukur dan terima kasih saya kepada:

1. Allah SWT, karena hanya atas izin dan karunia-Nyalah maka skripsi ini dapat selesai.
2. Orang tua saya, yang tidak pernah lelah memberikan saya dukungan dan doa. Terimakasih kepada Bapak Harjan, Om Ngadiman dan Bulek Marmiyem yang selalu memberikan doa kepada saya dan memberikan semangat supaya saya bisa menyelesaikan skripsi ini. Terimakasih banyak saya ucapkan untuk keduanya.
3. Saudara saya Mas Ameliano dan Mbak Ida yang senantiasa memberi semangat dan doa agar saya dapat menyelesaikan studi saya.
4. Dosen pembimbing Bapak Arief Setyanto, S.Si., MT, Ph.D yang selama ini telah tulus, sabar dan ikhlas meluangkan waktu untuk menuntun dan mengarahkan saya, memberikan bimbingan dan pelajaran yang tiada ternilai harganya, agar saya menjadi lebih baik.
5. Dosen penguji 1 Bapak Arifiyanto Hadinegoro, S.kom, MT dan Dosen penguji 2 Bapak Mei P Kurniawan, M.Kom yang sudah memberi masukan dan saran sehingga saya dapat menyelesaikan skripsi ini.
6. Bapak dan Ibu Dosen pengajar atas segala ilmu yang telah diberikan kepada saya. Semoga ilmu yang telah diajarkan kepada saya dan dapat bermanfaat bagi orang lain atau meneruskan jasa bapak dan ibu dosen.
7. Rekan-rekan kelas informatika 13, yang telah memberikan saya semangat. Terimakasih atas kenangan-kenangan nya.
8. Rekan-rekan Pemuda Dusun Krapyak yang senantiasa mendukung dan memberi semangat kepada saya.
9. Rekan-rekan Barbel (Baris belakang) yang telah menemani suka dan duka dalam pengerjaan tugas. Terimakasih kenangan – kenangan yang telah diberikan.

10. Keluarga besar Kontrakan ijo, terimakasih yang telah membantu saya dan menemani saya selama 2 tahun. Serta memberikan kecerian, kenakalan, suka duka dalam kehidupan.

Terimakasih yang sebesar-besarnya untuk kalian semua, akhir kata saya persembahkan skripsi ini untuk kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup saya. Semoga skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan kehadirat Allah SWT yang selalu melimpahkan rahmat serta hidayah-Nya kepada setiap hamba-Nya. Skripsi ini disusun sebagai salah satu syarat kelulusan Program Strata 1 Program Studi Informatika, Universitas AMIKOM Yogyakarta dan untuk memperoleh gelar Sarjana Komputer (S.Kom).

Dengan selesainya skripsi yang berjudul "***Analisis Dan Implementasi Manajemen User Dan Manajemen Bandwidth Menggunakan Queue Tree Dan Per Connection Queue Di Physical Fitness Jogja)***", dengan ini penyusun ingin mengucapkan terima kasih kepada:

1. Allah SWT atas rahmat, hidayah, serta karunia-Nya yang telah diberikan kepada penulis sehingga skripsi ini dapat terselesaikan.
2. Bapak Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta.
3. Bapak Hanif Al Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer.
4. Ibu Windha Mega Pradnya Dhuhita, M.Kom selaku Ketua Program Studi S1 Informatika.
5. Bapak Arief Setyanto, S.Si., MT, Ph.D selaku dosen pembimbing yang memberikan arahan, saran dan motivasi agar penulis bisa menyelesaikan naskah ini.
6. Bapak Arifiyanto Hadinegoro, S.Kom, MT dan Bapak Mei P Kurniawan, M.Kom selaku dosen penguji yang memberi saran agar penulisan naskah skripsi ini menjadi lebih baik.
7. Bapak, Om dan Tante yang selalu memberikan dukungan baik materi maupun doa.
8. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya selama penulis kuliah.
9. Keluarga besar kelas S1 Informatika 13 angkatan 2016.
10. Rekan-rekan Pemuda Dusun Krapyak.

11. Keluarga besar Barbel (Baris Belakang) dari masuk kuliah hingga sekarang masih memberikan semangat.

Akhirnya dengan kerendahan hati penulis mengucapkan terimakasih dan semoga skripsi ini dapat bermanfaat bagi penulis maupun pembaca.

