Implementasi Keamanan Jaringan Pada Cloudfri Dengan Metode *Hardening*

1st Muhammad Irwanda Irawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
irwandawan@telkomuniversity.ac.id

2nd Umar Yunan K.s. Hediyanto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

3rd Rd. Rohmat Saedudin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

Abstrak

Hardening adalah proses mengamankan sistem pada jaringan komputer untuk mengurangi kerentanan terhadap serangan *hacking*. Jenis *hardening* terdapat *backup, firewall, kriptografi, security policy, Intrusion policy system,* digital forensik. Metode *hardening* yang digunakan yaitu *penetration* dan *vulnerability* dengan menggunakan skenario yang telah dibuat. Penelitian ini menggunakan objek berupa website igame.cloudfri.id yang yang dikelola fakultas rekayasa industri. Penelitian bertujuan untuk menganalisa kerentanan terhadap *website* igame.cloudfri.id dan memberikan saran . Implementasi pengujian dalam penelitian ini menggunakan *tools* NMAP dan nikto yang tersedia pada sistem operasi kali linux. hasil dari penelitian dengan metode yang telah dianalisa kerentanannya bahwa *website* rentan terhadap serangan hacking dikarenakan tidak memiliki anti-clickjacking, XSS-protection, x-content-type-option.

Abstract

Hardening is the process of securing systems on a computer network to reduce vulnerability to hacking attacks. Hardening types there are backups, firewalls, cryptography, security policy, intrusion policy system, digital forensics. Hardening methods used are penetration and vulnerability by using scenarios that have been created. This research uses objects in the form of igame.cloudfri.id websites managed by the faculty of industrial engineering. Research aims to analyze vulnerabilities to websites igame.cloudfri.id and provide advice. The implementation of the tests in this study uses NMAP and nikto tools available on the kali linux operating system. The results of research with methods that have analyzed the vulnerability that the website is vulnerable to hacking attacks because it does not have anti-clickjacking, XSS-protection, x-content-type-option.

Kata Kunci : *Hardening, Penetration, Vulnerability, Website, Hacking*

Keywords: Hardening, Penetration, Vulnerability, Website, Hacking

I. PENDAHULUAN

Perkembangan teknologi internet sebagai alat yang dapat digunakan manusia untuk kebutuhan sehari-hari. Pada saat ini, Setiap perushaan yang membutuhkan alat untuk menyimpan informasi yang dibutuhkan agar data kostumer maupun data perushaan dapat dijaga dengan baik. Namun, dengan perkembangan teknologi informasi yang semakin berkembang pesat pasti ada kemungkinan informasi yang dapat dicuri. Karena itu penyerangan pada server sangat memunkinkan untuk terjadi untuk diambil datanya. Dengan menggunakan metode *hardening* kita dapat meminimalisir terjadinya pernyerangan terhadap server.

Jaringan komputer atau network adalah satu atau lebih komputer yang saling terhubung satu sama lain melalui jaringan server yang dapat berbagi informasi. Alat yang dibutuhkan untuk membuat sebuah jaringan komputer agar dapat terhubung adalah komputer, server, router, dan switch. Dengan mengkonfigurasi berbagai algoritma dan protocol agar dapat berbagi informasi. Jaringan komputer dapat dibuat dengan menggunakan teknologi kabel maupun wireless. Pada jaringan yang menggunakan kabel dibutuhkan kabel tembaga, coaxial kabel, dan fiber optic. Sedangakn wireless dapat menggunakan sinyal gelombang yang dapat menghungkan tanpa menggunakan kabel. jaringan komputer memiliki beberapa jenis yaitu Internet, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), dan Virtual Area Network (VPN).

