p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika

Intan Kamilah[1]* , Ritzkal[1] , Ade Hendri Hendrawan[1]

[1] Laboratorium Net Centric Computing, Teknik Informatika, Fakultas Teknik dan Sains, Universitas Ibn Khaldun Bogor, Kota Bogor, Jl. Sholeh Iskandar, Kedung Badang, Kec. Tanah Sareal, 16162
**Corresponding Author* : intan.kamil06@gmail.com

Abstrak

Vulnerability adalah suatu point kelemahan dimana suatu sistem rentan terhadap serangan. Hampir sebagian serangan yang ada saat ini merupakan hasil dari eksploitasi terhadap port-port yang terbuka. Eksploitasi kerentanan merupakan metode umum lain penyusupan. Dalam analisis keamanan jaringan peneliti menggunakan Nmap dan Nessus. Pada penelitian ini terdapat beberapa tujuan penelitian yang terdiri dari (i) Mendapatkan hasil monitoring pada port server absensi kehadiran laboratorium (ii) Mendapatkan hasil analisis keamanan vulnerability pada server absensi kehadiran laboratorium (iii) Mendapatkan rekomendasi dari sistem keamanan vulnerability pada server absensi kehadiran laboratorium. Metode penelitian dalam penelitian ini meliputi prepare, plan, design, implement, operate, optimize merupakan metode analisis yang dikembangkan oleh Cisco. Hasil dari penelitian ini adalah (i) Hasil monitoring keamanan yang dilakukan, didapatkan beberapa port yang terbuka pada server absensi kehadiran laboratorium diantaranya port 53 untuk domain name service, port 80 untuk web server, port 21 file transfer dan port 1723 untuk point-to-point tunelling,(ii) Hasil monitoring keamanan yang dilakukan, didapatkan 4 kategori vulnerability dari IP target absensi kehadiran laboratorium berupa 7 vulnerability untuk kategori info, 12 untuk kategori meduim, 7 untuk kategori high dan 2 untuk kategori critical dan (iii) Hasil rekomendasi yang disarankan untuk mengatasi vulnerability pada absensi kehadiran laboratorium jika diterapkan akan meningkatkan kinerja dan performa sistem keamanan pada absensi kehadiran laboratorium.

Kata kunci: *Vulnerability*,Analisis Keamanan Jaringan,Eksploitasi, Port server,Nessus.

Abstract

Vulnerability is a point of weakness where a system is vulnerable to attack. Almost all of the attacks that exist today are the result of exploitation of open ports. Vulnerability exploitation is another common method of infiltration. In the analysis of network security researchers use Nmap and Nessus. In this study there are several research objectives which consist of (i) Obtaining monitoring results on the laboratory attendance server port (ii) Obtaining the results of security vulnerability analysis on the laboratory attendance server (iii) Obtaining recommendations from security system vulnerability on the laboratory attendance attendance server. The research methods in this study include prepare, plan, design, implement, operate, optimize are analytical methods developed by Cisco. The results of this study are (i) The results of security monitoring carried out, obtained a number of open ports on the laboratory attendance server, including port 53 for domain name service, port 80 for web server, port 21 file transfer and port 1723 for point-to-point point tunneling, (ii) The results of security monitoring carried out, obtained 4 categories of vulnerability from IP attendance target laboratory in the form of 7 vulnerabilities for the info category, 12 for the meduim category, 7 for the high category and 2 for the critical category and (iii) The results of the recommendations It is recommended to overcome the vulnerability in the absence of laboratory attendance if implemented will improve the performance and performance of the security system in the absence of laboratory attendance.

Keywords : *Vulnerability, Network Security Analysis, Exploitation, Server port, Nessus.*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENDAHULUAN

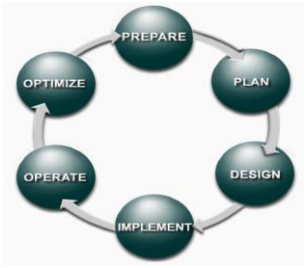
Jaringan yang terhubung dengan internet yang sifatnya publik dan global pada dasarnya tidak aman apalagi berkaitan dengan informasi atau data. Keberadaan suatu informasi atau data sangatlah berharga, maka tidaklah heran jika kemudian bermunculan beberapa pihak yang tidak bertanggung jawab, dimana pihak tersebut berusaha mencuri maupun merusak dan mengubah data atau informasi(Ritzkal R, Goeritno A, Hendrawan AHH. 2016). Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan. Dengan teknik-teknik tersebut kita dapat memblok, mengizinkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya (Setiawan, Thomas.2015).

