*JIKA (Jurnal of Informatics) Universitas Muhammadiyah Tangerang* *P ISSN : 2549-0710*
*Vol 7, No 2, April 2023, pp 183 – 192* *E ISSN : 2722-2713*
*DOI : 10.31000/jika.v7i2.7566*

# PENGGUNAAN WIRESHARK DAN NESSUS UNTUK ANALISIS SSL/TLS PADA KEAMANAN DATA PENGGUNA WEBSITE

**Alfin Syarifuddin Syahab[1)], Erik Iman Heri Ujianto[2)], Rianto[3)]**
[1,2,3] Magister Teknologi Informasi, Universitas Teknologi Yogyakarta, Jl. Siliwangi Jl. Ring Road Utara, Jombor Lor, Sendangadi, Kec. Mlati, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55285
Co Responden Email: alfin.syahab@bmkg.go.id

***Article history***
*Received 28 Dec 2022*
*Revised 04 Jan 2023*
*Accepted 03 Mar 2023*
*Available online 15 May 2023*

***Keywords***
*Website,*
*SSL/TLS,*
*Security,*
*Wireshark,*
*Nessus*

***Abstract***

***The development of websites in Indonesia has increased due to the increase internet service users. Websites with user data have information vulnerabilities. Attacks on website can exploit web servers. The attack was carried out to discover usernames, passwords, and sensitive files. The SSL/TLS protocol is a security on the web for secure between clients and servers. This research was conducted to analyze SSL/TLS on the National Agency for Meteorology Climatology and Geophysics (BMKG) website user data for area X, which provides the public with weather and climate data and information. Tests were carried out using data packet tracing method with the Wireshark and the website scanning method in a vulnerability assessment with the Nessus. The tracing results show web server has verified SSL/TLS certificates and public key server using TLS 1.2 protocol to protect user data with encryption using the SHA256 hash algorithm. The vulnerability assessment shows overall risk level is medium. The vulnerability priority rating (VPR) score finding three SSL/TLS vulnerability that requires follow-up actions to reduce the risk of vulnerabilities. The results of tracing data packages and vulnerability assessments help identify weaknesses in website that determine steps in strengthening website security to protect against cyberattacks.***

**Riwayat**
Diterima *28 Des 2022*
Revisi *04 Jan 2023*
Disetujui *03 Mar 2023*
Terbit *online* 15 Mei 2023

**Kata Kunci**
Website,
SSL/TLS,
Keamanan,
Wireshark,
Nessus

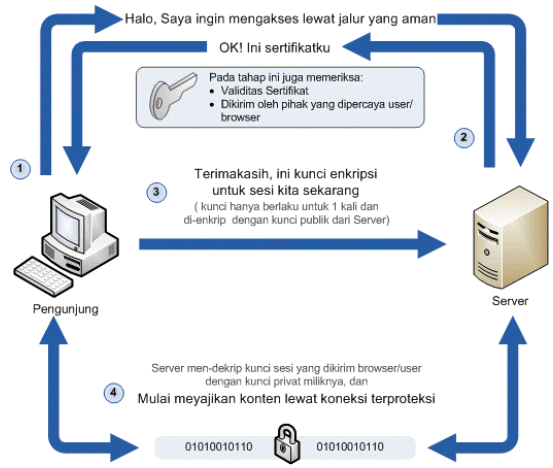
Abstrak

Perkembangan *website* di Indonesia meningkat signifikan dikarenakan bertambahnya pengguna layanan internet. Di sisi lain *website* yang memiliki data pengguna memiliki kerentanan. Serangan pada *website* dapat mengekploitasi sistem. Serangan tersebut dilakukan untuk mengetahui *username, password*, dan file sensitif. Protokol SSL/TLS merupakan bentuk keamanan pada web untuk komunikasi jaringan aman antara *client* dan *server* melalui koneksi terproteksi. Penelitian ini bertujuan untuk menganalisis SSL/TLS pada data pengguna website Badan Meteorologi Klimatologi dan Geofisika (BMKG) daerah X yang memberikan informasi cuaca dan iklim kepada masyarakat. Pengujian dilakukan menggunakan metode penelusuran paket data dengan aplikasi Wireshark dan menggunakan metode pemindaian website berupa *vulnerability assessment* dengan aplikasi Nessus. Hasil penelusuran paket data menunjukkan *web server* sudah diverifikasi sertifikat SSL/TLS dan *server public key* dengan protokol TLS 1.2 sehingga mampu melindungi data pengguna menggunakan enkripsi *client* dan *server* menggunakan algoritma hash SHA256. Hasil analisis pemindaian berupa vulnerability assessment menunjukkan level resiko keseluruhan adalah *medium. Vulnerability priority rating (VPR) score* menemukan tiga informasi kerentanan SSL/TLS yang membutuhkan tindakan evaluasi dan tindak lanjut dalam mengurangi resiko kerentanan website. Hasil penelusuran paket data dan *vulnerability assessment* pada SSL/TLS dapat membantu mengidentifikasi kelemahan sistem informasi website sehingga dapat menentukan langkah dalam penguatan performa keamanan *website* untuk melindungi dari serangan siber.