Serangan jaringan (*Hacking*) adalah serangan yang dapat dilakukan terhadap jaringan komputer yang terhubung dengan internet. Sehingga komputer atau server yang terkena dampaknya akan mengalami error atau malfungsi yang dapat berdampak besar terhadap sistem pada komputer maupun server yang diserang. Berbagai jenis serangan pada jaringan komputer atau server adalah Packet Sniffing, *Spoofing*, Distrbuted Denial of Service (DDoS), DNS Poisoning, Trojan Horse, SQL Injection, Script kiddies, LAND Attack, dll. Ancaman penyerangan dapat menjadi dua yaitu penyerangan internal dan penyerangan eksternal, ancaman internal bisa saja terjadi

pada saat suatu organisasai yang dapat mengalami kerusakan akibat oleh ancaman-ancaman yang mengakibatkan kehilangan atau kerugian aset akibat serangan yang terjadi pada organisasi tersebut. Ancaman eksternal itu dapat berupa sengaran malware, pencurian data, unauthorizad access, pengguna resource perusahaan secara illegal, dll. kurangnya kemampuan dan konfigurasi dalam jaringan mengakibatkan tidak amannya pada host yang dapat berakibat terbukanya celah kemanan pada sistem komputer.

Hardening adalah suatu proses untuk mengemankan jaringan atau *hardening*(Pengerasan). *Hardening* dapat mengamankan sistem pada jaringan komputer dengan metode yang ada. Perlindungan keamanan atau *hardening* ada dalam layer(lapisan) dan disebut juga dengan pertahanan mendalam (defense in depth). Dengan melindungi lapisan pada beberapa layer seperti pengguna, aplikasi, level host, sistem operasi, fisik ,dan sublevel.

Cloudfri merupakan sebuah web yang berisikan aplikasi yang digunakan oleh seluruh entitas seperti mahasiswa, dosen, maupun staff yang ada di Fakultas rekayasa industry. Ada beberapa aplikasi yang terhubung pada cloudFRI yaitu administrasi.cloudfri.id, ingram.cloudfri.id, labrecruitment.cloudfri.id, logbook.cloud.fri, Mentawai.cloudfri.id, sap.cloudfri.id, savsofrtqiuz.cloudfri.id, sikomo.cloudfri.id, tap2go.cloudfri.id.

II. KAJIAN TEORI

Fungsi *hardening* adalah mengurangi resiko keamanan yang menghindari potensi serangan dan melakukan pengerasan permukaan sistem dari serangan. Proses *hardening* betujuan pada metode untuk menganalisa, mengidentifikasi, menutup, dan mengontrol kelemahan dan kerentanan kemanan jaringan pada organisasi.

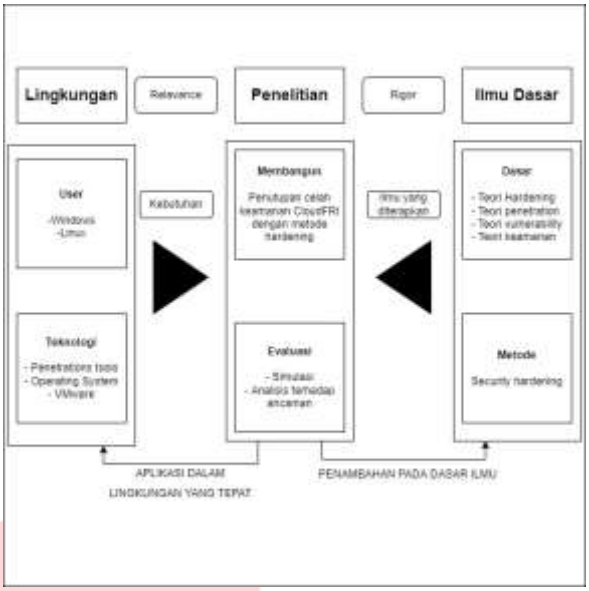
Vulnerability merupakan tahap scanning atau pemindaian pada website target untuk mengetahui seberapa rentan website tersebut terhadap ancaman. Vulnerability bertujuan menemukan celah ancaman yang diguanakn oleh penyerang sebagai ruang input dalam mengeksploitasi kesalahan dalam sistem dan mendapatkan keuntungan.