Dalam menganalisis keamanannya dapat dilakukan dengan menggunakan *tool* Nmap dan Nessus, dimana tool Nmap dapat difungsikan untuk mengetahui port-port yang terbuka dan melihat host yang aktih pada jaringan, sedangkan tool Nessus akan mengaudit keamanan suatu sistem dan menghasilkan output berupa vulnerability. Serangan yang ditujukan kepada server absensi kehadiran laboratorium bisa dilakukan oleh pihak luar. Serangan yang dilakukan oleh pihak luar misalnya berusaha melakukan Denial of sevice (DOS) terhadap server web yang ada atau berusaha menembus masuk kedalam sistem informasi.

Hampir sebagian serangan yang ada saat ini merupakan hasil dari eksploitasi terhadap port-port yang terbuka. Eksploitasi kerentanan merupakan metode umum lain penyusupan. Penyerang akan memindai komputer untuk memperoleh tentang nya (Ritzkal.2019). Untuk membantu menjaga keamanan jaringan dan layanannya pada server absensi kehadiran laboratorium, penelitian ini mencoba melakukan analisis kemanan vulnerability pada server absensi kehadiran laboratorium, melakukan monitoring pada port server, melakukan serangkaian pengujian dan merekomendasikan hal-hal terkait pengamanan jaringan dan layanannya pada server absensi kehadiran laboratorium. Rumusan masalah pada penelitian ini adalah (i) Bagaimana mendapatkan hasil monitoring pada port server absensi kehadiran laboratorium?, (ii) Bagaimana mendapatkan hasil analisis keamanan vulnerability pada server absensi kehadiran laboratorium?,(iii) Bagaimana mendapatkan rekomendasi dari sistem keamanan vulnerability pada server absensi kehadiran laboratorium?. Tujuan dari penelitian ini adalah (i) Mendapatkan hasil monitoring pada port server absensi kehadiran laboratorium, (ii) Mendapatkan hasil analisis keamanan vulnerability pada server absensi kehadiran laboratorium dan (iii) Mendapatkan rekomendasi dari sistem keamanan vulnerability pada server absensi kehadiran laboratorium sebagai solusi kepada pihak server.

METODE PENELITIAN

Tahapan Penelitian yang dilakukan dapat dilakukan pada Gambar 1.



Gambar 1. Metode Penelitian

PPDIOO *(Prepare Plan Design Implement Operate Optimize)* merupakan metode analisis pengembangan instalasi jaringan komputer yang di kembangkan oleh *Cisco* pada materi *Designing for Cisco Internetwork Solutions (DSGN)* yang di sampaikan oleh Diane Teare pada tahun 2008 yang mendefinisikan secara terus menerus siklus hidup layanan yang di butuhkan untuk pengembangan jaringan komputer(Wahyu Dwiyan.2018).

1. Persiapan (Prepare)

Dalam metode pengembangan sistem menggunakan PPDIOO, fase pertama dimulai dari fase *prepare* atau tahap persiapan.Pada tahap ini akan dilakukan proses perumusan masalah, mengidentifikasi konsep dari sistem, serta tahapan penelitian yang harus dilakukan meliputi desain topologi jaringan, konfigurasi Nmap dan Nessus sebagai tool untuk audit jaringan, melakukan proses monitoring, proses analisis dan proses rekomendasi.

2. Perencanaan (Plan)

Perencanaan dalam analisis keamanan *vulnerability* pada server kehadiran laboratorium, Pada tahap ini terdapat perencanaan seperti perangkat keras, perangkat lunak dan perangkat lainnya yang

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

harus diinstal serta dikonfigurasi untuk mendukung penelitian analisis keamanan vulnerability pada server kehadiran laboratorium.

3. Perancangan (Design)

Pada tahap ini akan di bahas gambaran topologi jaringan yang digunakan untuk memudahkan dan memahami konsep sistem keamanan yang ada pada server absensi kehadiran laboratorium.

