Penerapan Protokol SSL pada Autentifikasi Web untuk Pengamanan dari Man in Middle Attack (MITM)

Harits Wahyu Hidayatullah
Harits.wahyu.hid@gmail.com

Pembimbing : Triawan Adi Cahyanto, S. Kom, M.Kom
Teknik Informatika – Universitas Muhammadiyah Jember

Abstraksi

Penelitian ini berfokus pada dua metode autentikasi dengan protocol http dan https. Autentikasi https pada captive portal yang menampilkan error sertifikat akan diuji dengan MITM password sniff dan akan dibandingkan dengan autentikasi captive portal dengan protocol http dengan keamanan hash password dengan pengujian yang sama. Hal tersebut akan memberikan gambaran penggunaan protocol yang dapat dipilih oleh seorang teknisi jaringan hotspot untuk mempertimbangkan keamanan dari MITM password sniff dan error sertifikat pada browser *client*.

Kata Kunci : Security, SSL ,HTTPS,TLS , MITM , Man in Middle, Autentikasi, Captive Portal, Firewall.

I. Pendahuluan

A. Captive Portal

Captive portal awalnya didesain untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (open network). Captive portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi.

Beberapa hal yang perlu diperhatikan, bahwa Captive portal hanya melakukan tracking koneksi cilent berdasarkan IP dan MAC address setelah melakukan otentikasi. Hal ini membuat Captive portal masih mungkin digunakan tanpa otentikasi karena IP dan MAC address dapat di-spoofing. Dengan demikian, serangan dengan melakukan spoofing IP dan MAC. Ketika ada cilent yang akan terhubung ke AP buatan Anda dapat dibelokkan trafik ke AP sebenarnya. Tidak jarang Captive portal yang dibangun pada suatu hotspot memiliki kelemahan pada konfigurasi atau desain jaringannya. Misalnya, otentikasi masih menggunakan plain text (http), manajemen jaringan dapat diakses melalui wireless (berada pada satu network), dan masih banyak lagi. Kelemahan lain dan Captive portal adalah bahwa komunikasi data atau trafik ketika sudah melakukan otentikasi (terhubung jaringan) akan dikirimkan masih belum terenkripsi, sehingga dengan mudah dapat disadap oleh para hacker. Untuk itu, perlu berhati-hati melakukan koneksi pada jaringan hotspot, agar mengusahakan menggunakan komunikasi protokol yang aman seperti https, pop3s, ssh, imaps, dan seterusnya. (Wahana Komputer. 2010).

B. Https Pada Captive Portal

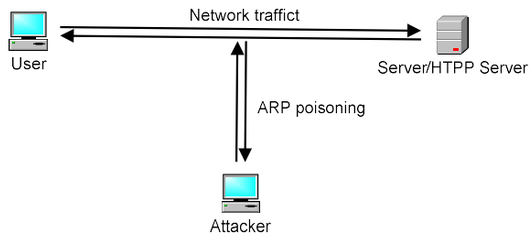
Penerapan protocol https memiliki permasalahan saat diterapkan pada autentikasi firewall atau sering disebut captive portal server yang mengautentikasi calon pengguna layanan akses internet berbasis web/http. Pada saat autentikasi client dilakukan pada protocol https, browser client yang berfungsi menampilkan interface halaman login akan menampilkan certificate error meskipun certificate SSL *server captive portal* telah terdaftar pada penyedia layanan otorisasi *certificate* SSL. *Client* tetap dapat melakukan proses autentikasi dengan mengabaikan peringatan *certificate error* yang artinya *client* mengabaikan validasi sertifikat SSL. *Error certificate* baru akan hilang setelah client diautentikasi oleh *server captive portal.*

Hal lain yang terjadi adalah autentikasi *captive portal hotspot* tidak lagi menggunakan https. Penggunaan https pada autentikasi captive portal dirasa akan merepotkan client. Permasalahan tersebutlah yang akan membuat seorang teknisi memikirkan penggunaan http dibanding https.

C. MITM(Man-in-the-middle-attack)

Man-in-the-middle-attack atau MITM adalah salah satu serangan pada jaringan dengan akses terbuka misalnya HOTSPOT. Dengan cara ini akan dilakukan penyadapan username dan

password.

