Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

ANALISIS AUDIT KEAMANAN INFORMASI WEBSITE DARI DROWN ATTACK MENGGUNAKAN NETWORK MAPPER DAN QUALYS SSL

Alfin Syarifuddin Syahab

[1]Magister Teknologi Informasi, Universitas Teknologi Yogyakarta, Yogyakarta
Jl. Siliwangi Jl. Ring Road Utara, Jombor Lor, Sendangadi, Kec. Mlati, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55285
[1] alfin.syahab@bmkg.go.id

Abstract

Stasiun Klimatologi D.I. Yogyakarta has a website with the domain staklimyogyakarta.com is a website used as a dissemination of climate, weather, and air quality information also the data services. The website has early warning system about climate condition in Yogyakarta region. Considering this website can be accessed widely and continuously, it is considered important to give attention to the security of the website to be able to operate optimally, the website must be guaranteed security. This study aims to audit information security on the website staklimyogyakarta.com using the NMap (Network Mapper) and Qualys SSL Labs. Network mapping helps to discover and visualize network connectivity by generating a network map. This map contains network diagrams, flowcharts, device inventories, and topology detection and Qualys SSL Labs gives the the group of information about documents, tools and thoughts related to SSL. Test results using NMap show that on the website staklimyogyakarta.com there are 17 ports open with 2 ports including filtered status and 983 ports are closed from 1000 ports that were successfully scanned on the Stasiun Klimatologi D.I. Yogyakarta website. The Stasiun Klimatologi D.I. Yogyakarta website has an SSL certificate and the SSL score obtained is A analyzed by Qualys SSL Labs and increase the security from DRWON attack with the SSL verse 2 is nonactive. Then there is a weakness on the website which is quite vulnerable to attacks from the open ports.

Keywords : *website, security, SSL, Nmap, drown*

Abstrak

Stasiun Klimatologi D.I. Yogyakarta memiliki situs web dengan domain staklimyogyakarta.com yang digunakan sebagai media dan sarana publikasi informasi cuaca, iklim, dan kualitas udara yang berlokasi di Sleman, D.I. Yogyakarta. Website ini berisi berbagai informasi yang berisi publikasi, iklim, cuaca, kualitas udara dan pelayanan data. Konten yang diunggah pada website tersebut diakses oleh publik secara ekstensif dan berkelanjutan, maka peru ditindaklajuti terkait kemampuan website dalam sisi keamanan informasi untuk dapat beroperasi optimal. Website tersebut harus terjamin keamanannya. Penelitian ini bertujuan untuk mengaudit keamanan informasi pada website staklimyogyakarta.com menggunakan tool NMap (Network Mapper) dan Qualys SSL Labs. Nmap membantu menemukan dan memvisualisasikan konektivitas jaringan dengan membuat peta jaringan. Peta ini berisi diagram jaringan, diagram alur, inventaris perangkat, dan deteksi topologi dan Qualys SSL Labs memberikan kumpulan dokumen, alat, dan pemikiran yang terkait dengan SSL. Hasil pengujian menggunakan NMap menunjukkan bahwa pada website staklimyogyakarta.com terdapat 17 port yang terbuka dengan 2 port diantaranya berstatus filtered dan 983 port tertutup dari 1000 port yang berhasil discan pada website Stasiun Klimatologi D.I. Yogyakarta. Hasil menggunakan Qualys SSL Labs menunjukkan website Stasiun Klimatologi D.I. Yogyakarta telah memiliki sertifikat SSL dan skor SSL yang didapat adalah A. Dengan status nonaktif pada SSL versi 2 dapat meningkatkan keamanan dari serangan DROWN melalui protokol SSL/TLS namun terdapat kerentanan pada 17 port terbuka.

Kata kunci : *website, keamanan, SSL, Nmap, drown.*

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

1. PENDAHULUAN

Perkembangan teknologi informasi secara signifikan dalam beberapa tahun ini memberikan pengaruh positif pada berbagai macam bidang. Salah satu bidang yang mendapat pengaruh positif dari perkembangan teknologi informasi adalah teknologi internet. Situs web adalah portal layanan yang dimanfaatkan banyak instansi pemerintah dan bisnis untuk melindungi data dan mendorong aktivitas operasional [1].

Informasi mempunyai bemacam bentuk format dianataranya adalah format teks, audio, visual, dan video. Berkaitan dengan hal tersebut maka diperlukan tindakan untuk melakukan manajemen pengelolaan informasi yang bertujuan untuk mengamankan aspek penting dari layanan situs web, yang dikenal sebagai CIA Triad. CIA Triad memiliki makna berupa kerahasian (confidentiality), keutuhan (integrity), dan ketersediaan (availability)[2].

Pada tahun 2017 serangan keamanan informasi menjadi kasus yang meningkat frekuensinya. Laporan kejadian pelanggaran atau serangan keamanan telah tercatat dengan rincian diperkirakan 32 % pada sektor bisnis dan 22 % pada badan amal [3]. Berdasarkan data serangan keamanan tersebut, maka diperlukan tindakan pelaksanaan audit untuk mengetahui dan mengevaluasi pengelolaan teknologi infomasi berupa situs web yang diterapkan dan dioperasikan.