4. Implemntasi (Implement)

Pada tahapan ini implementasi menerapkan semua yang sudah direncanakan. Pada tahap ini meliputi installasi serta konfigurasi. Adapunyang harus dilakukan adalah installasi Sistem Operasi, Installasi Nmap dan Installasi Nessus.

5. Operasi (Operation)

Pada tahap ini, dilakukan proses pengujian menggunakan parameter yang ditentukan meliputi proses monitoring, analisis dan rekomendasi serta sejumlah komponen pendukung agar dipastikan sudah berjalan dengan baik dan benar untuk menjawab permasalahan yang telah dirumuskan.

6. Optimal (Optimize)

Pada tahap ini memerlukan perhatian khusus terhadap kebijakan yang perlu dibuat untuk mengatur sebuah sistem agar selalu dapar berjalan dengan optimal. Perawatan, pemeliharaan dan pengelolaan terhadap server termasuk dalam fase ini.

HASIL DAN PEMBAHASAN

Hasil penelitian yang mengacu pada dua tujuan pada penelitian ini yang berjudul Analisis Keamanan *Vulnerability* Pada Absensi Kehadiran Laboratorium Di Fakultas Teknik Universitas Ibn Khaldun Bogor, maka pada tahap ini akan membahas hasil dari penelitian yang dilakukan.

Hasil dari tahapan penelitian analisis keamanan *vulnerability* pada absensi kehadiran laboratorium di fakultas teknik universitas ibn khaldun bogor melalui lima tahapan, yaitu prepare (persiapan), plan (perencanaan), design (desain), implement (penerapan), operation (operasi) dan optimize (optimal).

1. Prepare

Penelitian ini akan dilakukan pada jaringan server absensi kehadiran laboratorium. Pada server absensi kehadiran laboratorium ini akan ada beberapa celah yang bisa disusupi oleh seorang attacker untuk itu perlu adanya analisis keamanan pada sebuah server. Salah satunya peneliti akan menganalisis keamanannya menggunakan tool Nmap dan Nessus. Sistem operasi yang digunakan adalah Linux Ubuntu 14.04. Peneliti melakukan studi literatur untuk menambah wawasan dan panduan dalam mendukung penelitian ini.

2. Plan

Setelah semua kebutuhan dalam fase persiapan sudah dilakukan, analisis kebutuhan *hardware* serta kebutuhan *software* yang diperlukan dalam penelitian. Analisis mencakup verifikasi inventori *hardware* dan memperkirakan penggunaan sumber daya *hardware.* Inventori *hardware* mencakup tentang beberapa server yang digunakan, berapa perangkat jaringan yang ada, termasuk jumlah CPU, RAM, dan peripheral lainnya.

a. Perangkat keras (Hardware)

Penelitian yang dilakukan membutuhkan perangkat keras yang dibutuhkan untuk menunjang analisis keamanan *vulnerability* pada server absensi kehadiran lab adalah sebagai berikut :

1.Komputer server

Komputer server merupakan komputer yang digunakan sebagai pusat layanan dan sekaligus menjadi target untuk menganalisis keamanan *vulnerability* pada absensi kehadiran lab dengan spesifikasi sebagai berikut :

- CPU core, ruang penyimpanan 8 GB, memori 256 MB RAM

2.Komputer client

Komputer client merupakan komputer yang digunakan untuk pengujian dengan bertujuan mengetahui kerentanan yang ada pada penilitian ini. Kebutuhan yang digunakannya yaitu :

- CPU core, ruang penyimpanan 4 GB, memori 256 MB RAM
- *Operating System* Linux 14.04 LTS Dekstop

b. Perangkat Lunak

Penelitian yang dilakukan membutuhkan perangkat lunak yang dibutuhkan untuk menunjang analisis keamanan *vulnerability* pada server absensi kehadiran lab adalah sebagai berikut :

a. Nmap

Nmap menggunakan IP raw dalam menentukan host mana saja yang tersedia pada jaringan, layanan (nama

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paketyang digunakan dan sejumlah karakteristik lainnya.

b. Nessus
Nessus merupakan sebuah software scanning yang dapat digunakan untuk mengaudit keamanan sebuah sistem seperti *vulnerability*, misconfiguration, security patch yang belum diaplikasikan, default password dan denial of service. Nessus berfungsi untuk memonitoring lalu lintas jaringan dan mendeteksi adanya kelemahan ataupun galat dari suatu sistem

3. Design

Gambar 2. Topologi jaringan

Topologi jaringan menggambarkan pengalamatan *ip address* pada struktur jaringan komputer pada absensi kehadiran laboratorium, dimana server absensi kehadiran laboratorium dengan ip 103.3.59.154 dan client yang nantinya akan melakukan proses pengujian.