*JIKA (Jurnal of Informatics) Universitas Muhammadiyah Tangerang* *P ISSN : 2549-0710*
*Vol 7, No 2, April 2023, pp 183 – 192* *E ISSN : 2722-2713*
*DOI : 10.31000/jika.v7i2.7566*

## PENDAHULUAN

Protokol SSL/TLS adalah protokol keamanan yang digunakan pada web dalam memastikan komunikasi jaringan secara aman, seperti digunakan menjelajahi situs web dalam bentuk Hypertext Transport Protocol Secure (HTTPS) (Adeenze-Kangah & Chen, 2019). Aspek keamanan pada web browser diperlukan dengan maksud untuk melakukan proteksi dari berbagai macam serangan. *Netscape Communications* meluncurkan konsep *Secure Socket Layer* (SSL) sebagai komunikasi keamanan sensitif pada tahun 1994. *Internet Engineering TaskForce* (IETF) melakukan adopsi sebagai standar yang dikenal sebagai *Transport Layer Security* (TLS) untuk mengamankan HTTP menjadi HTTPS pada tahun 1999 (Wahanani, Aditiawan, & Mumpuni, 2020). TLS adalah penerus SSL yang dikembangkan dalam menangani kekurangan yang ditemukan di versi SSL sebelumnya. Server web yang menggunakan protokol autentikasi SSL dan TLS versi lama dalam HTTPS membuat sistem rentan terhadap serangan peretas, Sejak dirilisnya SSL v3.0, beberapa kerentanan telah teridentifikasi, terakhir di akhir tahun 2014 (S, Govindaraju, & Elango, 2019). Protokol TLS 1.3 adalah versi baru dan versi yang disempurnakan dari protokol TLS 1.2. Protokol ini menjamin komunikasi yang aman antara klien dan server melalui internet, yang memberikan keamanan *end-to-end* untuk komunikasi sistem *cyber-phisical* (Kumari & Mohapatra, 2022).

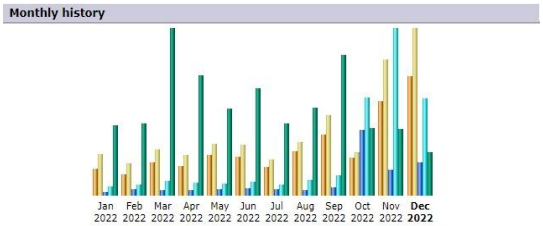


Gambar 1. Cara Kerja SSL

Cara kerja SSL secara sederhana seperti pada Gambar 1 dijelaskan secara berurutan dari sisi *client* dan *server*. Pertama, *client* meminta akses jalur aman kepada *server*. Kedua, server memberikan respon dengan sertifikat SSL beserta validitas sertifikat dan dikirim oleh pihak yang dipercaya pengguna. Ketiga, *client* memberikan akses kunci enkripsi. Keempat, server menyajikan konten lewat koneksi terproteksi kepada client (Fatimah, 2018). Proses tersebut merupakan gambaran umum terjadinya komunikasi terproteksi antara client dan server menggunakan enkripsi data. SSL/TLS melakukan operasi utama seperti otentikasi timbal balik antara klien dan server dan membangun saluran komunikasi yang aman dan andal di antara mereka (Arshad & Ali Hussain, 2016).

Perkembangan website di Indonesia meningkat secara signifikan. Fenomena ini terus tumbuh sebanding dengan meningkatnya jumlah pengguna layanan internet dari tahun ke tahun. Beberapa website yang sering diakses oleh pengguna antara lain; mesin pencarian, perdagangan elektronik, social, forum, dan portal berita. Di sisi lain penggunaan website mendapat peluang beberapa agresi siber yang terjadi antara lain *Internet social engineering attacks, Network sniffers, Packet spoofing, GUI (Graphical User Interface) intruder tools, Executable code attacks (against browsers), Techniques to analyse code with Vulnerabilities without source, Widespread attacks on DNS infrastructure, Wide-scale Trojan distribution, Distributed attack tools, Distributed Denial of service (DDoS) attacks, Targeting of specific users, Wide-scale use of worms,* dan *Sophisticated command and control attacks.* Serangan siber tersebut memiliki potensi yang terus berkembang sesuai dengan perubahan teknologi informasi yang semakin canggih (Vimy, Wiranto, Rudiyanto, Widodo, & Suwarno, 2022). Serangan-serangan dilakukan untuk mengetahui *username*, *password*, maupun *file* sensitif yang diunggah atau diunduh dari pengguna. (Sahren, 2021) Eksploitasi terhadap web server merupakan bentuk perilaku seseorang yang mengambil keuntungan dari kerentanan atau kelemahan keamanan suatu software (Budihardjo, Dewi,

& Noertjahyana, 2021). Persoalan keamanan diperlukan implementasi metode yang dapat menjalankan keamanan data dan komunikasi. Minimnya keamanan pada sistem akan memudahkan *hacker* mengambil alih sistem yang dibangun. Hal tersebut mengakibatkan persoalan data pribadi dan data penting pada perusahaan atau lembaga (Riadi, Yudhana, & Yunanri, 2020).




