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

Analisis Keamanan *Vulnerability* pada Server *Cloud Open Media Vault* di Fakultas Teknik Universitas Ibn Khaldun Bogor

Dicky Septian Firdaus[1*], Ritzkal[1], Ade Hendri Hendrawan[1]
[1,]Laboratorium Net-centric Computing, Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Ibn Khaldun Bogor, Jl. Sholeh Iskandar, Kedung Badak, Kec. Tanah Sareal, 16162
**Corresponding Author*: dickyseptianf21@gmail.com

Abstrak

Penyerangan adalah individu atau kelompok yang berusaha mengeksploitasi kerentanan untuk keuntungan pribadi atau keuangan. Rumusan masalah pada penelitian ini (i) Bagaimana mendapatkan hasil analisis dan monitoring keamanan vurnerability pada server Cloud Open Media Vault ?, (ii) Bagaimana mendapatkan rekomendasi dari sistem keamanan vulnerability pada server Cloud Open Media Vault ?. Tujuan Penelitian ini adalah (i) Mendapatkan hasil analisis dan monitoring keamanan vurnerability pada server Cloud Open Media Vault, (ii) Mendapatkan rekomendasi dari sistem keamanan vulnerability pada server Cloud Open Media Vault. metode penelitian ini meliputi Persiapan yang terdiri dari Instalasi Nmap dan Nessus, Topologi Jaringan yang terdiri dari Topologi jaringan fisik dan logic, Monitoring yang terdiri dari scan Nmap dan scan Nessus, Analisis yang meliputi pengolahan data dan tahapan Rekomendasi yang terdiri dari High, Critical, Medium dan Info.Hasil dari analisis dan monitoring didapatkan 6 port yang terbuka diantaranya port 21 FTP, Port 22 SSH, port 53 DNS, Port 80 HTTP/WEB, Port 111, Port 8443 dan Host detail yang statusnya up dari 65485 port, 43 port yang berstatus filltered serta 3 alamat IP yang berbeda mengakses kedalam server melalui Port 21 FTP dan Hasil dari rekomendasi didapatkan solusi sebanyak 13 solusi yang disarankan untuk menyelesaikan masalah 17 vulnerability. 4 kategori vulnerability berupa 1% vulnerability untuk kategori Critical, 1% untuk kategori High, 5% untuk kategori Medium, dan 10% untuk kategori Info. Berarti untuk server Cloud Open Media Vault mendapatkan kerentanan untuk diretas, karena memiliki celah keamanan sebesar 17%.

Kata kunci : Analisis Keamanan Jaringan, *Server, Nmap, Nessus, Vulnerability.*

Abstract

Assault is an individual or group that seeks to exploit vulnerability for personal or financial gain. The formulation of the problem in this study (i) How to get the results of security vurnerability analysis and monitoring on the Cloud Open Media Vault server? The objectives of this study are (i) Obtaining the results of security vurnerability analysis and monitoring on Cloud Open Media Vault servers, (ii) Obtaining recommendations from security system vulnerabilities on Cloud Open Media Vault servers. This research method includes preparation consisting of Nmap and Nessus Installation, Network Topology consisting of physical and logic network topology, Monitoring consisting of Nmap and Nessus scan, Analysis which includes data processing and Recommendation stages consisting of High, Critical, Medium and Info. The results of the analysis and monitoring obtained 6 open ports including 21 FTP ports, SSH Ports 22, 53 DNS ports, 80 HTTP / WEB ports, Port 111, Port 8443 and Host details whose status is up from 65485 ports, 43 ports are filltered status as well as 3 different IP addresses accessing to the server via Port 21 FTP and the results of the recommendation found 13 solutions suggested to solve the 17 vulnerability problems. 4 vulnerability categories in the form of 1% vulnerability for the Critical category, 1% for the High category, 5% for the Medium category, and 10% for the Info category. This means that for the Cloud Open Media Vault server, it has a vulnerability to be hacked, because it has a security gap of 17%.