4. Implement

Pada tahap ini peneliti membagi tahap implementasi menjadi beberapa bagian.
1. Instalasi Sistem Operasi
Penulis menginstalasi sistem operasi yang nantinya digunakan dalam proses penelitian. Pada penelitian ini menggunakan sistem operasi Linux 2. Instalasi Nmap
Penulis menggunakan untuk memonitoring dan melihat port-port yang terbuka pada jaringan. 3. Instalasi Nessus
Penulis menggunakan untuk scanning dan melihat vulnerability pada IP target.

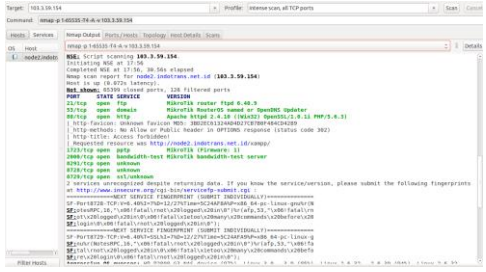
5. Operate

a. Monitoring

Pada tahap ini akan dilakukan proses monitoring data jaringan server absensi kehadiran laboratorium dengan menggunakan tool Nmap dan Nessus.

1. Monitoring jaringan menggunakan Nmap

Pada tahap ini dilakukan untuk mengetahui kerentanan yang didapat dengan memonitoring menggunakan Nmap. Prosesnya adalah melakukan scanning terus-menerus terhadap IP target dimana IP yang di scan adalah 103.3.59.153. Gambar berikut akan menjelaskan mengenai hasil dari scan jaringan pada server absensi kehadiran lab.



Gambar 3. Scan jaringan dengan Nmap

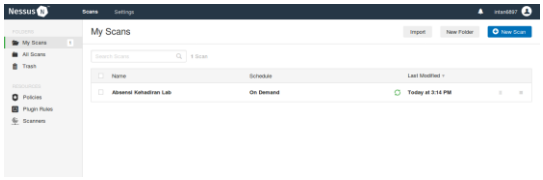
Berdasarkan gambar 4.2 tampak pada hasil *scan* yang dilakukan oleh Nmap menggunakan versi GUI pada sistem operasi linux ubuntu melalui IP 103.3.59.154 menunjukan *port*, *state*, *service* dan *version* dari IP yang di s*can*. Terdapat beberapa port yang terbuka pada server absensi kehadiran laboratorium diantaranya port 21, port 53, port 80 dan port 1723. Tugas dari port tersebut adalah sebagai berikut :

- Port 21 merupakan port *file transfer protocol*
- Port 53 merupakan port *domain name service*
- Port 80 merupakan webserver
- Port 1723 merupakan port *point-to-point tunneling protocol*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

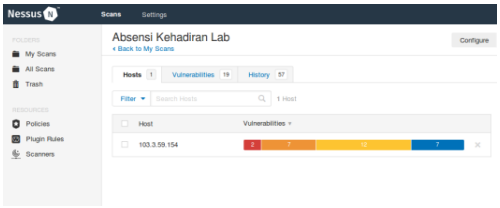
2. Monitoring jaringan menggunakan Nessus

Pada tahap ini dilakukan untuk mengetahui kerentanan yang didapat dengan memonitoring menggunakan Nessus. Dalam pengujiannya dilakukan 48 kali *scanning* terus-menerus terhadap IP target dimana IP yang di *scan* adalah 103.3.59.154. Gambar berikut akan menjelaskan mengenai *scan* jaringan pada server absensi kehadiran lab menggunakan Nessus.



Gambar 4. Scan jaringan dengan Nessus

Hasil scan IP 103.3.59.154 menggunakan Nessus menunjukkan secara rinci *vulnerability* dari IP target yang telah di *scan* oleh Nessus. Seperti ditunjukkan pada gambar berikut ini.



