

**PROGRAM STUDI TEKNIK INFORMATIKA**

**Analisis Keamanan Jaringan Hotspot Menggunakan Metode  
Security OpenSSL (Secure Socket Layer) Pada Kantor  
Perkebunan PTPN 7 Musi Landas.**

**Al Harits Athif**

**16142024P**

**Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer**



**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS BINA DARMA**

**2022**



**Analisis Keamanan Jaringan Hotspot Menggunakan Metode  
Security OpenSSL (Secure Socket Layer) Pada Kantor  
Perkebunan PTPN 7 Musi Landas.**

**Al Harits Athif**

**16142024P**

**Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BINA DARMA  
PALEMBANG  
2022**

**HALAMAN PENGESAHAN**

**Analisis Keamanan Jaringan Hotspot Menggunakan Metode  
Security OpenSSL (Secure Socket Layer) Pada Kantor  
Perkebunan PTPN 7 Musi Landas**

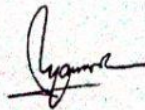
**AL HARITS ATHIF**

**16142024P**

Telah diterima sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Komputer pada Program Studi Teknik Informatika

**Palembang, 11 Oktober 2022**  
Fakultas Ilmu Komputer  
Universitas Bina Darma  
Dekan,

Pembimbing



**Dedy Syamsuar, S.Kom., M.I.T., Ph.D.**



Universitas Bina Darma  
Fakultas Ilmu Komputer

**Dr. Tata Sutabri, SKom, MMSI, MKM**

## HALAMAN PERSETUJUAN

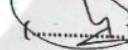
Skripsi Berjudul "Analisis Keamanan Jaringan Hotspot Menggunakan Metode Security OpenSSL (Secure Socket Layer) Pada Kantor Perkebunan PTPN 7 Musi Landas" Oleh "Al Harits Athif", telah dipertahankan di depan komisi penguji pada hari Selasa tanggal 11 Oktober 2022.

### Komisi Penguji

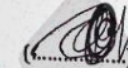
1. Ketua : Dedy Syamsuar, S.Kom., M.I.T., Ph.D.



2. Anggota : Fatoni, M.M., M.Kom.



3. Anggota : Timur Dali Purwanto, S.Kom., M.Kom.



Mengetahui,  
Program Studi Teknik Informatika  
Fakultas Ilmu Komputer  
Universitas Bina Darma  
Ketua,



Alek Wijaya, S.Kom., M.I.T.

## HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini :

**Nama : Al Harits Athif**

**NIM : 16142024P**

Dengan ini menyatakan bahwa :

1. Karya tulis saya (Skripsi) adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana) di Universitas Bina Darma atau perguruan tinggi lainnya;
2. Karya tulis ini murni gagasan, rumusan dan penelitian saya dengan arahan dari tim pembimbing;
3. Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau di publikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Saya bersedia tugas skripsi, di cek keasliannya menggunakan *plagiarism checker* serta di unggah ke internet, sehingga dapat diakses secara daring;
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidak benaran dalam pernyataan ini maka saya bersedia menerima sanksi dengan peraturan dan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, September 2022

Yang Membuat Pernyataan,

  
**Al Harits Athif**  
**16142024P**

## MOTTO DAN PERSEMBAHAN

### Motto :

- Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya. (QS. Al-Baqarah : 286).
- Tidak ada yang sulit jika engkau mencarinya melalui tuhanmu, tak ada yang mudah jika engkau mencarinya melalui dirimu sendiri.
- Ketika masalah datang hingga putus asa, bukan berarti Allah berdiam diri, Allah hanya meminta kita untuk bersabar, sholat, berdoa dan berusaha.
- Janganlah selalu membayangkan hasil yang besar, mulailah berusaha walaupun hasilnya kecil, walaupun sedikit asalkan nyata hasilnya.
- Maka apabila kamu telah selesai dari sesuatu urusanmu, kerjakanlah dengan sungguh-sungguh urusan yang lain, hanya kepada Tuhanmulah hendaknya kamu berharap. (QS. Al-Insyirah: 7-8).
- Tindakan mungkin tidak selalu membawa kebahagiaan, namun tidak ada kebahagiaan tanpa tindakan.