Penetration atau ethical hacking merupakan pengujian sistem komputer, jaringan, maupun aplikasi web untuk menemukan celah keamana yang dapat dieksploitasi oleh penyerang.

III. METODE

A. Model Konseptual

Model konseptual merupakan gambaran untuk memahami, melaksanakan, dan mengevaluasi penelitian sistem informasi (Hevner dkk., 2004). Pembuatan model konseptual ini Bertujuan untuk mendapatkan kerangka yang terstruktur dan memperjelas tujuan dari penelitian. Model konseptual dalam penelitian ini yaitu pada gambar III.1 berikut.

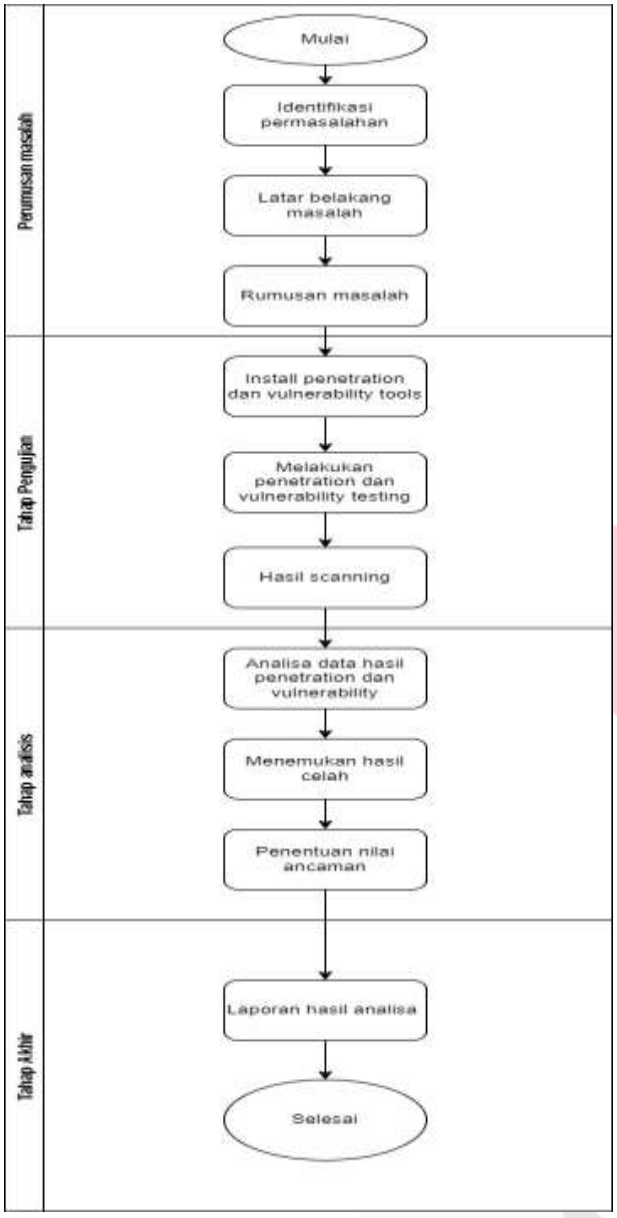


GAMBAR III. 1 Metodelogi Konseptual

Pada model konseptual dapat dijelaskan bahwa penelitian Keamanan Cloudfri menggunakan metode *hardening* memiliki terdapat tiga ruang lingkup yaitu Lingkungan, Penelitian, dan Ilmu dasar. Pada ruang lingkup terdapat "*User*" dan "Teknologi yang mendeskripsikan terdapat pengguna maupu teknologi yang dibutuhkan untuk melakukan proses *hardening*. *User* berperan sebagai pengguna *Operating system* windows dan linux. Lalu, Didalam Teknologi terdapat *Penetration*s dan vulnerability *tools*, *Operating system*, dan VMware yang berfungsi sebagai *tools* yang digunakan dalam proses penelitian. Pada lingkup penelitian terdapat "Membangun" yang mendeskripsikan proses penutupan celah keamanan pada cloudfri dengan metode *hardening* dan "Evaluasi" mendeskripsikan mensimulasikan maupun menganalisis ancaman terhadap cloudfri. Lalu, dalam lingkup "Dasar Ilmu" mendeskripsikan teori-teori dasar yang digunakan untuk diterapkan pada penelitian ini.