Gambar 5. Hasil scan vulnerability

Dari hasil *scan* IP 103.3.59.154 yang dilakukan Nessus didapatkan *vulnerability*, pada icon yang diwarnai terdapat keterangan dari setiap informasi, icon warna merah menunjukkan *critical*, icon *orange* menunjukkan *high*, icon kuning menunjukkan *medium*, icon hijau menunjukkan *low* dan icon biru menunjukkan info. Selain itu didapat juga informasi berupa deskripsi data yang diolah dalam sebuah tabel untuk mempermudah dalam menganalisa hasil dari pengolahan data. Berikut adalah data vulnerability dari hasil scan menggunakan Nessus berdasarkan tingkatan kategori kerentana

Tabel 1. Alert founds Nessus berdasarkan kategori kerentanan

No	Kategori	Tampilan
1	Critical	- Mikrotik RouterOS < 6.41.3 SMB Buffer Overflow. - Mikrotik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed).
2	High	- DNS Server Spoofed Request Amplification DDoS - HTTP Proxy CONNECT Request Relaying - OpenSSL Unsupported - PHP 5.6.x < 5.6.4 ‘process_nested_data’ RCE - PHP 5.6.x < 5.6.14 Multiple Vulnerabilities - OpenSSL < 1.0.2i Default Weak 64-bit Block Chiper (SWEET32) - Apache 2.4.x < 2.4.35 DoS
3	Medium	- DNS Server Chace Snooping Remote information Disclosure - PHP 5.6.x < 5.6.28 Multiple Vulnerabilies - Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed) - DNS Server Recursive Query Cache Poisoning Weakness - PHP 5.6.x < 5.6.33 Multiple Vulnerabilities - DNS Server Detection - PHP 5.6.x < 5.6.36 Multiple Vulnerabilities - PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS - PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability - PHP 5.6.x < 5.6.34 Stack Buffer Overflow - PHP 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)
4	Info	- FTP Server Detection. - Mikrotik RouterOS Detection. - Mikrotik RouterOS Winbox Detection. - Nessus SYN Scanner. - PPTP Detection. - Apache HTTP Server Version. - Inconsistent Hostname and IP Address.

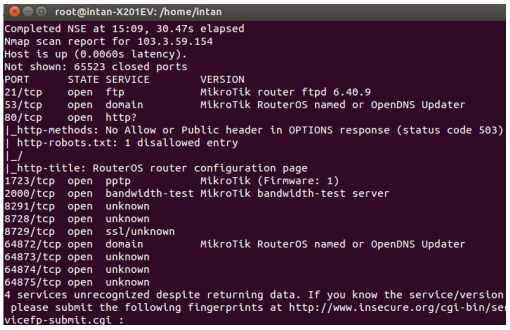
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

b. Analisis

Pada tahap analisis keamanan *vulnerability* pada server absensi kehadiran lab yang dilakukan adalah mengumpulkan semua data yang dibutuhkan dalam proses analisis *vulnerability*. Kemudian menghasilkan sebuah output berupa *vulnerability* dari IP yang di *scan*, hasil *scan* tersebut dapat memberikan informasi detail kerentanan yang nantinya dari data tersebut bisa ditemukan solusi untuk penanganan kerentanan pada server absensi kehadiran lab.

1. Pengujian keamanan vulnerability dengan tool Nmap

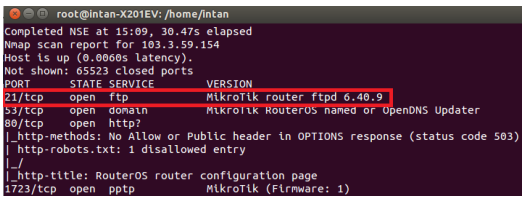
Nmap bekerja dengan melakukan scan terhadap komputer (host) *stand alone* ataupun host yang terhubung dalam sebuah jaringan dengan menggunakan *port random* untuk mencoba koneksi dengan *discovered* port target yang aktif, menentukan host-host yang aktif dalam suatu jaringan, *port-port* yang terbuka. Gambar ini menunjukkan hasil pengujian scan IP target absensi kehadiran lab menggunakan Nmap.



