ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

Skripsi

oleh:

NATHANAEL DHARMAWAN

71170240

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

2022

ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

Skripsi

Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh
NATHANAEL DHARMAWAN
71170240

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2022

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI/TESIS/DISERTASI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Kristen Duta Wacana, saya yang bertanda tangan di bawah ini:

Nama	:	Nathanael Dharmawan
NIM	:	71170240
Program studi	:	Informatika
Fakultas	:	Teknolog Informasi
Jenis Karya	:	Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Kristen Duta Wacana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Kristen Duta Wacana berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama kami sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

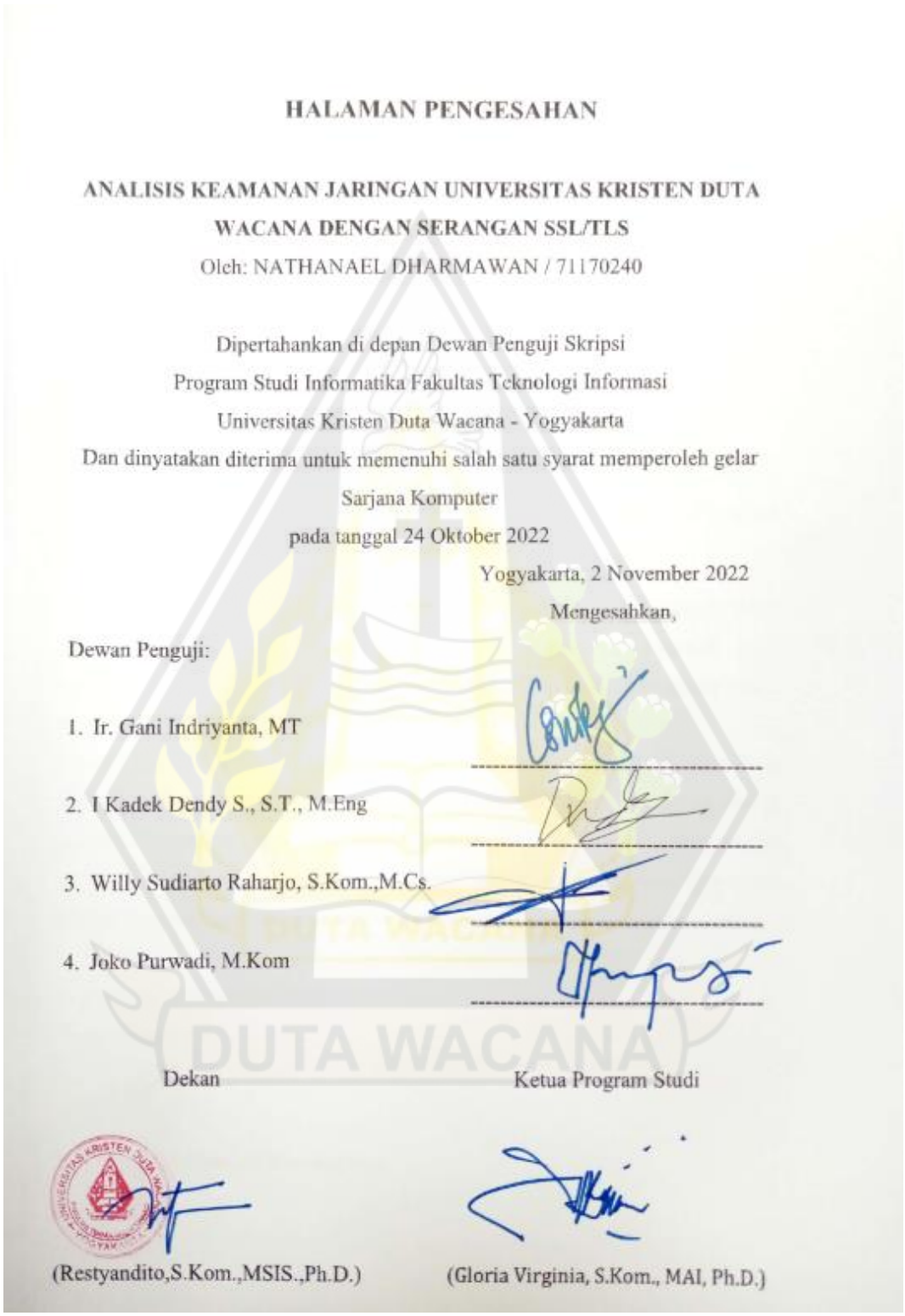
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Yogyakarta
Pada Tanggal : 1 November 2022