Keywords : *Network Security Analysis, Server, Nmap, Nessus, Vulnerability.*

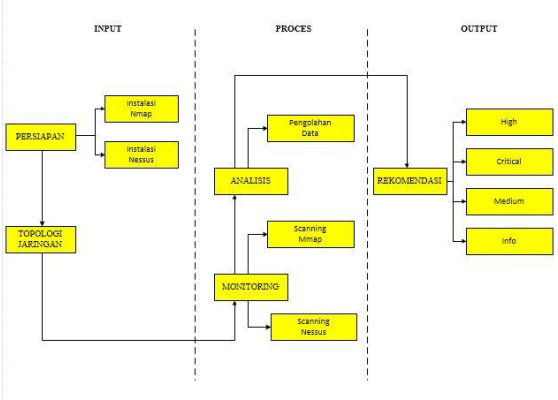
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENDAHULUAN

Penyerangan adalah individu atau kelompok yang berusaha mengeksploitasi kerentanan untuk keuntungan pribadi atau keuangan. Penyerang tertarik pada segala hal, dari kartu kredit hingga desain produk dan apapun yang berharga(Ritzkal, 2019). Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan, seperti packet *sniffing, network scanning,* dan monitoring layanan. Dengan teknik-teknik tersebut kita dapat memblok, mengizinkan, atau menyaring paket yang mencoba masuk ke dalam jaringan atau ingin mengakses sumberdaya atau layanan tertentu(Marti Widya Sari,2014). Salah satu cara didalam menganalisis keamanan jaringan yaitu menggunakan *tool* Nmap dan Nessus, dimana *tool* Nmap dapat digunakan untuk mengetahui port-port yang terbuka dan melihat *host* yang aktif dari jaringan lokal, dan *tool* Nessus akan mengaudit keamanan suatu sistem dan menghasilkan *output* berupa *vulnerability* dari ip *scan* target yang akan dianalisa. Serangan yang ditujukan kepada jaringan server *Cloud Open Media Vault* di Fakultas Teknik Universitas Ibn Khaldun Bogor bisa dilakukan baik oleh pihak luar ataupun bahkan dari civitas akademik Universitas Ibn Khaldun Bogor sendiri. Serangan yang dilakukan oleh pihak luar misalnya berusaha melakukan *Denial Of Service* (DOS) terhadap server web yang ada atau berusaha menembus masuk kedalam sistem informasi. Untuk membantu menjaga keamanan jaringan dan layanannya pada server *Cloud Open Media Vault*, penelitian ini mencoba melakukan analisis keamanan *vulnerability* menggunakan *tool* Nmap dan Nessus, membangun pertahanan terhadap serangan, melakukan serangkaian pengujian, dan merekomendasikan hal-hal terkait pengamanan jaringan dan layanannya pada server *Cloud Open Media Vault*. Berdasarkan berbagai macam permasalahan yang telah disebutkan di atas maka sangat diperlukan untuk membuat sebuah sistem yang dapat meminimalisasi berbagai macam permasalahan keamanan *vulnerability*, oleh karena itu akan dilakukan sebuah penelitian dengan judul "Analisis Keamanan *Vulnerability* Pada Server *Cloud Open Media Vault* Di Fakultas Teknik Universitas Ibn Khaldun Bogor". Rumusan masalah pada penelitian ini (i) Bagaimana mendapatkan hasil analisis dan monitoring keamanan vurnerability pada server Cloud Open Media Vault ?, (ii) Bagaimana mendapatkan rekomendasi dari sistem keamanan vulnerability pada server Cloud Open Media Vault ?. Tujuan Penelitian ini adalah (i) Mendapatkan hasil analisis dan monitoring keamanan vurnerability pada server Cloud Open Media Vault, (ii) Mendapatkan rekomendasi dari sistem keamanan vulnerability pada server Cloud Open Media Vault.

METODE

Pada tahapan ini dijelaskan bagaimana tahapan penelitian Analisis keamanan vulnerability ini dilakukan. Dalam metode ini menggunakan bagan alur kerjanya. Alur metode yang digunakan dalam penelitian ini seperti pada Gambar 1.



Gambar 1. Tahapan dalam penelitian

1. Persiapan

Pada tahap persiapan peneliti akan menginstal beberapa *Software* (perangkat lunak). Tahap pertama adalah menginstal *tool* Nmap dan yang terakhir menginstal *tool* Nessus.

