Terbit online pada laman web jurnal: **http://journal.isas.or.id/index.php/JACOST**

JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)

Vol. 2 No. 1 (2021) 7 – 11 | ISSN: 2723-1453 (Media Online)

Protokol HTTPS, Apakah Benar-benar Aman?

Deddy Prayama[1], Yuhefizar[2], Amelia Yolanda[3]

[1]Program Studi Teknik Komputer, Jurusan Teknologi Informasi, Politeknik Negeri Padang

[2]Program Studi Manajemen Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Padang

[3]Program Studi Teknik Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Padang

[1]deddy@pnp.ac.id, [2]yuhefizar@pnp.ac.id, [3]amelia@pnp.ac.id

Abstract

In particular, the method used in this research is a case study where previously the p3m.pnp.ac.id website still uses the http protocol. However http protocol does not have a method of securing data in its communication. The final result of this research is the design and implementation of the https protocol for data communication security that occurs between visitors and the p3m.pnp.ac.id website. The https protocol that has been implemented is tested to ensure the data traffic on the p3m.pnp.ac.id website is guaranteed to be safe and protected from possible piracy and data theft.

Keywords: protocol, http, https, website, security

Abstrak

Secara khusus metode yang digunakan dalam penelitian ini adalah studi kasus dimana sebelumnya website p3m.pnp.ac.id masih menggunakan protokol http dimana protokol ini tidak memiliki metode pengamanan data dalam komunikasinya. Hasil akhir penelitian ini merupakan perancangan dan penerapan protokol https untuk keamanan komunikasi data yang terjadi antara pengunjung dengan website p3m.pnp.ac.id. Protokol https yang telah diterapkan diuji untuk memastikan bahwa lalu lintas data di website p3m.pnp.ac.id dipastikan aman dan terhindar dari kemungkinan pembajakan dan pencurian.

Kata kunci: protokol, http, https, website, keamanan

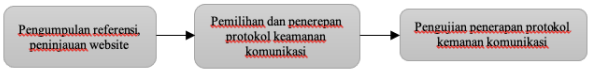
1. Pendahuluan

Tiga komponen utama dalam internet dan website adalah Lokator Sumber Seragam (LSS), yang juga dikenal dengan Uniform Resource Locator (URL), merupakan rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di Internet. Selanjutnya adalah Hypertext Markup Language (HTML) yaitu bahasa pembangkit halaman website agar bisa ditampilkan di layar monitor, dan terakhir adalah Hypertext Transfer Protocol (HTTP).

Hypertext Transfer Protocol (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hypermedia[1]. Penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan, yang disebut dengan dokumen hiperteks, yang kemudian membentuk World Wide Web pada tahun 1990 oleh fisikawan Inggris, Tim Berners-Lee. Hingga kini, ada dua versi mayor dari protokol HTTP, yakni HTTP/1.0 yang menggunakan koneksi terpisah untuk setiap dokumen, dan HTTP/1.1 yang dapat menggunakan koneksi yang sama untuk melakukan transaksi. Dengan demikian, HTTP/1.1 bisa lebih cepat karena memang tidak usah membuang waktu untuk pembuatan koneksi berulang-ulang. Namun baik HTTP/1.0 maupun HTTP/1.1 memiliki kelemahan dari sisi keamanan[2]. Kedua versi HTTP tidak memiliki jaminan untuk keamanan komunikasi data yang terjadi antara pengguna dengan website. Hal ini menjadi beresiko jika diterapkan pada website e-commerce, perbankan, website resmi milik pemerintah atau institusi dan organisasi. Masalah utama dari protokol HTTP adalah proses pengiriman HTTP *Request* dan HTTP *Response* dilakukan tanpa ada pengamanan sama sekali, sehingga seseorang yang memiliki akses di jaringan mampu menyadap informasi yang dikirimkan dan bahkan bisa data *tampering* tanpa diketahui oleh kedua belah pihak[3]. Hal inilah yang melatar belakangi penelitian ini, dimana website p3m.pnp.ac.id masih menerapkan protokol HTTP/1.1 sehingga kemungkinan terjadinya serangan siber terhadap keamanan website ini sangat tinggi. Namun apakah penerapan protokol keamanan komunikasi data sudah menjamin bahwa komunikasi data yang terjadi sudah benar – benar aman dan bebas dari kemungkinan serangan siber?