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah merupakan alur sebuah proses perencanaan mulai dari awal sampai akhir proses untuk mendapatkan sebuah data dari tujuan penelitian. Berikut adalah sistematika penyelesaian masalah pada penelitian ini :



GAMBAR III.2 Sistematika penyelesaian masalah

a. Perumusan Masalah

Perumusan maslah dimulai dengan melakukan identifikasi masalah pada latar belakang untuk bertujuan menggambarkan masalah hingga selesai. Lalu, setelah melakukan identifikasi yang telah terdapat masalah yang akan diteliti akan dibuat Batasan masalah. Batasan masalah berfokus lebih dalam pada masalah.

b. Tahap Pengujian

Tahap pengujian, dilakukan implementasi dengan menggunakan *tools* untuk menguji coba sebuah *website* untuk mengetahui *vulnerability* dan hasil *penetration* sehinggan akan mendapatkan hasil bagian celah keamanan yang terdapat kelemahan.

c. Tahap Analisis

Hasil dari tahap yang didapat pada hasil tahap pengujian, data yang didapatkan dari hasil scan *vulnerability* dan *penetration* test akan dilakukan penilaian terhadap kerentanan, keamanan, maupun resiko.

d. Tahap Akhir

Pada tahap akhir ini, hasil pengujian dan analisis akan dijadikan laporan akhir penelitian. Pada laporan akhir terdapat data dan hasil pengujian yang telah dinilai serta terdapat kesimpulan maupun saran agar *website* dapat dikembangkan.

a. Pengumpulan Data

Metode pengumpulan data pada penelitian ini menggunakan metode observasi non-partisipan, (Ghozali dkk., 2019) observasi non-partisipan di mana teknik ini menempatkan diri sebagai pengamat yang tidak secara langsung terlibat dalam sistem.

b. Pengolahan data

Pada tahap pengolahan data yang akan dijadikan acuan saat dalam melakukan pengujian yang diambil dari tahap pengumpulan data. Lalu, data tersebut akan ditentukan tingkat resiko yang berdapak kecil hingga berdampak besar.

c. Metode Evaluasi

Metode yang digunakan untuk melakukan evaluasi yaitu evaluasi *UCLA.* (Mathison, 2013;Alkin, 1968) mendefinisikan evaluasi sebagai suatu proses meyakinkan keputusan, memilih informasi yang tepat, mengumpulkan dan menganalisis informasi sehingga dapat melaporkan ringkasan data yang berguna bagi pembuat keputusan dan memilih beberapa alternatif. Salah satu evaluasinya adalah *Sistem Assessment*, *Sistem Assessment* adalah evaluasi yang memberikan informasi tentang keadaan dari sistem.

IV. HASIL DAN PEMBAHASAN

Hasil pengujian yang dilakukan kepada objek penelitian, serta melakukan analisis *vulnerability* yang terdapat pada *website* atau objek penelitian.

A. Hasil pengujian vulnerability menggunakan NMAP tools

GAMBAR V. 1 Hasil pengujian *vulnerability*

Dari hasil yang didapakatan setelah melakukan tes, *Vulnerability* dapat ditemukan dengan menggukanan perintah “nmap --open” didapatkan beberapa informasi. Hasil yang terlihat pada gambar bahwa banyak *port* yang berstatus “open” atau terbuka. *Port* yang dilihat yaitu:

TABLE V. 1 Hasil Pengujian *Vulnerability*

Port	**Service**	**State**
21/tcp	ftp	Open
53/tcp	Domain	Open

80/tcp	http	Open
110/tcp	Pop3	Open
143/tcp	Imap	Open
443/tcp	https	Open
587/tcp	Submission	Open
993/tcp	Imaps	Open
995/tcp	Pop3s	Open
3306/tcp	Mysql	Open

a. 21 FTP

Port ini merupakan *port* untuk FTP. *Port* ini digunakan untuk mengkoneksi FTP baik itu FTP Server atau FTP Client. FTP (File Transmission Protocol) dapat digunakan untuk tukar-menukar file dalam sutu network yang menggunakan koneksi TCP.

b. 53 DNS

DNS (Domain Name Sistem) berguna untuk menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer.

c. 80 HTTP

Port ini digunakan untuk web *server*, paling umum digunakan untuk mengakses internet atau bisa disebut HTTP *port server.*

d. 110 POP3

Port ini merupakan *port* untuk POP3.POP3 (*Post Office Protocol version* 3), merupakan protokol yang digunakan untuk mengambil surat elektronik (email) dari *server* email.

e. 143 IMAP

Port ini merupakan *port* untuk IMAP.IMAP (*Internet Message Access Protocol*) adalah protokol standar untuk mengakses/mengambil e-mail yang dikirim dari *server* maupun diterima dari *server.*

f. 443 HTTPS

Port ini merupakan *port* untuk HTTPS.HTTPS (*Hypertext Transfer Protocol Securre*). Dengan menggunakan HTTPS perintah dan data telah dilindungi dengan sistem *Encrypt*, sehingga ini akan menyulitkan bagi orang-orang yang mau membajak isi dari dokumen yang dikirim dengan menggunakan media HTTPS.

g. 587 MSA

MSA (Mail Submission Agent). MSA adalah *software* yang digunakan untuk menerima email Dari Mail *User* Agent (MUA) dan bekerjasama dengan Mail Transfer Agent (MTA) untuk mengirimkan sebuah email.

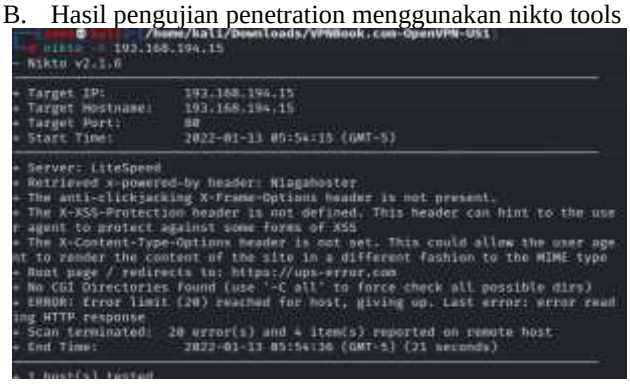
h. 995 POP3S

Port ini merupakan *port* untuk POP3S untuk menjalankan SSL/TLS. *Port* ini digunakan untuk menjalankan layanan POPS3 yang terenkripsi, dan digunakan oleh *server* email.

i. 3306 MYSQL

Port ini digunakan sebagai penghubung dengan klien MySQL dan utilitas seperti mysqldump.

B. Hasil pengujian penetration menggunakan nikto tools



GAMBAR V. 2 Hasil pengujian menggunakan nikto

Setelah melakukan tes, pada saat menggunakan perintah "nikto -h 193.168.194.15" maka nikto akan memulai *vulnerability scanning* pada *website* igame.cloudfri.id. hasil yang didapatkan sebagai berikut :

TABLE V. 2 Hasil pengjuian nikto

No	Status	Informasi	Risk Assesment
1	The anti-clickjacking x-frame-options header is not present	Tidak memiliki anti-clickjacking dalam web	Medium
2	The x-xss-protection header is not defined	x-xss-protection tidak terconfigurasi	Low
3	The x-content-type-options header is not set	x-contecnt-type-options header tidak terpasang	Low

a. The anti-clickjaking x-frame-options

Hasil dari data didapat menggunakan nikto *tools* bahwa *website* igame.cloudfri.id tidak tedapat x-frame-options. Jadi, perentas dapat membuat dan menanamkan sebuah script maupun kode pada *website* tesrsebut. Apabila pengguna mengklik salah satu script maupun kode tersebut akan berpotensi mencuri, merusak dan mengedalikan data tersebut yang dapat merugikan para pengguna *website* ini. Solusi yang dapat dilakukan dengan cara mengaktikan dan mengatur x-frame-options header pada ip tertentu