Yang menyatakan

(Nathanael Dharmawan)
NIM.71170240

HALAMAN PENGESAHAN



HALAMAN PENGESAHAN

ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

Oleh: NATHANAEL DHARMAWAN / 71170240

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 24 Oktober 2022

Yogyakarta, 2 November 2022

Mengesahkan,

Dewan Penguji:

1. Ir. Gani Indriyanta, MT
2. I Kadek Dendy S., S.T., M.Eng
3. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
4. Joko Purwadi, M.Kom

Dekan

(Restyandito,S.Kom.,MSIS.,Ph.D.)

Ketua Program Studi

(Gloria Virginia, S.Kom., MAI, Ph.D.)

HALAMAN PERSETUJUAN

HALAMAN PERSETUJUAN

Judul Skripsi	:	ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS
Nama Mahasiswa	:	NATHANAEL DHARMAWAN
NIM	:	71170240
Mata Kuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Ganjil
Tahun Akademik	:	2022/2023

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal, 3 Oktober 2022

Dosen Pembimbing I	Dosen Pembimbing II
Ir. Gani Indriyanta, MT	I Kadek Dendy S., S.T., M.Eng

I Kadek Dendy Senapartha
Reason : Ok untuk pendadaran
2022.10.03 16:36:48 +07'00'

Ket: persetujuan pendadaran!

PERNYATAAN KEASLIAN SKRIPSI

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 9 November 2022

NATHANAEL DHARMAWAN

71170240

KATA PENGANTAR

Segala puji dan syukur kepada Tuhan yang maha kasih, karena atas segala rahmat, bimbingan, dan bantuan-Nya maka akhirnya Skripsi dengan judul ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS ini telah selesai disusun.

Penulis memperoleh banyak bantuan dari kerja sama baik secara moral maupun spiritual dalam penulisan Skripsi ini, untuk itu tak lupa penulis ucapkan terima kasih yang sebesar-besarnya kepada:

1. Tuhan yang memberi Kasih Karunia dan Kebenaran dalam penulis melalui setiap masa dalam hidup,
2. Keluarga tercinta: yang dimana Tuhan menaruh, mempercayakan untuk bertumbuh dan menjadi berkat serta saling memberi dukungan bersama,
3. Bapak Restyandito S.Kom, MSIS., Ph.D selaku Dekan FTI, yang senantiasa memberi contoh serta mengusahakan yang terbaik bagi Mahasiswa/i nya,
4. Ibu Gloria Virginia S.Kom., MAI., Ph.D selaku Kaprodi Informatika, yang telah mengupayakan yang terbaik untuk prodi Informatika,
5. Bapak Ir. Gani Indriyanta, MT selaku Dosen Pembimbing 1, yang telah memberikan arahan, motivasi, ilmunya dan dengan penuh kesabaran membimbing penulis,
6. Bapak I Kadek Dendy Senapartha. S. T., M. Eng selaku Dosen Pembimbing 2, yang telah memberikan ilmu,waktu dan kesabaran dalam membimbing penulis,
7. Bapak Willy Sudiarto Raharjo, S.Kom., M.Cs yang telah bersedia meluangkan waktu untuk penulis untuk memberi masukan pada penelitian penulis,
8. Teman teman terkasih, Yulius, Riel, Paul, mahasiswa/i praktikum Jarkom dan Inlan, dan teman teman perkuliahan yang telah memberi dukungan moril serta menjadi tempat bertumbuh bersama dalam pengetahuan maupun karakter,

9. Keluarga PPLK (Pak Abet, Pak Arif, Pak Agung, Kak Richard) yang telah memberi dukungan tempat, *snack* dan fasilitas bagi penulis untuk melakukan penelitian,
10. Pihak Puspindika yang telah memberikan ijin bagi penulis untuk melakukan penelitian jaringan naungan Puspindika.