Gambar 6. Hasil pengujian dengan Nmap

Setelah dilakukan nya *scan* monitoring menggunakan Nmap pada absensi kehadiran laboratorium ada beberapa port yang terbuka seperti berikut :

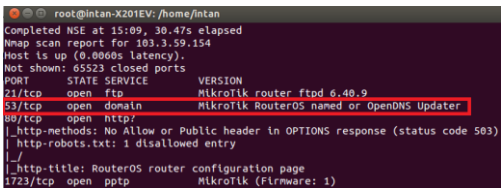
1. Pada port 21 (FTP) seperti pada gambar 4.8



Gambar 7. Open port pada port 21

Port 21 *File Transfer Protocol* (FTP) sebagai suatu protokol yang berfungsi untuk tukar-menukar file dalam suatu network menggunakan TCP. Pada *scan port* menggunakan Nmap mendeteksi adanya *port* terbuka dengan *port* 21 (FTP) dari IP *Address* target 103.3.59.154.

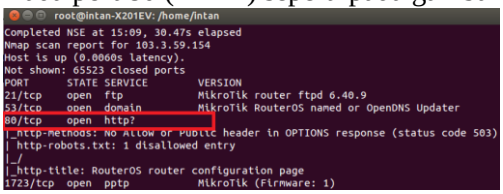
2. Pada port 53 (DNS) seperti pada gambar 4.8



Gambar 8. Open port pada port 53

Port 53 *Domain Name System* (DNS) sebagai sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (*distributed database*) didalam jaringan komputer. Pada *scan port* menggunakan Nmap mendeteksi adanya *port* terbuka dengan *port* 53 (DNS) dari IP *Address* target 103.3.59.154.

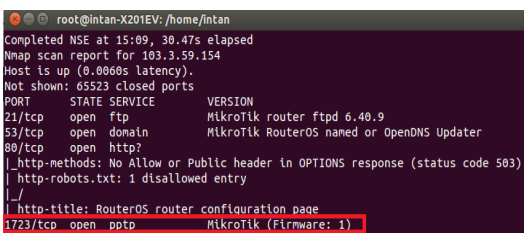
3. Pada port 80 (HTTP) seperti pada gambar



Gambar 9. Open port pada port 80

Port 80 *Hypertext Transfer Protocol* (HTTP) sebagai sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hypermedia. HTTP adalah pondasi komunikasi data untuk *World Wide Web*. Pada *scan port* menggunakan Nmap mendeteksi adanya *port* terbuka dengan *port* 80 (HTTP) dari IP *Address* target 103.3.59.154.

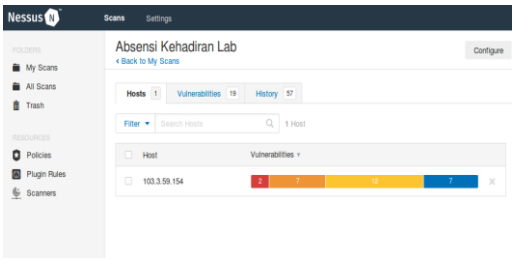
4. Pada port 1723 (PPTP) seperti pada gambar



Gambar 10. Open port pada port 1723

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Port 1723 *Point-To-Point Tunneling Protocol* (PPTP) sebagai teknologi jaringan baru yang mendukung multiprotocol *Virtual private Network* (VPN) yang memungkinkan pengguna untuk mengakses jaringan perusahaan secara lebih aman melalui internet. Pada *scan port* menggunakan Nmap mendeteksi adanya *port* terbuka dengan port 1723 (PPTP) dari IP *Address* target 103.3.59.154.



Gambar 11. Hasil pengujian dengan Nessus

2. Pengujian keamanan *vulnerability* dengan tool Nessus.

Nessus akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju. Hasil pengujian *scan* IP target menggunakan Nessus terdapat *vulnerability* pada jaringan absensi kehadiran lab dimana terdapat 4 kategori *vulnerability* dari 5 kategori yang ada, terdapat28 kerentanan yang terbagi dalam 4 kategori yaitu 2 kategori critical, 7 kategori high, 12 kategori medium dan 7 kategori info. Seperti ditunjukan pada gambar berikut ini.Adapun penjelasan setiap vulnerability yang didapat :

1. Critical

a. Mikrotik RouterOS < 6.41.3 SMB Buffer Overflow.

