

## **TUGAS AKHIR**

### **PENERAPAN PROTOKOL SSL PADA AUTENTIFIKASI WEB UNTUK PENGAMANAN DARI MAN IN MIDDLE ATTACK(MITM)**

Diajukan Untuk Memenuhi Persyaratan Guna Meraih Gelar Sarjana Komputer  
Teknik Informatika Universitas Muhammadiyah Jember



Harits Wahyu H  
1510651168

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH JEMBER**

**2017**

**HALAMAN PENGESAHAN**

**PENERAPAN PROTOKOL SSL PADA AUTENTIFIKASI WEB UNTUK  
PENGAMANAN DARI MAN IN MIDDLE ATTACK (MITM)**

**Harits Wahyu Hidayatullah  
1510651168**

Telah mempertanggung jawabkan Laporan Tugas Akhirnya pada Sidang Tugas Akhir Tanggal 25 Juli 2017 sebagai salah satu syarat kelulusan dan mendapatkan gelar Sarjana Komputer (S.Kom) di Universitas Muhammadiyah Jember

**Disetujui Oleh,**

**Dosen Pembimbing,**

**Triawan Adi Cahyanto, S. Kom, M.Kom  
NPK. 12 03 719**

**Dosen Penguji I,**

**Dosen Penguji II,**

**Ari Eko Wardoyo, S.T, M.Kom  
NIP. 19750214 200501 1 001**

**Taufiq Timur W, S.Kom, M.Kom  
NPK. 08 04 486**

**Mengesahkan,**

**Mengetahui,**

**Dekan Fakultas Teknik**

**Ketua Program Study Teknik  
Informatika**

**Ir. Suhartinah, M.T  
NPK. 95 05 264**

**Yeni Dwi Rahayu, S.ST, M.Kom  
NPK. 11 03 590**

## HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Harits Wahyu Hidayatullah

NIM : 1510651168

Fakultas : Teknik

Jurusan : Teknik Informatika

Dengan ini menyatakan bahwa Tugas Akhir dengan judul: **Penerapan Protokol SSL Pada Autentifikasi Web Untuk Pengamanan Dari Man In Middle Attack (MITM)**, murni merupakan Karya Ilmiah Sendiri serta Belum Pernah di publikasikan oleh siapapun dan di manapun.

Demikian pernyataan ini saya buat tanpa adanya paksaan dari pihak manapun untuk digunakan sebagaimana mestinya.

Jember,.....

Harits Wahyu H  
1510651168

## **MOTO**

“Ilmu tanpa agama adalah lumpuh, agama tanpa ilmu adalah buta”

(Albert Einstein)

“Iman tanpa ilmu bagaikan lentera di tangan bayi. Namun ilmu tanpa iman, bagaikan lentera di tangan pencuri.”

(Buya Hamka)

“Bacalah, dan Tuhanmulah Yang Maha Pemurah”

(QS. Al-Alaq. 3)

## **HALAMAN PERSEMBAHAN**

Atas rahmat dan karunia Puji Syukur kehadiran Allah SWT untuk segala limpahan rahmat-Nya sehingga Tugas Akhir ini dapat terselesaikan. Shalawat serta salam tetap tercurahkan kepada sang pelipur lara yang setetes embun syafaat kita nantikan darinya kelak di hari akhir yaitu baginda Nabi Mumammad SAW karena, kesabaran dan kegigihan beliau telah membawa umatnya dari zaman jahiliyah menuju jalan yang terang benderang yaitu ad-dinienul islam.

Dengan ketulusan dihati, saya persembahkan Tugas Akhir ini untuk:

- 1) Ayahanda dan Ibunda tercinta, yang selalu memberikan dukungan dan doa dalam setiap langkah hidupku
- 2) Guru beserta Dosen yang telah mengajriku ilmu dari sekolah dasar hingga bangku perkuliahan dengan semangat dedikasi penuh kesabaran
- 3) Keluarga, Saudara beserta teman – teman yang telah memberikan warna dan pengalaman dalam hidup ini
- 4) Almamater Fakultas Teknik, Universitas Muhammadiyah Jember.

