CoMBInES
CONFERENCE ON MANAGEMENT, BUSINESS, INNOVATION, EDUCATION AND SOCIAL SCIENCES

Volume 1 No 1 (2021)

Diterima : February 01, 2021
Disetujui : February 05, 2021
Diterbitkan: February 24, 2021

Conference on Management, Business, Innovation, Education and Social Science
https://journal.uib.ac.id/index.php/combines

Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing

Stefanus Eko Prasetyo[1], Ricky Chandra Lee[2]
Email korespondensi : stefanus@uib.ac.id[1], 1731019.ricky@uib.edu[2]

[1,2] Fakultas Ilmu Komputer, Universitas Internasional Batam, Batam, Indonesia

Abstrak

Penetration Testing merupakan sebuah metode yang digunakan dalam mencari celah pada sistem, guna untuk meminimalisir penyerangan dan pembobolan dalam sebuah jaringan website perusahaan. Dalam uji coba yang dilakukan pada jaringan pay2home yang berada pada shremit.p2hdevworks.com menggunakan beberapa aplikasi penetration testing untuk menguji coba keamanan jaringan diantaranya Nessus , Acunetix, W3af, dan Nmap. Dimana masing-masing aplikasi tersebut berfungsi untuk menguji coba penyerangan dan mencari celah keamanan pada jaringan maupun sistem, Variabel yang menjadi acuan dalam uji coba ini adalah celah yang didapatkan, dimana hasil penelitian menunjukkan bahwa website jaringan pay2home.com memiliki keamanan yang cukup tinggi.

Kata Kunci: *Penetration Testing, Keamanan jaringan, Celah keamanan*

Abstract

Penetration Testing is a method used in finding loopholes in the system, in order to minimize attacks and breaches in a company website network. In tests carried out on the pay2home network at shremit.p2hdevworks.com using several penetration testing applications to test network security including Nessus, Acunetix, W3af, and Nmap. Where each of these applications functions to test attacks and look for security gaps on the network and system, the variables that are the reference in this trial are the gaps that are obtained, where the results of the research show that the pay2home.com network website has a fairly high security.

Keywords: *Penetration Testing, Network Security, Loophole*

Pendahuluan

Jaringan merupakan sebuah kumpulan maupun rangkaian titik yang terhubung satu sama lain yang menciptakan sebuah pola dimana menghubungkan perangkat yang terhubung dengan internet sehingga dapat saling berkomunikasi serta bertukar data. Dalam masa sekarang jaringan adalah hal yang paling penting dalam kehidupan tetapi keamanan jaringan juga merupakan hal yang tidak kalah pentingnya (Wulandari, 2016). Keamanan jaringan

merupakan sebuah entitas dimana befungsi untuk menjaga keamanan sebuah informasi maupun data yang ditransfer melalui internet sehingga file yang dikirimkan maupun yang ditransfer dapat sampai ke tujuan tanpa distorsi gangguan (Wilman, Fitri, & Nathasia, 2018).

Seperti halnya sekarang sedang terjadi pembololan maupun hacking pada perusahaan maupun website tertentu yang mengakibatkan kerugian pada pihak yang bersangkutan. Dimana data data tersebut dijual dan disalahgunakan oleh pihak tidak berwajib dan diperjualbelikan untuk kepentingan tersendiri (Sari, Yamin, & Aksara, 2017). Penetration Testing merupakan aktivitas dimana seseorang mencoba melakukan serangan kepada perusahaan dimana serangan tersebut di targetkan kepada jaringan pada perusahaan guna untuk mencari titik lemah maupun kelemahan pada sistem di jaringan perusahaan (Denis, Zena, & Hayajneh, 2016).

Hal ini dilakukan bertujuan untuk mengetahui serta menentukan serangan yang mungkin terjadi dan dilakukan terhadap kelemahan maupun celah pada sistem tersebut, dan mengetahui dampak bagi bidang bisnis yang diakibatkan oleh hasil eksploitasi data yang dilakukan oleh penyerang (Yaqoob et al., 2017).Pay2home merupakan perusahaan spesialis pengiriman uang yang begerak dalam bidang jasa dimana memberikan penawaran yang lebih murah serta praktis dibandingkan dengan transfer bank alternatif.