### Persembahan:

Dengan kerendahan hati karya tulis ilmiah ini ku persembahkan untuk :

- Bapak Dedy Syamsuar, S.Kom., M.I.T., Ph.D. Saya ucapkan terima kasih atas bimbingan dan pemikirannya ini, sehingga terselesaikannya skripsi ini.
- Orangtua saya tercinta Bapak Marsidi dan Ibu Erna Susilawati, lalu kedua mertua saya Bapak Suprianto dan Ibu Rusmiati, kemudian adik kandung saya Nurul Athifah. Merekalah yang selalu menyemangati, memotivasi, dan mempertahankan agar aku tetap

kuliah, tanpa dukungan kalian semua karya tulis ilmiah ini tidak akan terselesaikan.

- Istriku Pratiwi Suprianto, terima kasih karena sudah meluangkan waktunya untuk mendengarkan keluh kesahku, memberikan dukungan dan motivasi sehingga saya semangat dan pantang menyerah dalam mengerjakan tugas akhir ini (Skripsi).
- Teman-teman satu angkatan di Universitas Bina Darma.



## KATA PENGANTAR

Assalamuallaikum.wr.wb Puji syukur atas kehadiran Allah subhanahu wa ta'ala karena atas Ridho dan Rahmat-Nya penulis dapat menyelesaikan skripsi ini yang berjudul "Analisis Keamanan Jaringan Hotspot Menggunakan Metode Security OpenSSL (Secure Socket Layer) Pada Kantor Perkebunan PTPN 7 Musi Landas." tepat pada waktu yang telah ditentukan. Adapun laporan ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Komputer program studi Teknik Informatika Universitas Bina Darma Palembang.

Setelah mengalami berbagai proses yang sangat berharga dalam menyelesaikan skripsi ini, sehingga dapat diselesaikan dengan baik. Tentu saja penulis menyadari banyak mendapat doa, bimbingan, arahan, dan petunjuk dari berbagai pihak, sehingga sangat membantu dalam menyusun skripsi ini, maka pada kesempatan ini penulis mengucapkan terima kasih kepada :

1. Allah subhanahu wa ta'ala.
2. Kedua orangtua dan keluarga yang telah memberikan dorongan baik dalam bentuk materi maupun moral.
3. Ibu Dr. Sunda Ariana, M.Pd., M.M., selaku Rektor Universitas Bina Darma Palembang.
4. Bapak Dedy Syamsuar, S.Kom., M.I.T., Ph.D, selaku Dekan Universitas Bina Darma Palembang dan selaku dosen pembimbing dalam penulisan Skripsi.
5. Bapak Alek Wijaya, S. Kom, M.I.T selaku Ketua Program Studi Teknik Informatika.
6. Bapak dan Ibu Dosen Universitas Bina Darma Palembang.
7. Seluruh staf, karyawan dan karyawan Universitas Bina Darma Palembang.
8. Teman-teman seangkatanku Alhimni, Khoirul Setiawan, & M. Romadhony.



Penulis menyadari dalam menyusun Skripsi ini masih terdapat kesalahan dan kekurang, maka kritikan dan saran yang bersifat membangun dari berbagai pihak sangat diharapkan untuk perbaikan di masa yang akan datang. Akhir kata penulis mengucapkan rasa syukur serta terima kasih dan semoga Skripsi ini dapat bermanfaat dan berguna bagi kita semua.

Palembang, September 2022

Penulis



## ABSTRAK

Untuk keamanan jaringan *wireless* pada perangkat *access point* metode *security* yang sering digunakan adalah metode *WEP/WPA/WPA2*, hampir semua pengguna jaringan *wireless* rata-rata mengimplementasikan perangkat *access point* nya dengan menggunakan metode tersebut. Metode tersebut dikenal baik dalam hal kemampuan pengamanan *security* jaringan *wireless* tetapi metode *WEP/WPA/WPA2* masih bisa ditembus oleh *software hacking* dengan metode *brute-force attack* dan *dictionary*, dimana *software* tersebut banyak terdapat di internet dan kelemahan berikutnya adalah metode tersebut hanya menggunakan *password* saat akan terkoneksi perangkat *access point* sehingga *password* tersebut mudah tersebar jika salah satu *user* memberi *password* nya kepada *user* lain dan dengan mudah diketahui oleh *user* lain begitu seterusnya. Metode *SSL (Secure Socket Layer)* telah banyak digunakan untuk pengamanan *website* yang membutuhkan pengamanan tingkat tinggi seperti *website* perbankan, *hosting*, jual beli *online* dan sebagainya yang biasanya pada *website* tersebut menggunakan *protocol HTTPS (Hyper Text Transfer Protocol Secure)*. Implementasi *server gateway* yang berfungsi sebagai *router internet* baik pada jaringan kabel maupun *wireless*. Hal ini menjadi sebuah solusi dimana dapat membantu komunikasi antar komputer serta sistem keamanan *internet hotspot* dimana pengguna akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan *Secure Socket Layer (SSL)*.