## KATA PENGANTAR

Puji syukur kehadiran Allah SWT atas limpahan rahmat dan hidayah sehingga penelitian dengan judul **“PENERAPAN PROTOKOL SSL PADA AUTENTIFIKASI WEB UNTUK PENGAMANAN DARI MAN IN MIDDLE ATTACK (MITM)”** dapat terselesaikan. Penulis menyadari bahwa dalam penelitian maupun penulisan laporan ini banyak pihak yang telah membantu menyelesaikannya. Maka dari itu, saya ucapkan terima kasih kepada:

1. Ibu Ir. Suhartinah, ST., MT., selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember
2. Ibu Yeni Dwi Rahayu, S.ST., M.Kom., selaku Ketua Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember
3. Bapak Triawan Adi Cahyanto, M. Kom. selaku dosen pembimbing yang telah banyak memberi petunjuk dan arahan
4. Bapak Ari Eko W, M.Kom. dan Taufiq Timur W, M.Kom. selaku dosen penguji.

Jember,.....

Penulis

## DAFTAR ISI

Cover .....	i
Halaman Pengesahan.....	ii
Halaman Pernyataan .....	iii
Moto.....	iv
Halaman Persembahan.....	v
Kata Pengantar .....	vi
Daftar Isi .....	vii
Daftar Tabel.....	x
Daftar Gambar .....	xi
Abstrak.....	xii
Abstract.....	xiii

## BAB I LATAR BELAKANG

1.1. Rumusan Masalah .....	1
1.2. Batasan Masalah .....	2
1.3. Tujuan .....	3
1.4. Manfaat .....	3

## BAB II DAFTAR PUSTAKA

2.1. ARP( <i>Address Resolution Protocol</i> ) .....	4
2.1.1. Manfaat Arp Protocol .....	4
2.1.2. Kelemahan ARP protocol .....	5
2.2. MITM ( <i>Man in The Middle Attack</i> ) .....	6
2.3. SSL( <i>Secure Socket Layer</i> ) .....	7
2.3.1. Sertifikat Secure Socket Layer (SSL) .....	8
2.4. Web Server .....	8
2.4.1. Apache .....	8
2.5. Wireshark .....	9

2.5.1. HTTP ( Hypertext Transfer Protocol ) .....	9
2.6. <i>Captive portal</i> .....	9
2.6.1. CoovaChilli .....	11
2.6.2. Freeradius Server .....	12
2.6.3. EasyHotspot .....	14

### **BAB III METODE PENELITIAN**

3.1. Studi Literatur .....	15
3.2. Rancang Bangun Sistem Jaringan Captive Portal .....	16
3.2.1. Konfigurasi Port Forwarding .....	17
3.2.2. Konfigurasi Chillispot.....	17
3.2.3. Konfigurasi Apache .....	18
3.2.4. Konfigurasi Freeradius.....	18
3.2.5. Konfigurasi MySQL .....	20
3.2.6. Konfigurasi Firewall .....	21
3.2.7. Menambahkan Hash Pada Login Script Captive Portal.....	22
3.3. Mitm Password Sniff Pada Autentikasi Protokol HTTP .....	24
3.3.1. Konfigurasi chillispot.....	25
3.3.2. Melakukan Scan IP address .....	25
3.3.3. Memastikan Target .....	26
3.3.4. Melakukan password sniffing .....	27
3.3.5. Analisa Trafick.....	29
3.4. Mitm Password Sniff Pada Autentikasi Protokol HTTPS/SSL Saat Client Mengabaikan Error Certificate .....	29
3.5. Mitm Password Sniff Pada Autentikasi Protokol HTTP Setelah Menambah Fungsi Hash .....	30
3.6. Hasil Analisa.....	30



## **BAB IV HASIL DAN PEMBAHASAN**

4.1. Mitm Password Sniff Pada Autentikasi Protokol HTTPS/SSL Saat Client Mengabaikan Error Certificate .....	19
4.1.1. Konfigurasi Chillispot.....	20
4.1.2. Hasil Password Sniffing.....	32
4.1.3. Hasil Analisa Traffick.....	32
4.2. Mitm Password Sniff Pada Autentikasi Protokol HTTP Setelah Menambah Fungsi Hash .....	34
4.2.1. Konfigurasi Chillispot.....	34
4.2.2. Hasil Password Sniffing.....	35
4.2.3. Hasil Analisa Traffick.....	36
4.3. Hasil Analisa.....	37

## **BAB V KESIMPULAN**

5.1. Kesimpulan .....	38
5.2. Saran .....	38
<b>Daftar Pustaka.....</b>	<b>39</b>

## DAFTAR TABEL

Tabel 2.1 Model TCP/IP .....	5
Tabel 3.1 <i>Software CP server</i> dan Fungsinya .....	16
Tabel 3.2 Konfigurasi IP .....	17
Tabel 3.3 Penggunaan Perangkat Lunak .....	24
Tabel 4.1 Perbandingan http dan https pada autentikasi captive portal .....	37