Laporan proposal/skripsi ini tentunya tidak lepas dari segala kekurangan dan kelemahan, untuk itu segala kritikan dan saran yang bersifat membangun guna kesempurnaan skripsi ini sangat diharapkan. Semoga proposal/skripsi ini dapat bermanfaat bagi pembaca semua dan lebih khusus lagi bagi pengembagan ilmu komputer dan teknologi informasi.

Yogyakarta, 3 Oktober 2022

Nathanael Dharmawan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS

Oleh

NATHANAEL DHARMAWAN

71170240

Keamanan komunikasi data melalui jaringan sudah menjadi kewajiban yang perlu di pertimbangkan dalam sebuah ekosistem teknologi. Keamanan data memiliki berbagai layer, salah satu layer yang perlu dilindungi adalah layer presentasi dimana SSL/TLS berada. Jika pada layer ini terdapat kerentanan dimana data sensitif seperti *cookie*, *username*, dan *password*, maka kebocoran data akan berdampak besar bagi semua pelaku kepentingan di bidang teknologi yang menggunakan teknologi SSL/TLS.

Dalam rangka penelitian dan peningkatan keamanan data di jaringan kampus Universitas Kristen Duta Wacana (UKDW), maka peneliti melakukan pengujian kerentanan SSL/TLS pada website SSAT UKDW dan E-Class UKDW menggunakan Test SSL dari Qualys dan *script* dari testssl.sh, penulis juga melakukan pengecekan *Mixed Content* dengan GeekFlare serta pengecekan HSTS Preload meenggunakan website HSTS Preload yang disediakan Google. Peneliti juga melakukan uji penetrasi SSL Strip di 12 titik gedung Universitas Kristen Duta Wacana dan juga di Lab D.

Berdasarkan hasil penelitian, ada beberapa hasil yang ditemukan. Hasil pada SSL Test menggunakan Qualys menemukan website SSAT dan E-Class sudah menggunakan aturan HTTP Strict Transport Security (HSTS) dengan Max-Age 31536000 (1 tahun) namun HSTS Preload belum di terapkan, pengujian *Mixed Content* dengan GeekFlare menunjukkan bahwa seluruh transaksi pada SSAT dan E-Class sudah menggunakan jalur HTTPS, lalu pada uji menggunakan script

testssl.sh terdapat kerentanan yang terbaca, serta serangan *SSL Strip* dimungkinkan terjadi di jaringan Universitas Kristen Duta Wacana dengan beberapa kondisi.

Kata-kata kunci : SSL Test, SSL Strip.

ABSTRACT

Network Security Analysis In Christian Duta Wacana University Using SSL/TLS Attacks

By

NATHANAEL DHARMAWAN

71170240

The security of data communication over the network has become an obligation that needs to be considered in a technology ecosystem. Data security has various layers, one layer that needs to be protected is the presentation layer where SSL/TLS is located. If at this layer there are vulnerabilities where sensitive data such as cookies, usernames, and passwords are present, then data leakage will have a major impact on all stakeholders in the technology sector using SSL/TLS technology.

In order to research and improve data security on the Duta Wacana Christian University (DWCU) campus network, the researchers conducted SSL/TLS vulnerability testing on the SSAT DWCU and E-Class DWCU websites using the SSL Test from Qualys and a script from testssl.sh, the author also conducted Checking Mixed Content with GeekFlare and checking HSTS Preload using the HSTS Preload website provided by Google. Researchers also conducted SSL Strip penetration tests at 12 points of the Duta Wacana Christian University building and also in Lab D.

Based on the results of the study, there were several results found. The results on the SSL Test using Qualys found that the SSAT and E-Class websites already use HTTP Strict Transport Security (HSTS) rules with Max-Age 31536000 (1 year) but HSTS Preload has not been implemented, Mixed Content testing with GeekFlare shows that all transactions on SSAT and E-Class already uses HTTPS paths, then in tests using the testssl.sh script there are vulnerabilities that are read,

and SSL Strip attacks are possible on the Duta Wacana Christian University network under several conditions.