| Month | Unique visitors | Number of visits | Pages | Hits | Bandwidth |
|---|---|---|---|---|---|
| Jan 2022 | 143 | 220 | 384 | 966 | 928.43 MB |
| Feb 2022 | 110 | 171 | 603 | 1,106 | 946.36 MB |
| Mar 2022 | 175 | 247 | 502 | 1,528 | 2.15 GB |
| Apr 2022 | 157 | 216 | 538 | 1,331 | 1.54 GB |
| May 2022 | 215 | 277 | 617 | 1,270 | 1.11 GB |
| Jun 2022 | 206 | 269 | 734 | 1,469 | 1.38 GB |
| Jul 2022 | 149 | 193 | 660 | 1,154 | 950.71 MB |
| Aug 2022 | 236 | 287 | 506 | 1,623 | 1.13 GB |
| Sep 2022 | 325 | 429 | 797 | 2,154 | 1.81 GB |
| Oct 2022 | 201 | 229 | 6,907 | 10,392 | 892.83 MB |
| Nov 2022 | 504 | 727 | 2,745 | 17,709 | 876.72 MB |
| **Dec 2022** | 636 | 893 | 3,512 | 10,323 | 568.34 MB |
| Total | 3,057 | 4,158 | 18,505 | 51,025 | 14.18 GB |

Gambar 2. Jumlah Pengunjung Website BMKG daerah X Tahun 2022

Pada penelitian ini dianalisis potensi celah keamanan pada website Badan Meteorologi Klimatologi dan Geofisika (BMKG) di suatu daerah X. Website ini dilakukan untuk melakukan diseminasi informasi cuaca dan iklim serta merupakan akses pelayanan data secara online kepada masyarakat. Pada Gambar 2 menunjukkan grafik dari admin yang melakukan pengecekan data jumlah pengunjung website pada 13 Desember 2022, website menunjukkan jumlah pengunjung yang fluktuatif dan meningkat secara drastis pada bulan November dan Desember 2022. Hal tersebut menunjukkan peningkatan pengguna *website* layanan data cuaca dan iklim tersebut. Maka diperlukan antisipasi dalam melakukan perlindungan data. Beberapa celah keamanan website yang diuji dilakukan menggunakan aplikasi Wireshark dan Nessus. Wireshark merupakan perangkat lunak yang memiliki kemampuan untuk menganalisis paket jaringan pada paket data yang melewati jaringan kemudian menampilkan dalam bentuk yang mudah dipahami. Wireshark mampu diterapkan pada kondisi berbeda seperti kasus jaringan, operasi keamanan, dan protokol pembelajaran internal. Wireshark tersedia pada berbagai protokol seperti TCP, UDP, dan HTTP ke protokol yaitu AppleTalk (Agustiara, Pratama, & Junaidi, 2022). Nessus memiliki kemampuan dalam melakukan pengujian *vulnerability scanning*. Hasil pengujian berupa daftar kerentanan dan penjelasan terhadap kerentanan, dampak dari kerentanan, persentase kerentanan, dan solusi dalam mengatasi kerentanan sehingga dapat digunakan untuk mengevaluasi dan meningkatkan keamanan terhadap *website* (Budiman, Ahdan, & Aziz, 2021).

Pada hasil analisis akan disusun beberapa model penanganan dalam mengantisipasi serangan pada *website*. Pada penelitian ini sisi keamanan yang diananlisis difokuskan pada penerapan SSL/TLS. Situs web yang aman biasanya memiliki sertifikat TLS/SSL. Sertifikat TLS/SSL adalah file data kecil berisi data kriptografi yang mengenkripsi tautan antara server dan browser. Manfaat menggunakan sertifikat TLS/SSL pada website selain untuk meningkatkan keamanan. TLS/SSL juga membantu meningkatkan peringkat situs web di mesin pencari internet dalam hasil pencarian mesin pencari (Ali, 2021). Protokol TLS/SSL memiliki dua kategori, antara lain *handshaking protocol*, dan *record protocol*. *Handshaking protocol* memiliki kemampuan menegosiasi *suite cipher*, melakukan autentikasi *server* dan klien dan menentukan *session keys*. Pada *record protocol* memiliki kemampuan mengamankan data aplikasi dengan *session keys* pada *record protocol* kemudian memverifikasi keaslian dan integritas aplikasi (Dastres & Soori, 2020). Keamanan dan keandalan pada sistem informasi adalah masalah penting bahwa pesan dikirim ke tujuan dengan kesalahan yang paling sedikit (Dewa, Pramukantoro, & Kartikasari, 2018).

## METODE PENELITIAN

Penelitian ini menggunakan aplikasi Wireshark. Wireshark adalah perangkat lunak untuk melakukan analisis jaringan yang berfungsi dalam menyediakan jaringan dan protokol serta memberikan informasi tentang data tertangkap pada jaringan. Perangkat lunak Wireshark dapat menganalisis transmisi paket data dalam jaringan, proses koneksi dan

transmisi data antar komputer (Ubaedila, Nurdiawan, Wijaya, & Sidik, 2021). Langkah selanjutnya pada penelitian ini adalah menganalisis website menggunakan *tool* Nessus yang merupakan alat untuk melakukan analisis kerentanan pada suatu website pada suatu jaringan (Aristian & Cholil, 2022). Analisis mendalam digunakan untuk menemukan kemampuan pada SSL/TLS yang diterapkan. SSL/TLS merupakan mekanisme situs web dalam membuat transmisi data yang aman dengan browser pengguna. Transmisi data seperti nama *user*, *password user*, informasi kartu kredit, dan semua informasi sensitif lain harus diamankan untuk mencegah pencurian data saat kita menjelajah suatu website. Keamanan memainkan peran penting dalam komunikasi data. SSL/TLS adalah protokol kriptografi untuk mengamankan komunikasi data melalui jaringan enkripsi data (Gunawan, Sitorus, Rahmat, & Hizriadi, 2018).