Di Singapura perusahaan ini beroperasi dengan nama Wandr.Pte.Ltd dan sudah mendapatkan lisensi oleh Monetary Authority of Singapore (MAS). Di Hongkong perusahaan ini beroperasi dengan nama P2H Hongkong Pte.Limited dan sudah mendapatkan lisensi dari Joint Financial Intelligence Unit (JFIU). Dan dalam waktu dekat ini sudah menawarkan layanan transfer untuk perorangan dan perusahaan yang ingin mengirim uang ke seluruh dunia.

Sekarang Pay2home sedang mengembangkan keberadaan retail di Singapore, Hongkong dan seluruh Asia. Berdasarkan uraian yang terpapar diatas mengenai keamanan jaringan server pada pay2home mengunakan metode penetration testing dimana hal ini berfungsi untuk mengetahui celah pada perusahaan serta tingkat keamanan pada perusahaan pay2home. Dengan ini penulis menggunakan metode penetration testing untuk menguji coba keamanan jaringan yang berjudul "Analisis Keamanan Jaringan Pada Perusahaan Pay2home Menggunakan Metode Penetration Testing".

Tinjauan Pustaka

Penelitian pertama yang berjudul "Analısıs Kerentanan Aplıkası Berbasıs Web Menggunakan Kombınası Security Tools Project Berdasarkan Framework Owasp Versı 4" (Yunus, 2019). Tujuan dilakukannya penelitian ini guna untuk mengetahui tingkat keamanan aplikasi dengan bantuan tools security berdasarkan hasil pengujian yang telah dilakukan.

Penelitian selanjutnya yang berjudul "Evaluası Kınerja Software Web Penetratıon Testıng" (Ula, 2019). Tujuannya dilakukan penelitian ini guna untuk mengetahui aplikasi yang paling cocok untuk mendeteksi kelemahan keamanan pada sebuah website, program tersebut memberikan informasi tentang cara melakukan berbagai scenario penyerangan terhadap sebuah website.

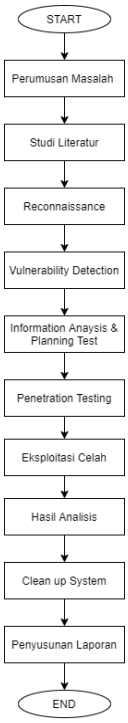
Penelitian selanjutnya yang berjudul "Analısıs Perbandıngan Penetratıon Testıng Tool Untuk Aplıkası Web" (Tarigan, Kusyanti, & Yahya, 2017). Tujuan dilakukannya penelitian ini guna untuk menganalisa perbandingan tools yang digunakan dalam melakukan penetration system, apa saja dan bisa terdeteksi oleh ketiga tools yang telah diuji dari kerentanan yang ada pada website.

Penelitian selanjutnya yang berjudul "Analısıs Keamanan Webserver Menggunakan Metode Penetrası Testıng" (Yunanri, Riadi, & Yudhana, 2016). Tujuan dilakukannya penelitian ini guna untuk mengidentifikasi dan mengeksploitasi celah kerentanan yang terdapat pada keamanan jaringan serta membantu memastikan ke efektivitas langkah-langkah pada keamanan yang telah dilakukan.

Penelitian selanjutnya yang berjudul "Penetratıon Testıng Sıstem Keamanan Aplıkası Web Berbasıs E-Commercepada Perusahaan Hptasık" (Abdurrohim, 2019). Tujuan dilakukannya penelitian ini guna untuk mengetahui guna penetration testing dalam meningkatkan keamanan pada website dengan mengetahui kelemahan pada sistem website lalu melakukan perbaikan pada celah yang rentan tersebut.