Keywords: SSL Test, SSL Strip.

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan komunikasi data melalui jaringan sudah menjadi kewajiban yang perlu di pertimbangkan dalam sebuah ekosistem teknologi. Keamanan data memiliki berbagai layer, salah satu layer yang perlu dilindungi adalah layer presentasi dimana SSL/TLS berada. Jika pada layer ini terdapat kerentanan dimana data sensitif seperti *cookie, username,* dan *password*, maka kebocoran data akan berdampak besar bagi semua pelaku kepentingan di bidang teknologi yang menggunakan teknologi SSL/TLS.

Dalam rangka penelitian dan peningkatan keamanan data di jaringan kampus Universitas Kristen Duta Wacana, maka peneliti akan melakukan pengujian kerentanan pada SSL/TLS baik secara pemindaian maupun pengujian penetrasi serangan SSL Strip.

Pembatasan pengujian penetrasi serangan SSL Strip dilakukan di bawah kepengurusan PUSPINDIKA dan PPLK. Lokasi uji penetrasi serangan SSL Strip di bawah kepengurusan PUSPINDIKA adalah di 12 titik gedung, sedangkan uji penetrasi serangan SSL Strip di bawah kepengurusan PPLK adalah di Lab D. Pada akhirnya penelitian ini bertujuan untuk melihat seberapa rentan jaringan UKDW terhadap kerentanan maupun serangan pada SSL/TLS.

1.2. Perumusan Masalah

Seberapa rentan jaringan Universitas Kristen Duta Wacana terhadap pengujian penetrasi *SSL Strip* beserta seberapa rentan jaringan Universitas Kristen Duta Wacana dengan pemindaian SSL/TLS?

1.3. Batasan Masalah

Batasan Masalah di antara lain:

a. Lokasi pengujian penetrasi *SSL Strip* dilakukan dengan mengambil sampel di 12 titik gedung dan 1 lab yaitu Lab D.
b. Infrastruktur Jaringan yang akan di coba di uji adalah alat di bawah manajemen PUSPINDIKA dan PPLK.
c. Analisis yang lebih mendalam dilakukan dengan serangan *SSL Strip*. Data yang ditargetkan adalah data *username* dan *password.*
d. Pengujian *SSL Strip* menggunakan *device* yang telah disediakan sebagai korban.
e. Pengujian difokuskan pada pencarian kerentanan SSL/TLS pada web www.eclass.ukdw.ac.id serta www.ssat.ukdw.ac.id .
f. Alat yang akan digunakan untuk uji penetrasi *SSL Strip* yaitu Bettercap. Alat uji penetrasi untuk *SSL Test* adalah SSL Lab dari Qualys dan *script* Testssl.sh. Operasi Sistem Kali Linux, dan alat untuk melakukan penangkapan data jaringan adalah Wireshark.

1.4. Tujuan Penelitian

Mendapat informasi dan memastikan apakah jaringan UKDW memiliki kerentanan terhadap pengujian penetrasi *SSL Strip* dan serangan SSL/TLS yang lain dengan *SSL Test*.

1.5. Manfaat Penelitian

Manfaat yang ingin dicapai adalah mengetahui sejauh mana pertahanan jaringan UKDW terhadap pengujian penetrasi SSL Strip, dan kerentanan SSL/TLS yang lain, sehingga terjadi peningkatan kesadaran yang akan membawa kepada peningkatan keamanan jaringan UKDW baik secara konfigurasi pada infrastruktur jaringan maupun peningkatan secara kesadaran keamanan dari sumber daya

manusia. Serta sebagai pengetahuan bagi mahasiswa yang akan melakukan penelitian serupa.

1.6. Metode Penelitian

Berikut metode yang peneliti lakukan:

1.6.1. Persiapan Kebutuhan Sistem

Pada tahap persiapan kebutuhan sistem, peneliti mengumpulkan perangkat keras dan perangkat lunak yang dibutuhkan untuk penelitian.