2. Metode Penelitian

Adapun metode penelitian yang dilaksanakan merupakan penelitian terapan dengan studi kasus. Secara garis besar, penelitian ini dilakukan terdiri atas tiga tahapan, diawali dengan studi pendahuluan yang meliputi pengumpulan referensi dan peninjauan terhadap penerapan protokol komunikasi pada website p3m.pnp.ac.id. Tahapan selanjutnya adalah pemilihan jenis protokol keamanan sekaligus perancangan dan implementasi protokol tersebut. Pada tahapan ketiga dilakukan pengujian terhadap penerapan protokol keamanan website tersebut. Untuk lebih jelasnya dapat kita lihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.1 Pengumpulan referensi dan peninjauan website p3m.pnp.ac.id

Adapun referensi utama yang digunakan adalah Jurnal Joiv Vol 2 nomor 4 Tahun 2018 dengan judul "*Network Security Assessment Using Internal Network Penetration Testing Methodology*". Pada publikasi ini dijelaskan beberapa metode yang dapat digunakan oleh penyerang untuk menyerang website, sedangkan saat peninjauan didapatkan informasi bahwa website p3m.pnp.ac.id belum menerapkan protokol https untuk keamanan komunikasi data antara pengunjung dengan website. Dari sisi platform perangkat lunak didapatkan informasi sebagai berikut :

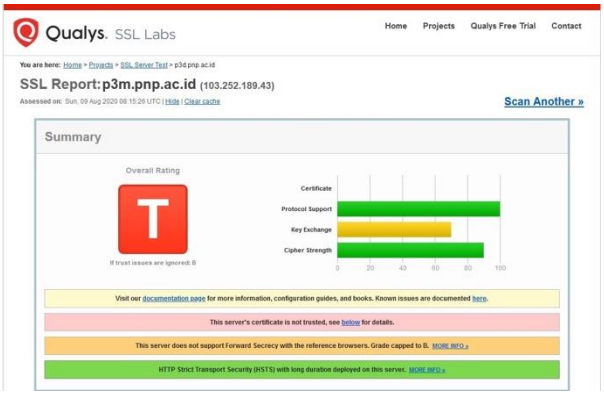
1. Sistem operasi : CentOS 7.8.2003
2. Apache webserver : versi 2.4.6.
3. MySQL Version : 5.5.65
4. PHP : Version 5.6.25
5. Virtual share hosting server.

Sebelum penerapan protokol https, dilakukan pengujian terlebih dahulu. Pertama adalah dengan memanfaatkan informasi yang diperoleh dari browser yang digunakan untuk mengakses website p3m.pnp.ac.id. Pada Gambar 2. berikut ini dapat dilihat bahwa website p3m.pnp.ac.id belum menerapkan protokol https, hal ini ditandai dengan icon gembok yang disilang merah. Saat icon gembok tersebut diklik akan muncul informasi koneksi ke website p3m.pnp.ac.id tidak aman.

Gambar 2. Koneksi ke website tidak aman

Informasi teknis yang ditampilkan sesuai dengan browser yang digunakan dinyatakan bahwa koneksi internet yang dilakukan ke website p3m.pnp.ac.id tidak dienkripsi, hal ini menyebabkan data yang dikirimkan dimungkinkan untuk dilihat oleh pihak lain.

Agar lebih akuratnya informasi yang diperoleh, data mengenai website p3m.pnp.ac.id juga diperoleh dengan memanfaatkan informasi pada website penyedia informasi keamanan website. Salah satunya adalah informasi yang diperoleh dari website ssllabs.com sesuai Gambar 3.



Gambar 3. Informasi web p3m.pnp.ac.id dari ssllabs.com

Dari gambar diatas dapat dilihat bahwa website p3m.pnp.ac.id memang benar belum menerapkan protokol keamanan atau belum memiliki sertifikat SSL dalam komunikasi data antara pengguna dan website p3m.pnp.ac.id, sehingga diberi rating T, dengan status sertifikat tidak dapat dipercaya.