Metodologi Penelitian

Pada bagian ini penulis membuat alur penulisan yang digunakan menjadi sebuah alur kerangka yang sistematis untuk penulisan yang dilakukan, awalan penulisan yang dilakukan dimulai dari merumuskan masalah hingga penyelesaian yaitu penyusunan laporan. Kerangka alur penulisan yang dirancang oleh penulis dapat dilihat pada Gambar 1.



Gambar 1 Langkah Alur Penulisan

1. Perumusan Masalah

Ditahap ini penulis melakukan pengumpulan serta mempelajari masalah yang terdapat pada bidang yang penulis dalami. Permasalahan yang penulis temukan akan diteliti lebih lanjut sehingga mendapatkan jawaban atas masalah yang diteliti dan mendapatkan manfaat dari penulisan yang sudah dilakukan

2. Studi Literatur

Ditahap ini penulis melakukan penulisan lebih lanjut pada permasalahan yang diteliti oleh penulis dengan cara mempelajari informasi , serta referensi seperti jurnal, buku serta artikel yang berhubuingan mengenai masalah yang diteliti oleh penulis sehingga dapat digunakan didalam penulisan ini.

3. *Reconnaissance*

Merupakan tahap dimana mencari informasi sebanyak mungkin dari target sebelum melakukan penyerangan.Informasi tersebut berhubungan dengan OS , IP address serta port service yang terbuka pada sistem.

4. *Vulnerabilty Detection*

Merupakan tahap dimana penulis melakukan pencarian celah dengan bantuan aplikasi. Aplikasi yang digunakan akan membantu penulis dalam menemukan berbagai celah dari sebuah sistem yang diuji. Dari hasil celah yang didapatkan setelah itu akan dimasukkan dalam rencana dalam tahap pengujian selanjutnya, Celah yang ditemukan hasil nya akan terbatas dari software yang digunakan yaitu Acunetix dan Nessus. Tahap ini biasanya dinamakan Vulnerability Scanning.

5. Analisis dan Perencanaan Pengujian

Di tahap ini penulis melakukan analisa dan membuat rencana uji coba dari pengintaian pada sistem dan pencarian celah yang sudah dilakukan di tahap sebelumnya. Analisa dan perencanaan yang telah dibuat untuk menentukan alur penetration testing.

6. *Penetration Testing*

Di tahap ini, penulis akan melakukan uji coba penyerangan pada target yang sudah ditentukan sebelumnya yaitu Shremit.p2hdevworks.com yang terdapat pada perusahaan Pay2home. Uji coba penyerangan dilakukan sesuai dengan perencanaan yang sebelumnya dilakukan. Tujuan nya dilakukan tahap ini ialah untuk memastikan kebenaran dari hasil penemuan celah yang di temukan di tahap sebelumnya.

7. Eksploitasi Celah

Setelah melewati tahap sebelumnya yaitu penetration testing kemudian tahap selanjutnya yang akan dilakukan yaitu melakukan ekspolitasi celah. Di tahap ini penulis akan mencoba dalam mengeksploitasi celah yang ada pada sistem tersebut. Eksploitasi disini adalah untuk menguji coba dalam hal melihat kerentanan pada service dan port.

8. Hasil Analisis

Di Tahap ini penulis melakukan analisis dahulu terhadap beberapa pengujian yang sudah dilakukan sebelumnya. Yaitu pencarian celah, serta eksploitasi celah dan semua akibat yang disebabkan oleh kerentanan celah tersebut. Dari celah yang didapatkan akan dibuat susunan celah dimana susunan tersebut berdasarkan besar kecilnya dampak yang dihasilkan menggunakan aplikasi Acunetix.

9. Clean Up System

Pada tahap ini, penulis akan melakukan pembersihkan dan perbaikan sistem terhadap target yang sudah diuji coba. Pembersihkan yang dimaksudkan ialah mengembalikan semua konfigurasi dan keadaan seperti awal. Aktivitas yang dilakukan tergantung dari sejauh mana penulis melakukan eksploitasi celah yang telah didapatkan. Selain itu penulis akan menghapus semua aktivitas serta data informasi yang penulis dapatkan selama melakukan uji coba penetration testing, hal ini dilakukan untuk menjaga kepercayaan dari target yang diuji coba.