Pertama, objek yang digunakan pada penelitian ini adalah *website* salah satu kantor Badan Meteorologi Klimatologi dan Geofisika (BMKG) di suatu daerah X dengan domain (.com) menggunakan Wireshark pada Kamis, 23 Desember 2022. Website tersebut telah dianalisis menggunakan Wireshark dengan beberapa tahap antara lain; sign in, penangkapan informasi, identifikasi proses, proses handshaking, analisis sertikat SSL dan *server public key*, verifikasi, dan selesai.

Kedua, metode penelitian yang digunakan adalah *vulnerability assesment* dengan langkah-langkah tahapan berupa; *Identifying, Gathering, Scanning, Analisis*, dan *Report*. Pada metode ini *tool* yang digunakan untuk melakukan *vulnerability assesment* terhadap *website* adalah aplikasi Nessus untuk mendapatkan informasi kerentanan dan rekomendasi dalam mengantisipasi kerentanan. Dari hasil pengujian pada Jumat, 23 Desember 2022 pada website diperoleh penilaian dari aspek kerentanan pada keamanan informasi yang dapat digunakan sebagai evaluasi dan peningkatan keamanan terhadap operasional kinerja website. Berdasarkan kategori kerentanan yang terbagi pada pengujian dapat dilakukan penilaian berdasarkan tingkat kerentanan (Sirait & Putra, 2018). Penilaian tingkat kerentanan ditampilkan pada Tabel 1.

Tabel 1. Penilaian Tingkat Kerentanan

| Tingkat Kerentanan | Skor |
|---|---|
| Sangat Tinggi (Critical) | 10 – 9 |
| Tinggi (High) | 8 – 7 |
| Sedang (Medium) | 6 – 5 |
| Rendah (Low) | 4 – 2 |

Kerentanan pada sistem dan infrastruktur jaringan komputer dapat terjadi disebabkan oleh kesalahan yang bersumber dari faktor internal dan eksternal. Faktor internal berupa minimnya kesadaran administrator dalam menjalankan sistem aplikasi tersebut. Pada faktor eksternal berupa tingginya potensi tingkat kejahatan *cyber*. Hal tersebut menjadi acuan dalam langkah awal untuk melindungi dan mengamankan jaringan dengan membuat kebijakan yang terstandarisasi sebagai panduan operasional keamanan jaringan.

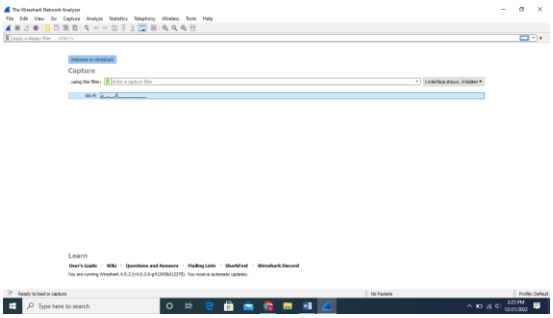
## HASIL DAN PEMBAHASAN

Pada pengujian pertama adalah analisis kemampuan SSL/TLS pada website BMKG daerah X menggunakan metode penelusuran paket data dengan bantuan aplikasi Wireshark. Aplikasi Wireshark dapat menangkap paket data secara langsung dari *network interface*. Aplikasi tersebut dapat menunjukkan informasi terperinci terkait hasil tangkapan. Kemampuan lain yang dimiliki adalah dapat melakukan *import* dan *export* hasil tangkapan antar perangkat. Langkah pertama yang dilakukan adalah melakukan akses masuk pada pengguna yang akan melakukan permohonan layanan data pada website.


Gambar 3. Halaman Login Website BMKG daerah X

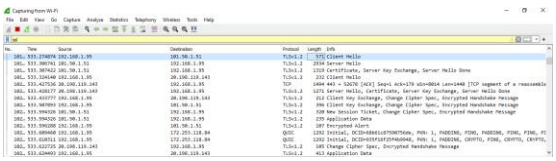
*JIKA (Jurnal of Informatics) Universitas Muhammadiyah Tangerang* *P ISSN : 2549-0710*
*Vol 7, No 2, April 2023, pp 183 – 192* *E ISSN : 2722-2713*
*DOI : 10.31000/jika.v7i2.7566*

Halaman login seperti pada Gambar 3 akan membuat koneksi SSL diperlukan dikarenakan pada halaman *login, web server* akan membuat koneksi SSL sebagai keamanan informasi *user* dari penyalahgunaan data. *Website* yang dioperasikan menggunakan alamat https telah menunjukkan bahwa *client* dan *server* telah melakukan koneksi SSL.



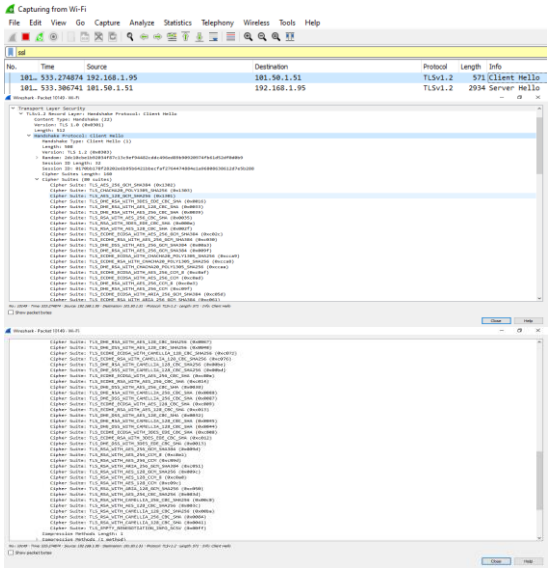
Gambar 4. *Interface Network* pada WiFi

Selanjutnya, masuk pada aplikasi Wireshark pada interface yang digunakan, pada pengujian ini koneksi internet yang diakses menggunakan Wi-Fi seperti ditunjukkan pada Gambar 4. Klik pada opsi wifi untuk melihat detail informasi bersamaan dengan mengakses *website*. Lakukan stop pada Wireshark saat *loading* sudah selesai. Pada proses tersebut Wireshark telah menangkap paket-paket yang diakses. Pada pengujian ini dilakukan pengambilan paket SSL dengan cara melakukan filter SSL.