**Kata Kunci :** *Security, Hotspot, Server, SSL, HTTPS*

## **ABSTRACT**

*For wireless network security on access point devices, the security method that is often used is the WEP/WPA/WPA2 method, almost all wireless network users on average implement their access point devices using this method. This method is well known in terms of the ability to secure wireless network security but the WEP/WPA/WPA2 method can still be penetrated by hacking software with the brute-force attack and dictionary methods, where the software is widely available on the internet and the next weakness is that this method only uses passwords when will be connected to the access point device so that the password is easily spread if one user gives his password to another user and it is easily known by other users and so on. The SSL (Secure Socket Layer) method has been widely used for securing websites that require a high level of security such as banking websites, hosting, buying and selling online and so on which usually use the HTTPS (Hyper Text Transfer Protocol Secure) protocol. Implementation of a gateway server that functions as an internet router on both wired and wireless networks. This is a solution that can help communication between computers and a hotspot internet security system where users will first log in by entering a user name and password when accessing the internet using the Secure Socket Layer (SSL) security method.*

**Keywords :** Security, Hotspot, Server, SSL, HTTPS

## DAFTAR ISI

HALAMAN COVER.....	
HALAMAN PENGESAHAN .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PERNYATAAN.....	iii
MOTTO DAN PERSEMBAHAN.....	iv
KATA PENGANTAR.....	vi
ABSTRAK.....	viii
DAFTAR ISI .....	x
DAFTAR GAMBAR.....	xii
DAFTAR TABEL .....	xiii
DAFTAR LAMPIRAN.....	xiv
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
<b>1.1 Latar Belakang .....</b>	<b>1</b>
<b>1.2 Rumusan Masalah.....</b>	<b>3</b>
<b>1.3 Ruang Lingkup .....</b>	<b>3</b>
<b>1.4 Tujuan dan Manfaat .....</b>	<b>3</b>
<b>1.5 Metodologi Penelitian .....</b>	<b>5</b>
a. Tahap pertama ( <i>Diagnosing</i> ).....	5
b. Tahap kedua ( <i>Action Planning</i> ).....	6
c. Tahap ketiga ( <i>Action Taking</i> ) .....	6
d. Tahap keempat ( <i>Evaluating</i> ).....	6
e. Tahap kelima ( <i>Learning / Reflecting</i> ).....	7
<b>1.6 Sistematika Penulisan .....</b>	<b>7</b>
<b>BAB II LANDASAN TEORI.....</b>	<b>9</b>
<b>2.1 Analisis.....</b>	<b>9</b>
<b>2.2 Jaringan Komputer.....</b>	<b>10</b>
<b>2.3 WLAN (Wireless Local Area Network).....</b>	<b>11</b>
<b>2.4 Security Wireless .....</b>	<b>12</b>

<b>2.5 MikroTik Router</b> .....	<b>19</b>
2.5.1 Sejarah MikroTik RouterOS.....	19
2.5.2 Jenis -jenis Mikrotik.....	20
2.5.3 Level Router OS dan Kemampuannya.....	20
2.5.4 Fitur – fitur Mikrotik.....	21
<b>2.6 Hotspot Gateway dan User Manager</b> .....	<b>24</b>
<b>2.7 Secure Socket Layer (SSL)</b> .....	<b>25</b>
<b>2.8 Algoritma Simetris</b> .....	<b>26</b>
<b>2.9 Arsitektur SSL</b> .....	<b>27</b>
<b>2.10 Tool Wireshark</b> .....	<b>27</b>
<b>BAB III METODOLOGI PENELITIAN</b> .....	<b>29</b>
<b>3.1 Waktu dan Tempat Penelitian</b> .....	<b>29</b>
<b>3.2 Metode Penelitian</b> .....	<b>29</b>
3.2.2.1 Analisis Kebutuhan .....	31
3.2.2.2 Perancangan Topologi Pengujian.....	32
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....	<b>34</b>
<b>4.1 Hasil</b> .....	<b>34</b>
<b>4.2 Pembahasan</b> .....	<b>38</b>
<b>BAB V PENUTUP</b> .....	<b>55</b>
<b>5.1 Kesimpulan</b> .....	<b>55</b>
<b>5.2 Saran</b> .....	<b>55</b>