10. Penyusunan Laporan

Pada tahap terakhir ini, penulis merangkum semua hasil yang didapatkan dari pengujian terhadap sistem. Dalam laporan ini akan berisikan tentang dokumentasi pengujian, hasil temuan celah serta kerentanan yang penulis temukan.

Belum adanya dilakukan uji coba penetration testing terhadap jaringan pay2home, apakah sudah memiliki tingkat keamanan jaringan yang aman terhadap serangan hacker, sehingga dilakukannya percobaan penetration testing terhadap keamanan jaringan pay2home untuk mengetahui keamanan yang terdapat memadai. Akan dirincikan kebutuhan software & hardware yang dibutuhkan oleh penulis dalam melakukan uji coba ini. Kebutuhan hardware dalam penelitian yang berjudul "Analisis keamanan jaringan Pay2home menggunakan metode penetration testing" yaitu :

1. Sebuah Laptop untuk wadah melakukan uji coba penetration testing Kebutuhan Software

Kebutuhan Software dalam penelitian yang berjudul "Analisis keamanan jaringan Pay2home menggunakan metode penetration testing" yaitu:

1. VMWare sebagai wadah uji coba penetration testing
2. ISO kali linux sebagai Sistem Operasi yang digunakan untuk melakukan Uji coba Penetration Testing
3. Acunetix sebagai aplikasi untuk menganalisa dampak yang dihasilkan dari celah
4. Nessus sebagai aplikasi untuk mencari celah serta memberikan laporan dari celah yang ditemukan
5. Nmap sebagai aplikasi yang digunakan untuk mencari informasi tentang target yang ingin di eksploitasi

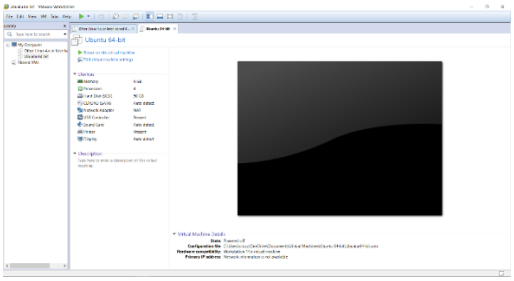
Hasil dan Pembahasan

Sebelum melakukan analisis pada keamanan jaringan terdapat beberapa hal yang harus di siapkan terlebih dahulu diantaranya Instalasi Software. Ketika memulai penerapan ini, sebelumnya terdapat beberapa software yang harus diinstall terlebih dahulu agar uji coba ini dapat berjalan dengan semestinya. Terdapat beberapa software yang diperlukan, yang harus didownload dan di install diinstall yaitu :

1. VMware Workstation 14 Pro V14.1.1

VMware merupakan sebuah perangkat lunak yang umumnya digunakan sebagai perangkat virtualisasi dengan menggunakan Operating System, alternatif dari server maupun pc fisik untuk lebih menghemat pengeluaran, Dengan menggunakan perangkat lunak VMWare

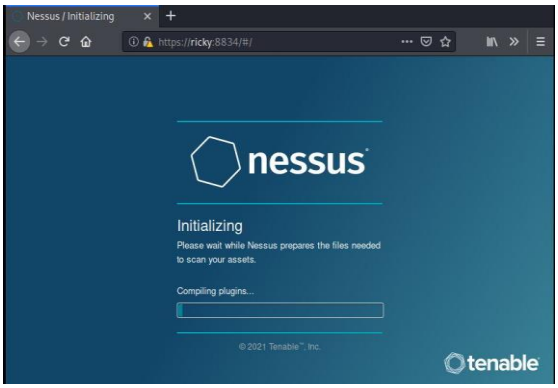
dapat membuat beberapa Sistem Operasi dalam satu wadah, Maka karena hal ini, penulis menggunakan operating system Kali Linux. Dibawah ini merupakan tampilan software VMware Workstation 14 Pro V14.1.1 (Lihat Gambar 2).