Salah satu portal website yang sedang dikembangkan pada instansi pemerintah adalah layanan informasi milik Stasiun Klimatologi D. I. Yogyakarta. Instansi tersebut memliki situs web staklimyogyakarta.com [4]. Website ini bertujuan untuk diseminasi kepada pengguna dan masyarakat dalam bentuk publikasi, informasi iklim, cuaca, kualitas udara, dan pelayanan data. Website ini dapat diakses melalui smartphone dan dijalankan melalui beragam sistem operasi, seperti Windows, iOS dan Android.

Metode dalam melakukan analisis evaluasi kemanan sitstem informasi adalah dengan menggunakan tool Qualys SSL Labs. Tool ini memiliki kemampuan untuk melihat pengelolaan website dalam aspek control dan security [5]. Metode yang dugunakan adalah menganalisis di bagian protokol SSL (Secure Socket Layer). SSL (Secure Socket Layer) adalah teknologi keamanan data menggunakan prinsip enkripsi dan digunakan untuk mengatasi keamanan data yang sensitif pada bidang situs perbankan, perdagangan saham, dan e-commerce [6]. Tool Qualys SSL Labs bertujuan untuk mengetahui dan menganalisis serta melakukan tes konfigurasi SSL yang digunakan secara online dan open-source. Hasil dari pengecekan adalah berupa grade SSL dan informasi yang merinci terkait web server dan SSL yang digunakan [7].

Pada penelitian ini penulis akan menganalisis tingkat keamanan dan penilaian mengenai website instansi BMKG di Stasiun Klimatologi D.I. Yogyakarta menggunakan metode Qualys SSL Labs. Metode lain dalam melakukan analisis keamanan informasi pada website Stasiun Klimatologi D.I. Yogyakarta adalah dengan cara menganalisis port menggunakan software Nmap. Nmap memiliki kemampuan untuk melakukan pemindaian jaringan dengan skala besar dan digunakan untuk melakukan pemindaian host tunggal. NMAP (Network Mapper) adalah tool yang dapat digunakan khusus untuk eksplorasi jaringan dan audit keamanan jaringan secara *open-source* [8]. Dengan menggabungan dua metode tersebut diharapkan mampu memberikan evaluasi yang mendalam terhadap tata kelola dalam aspek keamanan website Stasiun Klimatologi Daerah Istimewa Yogyakarta.

2. TINJAUAN PUSTAKA

Sistem manajemen keamanan informasi mencakup aturan, proses, prinsip panduan, dan aset dan tindakan terkait, yang dilakukan secara bersama oleh suatu organisasi, untuk menjaga informasinya. Sistem tersebut adalah metodologi yang tertata dengan baik untuk membangun, menerapkan, mengoperasikan, memeriksa, menilai, mempertahankan dan menyempurnakan keamanan informasi organisasi untuk mencapai tujuan [9]. Sistem komputer juga memiliki kerentanan, seperti otentikasi yang lemah, kurangnya kontrol akses, kesalahan dalam program, sumber daya yang terbatas atau tidak mencukupi, dan perlindungan fisik yang tidak memadai. Dipasangkan dengan serangan yang kredibel, masing-masing kerentanan ini dapat membahayakan kerahasiaan, integritas, atau ketersediaan. Setiap vektor serangan berusaha untuk mengeksploitasi kerentanan tertentu [10].

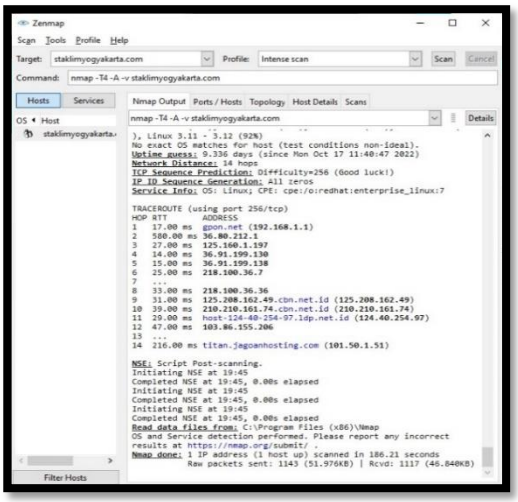
Celah kerentanan pada sitem informasi situs web mampu diidentifikasi menggunakan cara evaluasi keamanan situs web, evaluasi keamanan berfungsi untuk melacak celah-celah kerentanan yang menjadi kelemahan situs web. Kelemahan yang berpotensi mendapatkan serangan pada sistem yang terdapat pada sisi program, design, dan implementasi disebut sebagai *Vulnerability* [11].

Nmap memiliki kemampuan melakukan monitoring jaringan dengan skala long-distance dan dapat digunakan untuk melakukan pemindaian port. Tool Nmap bekerja dengan teknik mendeteksi alamat IP sebagai cara dalam

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

mendeteksi jumlah host aktif, port terbuka, penggunaan jenis sistem operasi, dan firewall [12]. Fitur pada Nmap memiliki peran tidak hanya untuk melakukan port scanning tetapi terus dikembangkan sebagai information gathering dan vulnerability scanning [13].

Nmap diakses pada untuk sistem operasi komputer seperti, Linux, Windows, dan Mac OS X. Pada Gambar 1 menunjukkan tampilan GUI Nmap pada menu halaman utama.