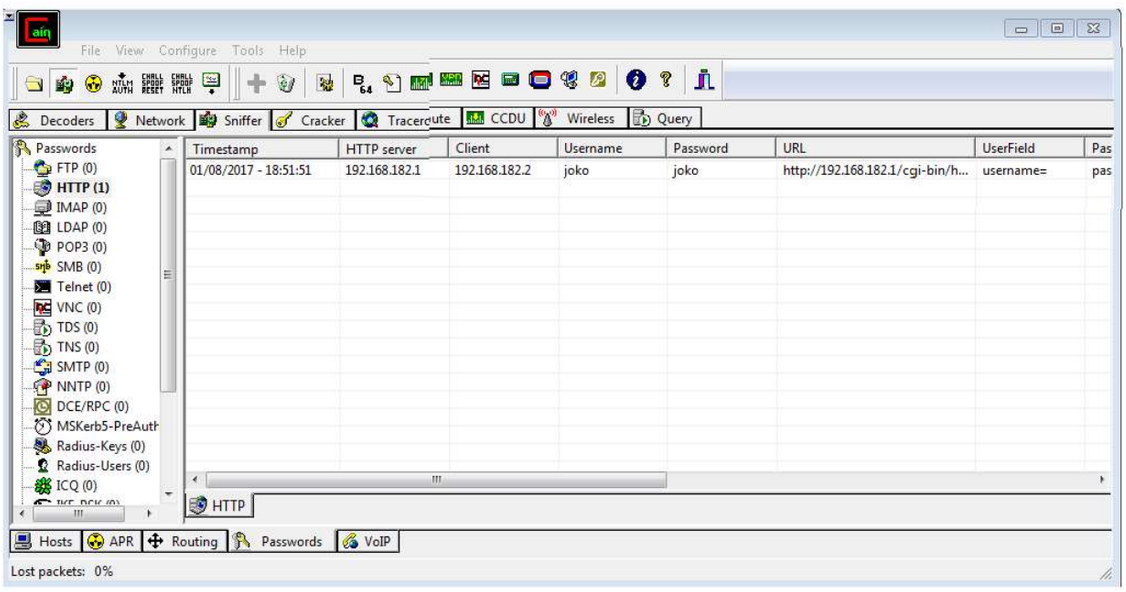


Gambar 1. Gambaran MITM

D. Cain & Abel MITM (Man-in-the-middle-attack) pada autentikasi captive portal.

Untuk melakukan proses autentikasi pertama buka browser client(target), dengan mengetikan google.com/ atau login/ pada tab url. Captive portal server akan meredirect dns request ke url halaman login. Setelah halaman login muncul masukkan username dan password lalu klik login.

Username dan password client captive portal akan muncul pada tab password cain & abel setelah cain abel mengaktifkan fitur sniffing dan telah melakukan scanning.



Hasil Sniffing password

E. Penggunaan http untuk mengamankan dari MITM pada captive portal.

Akses https captive portal akan menampilkan error . Hal ini disebabkan captive portal tidak memberikan hak akses internet sebelum user di autentikasi. Client tetap dapat melanjutkan dengan menekan *button* lanjut yang biasanya disediakan browser untuk mengakses mengabaikan peringatan keamanan integritas data. Uji MITM password sniffing ini dilakukan dengan mengabaikan dengan mengabaikain peringatan *certificate error*. Hal ini dilakukan untuk mengetahui apakah autentikasi tetap aman dari serangan *password sniffing* meskipun client mengabaikan peringatan *certificate error.*