Gambar 2 Tampilan Awal VMware

2. Nessus Scanner

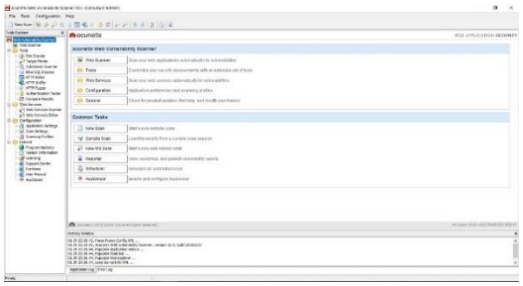
Nessus Scanner merupakan sebuah aplikasi yang dibuat oleh Tenable Security untuk menemukan celah maupun Vulnerability yang terdapat pada sebuah network, Nessus sendiri memiliki beberapa fungsi diantaranya untuk Vulnerability Scanning, Configuration Editing, Compliance Checks dan lainnya (Lihat Gambar 3).



Gambar 3 Tampilan Awal Nessus

3. Acunetix WVS 10.5

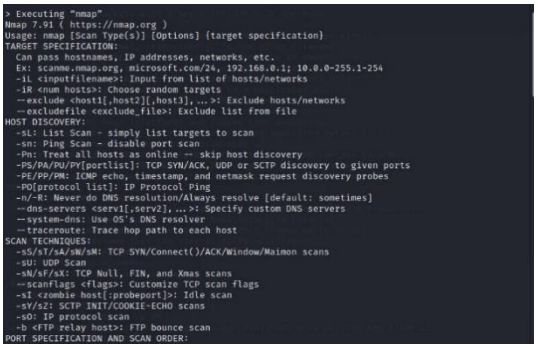
Acunetix WVS 10.5 merupakan sebuah perangkat lunak yang digunakan dalam layanan situs untuk menguji kerentanan keamanan secara otomatis dalam mengaudit aplikasi situs, contoh kerentanan diantaranya SQL Injection, Cross Site Scripting, dan lainnya. Aplikasi ini juga digunakan oleh banyak pihak dikarenakan kemudahan serta keakuratan dalam menemukan celah dan kerentanan tersebut (Lihat Gambar 4).