1.6.2. Pengujian Sistem Menggunakan Qualys

Pada tahap ini sistem konfigurasi situs web E-Class dan SSAT UKDW di uji menggunakan *SSL Test* dari Qualys.

1.6.3. Pengujian Sistem Menggunakan testssl.sh

Dalam rangka menemukan kerentanan yang berbeda maka peneliti menguji dengan menggunakan *SSL Test* yang berbeda yaitu testssl.sh.

1.6.4. Pengujian Mixed Content Menggunakan GeekFlare

Untuk memastikan bahwa situs web E-Class dan SSAT telah melalui jalur yang aman (https) maka peneliti menguji dengan menggunakan GeekFlare.

1.6.5. Pengujian HSTS Preload Menggunakan HSTS Preload

Untuk mendapatkan informasi tambahan mengenai HSTS Preload maka peneliti melakukan pengecekan pada domain “ukdw.ac.id” beserta subdomain “eclass.ukdw.ac.id” dan “ssat.ukdw.ac.id”.

1.6.6. Penetrasi SSL Strip

Dalam rangka mendapatkan analisis yang lebih mendalam, maka peneliti melakukan pengujian penetrasi *SSL Strip* di jaringan Universitas Kristen Duta Wacana.

1.7. Sistematika Penulisan

Laporan skripsi ini disusun dengan struktur yang terdiri dari empat bab:

Bab 1 yaitu Pendahuluan yang berisi tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

Bab 2 yaitu Tinjauan Pustaka dan Landasan Teori yang berisi tinjauan pustaka tentang penelitian-penelitian terkait, dan berbagai tinjauan pustaka spesifik yang peneliti perlukan untuk memahami topik penelitian mengenai SSL/TLS.

Bab 3 yaitu Metodologi Penelitian yang berisi, detail kebutuhan sistem, pemindaian baik sebelum dan sesudah pembaharuan menggunakan Qualys, pengujian menggunakan *script* testssl.sh, pengujian *mixed content* menggunakan GeekFlare, pengujian HSTS Preload, serta detail metode pengujian penetrasi *SSL Strip*.

Bab 4 yaitu Hasil dan Analisis yang membahas tentang hasil dan analisis pengujian yang dilakukan di bab 3.

Bab 5 yaitu Kesimpulan dan Saran mengenai keamanan jaringan serta langkah yang bisa diambil untuk kemajuan keamanan jaringan di Universitas Kristen Duta Wacana yang berhubungan dengan keamanan SSL/TLS dari segi *Administrator* maupun *User*.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Situs web E-class pada awal pengujian masih belum menggunakan aturan HSTS, masih mendukung protokol 1.1 dan mendapat hasil pada Qualys dengan nilai B. Setelah dilakukan pembaruan maka protokol yang digunakan pun hanya mengijinkan protokol 1.2 (sudah sesuai standar NIST) dan mendapat nilai A+. Aturan HSTS sudah ditambahkan pada pembaharuan dengan nilai Max-Age 31536000 (1 tahun), dan HSTS Preload belum ditambahkan.
2. Pada E-Class tidak ditemukan kerentanan untuk serangan Hearthbleed, BEAST, Secure Renegotiation, SWEET32, FREAK, DROWN, dan RC4, namun masih ditemukan potensi kerentanan terhadap serangan LUCKY13.
3. Situs web SSAT pada awal pengujian masih belum menggunakan aturan HSTS, masih mendukung protokol TLS 1.0 dan TLS 1.1 dan mendapat hasil pada Qualys dengan nilai B. Setelah dilakukan pembaruan maka protokol yang digunakan pun hanya mengizinkan protokol 1.2 (sudah sesuai standar NIST) dan mendapat nilai A+. Aturan HSTS sudah ditambahkan pada pembaharuan dengan nilai Max-Age 31536000 (1 tahun), dan HSTS Preload belum ditambahkan.
4. Pada situs web SSAT tidak ditemukan kerentanan untuk serangan Heartbleed, BEAST, Secure Renegotiation, FREAK, DROWN, sedangkan serangan LUCKY 13 berpotensi Rentan lalu pada SWEET32 dan RC4 adalah Rentan.
5. Fitur HSTS *directive* yang telah diaktifasi pada E-Class dan SSAT memberikan efek cukup signifikan dalam memberikan keamanan koneksi dan memangkas kemungkinan penyerang melakukan SSL Strip. Hanya saja belum ada HSTS Preload yang memungkinkan penyerang untuk melakukan *SSL Stripping* diawal koneksi dimana *user* belum mendapat aturan HSTS *directive*.