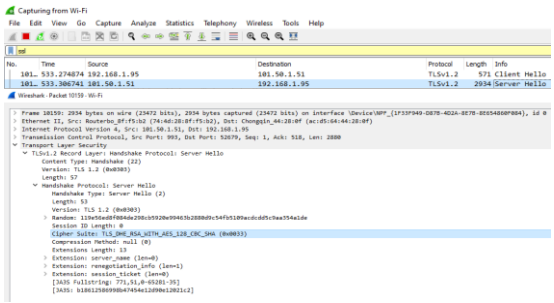
Gambar 5. Filter pada Identifikasi *Handshaking* SSL/TLS

Langkah kedua adalah identifikasi proses handshaking yang ditampilkan pada Gambar 5. IP 192.168.1.95 merupakan IP milik pengguna yang melakukan akses pada website tujuan, IP 101.50.1.51 adalah IP yang merupakan server website. Pada website tersebut SSL menggunakan protokol TLS versi 1.2. Langkah selanjutnya adalah mengidentifikasi *cipher suite* yang digunakan oleh TLS. *Cipher suite* adalah sekumpulan algoritma kriptografi. *Cipher suite* memberikan informasi penting tentang cara mengkomunikasikan data dengan aman saat menggunakan protokol HTTPS melalui TLS.



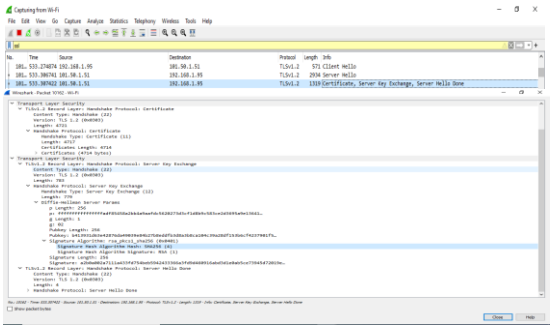
Gambar 6. Proses *Handshaking Client Hello*

Langkah ketiga adalah proses *handshaking* pada *client hello* yang ditampilkan pada Gambar 6. *Client hello* menggunakan TLS versi 1.2. *Session ID length* bernilai 32. *Client hello* menyediakan 80 *cipher suites* yang akan dipilih oleh server hello. *Client hello* juga memiliki satu *compression methods*.



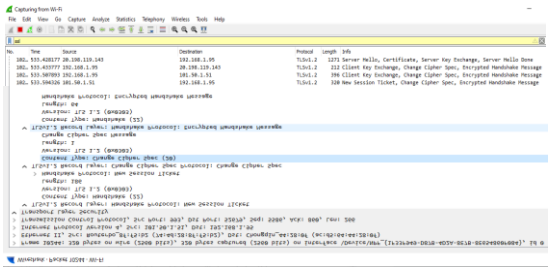
Gambar 7. Proses *Handshaking Server Hello*

Pada tahap proses handshaking menunjukkan *server hello* merespon yang terlihat pada gambar 7. *Server hello* menggunakan TLS 1.2. *Server hello* memilih *cipher suite* yang paling baik yang disediakan oleh *client hello* dan *server hello* memilih *methods compression null* (0) yang disediakan oleh *client hello*. Langkah keempat melakukan pemberian sertifikat SSL dan *server public key*.



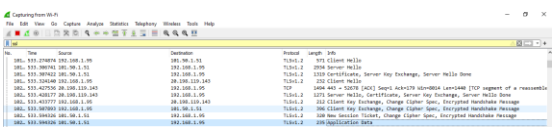
Gambar 8. Pemberian sertifikat SSL dan *Server Public Key*

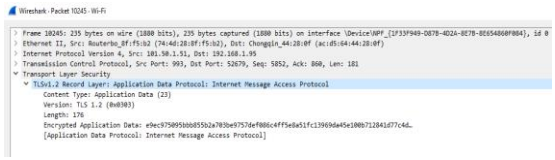
Setelah proses *handshaking* dilakukan, maka server akan memberikan sertifikat website kepada user beserta server public key yang bertujuan untuk mengamankan keamanan informasi pengguna dan memastikan pengguna adalah personal yang asli saat mengakses server website. Pada Gambar 8 ditampilkan bahwa *pubkey length* bernilai 256, kemudian dalam melakukan enkripsi data *web server* menggunakan algoritma hash SHA256. Kemudian langkah kelima adalah melakukan verifikasi sertifikat dan pemberian *client public key*.



Gambar 9. Verifikasi Sertifikat dan *Client Public Key*

*Client* telah melakukan verifikasi sertifikat yang diberikan *web server* ditunjukkan pada Gambar 9. Sertifikat SSL yang digunakan adalah TLS versi 1.2. TLS versi 1.2 dapat melakukan *handshake* protokol untuk mendapatkan *new session ticket*. Kemudian TLS versi 1.2 dapat melakukan *Change Cipher Spec Protocol* dan berhasil melakukan pesan *handshake* terenkripsi.