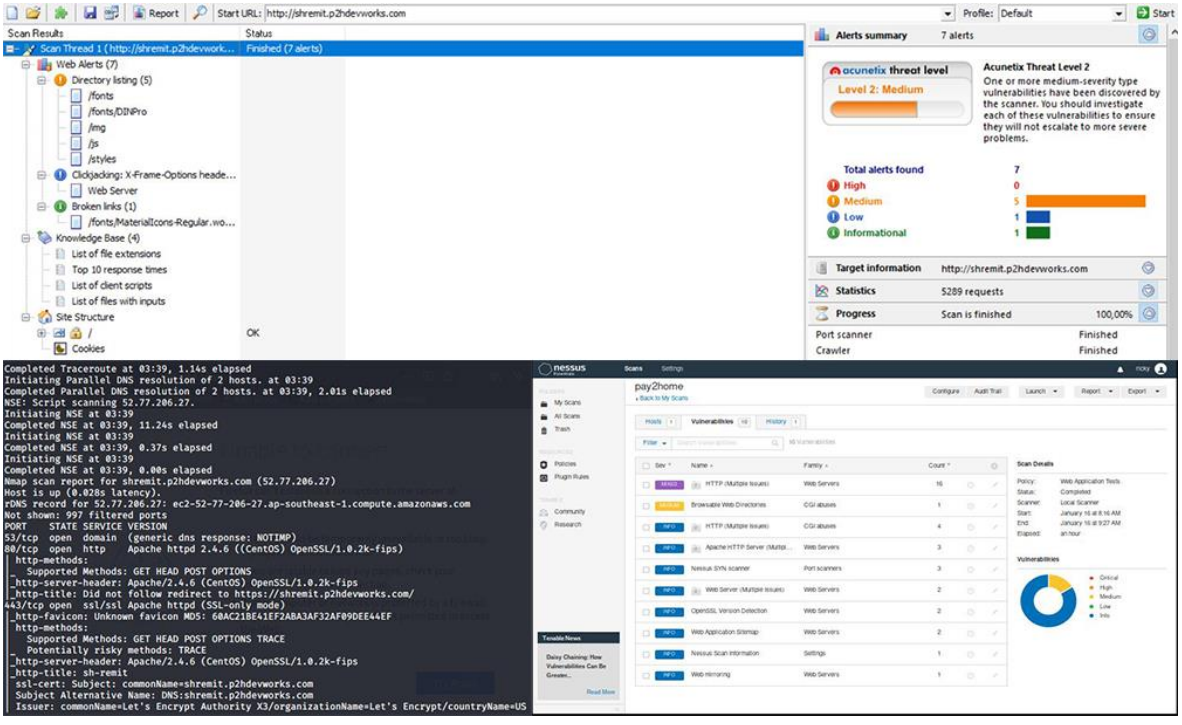
Gambar 4 Tampilan Awal Acunetix

4. Nmap

Nmap atau disebut juga sebagai Network Mapper merupakan sebuah perangkat lunak yang berfungsi untuk mengeksplorasi serta mengaudit keamanan jaringan. Dibuat dengan tujuan untuk memeriksa cangkupan jaringan besar dengan cepat, tetapi perangkat lunak ini juga dapat berjalan pada satu host (Lihat Gambar 5).



Gambar 5 Tampilan Awal Nmap



Gambar 6 Hasil Scan Acunetix, Nmap dan Nessus

Uji coba dilakukan dengan menggunakan Nmap dengan menggunakan command nmap -v -A -Pn shremit.p2hdevworks.com dimana command tersebut berfungsi -v untuk menampilkan hasil secara tertulis , -A berfungsi untuk mendeteksi versi OS, mendeteksi versi,

scanning script dan traceroute , dan -Pn berfungsi untuk menganggap semua host menjadi online serta shremit.p2hdevworks.com merupakan target tersebut. Maka didapatkan bahwa terdapat port terbuka diantaranya port 53 , 80 dan 443 pada shremit.p2hdevworks.com kemudian diketahui juga bahwa shremit.p2hdevworks.com menggunakan amazon dalam keamanannya, dengan menggunakan OS Linux 2.4 dan OS linux 3.2

Kemudian uji coba dilakukan dengan menggunakan aplikasi Nessus, dengan menggunakan opsi full scan, scan all port, service and vulnerability. setelah selesai melakukan scanning maka dapat diketahui bahwa terdapat port yang terbuka diantaranya port 80. 443 dan 8081.

Setelah itu uji coba yang terakhir menggunakan aplikasi Acunetix Scanner, dengan memasukkan target host menggunakan opsi web scanner, tunggu hingga selesai dan dapat diketahui terdapat beberapa celah yang terdapat pada website tersebut seperti Clickjacking X frame Options, Header Missing, dan Directory Listing.

Dapat dilihat hasil dari scan beberapa aplikasi yang digunakan yaitu Acunetix, Nmap dan Nessus Scanner dimana sistem masi dapat membaca informasi tentang host dan menemukan celah yang terbuka pada port dengan menggunakan Nmap dan pada gambar 7 dapat dilihat bahwa terdapat kerentanan situs pada shremit.p2hdevworks.com menggunakan Acunetix dengan tabel sebagai berikut :

Domain	Kerentanan
Domain Pertama (Level Threat Low)	Clickjacking X Frame Option Header Missing
Domain Kedua (Level Threat Medium)	Directory Listing
Domain Ketiga (Level Threat High)	