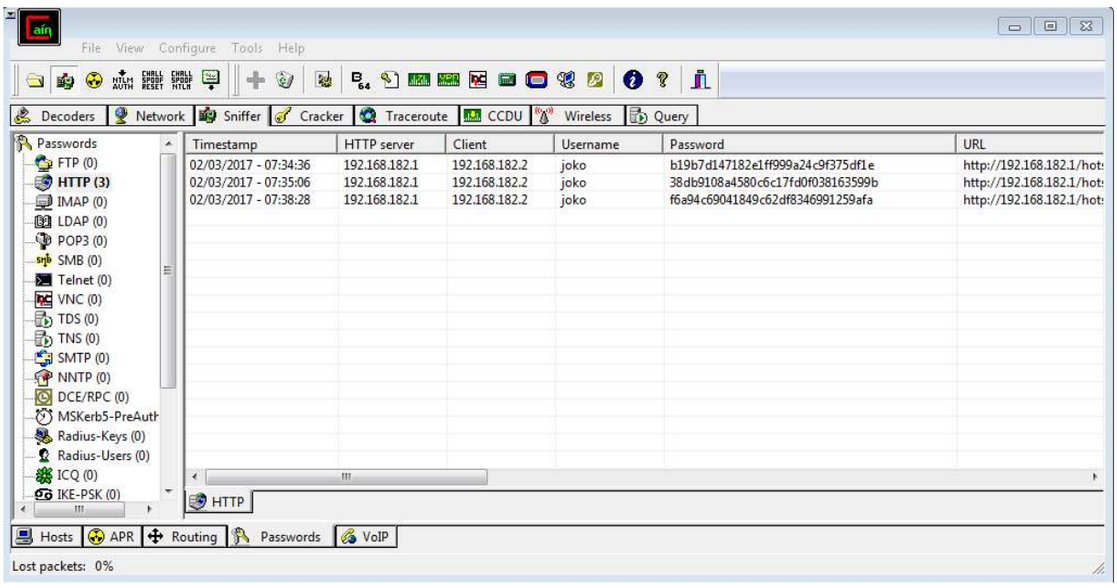
Pertukaran data yang dilayani apache pada port 80 tidak ditemukan. Data yang ada hanya pada http port 3990. Data tersebut adalah data pertukaran *service chillispot*. Header yang muncul hanya username dengan data lain yang mirip data hasil hash.

Cain&Abel tidak dapat menemukan data username dan password seperti pada uji http. Artinya data http telah benar benar diamankan dengan ssl menjadi https. Jadi autentikasi saat client mengabaikan peringatan error certificate telah **aman dari MITM password sniffing.**

F. Mitm Password Sniff Pada Autentikasi Protokol HTTP Setelah Menambah Fungsi Hash

Uji coba ini adalah uji coba pada autentikasi http dengan menambahkan fungsi keamanan. Fungsi keamanan ini akan mengamankan data password client. Jika data password client berhasil diamankan maka penggunaan http dibanding https yang menampilkan *error certificate* mungkin keputusan yang baik.

G. Hasil Sniffing



MITM Password sniffing oleh cain&Abel berhasil mendeteksi data username dan passoword. Namun password yang muncul pada list password sniffing adalah hasil hash dinamis. Artinya data password telah terlindungi dengan cukup baik.

No	Protokol/Cara autentikasi yang digunakan	Kelebihan	Kekurangan
1.	Http *Raw*	Mudah diterapkan pada sisi *server* atau klien	*User* dan *Password* mudah dicuri
2.	Https/SSL	Keamanan Lebih dijamin.	Memerlukan installasi sertifikat pada sisi klien untuk menjamin Integritas server.
3.	Http dengan keamanan kriptografi	Password Aman	Integritas server dipertanyakan keamanannya

H. Kesimpulan

Dari hasil uji coba dan pengamatan yang telah dilakukan pada bab IV dapat ditarik kesimpulan.

1) Peringatan *certificate error* pada *browser client* yang diabaikan tetap aman dari serangan MITM *password sniffing* (*eavesdropping*) .

2) Melakukan *hash password* pada autentikasi *captive portal server* pada sisi http dapat menghindari celah MITM *password sniffing*(*eavesdropping*).

3) Autentikasi http dengan pengamanan menggunakan kriptografi hash dapat menggantikan penggunaan autentikasi https jika client lebih memilih mengabaikan integritas *server* yang mengharuskan installasi *certificate.*

I. Saran

Adapun saran yang dapat diberikan setelah penelitian ini jika ingin menguji autentikasi captive portal melalui https.

1) Uji coba keamanan integritas *server captive portal*, Hal yang dapat dilakukan untuk membuktikan keamanan integritas *server* adalah MITM *routing*/*redirecting* pada proses autentikasi captive portal server saat menggunakan http dengan hash password, https dengan mengabaikan *error certificate*, keamanan penggunaan DNS Server dan penggunaan Alamat IP static untuk *alamat server captive portal*.

2) Melakukan survei pada user, akan lebih nyaman memilih menggunakan http dengan keamanan hash atau penggunaan https dengan install certificate manual pada proses autentikasi captive portal

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.

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

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.