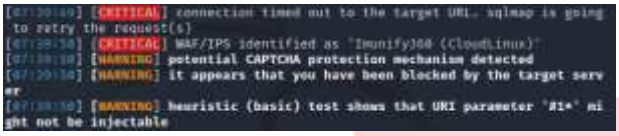
b. The x-xss-protection header

Hasil dari data didapat menggunakan nikto *tools* bahwa *website* igame.cloudfri.id tidak tedapat x-xss-protection. Jadi, Perentas dapat melakukan penyerangan dengan menggunakan serangan XSS(Cross Site Scripting) yaitu salah satu serangan yang dapat dilakuka penyerang mengambil data cookie atau memperoleh autentifikasi ID session yang tersimpan pada cookie *website*.

c. The x-content-type-options

Hasil dari data didapat menggunakan nikto *tools* bahwa *website* igame.cloudfri.id tidak tedapat x-content-type-options. Jadi, perentas dapat melakukan serangan dengan cara sniffing bertipe MIME (Multi-Purpose Internet Extentions) yaitu menyerang pertahanan pada tipe konten pada aplikasi web. Solusi yang dapat dilakukan adalah mengatur web untuk mengaktifkan dan menonaktifkan pengiriman x-xss-protectio:1; Nosniff x-content-type-options: nosniff pencegahan sniffing bertipe MIME diaktifkan secara default.

C. Hasil Pengujian penetration menggunakan SQLinjection



GAMBAR V. 3 hasil pengujian menggunakan *SQLinjection*

Berdasarkan hasil *penetration* testing menggunakan SQLinjection pada gambar V.3 dapat diurakan bahwa *website* igame.cloudfri.id telah dilindungi oleh WAF(WEB Aplication *Firewall*) dari Imunify360 dikarenakan *website* tersebut menolak dan memblokir traffic yang datang seletah menemukan atau mendeteksi adanya ancaman. Dengan demikian, perentas tidak dapat menyerang server kembali dikarenakan pemblokiran yang telah melindungi database *website* igame.cloudfri.id dari serangan. dapat disimpulkan bahwa *website* aman dari perentas yang menggunakan aplikasi SQLinjection. Akan tetapi, tidak dapat menutup kemungkinan bahwa *website* sepenuhnya aman.

D. Hasil Pengujian *penetration* menggunakan burpsuite

GAMBAR V. 4 Hasil pengujian *Penetration* menggunakan burpsuite

Berdasarkan hasil *penetration* testing yang ditampilkan pad gamber V.4 pada saat proses login sedang berlangsung dan aplikasi burpsuite berjalan pada *website* igame.cloudfri.id. aplikasi burpsuite mencapture dan mendapatkan celah keamanan *user*name dan password pada saat proses login berlangsung dikarenakan *website* tidak mengenskripsi *user*name dan password pada saat *user* login.

V. KESIMPULAN

Setelah melakukan pengujian pada *website* igame.cloudfri.id dan mendapatkan data hasil dari analisis *vulnerability* dan *penetration* menggunakan *tools* NMAP, Nikto, brupsuite, SQLmap. Dapat disimpulkan Terdapat beberapa celah keamanan yaitu :

A. terdapat pada *website* igame.cloudfri.id yang keamanan *website* tersebut dapat diserang, Dikarenakan pada *website* igame.cloudfri.id ada beberapa fitur kemanan belum diaktifkan sehingga penyerang dapat dengan cara menanamkan malware, phising,DDos attack, dst.
B. terdapat fitur login yang tidak terenskripsi yang dapat berdampak pencurian data.