Pada kerentanan ini ditemukan exploitasi buffer overflow kerentanan yang mempengaruhi Mikrotik RouterOS dalam versi yang sudah lama. Jenis kerentanan Buffer overflow yang bisa dimanfaatkan oleh hacker remote akses ke layanan untuk mengeksekusi kode pada sistem. Berikut adalah deskripsi untuk jenis vulnerability Mikrotik RouterOS < 6.41.3 SMB Buffer Overflow.

Gambar 12. *Vulnerability Mikrotik RouterOS < 6.41.3 SMB Buffer Overflow*.

b. Mikrotik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed).

Mikrotik RouterOS adalah sistem dan perangkat lunak yang dapatdigunakan untuk menjadikan komputer menjadi router network (PC Router), sedangkan HTTP (Hypertext Transfer Protocol) adalah sebuah protokol untuk mengatur komunikasi antara client dan server.dalam hal ini, client adalah browser atau perangkat yang dapat menampilkan konten web. Pada kerentanan ini ditemukan kerusakan dalam proses web server HTTP pada Mikrotik RouterOS karena validasi yang tidak tepat dari input yang disediakan pengguna. Penyerang yang tidak terauthentikasi dapat mengeksploiasi ini. Berikut adalah deskripsi untuk jenis vulnerability Mikrotik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed).

Gambar 13. *Vulnerability Mikrotik RouterOS HTTP*.

1. High

Dari 7 kategori high yang didapat berikut salah satu vulnerability nya yaitu :

a. DNS Server Spoofed Request Amplification DDoS.

Pada kerentanan ini ditemukan dengan spoofing IP sumber alamat, penyerang dapat memanfaatkan amplifikasi ini untuk melakukan serangan penolakan terhadap layanan terhadap host menggunakan remote DNS server. Berikut adalah deskripsi untuk jenis

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

vulnerability DNS Server Spoofed Request Amplification DDoS.

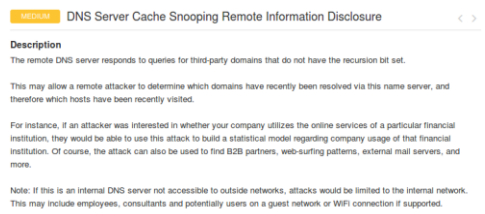
Gambar 14. *Vulnerability DNS Server Spoofed Request Amplification DDoS*.

2. Medium

Dari 12 kategori medium yang didapat berikut salah satu vulnerabilty nya yaitu :

a. DNS Server Chace Snooping Remote information Disclosure.

DNS (Domain Name System) adalah sebuah sandar teknologi yang mengatur penamaan publik dari subuah situs web. Snooping memungkinkan dilakukan pemantauan terhadap suatu elektronik terhadap jaringan digital untuk dapat mengetahui passsword atau data lainnya. Pada kerentanan ini ditemukan ketika seseorang meminta DNS server untuk mencari tahu jika DNS server memliki record cached DNS tertentu. Penyerang akan dengan mudah menemukan informasi tentang pemilik DNS server. Berikut adalah deskripsi dari jenis kerentanan *DNS Server Chace Snooping Remote information Disclosure.*



Gambar 15. Vulnerability DNS Server Chace Snooping.

3. Info

Dari 7 kategori info yang didapat berikut salah satu vulnerability nya.

c. Rekomendasi

Dari proses analisis yang dilakukan pada tahap sebelumnya sudah didpatkan data *vulnerability* dari IP target, dimana IP target mempunyai *vulnerability* yang berbeda-beda dalam setiap kategori, mulai dari *high, medium*, info sampai ke *critical*, tahap ini menjelasakan bagaimana solusi yang disarankan untuk mengatasi masalah *vulnerability* dari data yang sudah di dapat, untuk solusi dari IP target Absensi Kehadiran Lab. Keamanan yang direkomendasikan hanya di tingkat kerentanan *critical* dan *high*.

1. Kategori critical
   - Mikrotik RouterOS < 6.41.3 SMBBuffer Overflow .
     Solusi : Upgrade ke Mikrotik RouterOS 6.41.3 atau lebih baru.
   - Mikrotik RouterOS HTTP Server Arbitary Write RCE
     Solusi : Upgrade ke Mikrotik RouterOS versi 6.38.5 atau lebih baru.
2. Kategori high
   - DNS Server Spoofed Request Amplification DdoS.
     Solusi : Batasi akses ke server DNS dari jaringan publik atau konfigurasikan ulang untuk menolak permintaan semacam itu.
3. Kategori Medium
   - DNS Server Chace Snooping Remote information Disclosure
     Solusi : Hubungi vendor perangkat lunak DNS untuk perbaikan.