**DAFTAR PUSTAKA**

**LAMPIRAN**

## DAFTAR GAMBAR

<b>Gambar 2.1</b> Proses Enkripsi dan Deskripsi Algoritma Simetris.....	26
<b>Gambar 3.1</b> Siklus Metode Action Reserch .....	30
<b>Gambar 3.2</b> Topologi Pengujian .....	33
<b>Gambar 3.3</b> Implementasi Wireless Hotspot dengan SSL.....	33
<b>Gambar 4.1</b> Instalasi Openssl .....	34
<b>Gambar 4.2</b> Membuat File Kunci .....	35
<b>Gambar 4.3</b> Membuat Kunci Request.....	35
<b>Gambar 4.4</b> Membuat File Sertifikat dan File Kunci.....	35
<b>Gambar 4.5</b> Mengupload Certificate dan Key Security Hotspot Mikrotik .....	36
<b>Gambar 4.6</b> Mengimpor File Certificate .....	36
<b>Gambar 4.7</b> Mengaktifkan Service SSL Menggunakan Certificate .....	36
<b>Gambar 4.8</b> Mengaktifkan Service SSL Menggunakan Certificate .....	37
<b>Gambar 4.9</b> Tampilan Login Hotspot Mikrotik.....	37
<b>Gambar 4.10</b> Tampilan Protocol TLS .....	39
<b>Gambar 4.11</b> Tampilan Enkripsi SSL.....	39
<b>Gambar 4.12</b> Ethernet Protocol Wireshark.....	40
<b>Gambar 4.13</b> Internet Protocol Wireshark.....	40
<b>Gambar 4.14</b> Transmission Control Protocol .....	41
<b>Gambar 4.15</b> Paket Header Secure Sockets Layer .....	42
<b>Gambar 4.16</b> Paket Header Tanpa Secure Sockets Layer .....	43
<b>Gambar 4.17</b> Paket Ethernet Protocol Wireshark tanpa SSL.....	43
<b>Gambar 4.18</b> Paket Transmission Control Protocol tanpa SSL .....	44
<b>Gambar 4.19</b> Paket Hypertext Transfer Protocol.....	45
<b>Gambar 4.20</b> Setting Interface Card Komputer Penyusup .....	45
<b>Gambar 4.21</b> Scan Host dan Hasil Scanning .....	46
<b>Gambar 4.22</b> Mengaktifkan Arp Poisoning .....	47
<b>Gambar 4.23</b> Hasil Sniffing Ettercap.....	48
<b>Gambar 4.24</b> Tampilan Mac Address Asli Penyusup .....	49
<b>Gambar 4.25</b> Hasil Perubahan Mac Address .....	50

## DAFTAR TABEL

**Tabel 4.1** Hasil pengukuran *delay* responsibilitas *security* WPA2.....52

**Tabel 4.2** Hasil pengukuran *delay* responsibilitas *security* SSL.....53



## DAFTAR LAMPIRAN

- Lampiran 1** Halaman Pengajuan Judul
- Lampiran 2** Surat Pengantar Izin Penelitian dari Universitas Bina Darma
- Lampiran 3** Surat Balasan Izin Penelitian dari Objek
- Lampiran 4** Surat Keterangan Pembimbing
- Lampiran 5** Lembar Konsultasi Proposal Skripsi
- Lampiran 6** Lembar Perbaikan Proposal Skripsi
- Lampiran 7** Lembar Konsultasi Komprehensif
- Lampiran 8** Lembar Perbaikan Komprehensif
- Lampiran 9** Surat Keterangan Lulus Ujian Proposal Skripsi
- Lampiran 10** Surat Keterangan Lulus Ujian Komprehensif
- Lampiran 11** Hasil Turnitin