Gambar 1 Tampilan NMap

Nmap memliki beberapa fitur [14] antara lain:

a. Host Discovery untuk mengidentifikasi perangkat komputer pada jaringan.
b. Port Scanning untuk menghitung port yang terbuka pada perangkat komputer.
c. Version Detection untuk menilai layanan yang digunakan pada jaringan dan menentukan aplikasi dan versi yang digunakan.
d. OS Detection untuk menentukan sistem operasi yang digunakan perangkat komputer pada jaringan.
e. NMap Scripting Engine (NSE) untuk menulis dan membagi skrip sederhana untuk mengotomasi beragam tugas jaringan.

Berikut merupakan hasil pemindaian port yang terdiri dari beberapa kategori status. Pada Nmap memiliki enam kategori status pada port scanning yang dilakukan [15] antara lain:

a. Open

Status open menjelaskan bahwa aplikasi menerima koneksi paket TCP/UDP secara aktif pada port tersebut. Port terbuka ini dapat menjadi celah pada serangan kemanan informasi dengan cara eksploitasi dan dapat administrator antisipasi dengan fitur *firewall.*

b. Closed

Port tertutup berarti menutup akses aplikasi untuk menerima paket. Port tertutup menunjukkan host up untuk alamat IP (host discovery atau ping scanning) dan sebagai bagian deteksi sistem operasi.

c. Filtered

Status filtered menunjukan Nmap tidak mampu menentukan port terbuka karena packet filtering menghalangi probe dalam menjangkau port. Filter dapat dilakukan mengunakan device firewall, pengaturan router, atau software firewall pada host. Port tidak memberikan banyak informasi kepada penyerang. Sesekali mereka merespon dengan pesan kesalahan ICMP seperti tipe 3 kode 13 (tujuan tidak mampu dijangkau: komunikasi dilarang secara administrating).

d. Unfiltered

Status unfiltered menunjukkan port dapat diakses tetapi Nmap tidak mampu menentukan open atau closed. Pemindaian ACK saja yang digunakan untuk mengecek pengaturan firewall, menggolongkan port pada status ini. Pemeriksaan port unfiltered dengan tipe pemeriksaan seperti Window scan, SYN scan, atau FIN scan, mampu membantu melacak kondisi port terbuka.

e. Open filtered

Status open filtered adalah dalam kondisi tidak mampu menentukan port open atau filtered. Jenis pemeriksaan open filtered saat port terbuka tidak melakukan respon. Tidak ada tanggapan menunjukkan kondisi juga bahwa packet filter menurunkan respon yang diberikan. Nmap tidak dapat mengetahui dengan tepat kondisi port terbuka atau difilter. Kondisi ini digunakan untuk memindai UDP, IP protocol, FIN, NULL, dan Xmas.

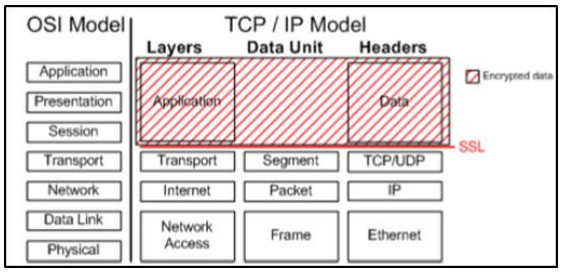
f. Closed filtered

Status closed filtered adalah kondisi ketika Nmap tidak dapat menentukan port dalam status tertutup atau filtered. Port kondisi ini diterapkan dalam scan idle ID IP saja.

SSL (Secure Socket Layer) merupakan sistem sebuah situs web yang memiliki koneksi secara aman melalui browser web pengguna. Setiap pengguna mengakses situs yang menerapkan teknologi SSL akan terpasang koneksi aman selama sesi browsing berlangsung antara browser pengguna dan web server. SSL merupakan standar industri dalam komunikasi website dengan aman dan diterapkan sebagai proteksi dari jutaan transaksi online setiap hari. Web server perlu mempunyai sertifikat SSL agar dapatl melakukan koneksi SSL [16].

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

SSL/TLS memiliki kedudukan di bawah protokol aplikasi dan mampu digunakan oleh berbagai aplikasi. Pengguna internet dapat mengecek melalui alamat https:// yang menandakan koneksi terenkripsi daripada melalui http://. Menurut OSI Model standard, protokol SSL terletak diantara application layer dan transport layer. Pada arsitektur TCP/IP, SSL terletak di layer application, seperti pada Gambar 2 berikut ini.



Gambar 2 Letak SSL

Qualys SSL Labs merupakan suatu tool yang digunakan untuk analisis terhadap konfigurasi server web SSL di internet publik. SSL Labs menggunakan empat langkah untuk memberikan rating maupun nilai pada suatu halaman website dengan protokol SSL/TLS [17] yaitu:

a. Pertama, memastikan sertifikat valid dan terpercaya.
b. Kedua, memeriksa konfigurasi server dalam tiga kategori yaitu protocol support, key exchange dan password.
c. Ketiga, menggabungkan grade kategori menjadi grade keseluruhan (dituliskan berupa angka 0 sampai 100).
d. Terakhir, grade huruf merupakan konversi dari rentang grade angka, seperti pada Tabel 1.

Selain itu, SSL Labs juga menerapkan serangkaian aturan untuk mengecek beberapa konfigurasi server dalam beberapa aspek yang tidak dapat diekspresikan melalui nilai numerik. Aspek tersebut dapat mengurangi atau menambah nilai tergantung pada konfigurasi yang ditemukan.