REFERENSI

[1] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science In IS Research. Management Information Sistems, 28(1), 75–105.

[2] Yulianingsih, Y. (2017). Melindungi Aplikasi dari Serangan Cross Site Scripting dengan Metode Metacharacter. Jurnal Nasional Teknologi dan Sistem Informasi, 3(1), 83-88.

[3] Zulkifli, S., & Samsir, S. (2020). Implementasi Sistem Keamanan SQL Injection Dalam berbasis web. Ejurnal. Univalabuhanbatu. Ac. Id, 4(01), 13-17.

[4] Listartha, I. M. E., Saskara, G. A. J., & Santyadiputra, G. S. (2021). PENGUJIAN KERENTANAN DAN PENETRASI KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ. ScientiCO: Komputer Science and Informatics Journal, 4(2), 1-14.

[5] Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver Menggunakan *Penetration* Test. Jurnal Informatika, 8(2), 183-190.

[6] Kholiq, A., & Khoirunnisa, D. (2019). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) DENGAN METODE *PENETRATION* TESTING EXECUTION STANDARD (PTES)(STUDI KASUS: PT. WIN PRIMA LOGISTIK). Jurnal Ilmiah Fakultas Teknik LIMIT'S Vol, 15(1).

[7] Pangalila, R., Noertjahyana, A., & Andjarwirawan, J. (2015). *Penetration* Testing Server Sistem Informasi Manajemen dan *Website* Universitas Kristen Petra. Jurnal Infra, 3(2), 271-276.

[8] Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis Keamanan Aplikasi Data Pokok Pendidikan (DAPODIK) Menggunakan *Penetration* Testing Dan SQL Injection. INFOTECH journal, 6(2), 65-70.

[9] Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration* Testing Menggunakan Framework ISSAF. J. Ilm. Merpati, 8(2), 113-124.

[10] Sakti, B., Aziz, A., & Doewes, A. (2013). Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan *Penetration* Testing. ITSMART: Jurnal Teknologi dan Informasi, 2(1), 44-51.

[11] Sahtyawan, R. (2019). Penerapan zero entry *hacking* didalam security misconfiguration pada VAPT (*vulnerability* assessment and *penetration* testing). Journal of Information Sistem Management (JOISM), 1(1), 18-22.

[12] Sahtyawan, R. (2019). Penerapan zero entry *hacking* didalam security misconfiguration pada VAPT (*vulnerability* assessment and *penetration* testing). Journal of Information Sistem Management (JOISM), 1(1), 18-22.

[13] Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver Menggunakan *Penetration* Test. Jurnal Informatika, 8(2), 183-190.

[14] Hidayatulloh, S., & Saptadiaji, D. (2021). *Penetration* Testing pada *Website* Universitas ARS Menggunakan Open Web Application Security Project (OWASP). Jurnal Algoritma, 18(1), 77-86.

[15] Sutrisna, E., Hidayat, T., & Ramdhani, I. (2020). Workshop Web Development Menggunakan PHP Data Object di SMK Cyber Media Jakarta. JAMAIKA: Jurnal Abdi Masyarakat, 1(2), 53-59.

[16] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science In IS Research. Management Information Systems, 28(1), 75–105.

[17] Mathison, S. (2013). Evaluation Theory. Encyclopedia of Evaluation, 89–112. https://doi.org/10.4135/9781412950558.n191

[18] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

[19] Mazhar, N., Salleh, R., Zeeshan, M., Hameed, M. M., & Khan, N. (2021, October). R-IDPS: Real time SDN based IDPS system for IoT security. In 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) (pp. 71-76). IEEE.

[20] Mandal, N., & Jadhav, S. (2016, March). A survey on network security tools for open source. In 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC) (pp. 1-6). IEEE.

[21] Markowsky, L., & Markowsky, G. (2015, September). Scanning for vulnerable devices in the Internet of Things. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 463-467). IEEE.