## DAFTAR GAMBAR

Gambar 2.1 Cara Kerja Arp Protocol.....	4
Gambar 2.2 Gambaran MITM .....	6
Gambar 2.3 Radius AAA .....	13
Gambar 3.1 Tahapan penelitian .....	15
Gambar 3.2 Topologi Pengujian .....	16
Gambar 3.3 Konfigurasi chillispot.firewall .....	22
Gambar 3.4 konfigurasi uamserver .....	23
Gambar 3.5 Teknis Serangan .....	24
Gambar 3.6 Scanning ip <i>address</i> .....	25
Gambar 3.7 Melihat ip target .....	26
Gambar 3.8 Memasukkan ip target ke <i>table APR</i> .....	26
Gambar 3.9 Http Password Sniff list .....	27
Gambar 3.10 Melakukan autentikasi.....	28
Gambar 3.11 Password Tercuri.....	28
Gambar 3.12 Analisa Trafick http.....	29
Gambar 4.1 Error Certificate.....	31
Gambar 4.2 Tidak ditemukan data username dan password.....	32
Gambar 4.3 Data http pada port 3990 .....	33
Gambar 4.4 data aplikasi pada ssl.....	34
Gambar 4.5 Hasil Sniffing .....	35
Gambar 4.6 Analisa HTTP dengan hash password.....	36

## Daftar Pustaka

- Albertus dwiyoga W. (2005). Membangun Mail server anda dengan Fedora dan Qmail. Elex Media Komputindo.
- Arran Cudbard-Bell. ( 2016). FreeRADIUS. Site : <http://wiki.freeradius.org/>
- Chen, W., Wu, Q., & Wu, Q. (2010). A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal, 66–69.
- Cheshire, S. (2008). RFC 5227 - IPv4 Address Conflict Detection". Internet Engineering Task Force. Why Are ARP Announcements Performed Using ARP Request Packets and Not ARP Reply Packets?
- Chillispot organisation. Chillispot Captive Portal. Website : <http://www.chillispot.org/>.
- Douglas E. Comer (1993). Internetworking with TCP/IP – Principles, Protocols and Architecture. ISBN 86-7991-142-9
- EasyHotspot Team. (2010). About Easyhotspot. Website : <http://easyhotspot.inov.asia/index.php/about>
- Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (1999). Hypertext Transfer Protocol -- HTTP/1.1. IETF. RFC 2616.
- Hendriana, Y. (2012). Evaluasi Implementasi Keamanan Jaringan Virtual Private, 5, 132–142.
- Herwin. (2015). Freeradius - Overview and Features. Network Radius. <http://wiki.freeradius.org/Overview-and-Features> (2015-11-26)
- Irwan se sh, Onno W. Purbo. (2011).WiFi: HotSpot - CoovaChilli Pendahuluan. Telkomspeedy. Blog Url : [http://opensource.telkomspeedy.com/wiki/index.php/WiFi:\\_HotSpot\\_-\\_CoovaChilli\\_Pendahuluan](http://opensource.telkomspeedy.com/wiki/index.php/WiFi:_HotSpot_-_CoovaChilli_Pendahuluan).
- Lockhart, Andrew (2007). Network security hacks. O'Reilly. p. 184. ISBN 978-0-596-52763-1.
- Munir,R, Ir, M.T.(2004) Kriptografi dalam Kehidupan Sehari - hari . ITB – Departemen Teknik Informatika.

[http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Kriptografi%20dalam%20Kehidupan%20Sehari-hari%20\(Bagian%202\).pdf](http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Kriptografi%20dalam%20Kehidupan%20Sehari-hari%20(Bagian%202).pdf)

Prasetyo, I. (2007). S S L ( S e c u r e S o c k e t L a y e r ), 1–12.  
IlmuKomputer.Com.

Perkins, C. (1996). "RFC 2002 - IP Mobility Support". Internet Engineering Task Force.

QuarkXpress team. (2006). Why You Need an SSL Certificate. Starfield Technologies Secure Certificate Services.  
<https://products.secureserver.net/SSLMarketingGuide.pdf>.

Raf Knowledge. (2010). Trik Memonitor Jaringan. Elex Media Komputindo. Jakarta.

Ramachandran, Vivek & Nandi, Sukumar (2005). "Detecting ARP Spoofing: An Active Technique". In Jajodia, Suchil & Mazumdar, Chandan. *Information systems security: first international conference, ICISS 2005, Kolkata, India, December 19-21, 2005*.

Wahana Komputer. (2010). Tip Jitu Optimasi Jaringan Wi-Fi. Andi Offset, CV. Yogyakarta.