Gambar 7 Celah Keamanan yang ditemukan

Dari hasil pengujian diatas dimana terdapat 3 level yaitu kerentanan dengan ancaman tingkat rendah, sedang dan tinggi, pada gambar 7 diatas terdapat kerentanan dengan ancaman tingkat rendah dan sedang, dimana ancaman tingkat rendah yaitu *Clickjacking X Frame Option Header Missing* dimana hal tersebut merupakan sebuah teknik untuk mencuri data maupun informasi penting dari pengguna, kemudian ancaman tingkat sedang yaitu *Directory Listing* dimana webserver dikonfigurasi untuk menampilkan list file yang terdapat pada direktori, hal tersebut dikhawatirkan dapat memberikan informasi yang seharusnya diketahui oleh pengguna pada website, dengan menganalisa sistem keamanan dengan menggunakan aplikasi Acunetix tidak dapat menampilkan detail *host* pada jaringan Pay2home dikarenakan celah celah keamanan sudah ditutup dengan mematikan *service port* agar tidak dapat disusupi maupun dibaca oleh pihak ketiga. Dari hal tersebut penulis memberikan rekomendasi untuk perushaan dengan menggunakan *Mikrotik* dimana terdapat fitur dalam menutup *port service* serta penambahan perintah *Deny* dan *SameOrigin* pada shremit.p2hdevworks.com dimana perintah yang digunakan seperti: *x-frame-options: deny / x-frame-options:* SAMEORIGIN. Penelitian

yang dilakukan ini semoga dapat membantu penelitian selanjutnya dalam hal *Penetration Testing* dan *Vulnerability Assesment.*

Kesimpulan

Melalui analisis keamanan yang dilakukan oleh penulis dengan metode penetration testing pada Pay2home, penulis dapat menyimpulkan bahwa sistem keamanan jaringan yang terdapat pada sistem pay2home pada bagian namun pada bagian website masih terdapat celah, pada bagian port service terdapat service yang terbuka sehingga memungkinan terjadinya penyerangan, Sistem keamanan jaringan yang baru dapat dicapai dengan mematikan *sevice port* serta menggunakan perintah *Deny dan Sameorigin.*

Daftar Pustaka

Abdurrohim, I. (2019). Penetration Testing Sistem Keamanan Aplikasi Web Berbasis e-Commerce Pada Perusahaan Hptasik. *Jurnal Ilmu Komputer*, *1*, 125–131.

Denis, M., Zena, C., & Hayajneh, T. (2016). Penetration testing: Concepts, Attack Methods, and Defense Strategies. *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*. https://doi.org/10.1109/LISAT.2016.7494156

Sari, D. M., Yamin, M., & Aksara, L. B. (2017). Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing. *SemanTIK*, *3*(2), 203–208. https://doi.org/10.1016/j.neuropharm.2007.08.010

Tarigan, B. V., Kusyanti, A., & Yahya, W. (2017). Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(3), 206–214.

Ula, M. (2019). Evaluasi Kinerja Software Web Penetration Testing. *TECHSI - Jurnal Teknik Informatika*, *11*(3), 336. https://doi.org/10.29103/techsi.v11i3.1996

Wilman, W., Fitri, I., & Nathasia, N. D. (2018). Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual. *J I M P - Jurnal Informatika Merdeka Pasuruan*, *3*(1), 27–33. https://doi.org/10.37438/jimp.v3i1.86

Wulandari, R. (2016). Analisis QoS (Quality Of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon – LIPI). *Jurnal Teknik Informatika Dan Sistem Informasi*, *2*(2), 162–172. https://doi.org/10.28932/jutisi.v2i2.454

Yaqoob, I., Hussain, S. A., Mamoon, S., Naseer, N., Akram, J., & Rehman, A. ur. (2017). Penetration Testing and Vulnerability Assessments. *Journal of Network Communications and Emerging Technologies (JNCET)*, *1*(August 2017), 10–18.

Yunanri, Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *Annual Research Seminar*, *2*(1), 300–304.

Yunus, M. (2019). Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4. *Jurnal Ilmiah Informatika Komputer*, *24*(1), 37–48. https://doi.org/10.35760/ik.2019.v24i1.1988