2.2 Pemilihan dan perancangan protokol keamanan komunikasi.

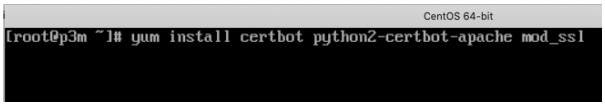
Terkait dengan platform dari webserver penempatan website p3m.pnp.ac.id yaitu webserver Apache dengan database MySQL, standar enkripsi untuk webserver dan berbagai perangkat pendukung website, ditetapkanlah (versi) protokol keamanan website p3m. Langkah awal penerapan protokol ini adalah dengan merancang atau membuat sebuah *private key* atau kunci pribadi. *Private key* ini atau dalam penamaan disistem disebut dengan *server.key*. Selanjutnya server.key ini akan digunakan untuk permintaan penandatanganan sertifikat atau *certificate signing request* (CSR). CSR berisi informasi domain atau website yang diajukan, dalam hal ini adalah p3m.pnp.ac.id. Kombinasi *private key* dan *certificate signing request* (CSR) akan menghasilkan *server.csr*. File server.csr inilah yang diajukan atau di*submit* ke provider atau Certificate Authority (CA) yaitu organisasi yang berwenang untuk memvalidasi atau mengeluarkan sertifikat enkripsi domain atau website, diantaranya Symantec, VeriSign, GoDaddy, GeoTrust, LetsEncrypt dan lain sebagainya.[] Setelah proses validasi disetujui, Certificate Authority akan mengirimkan dua files dengan ekstensi **.pem* dan **.crt* termasuk *server.key*

DOI : https://doi.org/10.52158/jacost.v2i1.118

yang sebelumnya dikirimkan. File **.pem* dan **.crt* atau yang disebut dengan Sertifikat *Secure Socket Layer* (SSL) inilah yang harus ditempatkan di webserver p3m.pnp.ac.id.

2.2.1. Pemilihan Protokol SSL

Sebelum implementasi protokol keamanan komunikasi seperti penerapan sertifikat SSL, pastikan layanan webserver telah bekerja. Berikut ini langkah penerapan protokol :



Gambar 4. Install mod_ssl

Pada gambar 4. diatas dapat kita lihat bahwa implementasi protokol terlebih dahulu harus dilakukan pada sisi webserver, dalam hal ini apache webserver. Langkah selanjutnya adalah dengan menetapkan domain yang akan menggunakan sertifikat SSL tersebut.

Gambar 5. Penetapan domain SSL

Domain yang dipilih adalah domain p3m.pnp.ac.id seperti terlihat pada Gambar 4. diatas.

2.2.2 Perancangan protokol keamanan komunikasi.

Untuk lebih amannya komunikasi yang berlangsung antara pengunjung dengan website p3m.pnp.ac.id maka ditetapkanlah beberapa kriteria atau parameter yang digunakan untuk sertifikat SSL yaitu :

1. Public Key Algorithm : RSA
2. Key Length : 2048 bit
3. Signature Algorithm : SHA-256 V3
4. Domain Name : p3m.pnp.ac.id
5. Key Purposes : Digital Signature
6. Extended : Server and Client Authentication
7. Authority Method : Online Certificate Status Protocol (OCSP)
8. Certificate Policies : Domain validation.
9. Authority Info : Letsencrypt.org

Parameter diatas merupakan parameter minimal yang wajib disediakan untuk meminta konfirmasi kepada Certificate Authority(CA) yang memiliki wewenang dalam memberikat sertifikat. Sedangkan informasi yang diberikan atau diisi disesuaikan dengan kebutuhan.

Sesaat setelah konfirmasi dilakukan sesuai Gambar 5. dan proses akses ke domain berhasil dilakukan maka akan muncul pesan untuk konfirmasi email dan persetujuan untuk *Term of Service* dari Certificate Authority dalam hal ini Letsencrypt. Untuk lebih jelasnya dapat dilihat pada Gambar 5. berikut ini :

Gambar 5. Certificate Authority Verification

Pada Gambar 5. diatas dapat dilihat bahwa proses otentifikasi terhadap keberadaan website mutlak diperlukan jika ingin mengusulkan sertifikat untuk enkripsi website. Jadi hal yang paling utama diperlukan adalah website yang diajukan harus dapat diakses tanpa ada hambatan.

Langkah selanjutnya adalah dengan mengatur bagaimana pengunjung atau klien dapat mengakses website p3m.pnp.ac.id. Apakah bisa tetap menggunakan protokol http, sehingga sertifikat SSL tidak diperlukan, atau wajib menggunakan protocol https.

Dalam penelitian ini ditetapkan bahwa setiap klien atau pengunjung wajib menggunakan protocol https untuk dapat mengakses halaman website p3m.pnp.ac.id. Untuk dapat mengimplementasikan hal tersebut, maka diperlukan perubahan atau menambahkan sebuah file dengan extension .htaccess.