6. Optimize

Pada tahap terakhir dari PPDIOO ini adlah meliputi perawatan dan pemeliharaan. Dalam tahap pemeliharaan ini terdapat beberapa proses diantaranya proses pengelolaan dan proses perawatan yang dilakukan untuk bertujuan melakukan penyesuaian dan perangkat keras pada server absensi kehadiran laboratorium agar dapat beradaptasi dengan perkembangan kebutuhan sistem, seperti penambahan RAM, peningkatan kapasitas dari media penyimpanan, mengupgrade Router OS, sistem operasi dan mengupgrade web server.

KESIMPULAN

Berdasarkan penelitian yang dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Hasil monitoring keamanan yang dilakukan, didapatkan beberapa port yang terbuka pada server absensi kehadiran laboratorium diantaranya port 53 untuk *domain name service*, port 80 untuk web server, port 21 *file*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

transfer dan port 1723 untuk *point-to-point tunelling*.

2. Hasil monitoring keamanan yang dilakukan, didapatkan 4 kategori *vulnerability* dari IP target absensi kehadiran laboratorium berupa 7 *vulnerability* untuk kategori info, 12 untuk kategori *meduim, 7* untuk kategori *high* dan 2 untuk kategori *critical*.
3. Hasil rekomendasi yang disarankan untuk mengatasi *vulnerability* pada absensi kehadiran laboratorium jika diterapkan akan meningkatkan kinerja dan performa sistem keamanan pada absensi kehadiran laboratorium.

DAFTAR PUSTAKA

Antonio H, Safriadi N. 2015. *Rancang Bangun Sistem Informasi Administrasi Informatika*. Jurnal ELKHA.

Babys, Jemi Yohanis. 2018. *Analisis Vulnarable Port Pada Client Pengguna Publik Wifi*. Jurnal SIMETRIS. Kupang.

Daniel, Ilham. 2015. *Evaluasi Celah Keamanan Web Server Pada LPSE Kota Palembang.* Muhammad. Palembang.

Dwiyan, Wahyu. 2018. *Perbandingan Kecepatan Server Tunggal Dengan Load Balancing Serta Mirroring Server Dalam Mengakses Layanan E-Mading*. Skripsi tidak di terbitkan. Bogor : Universitas Ibn Khaldun Bogor.

Juardi, Didi. 2017. *Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus*. Jurnal Informatika. Karawang.

Jusuf, Heni. 2015. *Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online*. Bina Insani ICT Journal. Jakarta.

Kunang, Yesi Novaria. 2015. Pengujian Celah Keamanan Pada CMS (Content Management System). Prosiding Seminar Nasional Ilmu Komputer. Palembang.

Nazwita Ramdhani, Siti. 2017. *Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata*. Jurnal Seminar Nasional Teknologi Informasi, Komunikasi dan Industri. Padang.

Maharani, Mia Zattu. 2017. *Analisis keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks*. e-Proceeding of Applied Science : Vol.3, No.3 Desember 2017. Bandung.

Prabowo, Yunan Arie. 2014. *Penggunaan Nmap dan HPING3 Dalam Menganalisa Keamanan Jaringan Pada B2P2TO2T*. Skripsi tidak di terbitkan. Surakarta : Universitas Muhammadiyah Surakarta

Purwantoro. 2017. *Implementasi Metode Online Scanner Untuk Mencari Kerentanan Keamanan (Vulnerability) Server. Jurnal Rekayasa Informasi*. Karawang.

Ritzkal R, Goeritno A, Hendrawan AHH. 2016. *Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor*. Seminar Nasional Sains dan Teknologi 2016.

Ritzkal S.Kom., M.Kom. 2018. *Manajemen Jaringan*. Bogor : UIKA Press.

Ritzkal S.Kom., M.Kom. 2019. *Keamanan Jaringan Cyber*. Bogor : UIKA Press.

Setiawan, Thomas. 2015 *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal*. Skripsi tidak di terbitkan. Bandung : Institut Teknologi Bandung.