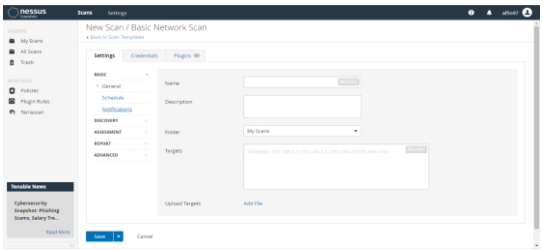
Gambar 10. Pertukaran Data *Client* dan *Server*

Langkah keenam pada Gambar 10 menunjukkan bahwa *client* dan *server* sudah siap dalam melakukan pertukaran data. Setelah *session ticket* dikirim oleh *client* ke web server, maka *web server* akan melakukan dekripsi *ticket* dan kemudian *client* dan *server* siap melakukan pertukaran data.

Pada pengujian kedua adalah melakukan analisis kerentanan suatu website. Aplikasi *tool* yang digunakan adalah Nessus. Nessus mampu melakukan *multiple network scanning* (IP, IPv6, Hybrid), *automatic scanning scheduler*, *custom report* dan *notification*. Tahapan pertama yang dilakukan adalah mengidentifikasi *website* sebagai objek pemindaian, *website* yang akan dilakukan pemindaian adalah website BMKG daerah X dengan domain .com dan langkah kedua adalah menentukan *tool* yang digunakan.


Gambar 11. Halaman Login Nessus

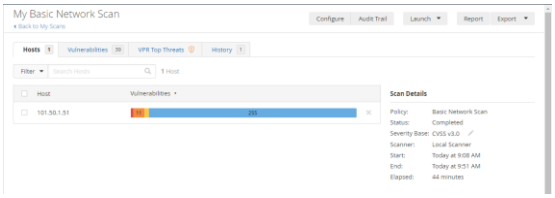
Gambar 11 merupakan tampilan awal *dashboard* pada *login* aplikasi *browser* dari Nessus menggunakan alamat dari *localhost*. Sebelum memulai aktivitas aplikasi, pengguna perlu mendaftarkan terlebih dahulu. Akses *login* yang diperoleh berupa *username* dan *password*.



*JIKA (Jurnal of Informatics) Universitas Muhammadiyah Tangerang* *P ISSN : 2549-0710*
*Vol 7, No 2, April 2023, pp 183 – 192* *E ISSN : 2722-2713*
*DOI : 10.31000/jika.v7i2.7566*

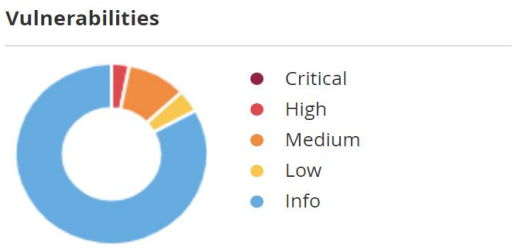
Gambar 12. Tampilan *Fitur Basic Network Scan*

Sebelum melakukan pemindaian jaringan pada *website*, kita tentukan fitur pada Nessus dalam melakukan pemindaian. Pada Gambar 12 menunjukkan pengujian menggunakan fitur *basic network scan*. Kemudian memasukkan target *website* berupa nama *website* atau alamat IP *website* yang akan dilakukan pengujian.



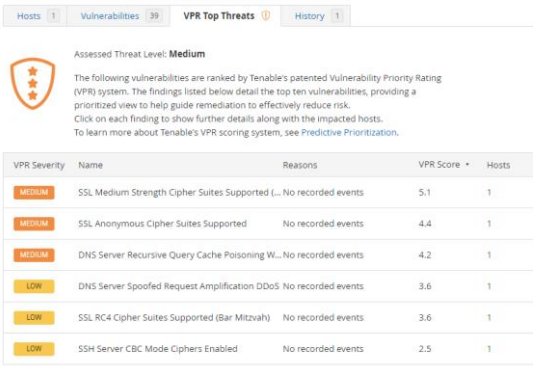

Gambar 13. Hasil Pemindaian Kerentanan

Setelah selesai melakukan pemindaian, aplikasi Nessus akan merangkum hasil pemindaian *vulnerability* berupa persentase tingkat kerentanan yang ditemukan seperti pada Gamabr 13. Pada tahapan ini merupakan langkah analisis Tingkatan kerentanan yang ditemukan pada Nessus ini antara lain; *critical*, *high*, *medium*, *low*, dan *info*. Pada proses pemindaian menggunakan pemindai lokal dimulai dari jam 9.08 AM sampai 9.51 AM. Durasi pemindaian selama 44 menit.




Gambar 14. Persentase Hasil Pemindaian Kerentanan

Pada Gamabr 14 menunjukkan persentase kerentanan diperoleh dari angka kerentanan dari seluruh informasi yang ditemukan pada proses pemindaian. Hasil persentase memudahkan untuk mengetahui tingkat kerentanan yang dimiliki *website*. Dari hasil tersebut dapat dijadikan bahan dalam menentukan evaluasi yang dilakukan. Pada website BMKG daerah X ditemukan *0% critical, 3% high, 10% medium, 4% low,* dan 83% berupa informasi.