Berikut ini adalah script untuk meneruskan setiap akses pengunjung ke website p3m.pnp.ac.id agar selalu menggunakan protocol https :

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Gambar 6. Script .htaccess

Script .htaccess sesuai Gambar 6. diatas, ditempatkan pada webserver p3m.pnp.ac.id, sehingga setiap permintaan koneksi ke website tersebut akan diteruskan ke protokol https, meskipun pengunjung tidak menuliskan nama protokolnya di alamat yang dituju pada web browser.

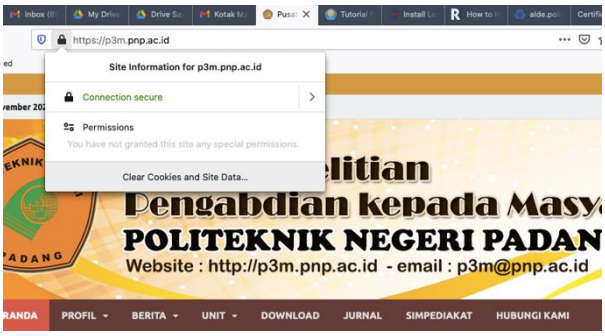
3. Hasil dan Pembahasan

3.1 Hasil

Setelah melalui serangkaian tahapan yang telah dikemukakan dalam metode penelitian diperoleh protokol komunikasi yang lebih aman ke website p3m.pnp.ac.id. Penerapan protokol https untuk komunikasi antara pengunjung dengan website p3m.pnp.ac.id berhasil diimplementasikan. Hal ini dapat

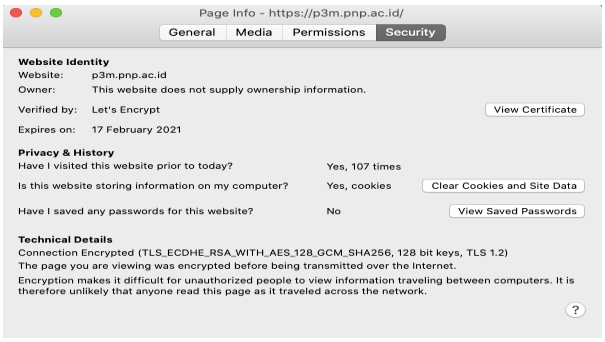
DOI : https://doi.org/10.52158/jacost.v2i1.118

dibuktikan pada saat pengunjung mengakses website p3m.pnp.ac.id. Pada alamat url yang ada diweb browser sudah ditandai dengan icon gembok berwarna hijau, seperti pada Gambar 7.



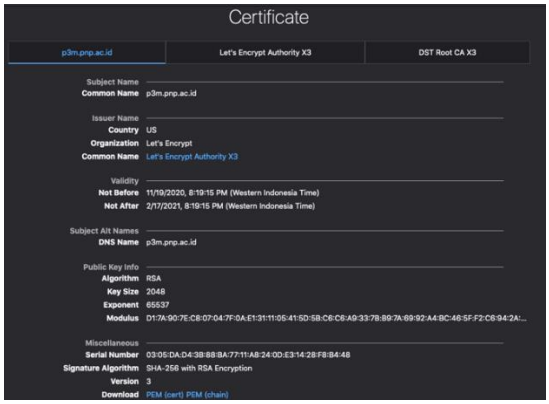
Gambar 7. Protokol https

Jika digali lebih jauh, informasi teknis yang ditampilkan mengenai website p3m.pnp.ac.id dinyatakan bahwa website sudah mendukung enkripsi data, sehingga data yang dikirimkan melalui internet akan menyulitkan bagi orang yang tidak berhak untuk melihat. Hal ini dapat kita lihat pada Gambar 8.



Gambar 8. Informasi teknis website

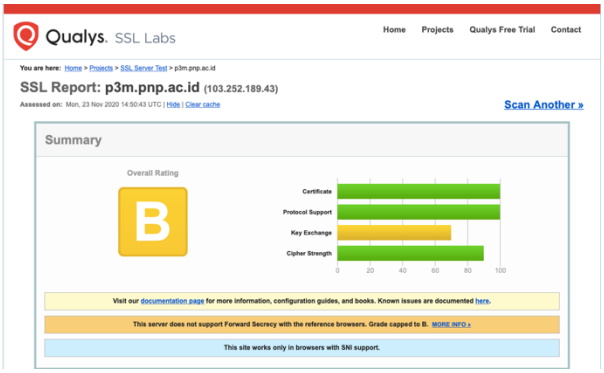
Gambar 8 memberikan informasi berupa alamat website yang diakses, kepemilikan, verifikasi untuk keamanan dan tanggal kadaluarsa. Agar informasi yang didapatkan dalam penelitian ini lebih akurat, dengan menggunakan browser firefox, dapat dilihat bahwa parameter yang dipilih untuk sertifikat SSL sudah sesuai dengan yang diharapkan. Ini dapat dilihat pada gambar 9.