Tabel 1 Penilaian Qualys SSL Labs

Numeric Value	Grade
Nilai ≥ 80	A
Nilai ≥ 65	B
Nilai ≥ 50	C
Nilai ≥ 35	D
Nilai ≥ 20	E
Nilai < 20	F

SSL merupakan protokol keamanan yang dirancang untuk dioperasikan ke dalam TCP/IP yang efektif dalam melakukan pengidentifikasian keamanan informasi. Selain untuk aspek keamanan, situs wes yang menggunakan SSL dapat tampil lebih baik dalam hasil pencarian pada mesin pencarian seperti Google [18].

Pada penelitian ini merupakan analisis mendalam terkait website yang menggunakan dua metode yang berbeda untuk saling melengkapi dalam sisi SSL/TLS dan HHTPS network pada sebuah website dimana hal tersebut merupakan aspek penting dalam system keamanan informasi terutama dampak dari serangan DROWN. DROWN merupakan kerentanan serius memiliki dampak pada HTTPS dan layanan pada SSL dan TLS. DROWN memberikan peluang pada penyerang untuk membuka enkripsi dan membaca kemudian mengambil alih komunikasi sensitif, termasuk kata sandi, nomor kartu kredit, rahasia dagang, atau data keuangan [19].

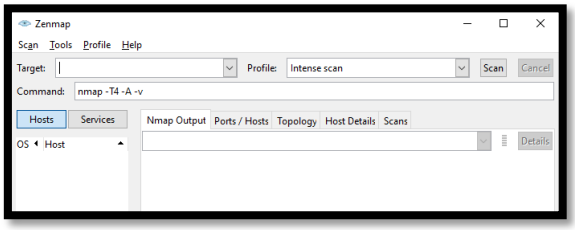
3. METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Pengujian dilaksanakan pada Rabu, 26 Oktober 2022 pukul 19.30 WIB di website Stasiun Klimatologi D.I. Yogyakarta. Metode pengujian dilakukan dengan menggunakan dua alat yaitu Qualys SSL Labs dan Network Mapper. Kedua alat ini saling terkait untuk memberikan analisis mengenai keamanan protokol SSL/TLS melalui HTTPS. Transport Layer Security (TLS) adalah versi baru dari protokol Secure Sockets Layer 3 (SSLv3) yang tidak lagi direkomendasikan untuk digunakan karena kerentanan keamanannya. Ini memberikan kerahasiaan, integritas data, non-penolakan, perlindungan replay, dan otentikasi melalui sertifikat digital langsung melalui protokol TCP.

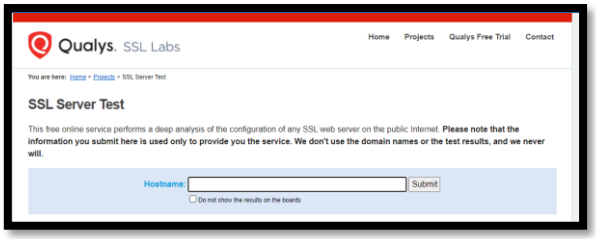
Protokol TLS saat ini digunakan untuk mengamankan protokol jaringan yang paling umum, seperti HTTP, FTP, dan SMTP, dan merupakan bagian dari protokol Voice over Internet Protocol (VoIP) dan Virtual Private Network (VPN). Dalam analisis ini akan fokus pada penggunaan SSL/TLS dalam protokol HTTP yang dikenal dengan HTTPS (Husák et al, 2016) yang merupakan penggunaan TLS. Berikut pembahasan metode penelitian yang dilakukan dengan menggunakan Network Mapper dan Qualys SSL Labs.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 3 Halaman Utama Software NMAP

Pertama, membuka software Nmap menggunakan sistem operasi windows, Pada halaman utama masukkan pada kolom target berupa nama situs web yang akan dilakukan *scanning* dan pilih profile scan adalah intense scan dengan menggunakan perintah nmap, yaitu nmap -T4 -A -v staklimyogyakarta.com., kemudian klik scan dan tunggu hingga proses *scanning* selesai. Diperoleh hasilnya pada opsi nmap output, port/host, topology, host detail, dan scans.



Gambar 4 Halaman Utama Qualys SSL Labs

Kedua, pengecekan sertifikat SSL bisa menggunakan Qualys SSL Labs. Tahapan ini dilakukan dengan memasukkan alamat web staklimyogyakarta.com pada laman web https://www.ssllabs.com/ssltest/index.html kemudian lakukan submit. Stelah melakukan submit sistem akan melakukan *scanning* terhadap target untuk mengumpulkan informasi terkait keamanan dan fitur yang digunakan. Kemudian akan diperoleh sertifikat-sertifikat yang berisi terkait fitur kemanan yang digunakan dan *grade* sistem keamanan yang diterapkan.

3.2. Pengumpulan Data

Pengumpulan data adalah dengan mengambil informasi penting yang berada dalam hasil testing pada setiap tools yang digunakan. Pada tool Qualys SSL Lab data diperoleh pada sertifikat yang tertera secara valid. Dari sertifikat diperoleh fitur dan protocol SSL/TLS yang digunakan sebagai indeks dari tingkat keamanan website.

Pengumpulan data selanjutnya menggunakan tool Nmap adalah dengan melakukan tahapan analisis. Dengan cara melihat output dari scanning port yang dilakukan diperoleh daftar port-port dengan status kondisi, topology jaringan, dan detail pada host yang digunakan.