Gambar 15. Hasil Kerentanan dengan Skor Tertinggi

Dari hasil kerentanan yang ditampilkan pada Gambar 15, sistem pemindai memberikan skor pada setiap kerentanan yang ditemukan. Skor yang tinggi menunjukkan prioritas untuk dilakukan tindak lanjut keamanan *website*. Nessus memberikan rekomendasi pada kerentanan yang memiliki skor tertinggi. Pada pengujian ini ditemukan enam kerentanan pada SSL/TLS dengan tingkat *low* dan *medium* dengan skor tertinggi. Berikut deskripsi dan identifikasi faktor yang menimbulkan serta resiko yang dapat terjadi pada setiap kerentanan pada SSL/TLS yang ditemukan sebagai *Vulnerability Priority Rating* (VPR) antara lain:

**a. SSL Medium Strength Cipher Suites Supported (SWEET32)**

Informasi kerentanan pada SSL/TLS yang memiliki skor 5,1 dengan tingkat medium. Kerentanan ini ada di tingkat medium karena ditemukan host jarak jauh mendukung penggunaan penyandian SSL yang menawarkan enkripsi berkekuatan sedang. Faktor pencetusnya adalah Nessus menganggap kekuatan sedang sebagai enkripsi yang menggunakan panjang kunci setidaknya 64 bit dan kurang dari 112 bit atau yang menggunakan rangkaian enkripsi 3DES. Resiko yang dapat terjadi adalah layanan jarak jauh lebih mudah untuk menghindari enkripsi kekuatan sedang jika penyerang berada di jaringan fisik yang sama. Solusi yang disarankan adalah melakukan konfigurasi ulang aplikasi yang terpengaruh jika

memungkinkan untuk menghindari penggunaan *cipher* berkekuatan sedang.

**b. SSL Anonymous Cipher Suites Supported**

Informasi kerentanan SSL/TLS yang memiliki skor 4,4 dengan tingkat medium. Kerentanan ini berada di tingkat medium karena ditemukan host jarak jauh mendukung penggunaan penyandian SSL anonim. Faktor pencetusnya adalah kasus ini jauh lebih mudah untuk terjadi eksploitasi jika penyerang berada di jaringan fisik yang sama. Resiko yang dapat terjadi adalah memungkinkan administrator untuk menyiapkan layanan yang mengenkripsi lalu lintas tanpa harus membuat dan mengonfigurasi sertifikat SSL. Layanan ini tidak menawarkan cara untuk memverifikasi identitas host jarak jauh dan membuat layanan rentan terhadap serangan *man-in-the-middle*. Solusi yang disarankan adalah konfigurasikan ulang aplikasi yang terpengaruh jika memungkinkan untuk menghindari penggunaan *cipher* yang lemah.

**c. SSL RC4 Cipher Suites Supported (Bar Mitzvah)**

Informasi kerentanan yang memiliki skor 3,6 dengan tingkat *low*. Kerentanan ini berada di tingkat *low* karena ditemukan layanan jarak jauh mendukung penggunaan *cipher RC4*. Faktor pencetusnya adalah terdapat *host* jarak jauh mendukung penggunaan RC4 dalam satu atau lebih *cipher suite. Cipher RC4* memiliki kekurangan dalam menghasilkan aliran byte pseudo-random sehingga berbagai bias kecil dimasukkan ke dalam aliran, mengurangi keacakannya. Resiko yang dapat terjadi adalah jika teks biasa dienkripsi berulang kali seperti *cookie* HTTP dan penyerang dapat memperoleh banyak yaitu, puluhan juta teks sandi, penyerang mungkin dapat memperoleh teks biasa. Solusi yang disarankan adalah melakukan konfigurasi ulang aplikasi yang terpengaruh, jika memungkinkan, untuk menghindari penggunaan *cipher RC4*. Solusi yang disarankan adalah pertimbangkan untuk menggunakan TLS 1.2 dengan *suite* AES-GCM yang dapat dikendalikan pada dukungan *browser* dan *web server*.

Berdasarkan analisis dan laporan kerentanan pada sebuah website BMKG daerah X menunjukkan level resiko secara keseluruhan adalah "*Medium*" ditunjukkan pada *Assessed Threat Level* pada SSL/TLS menunjukkan skor 5.1, 4.4, dan 3,6 pada *Vulnerability Priority Rating (VPR) Score*. Terdapat tiga informasi prioritas pada SSL/TLS yang mendapatkan rekomendasi pada kerentanan memerlukan tindak lanjut perbaikan dalam mengurangi resiko kerentanan. Jadi pada *vulneravility assessment* yang dilakukan pada website menggunakan aplikasi Nessus menunjukkan tingkat kerentanan level menengah. karena mempunyai dampak pada pada keamanan informasi pengguna website, maka pihak pengelola *website* perlu melakukan evaluasi terhadap kerentanan yang ditemukan untuk mengurangi dampak resiko yang terjadi.

## KESIMPULAN

Pada analisis *website* BMKG daerah X dapat dilakukan menggunakan aplikasi Wireshark. Hasil menunjukkan pada metode penelusuran paket data pada kemampuan SSL/TLS menunjukkan bahwa web server sudah dilakukan verifikasi sertifikat SLL dan server public key dengan protokol terbaru TLS versi 1.2 sehingga mampu melakukan perlindungan data pengguna dengan cara melakukan enkripsi antara client dan web server menggunaka algoritma hash SHA256 untuk melakukan pertukaran data secara aman. Pada analisis *website* BMKG daerah X menggunakan metode pemindaian berupa *vulnerability* assessment dengan aplikasi Nessus menunjukkan bahwa level resiko secara keseluruhan pada Assessed Threat Level adalah "Medium". Hasil pemindaian merangkum dengan *vulnerability priority rating (VPR) score* menemukan tiga informasi kerentanan SSL/TLS yang membutuhkan tindakan evaluasi dan tindak lanjut dalam mengurangi resiko kerentanan pada *website*.