Yogyakarta, 5 Februari 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL.....i
HALAMAN PERSETUJUAN.....ii
HALAMAN PENGESAHAN.....iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....iv
HALAMAN PERSEMBAHAN.....v
KATA PENGANTAR.....vii
DAFTAR ISI.....ix
DAFTAR TABEL.....xiii
DAFTAR GAMBAR.....xiv
INTISARI.....xvii
ABSTRACT.....xviii
BAB I PENDAHULUAN.....1
1.1 Latar Belakang.....1
1.2 Rumusan Masalah.....2
1.3 Batasan Masalah.....2
1.4 Tujuan Penelitian.....3
1.5 Manfaat Penelitian.....3
1.6 Metode Penelitian.....3
1.6.1 Metode Pengumpulan Data.....3
1.6.1.1 Metode Observasi.....3
1.6.1.2 Metode Analisis dan Perancangan.....4
1.7 Sistematika Penulisan.....4
BAB II TINJAUAN PUSTAKA.....5
2.1 Studi Literatur.....5
2.2 Dasar Teori.....9
2.2.1 Mikrotik.....9

2.2.2 Jaringan Komputer 9
2.2.2.1 Jenis-Jenis Jaringan 11
2.2.2.2 Topologi Jaringan 14
2.2.3 IP Address Versi 4 16
2.2.3.1 Jenis-Jenis Alamat IP 17
2.2.4 MAC Address 18
2.2.5 Konfigurasi User 18
2.2.6 Wireless 19
2.2.7 Hotspot Server 20
2.2.7.1 Authentication Captive Portal 20
2.2.7.2 Manajemen User 21
2.2.8 Jenis-Jenis Serangan yang Digunakan 21
2.2.9 Perangkat Lunak yang Digunakan 22
2.2.9.1 Winbox 22
2.2.9.2 Fluxion 22
2.2.9.3 Mikhmon 23
BAB III METODE PENELITIAN 24
3.1 Objek penelitian 24
3.2 Analisis Masalah 26
3.3 Metode Perancangan Sistem 26
3.4 Analisis Kebutuhan Sistem 28
3.4.1 Analisis Kebutuhan Fungsional 28
3.4.2 Analisis Kebutuhan Non Fungsional 28
3.4.3 Analisis Kebutuhan SDM 29
3.5 Analisis Kelayakan Sistem 30
3.5.1 Kelayakan Hukum 30
3.6 Perancangan Jaringan 30
3.6.1 Perancangan Topologi Jaringan 31
3.6.2 Perancangan Captive Portal 32
3.6.3 Perancangan User Manager 33
3.7 Pengujian 33
3.8 Alur Penelitian 34

BAB IV HASIL DAN PEMBAHASAN 35
4.1 Instalasi Jaringan 35
4.1.1 Instalasi Perangkat Jaringan 35
4.1.1.1 Instalasi Modem Huawei EG8245H5.....35
4.1.1.2 Konfigurasi Router Mikrotik RB941-2nD-TC dan Router Xiaomi 4C 36
4.1.1.2.1 Konfigurasi Interface List.....36
4.1.1.2.2 Konfigurasi IP Address.....36
4.1.1.2.3 Konfigurasi Default Route.....37
4.1.1.2.4 Konfigurasi DNS Server.....37
4.1.1.2.5 Konfigurasi NAT 38
4.1.1.2.6 Konfigurasi SNTP 38
4.1.1.2.7 Konfigurasi Hotspot.....39
4.1.1.2.8 Konfigurasi Access Point Xiaomi Router 4C 42
4.1.1.2.9 Konfigurasi User Profiles dengan Mikhmon 44
4.1.1.2.10 Konfigurasi Voucher 48
4.1.1.2.11 Membuat User Hotspot.....48
4.1.1.2.12 Konfigurasi Captive Portal 51
4.2 Pengujian Sistem 52
4.2.1 Pengujian Koneksi Router Mikrotik dengan Modem dan Internet ..52
4.2.2 Pengujian Konfigurasi Hotspot 53
4.2.2.1 Pengguna Melakukan Login 53
4.2.2.2 Pengujian Pembatasan Jumlah Perangkat 55
4.2.2.3 Pengujian Fitur Lock User.....56
4.2.2.4 Pengujian Pembatasan Waktu Penggunaan.....57
4.2.2.5 Pengujian Login dengan Akun yang Mencapai Limit Waktu 58
4.2.3 Pengujian Keamanan Jaringan Lama dan Jaringan Baru 58
4.2.3.1 Pengujian Keamanan Menggunakan Software Fluxion 60
4.2.3.1.1 Pengujian Keamanan Jaringan Lama.....60
4.2.3.1.2 Pengujian Keamanan Jaringan Baru 67
BAB V PENUTUP.....68
5.1 Kesimpulan 68