3.3. Analisa Data

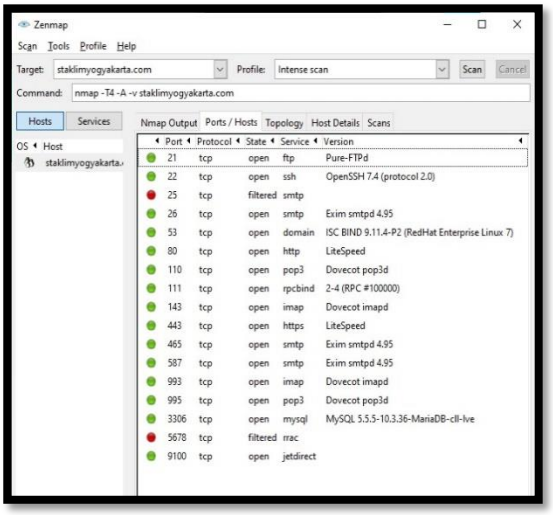
Data yang diperoleh pada Qualys SSL/Lab digunakan untuk melakukan analisis tingkat kemanan informasi pada sebuat situs web agar pengguna dapat mengetahui bagaimana melakukan pengelolaan dan antisipasi untuk melindungi dari serangan informasi dengan mengetahui protocol SLL/TLS yang diterapkan dan kemampuan yang dimiliki dalam melakukan keamanan informasi pada tingkat data dan aplikasi situs *web*.

Data yang diperoleh dari proses *scanning* yang dilakukan tool Nmap dilakukan untuk memperoleh kondisi status seluruh port-port yang digunakan, kemudian topologi jaringan yang digunakan, dan informasi rinci terkait host yang digunakan pengguna untuk menentukan celah-celah serangan informasi yang dapat dilakukan pada setiap port yang dipindai.

4. HASIL DAN PEMBAHASAN

Pengujian yang dilakukan menggunakan aplikasi *zenmap* memberikan beberapa hasil seperti jumlah dan jenis *port,* service tiap *port, topology,* dan deskripsi host. Fitur-fitur tersebut terletak pada navbar yang sejajar di sebelah bawah *command*. Fitur-fitur memudahkan untuk melihat informasi hasil dari *scanning* yang telah dilakukan. Berdasarkan hasil pengujian, dapat diketahui bahwa pada *website* BMKG Klimatologi Yogyakarta terdapat 15 *port* yang terbuka, 2 *port filtered* dan 983 *port* yang tertutup dari jumlah total 1000 *port* yang di *scanning.* Tampilan dari *port* yang terbuka dapat dilihat pada Gambar 5. Dari gambar tersebut dapat diketahui jumlah *port* yang terbuka dan *port* yang mana saja yang sedang aktif. Dapat dilihat juga alamat website yang sedang dianalisis serta *command* yang dipakai pada aplikasi ini.

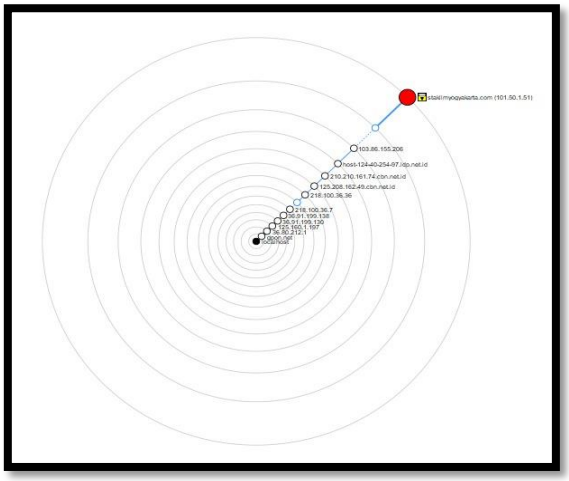
Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 5 Port Hasil Scan Nmap

Berdasarkan Gambar 5 diatas *port* yang terbuka adalah *port 80 dan port 110. Port 80* adalah jenis *port* pada sebuah jaringan yang sering digunakan sebagai *port* sebagai koneksi menuju *web server.* Kemudian *port 110* adalah *port* yang digunakan untuk mengoperasikan sebuah *server* yang aman yang disebut dengan *Secure Server Layer.*

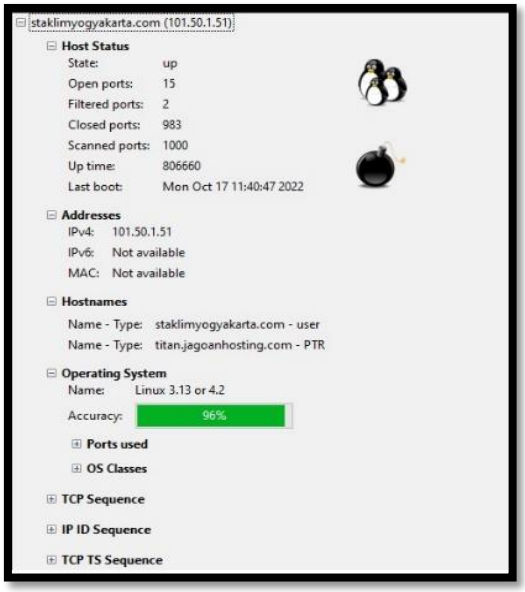
Setelah diketahui informasi port dapat diketahui informasi host dengan melihat pada aplikasi Nmap yang tersedia. Pada sebelah kanan fitur host/ports terdapat fitur topology untuk melihat skema dan traceroute jaringan yang digunakan.