Saran untuk penelitian selanjutnya adalah dapat menggunakan tool yang lebih detail dalam mengukur kerentanan suatu sistem informasi beserta dampak yang lebih

rinci. Penelitian untuk mengukur kerentanan suatu website dapat dilakukan secara spesifik terhadap jenis serangan siber yang paling berpeluang terjadi di masa mendatang dan ditambahkan pengembangan pada sistem peningkatan keamanan yang diterapkan lebih baik dari metode penelitan sebelumnya dibuktikan dengan pengujian yang dilakukan

## UCAPAN TERIMA KASIH

Ucapan rasa terima kasih saya haturkan kepada Bapak Dr. Erik Iman Heri Ujianto, ST., M.Kom., Dr. Rianto, S.Kom., M.Eng. selaku dosen Information Sistem Security Magister Teknologi Informasi Universitas Teknologi Yogyakarta yang telah membimbing dan memberikan dukungan secara teknis dan materi dalam proses penulisan naskah jurnal sehingga dapat menyelesaikan penelitian ini.

## REFERENSI

Adeenze-Kangah, J., & Chen, Y. (2019). Detecting Proper SSL/TLS Implementation with Usage Patterns. *Journal of Physics: Conference Series, 1176*, 1-7 www.google.com.

Agustiara, W., Pratama, A., & Junaidi, S. (2022). Analisis Keamanan Protokol Secure Socket Layer terhadap Serangan Packet Sniffing pada Website Portal Berita Harian Umum Koran Padang. *JTIK (Jurnal Teknik Informatika Kaputama), 6(1)*, 10-15.

Ali, I. (2021). Examining cyber security implementation through TLS/SSL on academic institutional repository in Indonesia. *Berkala Ilmu Perpustakaan dan Informasi, 17(2)*, 238-249.

Aristian, & Cholil, W. (2022). Analisis Vulnerability Terhadap Website Lembaga Bahasa LIA Palembang Menggunakan Nessus, Netsparker dan Acunetic. *Jurnal Pendidikan dan Konseling, 4(4)* , 2459-2473.

Arshad, M., & Ali Hussain, M. (2016). Secure Framework to Mitigate Man-in-the-Middle Attack over SSL Protocol. *Indian Journal of Science and Technology, 9*(47), 1-5.

Budihardjo, E. W., Dewi, L. P., & Noertjahyana, A. (2021). Pembuatan Konfigurasi SSL yang Aman untuk Diimplementasikan pada Apache dan Nginx . *Jurnal Infra , 9(2)*, 1-6.

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas ABC dengan Vulnerability Assesment. *Jurnal Komputasi , 9(2)* , 1-10.

Dastres, R., & Soori, M. (2020). Secure Socket Layer in the Network and Web Security. *International Journal of Computer and Information Engineering, 14(10)*, 330-333.

Dewa, D. H., Pramukantoro, E. S., & Kartikasari, D. P. (2018). Analisis Mekanisme Keamanan Antara TLS/SSL Dan Crypto Pada Komunikasi IoT Middleware Dengan Subscriber Berbasis Protokol HTTP. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2(10)*, 4027-4033.

Fatimah. (2018, January 9). *Analisis SSL (Secure Socket Layer) Pada Website*. Retrieved from Nanachan: https://nanachan1924.wordpress.com/2018/01/09/analisis-ssl-secure-socket-layer-pada-sebuah-website/

Gunawan, D., Sitorus, E. H., Rahmat, R. F., & Hizriadi, A. (2018). SSL/TLS Vulnerability Detection Using Black Box Approach. *Journal of Physics: Conference Series , 978*, 28-30.

Kumari, N., & Mohapatra, A. (2022). A comprehensive and critical analysis of TLS 1.3. *Journal of Information and Optimization Sciences, 43*(4), 689-703.

Riadi, I., Yudhana, A., & Yunanri. (2020). Analisis Keamanan Website Open Journal System menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 7*, 853-860.

S, G., Govindaraju, & Elango. (2019). An Approach to Implement Cryptographic Protocol Version Downgrade Within a Secure Internal Network: TLS 1.x to SSL. *International Journal of Interactive Mobile Technologies (iJIM), 13*, 179-187.

Sahren. (2021). Implementasi SSL untuk Pencegahan Man in the Middle Attack pada FTP Server. *Journal of Science and Social Research, IV(1)*, 28 - 33.

Sirait, F., & Putra, M. S. (2018). Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. *Jurnal Teknologi Elektro, 9*, 16-22.

Ubaedila, I., Nurdiawan, O., Wijaya, Y. A., & Sidik, J. (2021). Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark. *INFORMATICS FOR EDUCATORS AND PROFESSIONALS, 6*, 95-104.

Vimy, T., Wiranto, S., Rudiyanto, Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan, 6*, 2319-2317.

Wahanani, H. E., Aditiawan, F. P., & Mumpuni, R. (2020). Uji Coba Serangan Man in The Middle pada Keamanan SSL Protokol HTTP. *Jurnal Sistem Informasi Dan Bisnis Cerdas, 13*(1), 21-26.