5.2 Saran 68
REFERENSI.....69

DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian 7
Tabel 2.2 Luas Cakupan Area Jaringan Komputer 14
Tabel 3.1 Spesifikasi Huawei EG8245H5.....25
Tabel 3.2 Spesifikasi RB941-2nD-TC 29
Tabel 3.3 Spesifikasi ASUS X200M.....29
Tabel 3.4 Pembagian IP Address 31
Tabel 3. 5 Pembagian Jumlah Waktu.....33
Tabel 4. 1 Daftar Perangkat yang Terhubung 59
Tabel 4. 2 Perangkat Penyerang 60
Tabel 4. 3 Perangkat Pendukung Serangan.....60

DAFTAR GAMBAR

Gambar 2.1 Peer to peer 10
Gambar 2.2 Simple Client Server Model 11
Gambar 2.3 Local Area Network atau LAN (Sumber: it-jurnal.com) 12
Gambar 2. 4 Metropolitan Area Network atau MAN (Sumber: it-jurnal.com) 12
Gambar 2.5 Wide Area Network atau WAN (Sumber: ecomputernotes.com) 13
Gambar 2.6 Topologi Bus 15
Gambar 2.7 Topologi Tree/Hierarchical 16
Gambar 2.8 Implementasi Jaringan Wireless 19
Gambar 2.9 Penerapan Hotspot Server 20
Gambar 2.10 Logo Winbox (Sumber: png.download.id) 22
Gambar 2.11 Tampilan Fluxion 23
Gambar 2.12 Tampilan Mikhmon (Sumber: laksa19.github.io/?mikhmon/v3) 23
Gambar 3.1 Foto Mapan Coffee 24
Gambar 3.2 Topologi jaringan Mapan Coffee 25
Gambar 3.3 Perancangan Sistem 27
Gambar 3.4 Topologi jaringan yang baru 31
Gambar 3.5 Rancangan *interface captive portal* 32
Gambar 3.6 Alur Penelitian 34
Gambar 4.1 Mematikan *wlan* pada modem Huawei EG8245H5 35
Gambar 4.2 Konfigurasi *interface* 36
Gambar 4.3 Konfigurasi *IP address* 37
Gambar 4.4 Konfigurasi *default gateway* 37
Gambar 4.5 Konfigurasi *DNS server* 38
Gambar 4.6 Konfigurasi NAT 38
Gambar 4.7 Konfigurasi SNTP 39
Gambar 4.8 Hotspot setup 39
Gambar 4.9 Pengisian IP address pada hotspot 40
Gambar 4.10 IP pool pada hotspot 40
Gambar 4.11 DNS pada hotspot 40

Gambar 4.12 DNS name pada hotspot.....41
Gambar 4.13 Hotspot user.....41
Gambar 4.14 Tampilan Hotspot server 41
Gambar 4.15 Mematikan fitur login dengan cookie 42
Gambar 4.16 Tampilan awal Xiaomi router.....42
Gambar 4.17 Pilihan mode pada Xiaomi router.....43
Gambar 4.18 Pengaturan nama SSID, password, dan password administrator 43
Gambar 4.19 Tampilan router Xiaomi 4C setelah selesai dikonfigurasi 44
Gambar 4.20 Tampilan home router Xiaomi 4C.....44
Gambar 4.21 Tampilan Mikhmon server 45
Gambar 4.22 Tampilan halaman login Mikhmon 45
Gambar 4.23 Tampilan konfigurasi session mikhmon.....46
Gambar 4.24 Tampilan halaman Mikhmon setelah berhasil dihubungkan ke router mikrotik 46
Gambar 4.25 Tampilan halaman konfigurasi user profile pengelola 47
Gambar 4.26 Tampilan halaman konfigurasi user profile pelanggan 47
Gambar 4.27 Tampilan halaman konfigurasi template voucher 48
Gambar 4.28 Tampilan template voucher.....48
Gambar 4.29 Tampilan pembuatan voucher 30 menit 49
Gambar 4.30 Tampilan pembuatan voucher 1 jam 49
Gambar 4.31 Tampilan pembuatan voucher 1,5 jam 50
Gambar 4.32 Tampilan voucher yang telah dibuat 50
Gambar 4.33 Tampilan users hotspot di Mikrotik 50
Gambar 4.34 File halaman login.....51
Gambar 4.35 Tampilan halaman login hotspot versi desktop.....51
Gambar 4.36 Tampilan halaman login hotspot versi mobile 52
Gambar 4.37 Test koneksi ke modem.....52
Gambar 4.38 Test koneksi ke internet.....53
Gambar 4.39 Pengujian Login dengan data acak.....54
Gambar 4.40 Hasil login username dan password acak.....54
Gambar 4.41 Hasil login dengan username dan password yang sah 55