Gambar 7 Traceroute website Stasiun Klimatologi D.I. Yogyakarta

Traceroute merupakan jalur yang menunjukkan rute yang dilewati paket untuk mencapai tujuan yaitu *website staklimyogyakarta.com.* Rute yang ditampilkan adalah daftar *interface router* yang terdapat pada jalur antara *client* dan *host* yang diuji *traceroute* dapat dilihat pada gambar 7.

Dari hasil pengujian juga dapat diketahui host secara menrinci dengan cara melihat pada menu host detail pada aplikasi Nmap. Fitur host detail terletak pada sebelah kanan dari fitur topology. Host detail akan mendeteksi dan meberikan informasi terkait host status, addresses, hostnames, operating system, dan informasi lainnya. Pada host detail menunjukkan bahwa *web server* yang digunakan menggunakan layanan dari Google.



Gambar 6 Deskripsi Host pada Hasil Pengujian

Hasil pengujian juga menunjukkan deskripsi dari *host* yang diuji. Parameter yang terdapat pada deskripsi *host* antara lain *host status, addresses, hostnames, operating system, TCP sequence, IP ID sequence, TCP TS sequence,* dan *comment.* Deskripsi *host* hasil pengujian pada *website* BMKG Klimatologi Yogyakarta dapat dilihat pada Gambar 6.

Berdasarkan Gambar 6 dapat diketahui bahwa alamat IPv4 dari *website* BMKG Klimatologi Yogyakarta adalah 101.50.1.51 dan statusnya adalah *up.* Detail sistem operasi (OS) yang digunakan adalah sebagai berikut:

- *Type = general purpose*
- *Vendor = Linux*
- *Family = Linux*
- *Generasi = 4X*

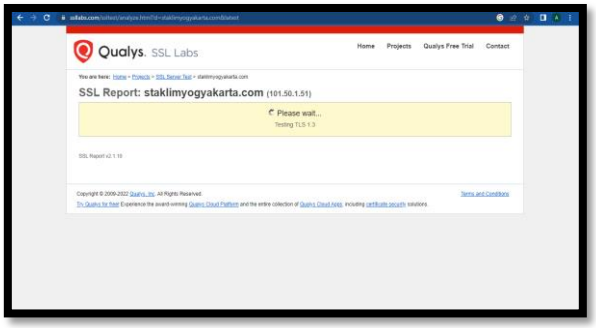
Hasil *scanning* menggunakan Network Mapper pada *website* Stasiun Klimatologi D.I. Yogyakarta mendapatkan port-port yang terbuka, topologi, dan detail host. Dari hasil tersebut dapat mengetahui port-port mana yang memerlukan

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

tindakan prefentif keamanan. Kemudian dari topologi dan detail host dapat diketahui sistem operasi dan address port yang digunakan.

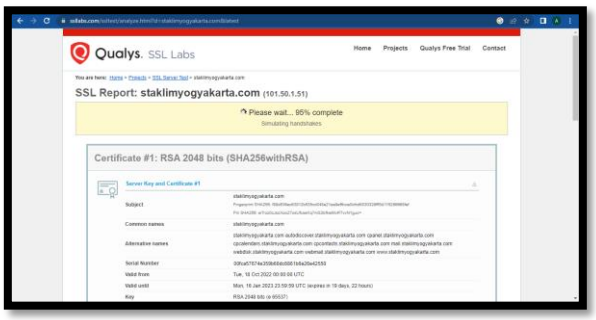
Pengujian sertifikat SSL dilakukan guna mengetahui apakah *website* Stasiun Klimatologi D. I. Yogyakarta menggunakan sistem keamanan digital yang memungkinkan komunikasi dienkripsi antar *website* dan *web browser.* Hal ini dikarenakan SSL adalah dengan mengunci *cryptographic key* sehingga data akan terenkripsi dengan baik selama proses transfer.

Langkah pertama yang dilakukan untuk mendapatkan hasil penilaian pada website adalah dengan memasukkan alamat website yang akan diuji pada menu utama dari Qualys SSL Labs. Setelah memasukkan alamat web kemudian melakukan submit pada website yang akan diuji. *Tool* Qualys SSL Labs akan melakukan pemindaian pada target yang dimasukkan. Pada Qualys SSL Labs, langkah kedua adalah pengujian protokol SSL/TLS yang digunakan. Pada website ini menerapkan SSL/TLS versi 1.2 dan versi 1.3 yang ditunjukkan pada Gambar 8.



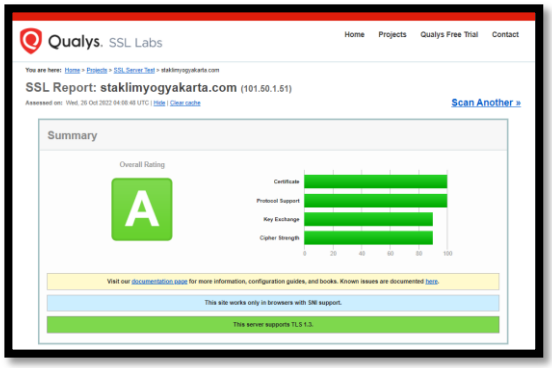
Gambar 8. Proses pengujian SSL/TLS

Langkah ketiga yang dilakukan adalah mengumpulkan informasi cipher suites yang digunakan dan melakukan simulasi handshakes pada client dan server yang ditunjukkan pada Gambar 9.