6. Tidak ada konten yang menggunakan jalur tanpa enkripsi (HTTP). Pada kasus kali ini E-Class dan SSAT sudah menggunakan jalur HTTPS. Dimungkinkan dengan adanya implementasi HSTS memungkinkan untuk memaksa seluruh *resource* di akses secara terenkripsi.
7. Penempatan HSTS *Directive* masih dilakukan pada domain dan subdomain dimana seharusnya dilakukan pada domain dan bukan ditambahkan juga pada subdomain. Penempatan HSTS *Directive* pada subdomain diduga karena memperhitungkan kesiapan insfrastruktur.
8. Penetrasi SSL Strip di Universitas Kristen Duta Wacana masih dimungkinkan dengan beberapa kondisi. *Cache* SSAT dan E-Class pada korban harus tidak ada, terkoneksi dengan WAP yang sama, WAP tidak memiliki fitur *antispoofing*, dan *user* harus mengetik URI (eclass.ukdw.ac.id dan ssat.ukdw.ac.id).
9. Waktu tunggu sebuah *request* untuk melakukan *load* pada halaman situs web yang terkena *ssl strip* relatif lebih lama dibanding koneksi normal. Pada E-Class waktu tunggu berkisar 10-45 detik, dan SSAT berkisar 2-10 detik. Dimana pada koneksi normal *load* pada kedua website tidak mencapai 3 detik.
10. Penetrasi *SSL Strip* di Universitas Kristen Duta Wacana akan gagal apabila, *User* memiliki cache SSAT dan E-Class, *User* terkoneksi dengan WAP yang berbeda, *User* terkoneksi dengan WAP yang sudah memiliki atau mengaktifkan *antispoofing*, serta *User* yang tidak menulis URI (eclass.ukdw.ac.id dan ssat.ukdw.ac.id) tidak akan mendapat koneksi ketika *ssl strip* berjalan, maka *user* akan menyadari bahwa *user* tidak mendapat internet dan bisa saja *User* memilih tidak melanjutkan proses menuju situs web dan mengganti jaringannya.

5.2 Saran

Saran dari penelitian ini adalah sebagai berikut:

1. Untuk pengguna atau *user* agent dapat membedakan logo gembok yang berarti *secure* dan logo "*dangerous*" yang melambangkan koneksi melalui koneksi tidak ter-enkripsi. Sehingga ketika sedang melakukan *input* data sensitif maka sebaiknya menggunakan situs web dengan logo gembok.
2. *User* bisa melakukan pengecekan kemampuan SSL/TLS *browser client* di https://clienttest.ssllabs.com/ dari Qualys.
3. *User* perlu mengamati apabila terjadi *load* yang lama ketika melakukan *request* pada sebuah website. Ketika *load* terasa lama, sebaiknya perlu di cek kembali logo pada *browser*.
4. Administrator jaringan perlu melakukan pengecekan rutin pada server. Sehingga perubahan pada *server* yang mendadak mengalami perubahan dapat ditangani segera.
5. Baik *user* dan *administrator* lebih baik sering melakukan pembaruan perangkat lunak (*browser*, OS, aplikasi, dll) atau *update fitur* yang cukup, tentunya dalam melakukan pembaruan juga perlu mengecek apakah pembaruan yang akan di pasang mengalami kerentanan fatal/menengah/tidak fatal.
6. Uji coba serangan SSL Strip sangat bergantung pada *tools* (software dan versi yang dipakai), sistem pertahanan yang digunakan pada jaringan (*firewall*, *anti arpspoofing*) maupun konfigurasi *server*. Untuk itu penelitian yang lebih mendalam bisa lebih lagi meneliti seperti modifikasi *tools*, analisis fitur, analisis paket pada sebuah jaringan lokal area, dll.