Gambar 9. Sertifikat SSL website p3m

Informasi penting yang dapat dilihat pada Gambar 9. diatas diantaranya adalah algoritma kunci publik yang sudah menggunakan RSA, Panjang kunci public 2048, penanda algoritma yang menggunakan SHA-256 dengan enkripsi RSA dan kegunaan kunci yang menyatakan untuk penanda digital, pembuka enkripsi serta otentifikasi antara klien dan server. Adapun negara yang mengeluarkan sertifikat enkripsi adalah United Stated (US) dengan organisasinya Letsencrypt.

Sesuai dengan informasi awal yang diperoleh dari website ssllabs.com, langkah terakhir untuk hasil penerapan protokol keamanan komunikasi pada website p3m.pnp.ac.id diuji kembali di website yang sama. Hasilnya dapat kita lihat pada Gambar 10.



Gambar 10. Informasi website p3m.pnp.ac.id setelah implementasi SSL

Dari Gambar 10. diatas website ssllabs.com sudah memberikan rating B untuk sertifikat SSL, dimana sebelumnya masih memberikan rating T untuk sertifikat yang dimiliki website p3m.pnp.ac.id.

3.2 Pembahasan

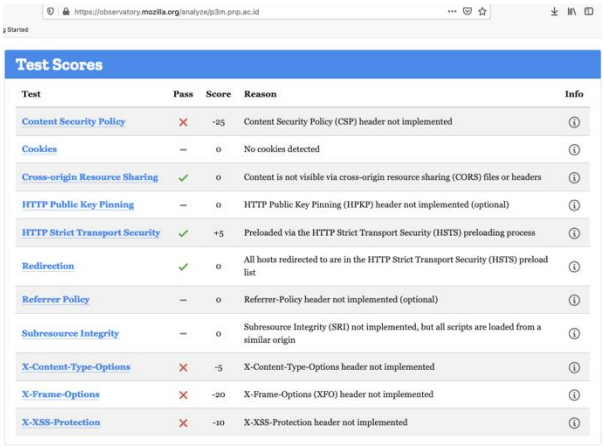
Dari serangkaian tahapan penelitian yang telah dilakukan, saat ini website p3m.pnp.ac.id telah memiliki sertifikat SSL untuk komunikasi data antara pengunjung dengan website p3m.pnp.ac.id. Enkripsi data berlangsung saat komunikasi data terbentuk antara pengunjung dengan website. Peran kunci publik dan algorima RSA menyulitkan pihak yang tidak berhak untuk menggunakan data meskipun data berhasil di *capture* saat komunikasi berlangsung.

Kembali ke pertanyaan awal penelitian ini, apakah protokol https benar – benar aman? Untuk membuktikan hasil implementasi keamanan protokol https diwebsite p3m.pnp.ac.id Kembali digunakan salah satu fitur dari browser mozilla yaitu *observatory*. Gambar 11 adalah informasi yang dihasilkan.

Ada empat kriteria yang tidak lulus uji pencegahan terhadap keamanan website berdasarkan metode *observatory mozilla* yang mengamati *header* dan *content* dari sebuah website. Pertama adalah *Content Security Policy*, ini berhubungan dengan isi atau konten yang ada dalam sebuah website, kedua adalah *X-Content Type Options*, ini berkaitan erat dengan kriteria yang ke empat

DOI : https://doi.org/10.52158/jacost.v2i1.118

yaitu *X-XSS Protection* dimana dua kriteria ini berkaitan erat dengan kode – kode pendukung tampilan website yang diakses oleh user, maksudnya adalah bagaimana sebuah browser dalam menampilkan informasi sesuai dengan standar penulisan halaman html dengan desain yang sudah diatur agar lebih menarik. Kriteria selanjutnya adalah *X-Frame Option*, kriteria ini berkaitan erat dengan frame atau objek – objek tertentu dihalaman website. Keempat kriteria tersebut merupakan aspek minimal yang harus diperhatikan dalam menerapkan keamanan pada sebuah website.



Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	–	0	No cookies detected	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✓	+5	Preloaded via the HTTP Strict Transport Security (HSTS) preloading process	ⓘ
Redirection	✓	0	All hosts redirected to are in the HTTP Strict Transport Security (HSTS) preload list	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Gambar 11. Observatory p3m.pnp.ac.id

4. Kesimpulan dan Saran

Setelah melewati tahapan sesuai metode yang dilakukan, maka penelitian telah berhasil mengimplementasikan dan menguji keamanan protokol https atau sertifikat SSL website p3m.pnp.ac.id. Terkait dengan keamanan protokol komunikasi, disimpulkan bahwa komunikasi antara pengunjung dan website p3m.pnp.ac.id sudah aman karena telah terjadi proses enkripsi data. Namun implementasi protokol https saja tidak cukup untuk mengamankan sebuah website. Untuk itu disarankan kepada pengelola dan peneliti selanjutnya agar dapat mengamankan bagian *header* dan *content* dari website agar benar – benar aman dari kemungkinan serangan siber.

Ucapan Terimakasih

Tim peneliti mengucapkan terima kasih kepada Pusat Penelitian dan Pengabdian Kepada Masyarakat Politeknik Negeri Padang yang telah menyediakan dana penelitian melalui DIPA Tahun Anggaran 2020 dengan kontrak nomor : 414/PL9.15/PG/2020

Daftar Rujukan

[1] Fielding, R., Reschke, J.,2014, RFC 7230 - Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, IETF
[2] Fielding, et al, RFC 2616 – Hypertext Transfer Protocol (HTTP/1.1) 15 Security Consideration
[3] Willy Sudiarto Raharjo, Aloysius Airlangga Bajuadji, 2016, *Analisa Implementasi Protokol HTTPS pada situs web perguruan tinggi di pulau Jawa*, Ultimatics, Jurnal Ilmu Teknik Informatika, Universitas Multimedia Nusantara.
[4] Evan Gilman, Doug Barth, 2017, *Zero Trust Network, Building Secure Systems in Untrusted Networks (Kindle Edition),*UK , O-Reilly
[5] Forshaw, James, 2017, *Attacking Network Protocol: A Hacker's Guide to Capture, Analysis, and Exploitation 1st Edition*, San-Francisco, No Starch Press
[6] Rahim, Robbi & Ratnadewi, Ratnadewi & Prayama, D & Asri, E & Satria, D., 2018. *Base64, End of File and One Time Pad for Improvement Steganography Security*. IOP Conference Series: Materials Science and Engineering. 407. 012161. 10.1088/1757-899X/407/1/012161.
[7] Satria, Deni & Alanda, Alde & Erianda, Aldo & Prayama, Deddy. (2018). *Network Security Assessment Using Internal Network Penetration Testing Methodology*. JOIV : International Journal on Informatics Visualization. 2. 360. 10.30630/joiv.2.4-2.190.
[8] Tanenbaum, Andrew, S; Weatherall, David, J , 2011, *Computer Network* , Fifth Edition, USA, Prentice Hall
[9] Rice, Liz, 2020, Container Security: Fundamental Technology Concepts that Protect Containerized Applications, O'Reilly Media, Inc.
[10] Justin Meza, Tianyin Xu, Kaushik Veeraraghavan, and Onur Mutlu, 2018, *A Large Scale Study of Data Center Network Reliability*, Proceedings of the Internet Measurement Conference 2018, Association for Computing Machinery, 2018. https://doi.org/10.1145/3278532.3278566.
[11] K, Allen Scott, 2012, *What Every Web Developer Should Know About HTTP*, OdeToCode LLC; 3rd Edition, US, OdeToCode
[12] Qualys. Inc, 2020, SSLLabs, [update 2020] tersedia di https://www.ssllabs.com/index.html [Accessed 23 November 2020]
[13] Xiong G., Tong J., Xu Y., Yu H., Zhao Y. (2014) A Survey of Network Attacks Based on Protocol Vulnerabilities. In: Han W., Huang Z., Hu C., Zhang H., Guo L. (eds) Web Technologies and Applications. APWeb 2014. Lecture Notes in Computer Science, vol 8710. Springer, Cham. https://doi.org/10.1007/978-3-319-11119-3_23
[14] Mozilla Observatory, 2017, Web Security, [updated 2017] tersedia di https://infosec.mozilla.org/guidelines/web_security [Accessed 25 November 2020]