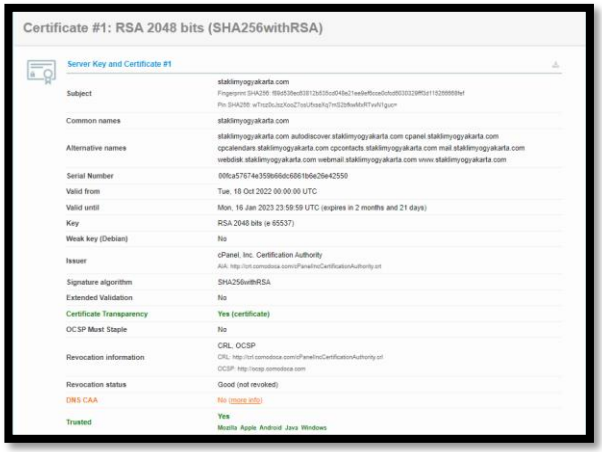
Gambar 9. Proses simulasi handshakes

Hasil akhir pengujian yang didapatkan dari QUALYS SSL Labs menunjukkan rating keamanan untuk *website* Stasiun Klimatologi D. I. Yogyakarta adalah A sebagaimana ditunjukkan oleh Gambar 10. Ketika pemindaian sudah selesai, maka Qualys SSL Lab akan merangkum hasil pemindaian dengan pemberian skor sesuai dengan tingkat keamanan website yang diuji. Dari gambar tersebut dapat dilihat terdapat rangkuman rating untuk *Certificate, Protocol Support, Key Exchange* dan *Cipher Strength.* Rata-rata yang dihasilkan diatas 80 yang menunjukkan nilai A.



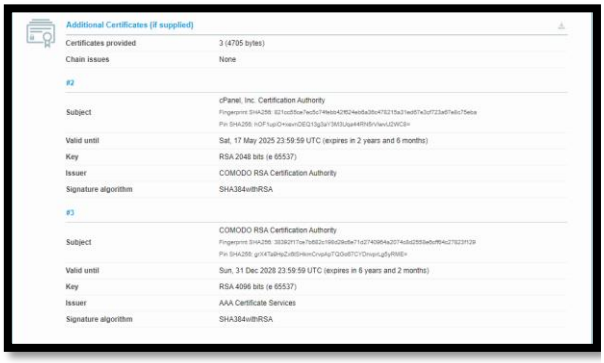
Gambar 10 Nilai SSL dari situs Stasiun Klimatologi D.I. Yogyakarta

Berdasarkan Gambar 10 *website* Stasiun Klimatologi D.I. Yogyakarta memiliki sertifikat SSL yang menandakan bahwa *website* tersebut menggunakan protokol HTTPS dalam mengkoneksikan dengan server. Dengan adanya sertifikat SSL akan tidak mudah pengguna menembus koneksi dan melakukan pencurian data.



Gambar 11 Sertifikat dari situs Stasiun Klimatologi D.I. Yogyakarta.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 6, Nomor 1, Januari 2023.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 12 Sertifikat tambahan dari situs Stasiun Klimatologi D.I. Yogyakarta.

Sertifikat yang dimiliki oleh *website* Stasiun Klimatologi D.I. Yogyakarta ditampilkan pada Gambar 11 dan Gambar 12. Sertifikat merupakan informasi secara rinci pada website dalam aspek keamanan dan implementasi yang digunakan.

Gambar 13 Protokol SSL *Website* Stasiun Klimatologi D.I. Yogyakarta

Protokol yang dapat digunakan untuk mengenkripsi komunikasi antara browser web dan situs web yang adalah TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, SSL 3 dan SSL 2. Pada situs Stasiun Klimatologi D.I. Yogyakarta sudah *support* protokol TLS 1.2 dan 1.3. Protokol TLS 1.0 dan 1.1 banyak di *support* oleh *web browser* namun kecepatannya tidak secepat dan seaman dari TLS 1.2 dan TLS 1.3. Untuk menjamin kerahasiaan dan keutuhan data yang dikirim melalui media yang tidak terpercaya, digunakan protokol Transport Layer Security (TLS). Ini adalah bagian penting dari infrastruktur keamanan internet saat ini.

TLS dirancang untuk keaslian, integritas, dan perlindungan kerahasiaan saluran komunikasi yang mendasarinya dengan menawarkan otentikasi yang aman, perlindungan integritas data, dan kerahasiaan melalui kriptografi asimetris dan simetris. TLS terletak di lapisan aplikasi tumpukan protokol kontrol transmisi (TCP)/protokol internet (IP) dan dapat membungkus serta mengamankan koneksi HTTP. Koneksi HTTP yang diamankan TLS disebut koneksi HTTP Secure (HTTPS). Tampilan dari *protocol* yang digunakan dapat dilihat pada Gambar 11.