DAFTAR PUSTAKA

Bettercap. (t.thn.). Diambil kembali dari https://www.bettercap.org/

Check Mixed Content (HTTP). (t.thn.). (GeekFlare) Dipetik November 7, 2022, dari https://geekflare.com/tools/mixed-content-test

Chen, W.-L., & Wu, Q. (t.thn.). A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal.

CVE. (t.thn.). Diambil kembali dari CVE-2016-2183: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183

CVE. (t.thn.). Diambil kembali dari CVE-2015-4000: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

Duddu, S., Sowjanya, C. L., Sai, A. R., & Rao, D. (2020). Secure Socket Layer Stripping Attack Using Address Resolution Protocol Spoofing. *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020)* (hal. 973-978). IEEE.

Github. (t.thn.). Diambil kembali dari sslstripping is missing on the 2.x version #154: https://github.com/bettercap/bettercap/issues/154

Github. (2020, February 4). Diambil kembali dari SSL Server Rating Guide: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

Github. (2022, Oktober). Diambil kembali dari testssl.sh: https://github.com/drwetter/testssl.sh

Hearthbleed. (t.thn.). (Hearthbleed) Dipetik November 7, 2022, dari https://heartbleed.com/

Hossain, M. S., Paul, A., & Islam, M. H. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. *Network Protocols and Algorithms*, 83-108.

K, A. P. (2017). Analisis Implementasi Protokol HTTPS Pada Website Internet Banking Di Indonesia. Yogyakarta, Yogyakarta, Indonesia.

K, K. V., & P, A. R. (2016). Taxonomy of SSL/TLS Attacks. *I. J. Computer Network and Information Security*, 15-24.

Kampourakis, V., Kambourakis, G., Chatzoglou, E., & Christos, Z. (2022). Revisiting man-in-the-middle attacks against HTTPS. *Network Security*.

Kohlios, C. P., & Hayajneh. (2018). A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics*, 01-28.

Li, X., Wu, C., Ji, S., Gu, Q., & Beyah, R. (2017). HSTS Measurement and an Enhanced Stripping Attack Against HTTPS. *SecureComm*, 489-509.

McKay, K. A., & Cooper, D. A. (2019). Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. *NIST Special Publication 800-52 Revision 2*.

OpenSSL. (t.thn.). Diambil kembali dari SSL and TLS Protocols: https://wiki.openssl.org/index.php/SSL_and_TLS_Protocols

Pranata, H., Abdillah, L. A., & Ependi, U. (2015). Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. *Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI)*, 01-06.

Raharjo, W. S., & Bajuadji, A. A. (2016). Analisa Implementasi Protokol HTTPS pada Situs Web Perguruan Tinggi di Pulau Jawa. *ULTIMACS*, 102-111.

Rescorla, E., Ray, M., Dispensa, S., & Oskov, N. (2010, February). *Transport Layer Security (TLS) Renegotiation Indication Extension*. Diambil kembali dari RFC: https://www.rfc-editor.org/rfc/rfc5746

Ristić, I. (2015). *Bulletproof SSL and TLS.* London: Feisty Duck Limited.

Susanto, A., & Raharja, W. K. (2021). Simulation and Analysis of Network Security Performance Using Attack Vector Method for Public Wifi Communication. *The IJICS (International Journal of Informatics and Computer Science)*, 07-15.

testssl.sh. (t.thn.). Diambil kembali dari Testing TLS/SSL encryption: https://testssl.sh/

University Information Technology Services. (2018, May 14). Diambil kembali dari About fully qualified domain names (FQDNs): https://kb.iu.edu/d/aiuv#:~:text=A%20fully%20qualified%20domain%20name,be%20mymail.somecollege.edu%20.