Gambar 4.42 Hasil login pada perangkat kedua 56
Gambar 4.43 Hasil login dengan akun yang sudah pernah login di perangkat yang lain. 57
Gambar 4.44 Tampilan halaman login jika pengguna mencapai limit waktu.....57
Gambar 4.45 Tampilan halaman login jika pengguna mencapai limit waktu.....58
Gambar 4.46 Tampilan Fluxion 61
Gambar 4.47 Tampilan halaman wifi list 61
Gambar 4.48 Tampilan halaman Access point service 62
Gambar 4.49 Tampilan halaman capture handshake 63
Gambar 4.50 Tampilan proses serangan 64
Gambar 4.51 Tampilan pilihan wifi di perangkat 3 64
Gambar 4.52 Tampilan pilihan wifi di perangkat 2 65
Gambar 4.53 Tampilan pilihan wifi di perangkat 1 65
Gambar 4.54 Tampilan website phising.....66
Gambar 4.55 Tampilan website jika korban memasukkan kata sandi yang salah .66
Gambar 4.56 Tampilan fluxion sukses mendapatkan kata sandi.....67
Gambar 4.57 Tampilan fluxion sukses mendapatkan kata sandi di jaringan baru .67

INTISARI

Keamanan fasilitas jaringan *wifi* di Mapan Coffee menggunakan metode WPA2/PSK yang mana 1 *password* dapat digunakan oleh banyak *user* dan tidak adanya sistem pembatasan waktu bagi perangkat yang terhubung ke jaringan. Oleh karena itu muncul permasalahan adanya pihak yang tidak berhak yang turut menggunakan fasilitas ini dan terdapat pula pengunjung Mapan Coffee yang menggunakan fasilitas ini terlalu lama tanpa melakukan pembelian menu lagi. Maka dari itu diperlukan metode keamanan yang dapat membatasi jumlah perangkat yang dapat terhubung dengan 1 *password* dan diperlukan juga sistem yang dapat membatasi waktu perangkat terhubung ke jaringan.

Untuk mengatasi permasalahan tersebut diperlukan router Mikrotik yang memiliki fitur *Hotspot* yang dapat membatasi jumlah perangkat terhubung dengan 1 *password* beserta waktu aksesnya.

Hasil dari penggunaan fitur *Hotspot* pada router Mikrotik ini dapat lebih baik dalam mengamankan dan membatasi waktu akses ke jaringan karena pengguna dari fasilitas ini akan diarahkan untuk melakukan *login* di halaman *captive portal* terlebih dahulu dengan *username* dan *password*, setelah itu pengguna baru akan terhubung ke internet dengan batas waktu yang ditentukan oleh pengelola. *Username* dan *password* yang diberikan hanya dapat digunakan oleh 1 perangkat dan memiliki waktu akses yang berbeda tergantung dari jumlah transaksi pembelian menu di Mapan Coffee.

Kata kunci: Keamanan, Jaringan, *Wifi*, WPA2/PSK, *Password*, *Username*, *User*, Perangkat, *Hotspot*, Waktu Akses, *Login*.

ABSTRACT

The security of wifi network facilities at Mapan Coffee uses the WPA2 / PSK method where 1 password can be used by many users and there is no time limitation system for devices connected to the network. Therefore, the problem arises that there are unauthorized parties who also use this facility and there are also Mapan Coffee visitors who use this facility for too long without purchasing the menu again. Therefore, a security method is needed that can limit the number of devices that can be connected with 1 password and a system that can limit the time the device is connected to the network is also needed.

To overcome these problems, a Mikrotik router is needed which has a Hotspot feature that can limit the number of connected devices with 1 password and access time.

The results of using the Hotspot feature on this Mikrotik router can be better at securing and limiting access time to the network because users of this facility will be directed to log in on the captive portal page first with a username and password, after which new users will connect to the internet with a time limit determined by the manager. The username and password given can only be used by 1 device and has a different access time depending on the number of menu purchase transactions at Mapan Coffee.

Keywords: *Security, Network, Wifi, WPA2/PSK, Password, Username, User, Device, Hotspot, Access Time, Login.*