Hasil penilaian dari Qualys SSL Labs pada *website* Stasiun Klimatologi D.I. Yogyakarta mendapatkan skor A. Protokol yang diterapkan pada website tersebut sudah menggunakan TLS 1.3. Protokol TLS 1.3 memiliki keunggulan dalam perlindungan terhadap serangan *downgrade* dan memiliki kinerja privasi kepada pengguna. Penggunaan protokol TLS versi 1.2 dan TLS versi 1.3 juga dapat meningkatkan keandalan dalam mengatasi serangan DROWN. Antisipasi dalam meningkatkan pertahanan terhadap serangan DROWN dapat dilakukan juga dengan cara menonaktifkan protokol SSLv2 di semua server SSL/TLS dan menonaktifkan semua cipher SSLv2 dengan ketentuan patch untuk CVE-2015-3197 telah diterapkan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis yang telah dilakukan dapat diambil beberapa kesimpulan, antara lain, Pertama, pada analisis situs web Stasiun Klimatologi D.I. Yogyakarta menggunakan tool NMAP menunjukkan bahwa kondisi aman terhadap potensi serangan informasi ditunjukkan dengan terdapat 17 *port* yang terbuka dengan 2 port diantaranya berstatus *filtered* dan 983 *port* yang tertutup dari 1000 *port* yang berhasil discan pada *website* tersebut. Kedua, *Website* Stasiun Klimatologi D.I. Yogyakarta menggunakan tool Qualys SSL Labs telah memiliki sertifikat SSL/TLS dan skor SSL yang baik dalam aspek *Certificate, Protocol Support, Key Exchange* dan *Cipher Strength* ditunjukkan dengan mendapatkan grade A. Hal tesebut menunjukkan keamanan yang handal pada website dari sisi Jaringan dan SSL/TLS terhadap serangan luar sistem berupa DROWN attack.

6. UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada Bapak Andri Setiyaji selaku Dosen Mata Kuliah Sistem Keamanan Informasi dan Rekan-Rekan di Badan Meteorologi Klimatologi dan Geofisika yang telah memberikan dukungan dalam penyusunan naskah jurnal ini.

DAFTAR PUSTAKA

[1] A. Hermawan, T. Hartati and Y. A. Wijaya, "Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad," *Jurnal Informatika: Jurnal pengembangan IT (JPIT),* vol. 7 Nomor 3, pp. 125-130, 2022.

[2] A. Pambudi, "Audit Keamanan Informasi Berdasarkan Triangle CIA Menggunakan

Framework COBIT® 4.1," *INTECHNO JOURNAL,* vol. 1 No.4, pp. 47-56, 2019.

[3] D. Digital Culture Media & Sport, "Cyber Security Branches Survey 2019," University of Portsmouth, 1 Juli 2009. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019. [Accessed 1 November 2022].

[4] S. Yogyakarta, "Stasiun Klimatologi Yogyakarta," BMKG, 20 Oktober 2022. [Online]. Available: https://staklimyogyakarta.com/. [Accessed 1 November 2022].

[5] Safarudin and M. S, "Analisis Kepuasan Pengguna MarketplaceTokopedia Dengan Metode PIECES di Tokopedia Community Batam," *SNISTEK,* vol. 1, pp. 109-114, 2018.

[6] Novi and Zaini, "Secure Socket Layer untuk Keamanan Data Rekam Medis Tumorotak Pada Health Information System," *Jurnal Nasional Teknik Elektro* , vol. 6 Nomor 3, pp. 137-142, 2017.

[7] E. W. Budihardjo, L. P. Dewi and A. Noertjahyana, "Pembuatan Konfigurasi SSL yang Aman untuk Diimplementasikan pada Apache dan Nginx," *JURNAL INFRA,* vol. 9 Nomor 2, pp. 1-6, 2021.

[8] D. B. Rendro, Ngatono and W. N. Aji, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di SMK Negeri 1 Kota Serang).," *Jurnal PROSISKO* , vol. 7 Nomor 2, pp. 108-115, 2020.

[9] W. Yustanti, A. Qoiriah, R. Bisma and A. Prihanto, "An analysis of Indonesia's information security index: a case study in a public university," *The Consortium of Asia-Pacific Education Universities (CAPEU),* vol. 296, pp. 1-7, 2018.

[10] B. Raharjo, Keamanan Sistem Informasi, Semarang: Yayasan Prima Agus Teknik, 2021.

[11] A. M. Tania, D. Setiyadi and F. N. Khasanah, "Keamanan Website Menggunakan Vulnerability," *INFORMATICS FOR EDUCATORS AND PROFESSIONALS,* vol. 2 Nomor 2, pp. 171-180, 2018.

[12] M. R. Fahlevi and D. R. D. Putri, "Analisis Monitoring & Kinerjasistem Keamanan Jaringan Komputer Menggunakan Nmap (Studi Kasus: Raz Hotel & Convention Medan)," *IT Journal,* vol. 9 Nomor 1, pp. 35-43, 2021.

[13] M. Doel, Panduan Hacking Website dengan Kali Linux, Jakarta: Elex Media Komputindo, 2016.

[14] N. Mapper, "NMAP," NMAP, 1 Oktober 2022. [Online]. Available: https://nmap.org/book/man.html. [Accessed 15 Oktober 2022].

[15] D. Sudirman and A. N. Yaqin, "Network Penetration dan Security Audit Menggunakan Nmap," *SATIN Sains dan Teknologi Informasi,* vol. 7 Nomor 1, pp. 32-44, 2021.

[16] M. Huda, Keamanan Informasi., Nulisbuku.com, 2020.

[17] Q. S. Labs, "SSL Server Test," Qualys SSL Labs, 1 Oktober 2022. [Online]. Available: https://www.ssllabs.com/ssltest/. [Accessed 20 Oktober 2022].

[18] S. Rahman, Buku Pintar Web Desain dan SEO WordPress 5 PLUS, Jakarta : Elex Media Komputindo, 2019.