2. Topologi Jaringan

Pada tahap ini akan dibahas topologi jaringan fisik dan logic yang digunakan untuk memudahkan dan memahami konsep komunikasi sistem keamanan yang ada pada server *Cloud Open Media Vault.*

3. Monitoring

Pada tahap ini akan dilakukan monitoring data pada server *Cloud Open Media Vault* dengan menggunakan *tool* Nmap dan Nessus. Dimana hasil scan menggunakan Nmap akan terlihat port-port IP ada pada server *Cloud Open Media Vault* sebagai IP target. Selain itu hasil scan menggunakan Nessus akan terlihat

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

banyaknya kategori *vulnerability* dari hasil monitoring menggunakan *tool* Nessus.

4. Analisis

Pada tahapan ini dilakukan proses analisis berupa pengolahan data yang didapatkan dari hasil monitoring dan *scan* yang dilakukan pada tahap sebelumnya dengan *tool* Nmap dan Nessus. Hasil scan dengan *tool* tersebut menampilkan *vulnerability* dan port-port yang terbuka pada server *Cloud Open Media Vault.* Data *vulnerability* yang telah di dapatkan selanjutnya akan diolah menjadi sebuah solusi untuk mengurangi *vulnerability* yang ada pada server *Cloud Open Media Vault.*

5. Rekomendasi

Tahap rekomendasi ini akan dibahas mengenai rekomendasi yang disaran kan untuk mengatasi *vulnerability* yang didapat dari hasil *scan* menggunakan *tool* Nessus, dimana saja yang sudah diolah berdasarkan tahap analisis sebelumnya akan terlihat beberapa kategori *vulnerability* yang telah di scan menggunakan *tool* Nessus, setiap *vulnerability* akan diberikan solusi atau rekomendasi bagaimana cara mengatasi masalah tersebut.

HASIL DAN PEMBAHASAN

Pada tahapan hasil dan pembahasan ini akan meliputi beberapa tahapan yaitu, Persiapan, Topologi Jaringan, Monitoring, Analisis dan Rekomendasi.

1. Persiapan

- Instalasi dan Kofigurasi Nmap

Penulis menggunakan untuk memonitoring dan melihat port-port yang terbuka pada jaringan. Untuk tahap proses instalasi Nmap dapat dilihat sebagai berikut :

a. Pastikan terlebih dahulu komputer terkoneksi ke dalam internet.
b. Sebelum melakukan installasi dan menjalankan nmap, kita harus terlebih dahulu menginstall WinPcap. Fungsi dari WinPcap ini seperti driver, jadi kalau tidak terinstall maka nmap tidak dapat berjalan.
c. Klik *I Agree* ketika install Nmap dimulai.
d. Centang semua omponen atau fitur dari Nmap.
e. Atur lokasi direktori instalasi Nmap, atau biarkan secara default terinstall di direktori C:\Program Files(x86)\Nmap.
f. Tunggu proses hingga selesai

- Instalasi dan konfigurasi Nessus

Penulisan menggunakan untuk scanning dan melihat *vulnerability* pada IP target. Utnuk tahap proses instalasi Nessus dapat dilihat sebagai berikut :

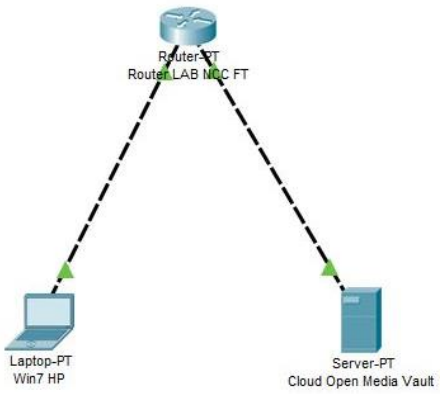
a. Pastikan terlebih dahulu komputer sudah terkoneksi ke dalam internet.
b. *Download packet* Nessus terlebih dahulu.
c. Setelah Nessus terdownlaod, install seperti bisa (nest sampai finish).
d. Setelah penginstalan selesai, buka nessus dan akan diarahkan pada alamat http://localhost:8834/register.
e. Masukan nama, password dan confirm password.
f. Setelah itu akan diminta kode aktifasi
g. Pilih home dan klik register
h. Masukan email untuk menerima kode aktifasi
i. Setelah register buka kembali email dan copy-paste kode aktifasi yang sudah dikirimkan.
j. Masukan kode aktifasi pada kolom yang diminta
k. Tunggu beberapa menit hingga proses plugin selesai.

2. Topologi Jaringan

Pada tahap ini meliputi infrastruktur dan topologi jaringan yang disesuaikan dengan keadaan infrastruktur jaringan pada server *Cloud Open Media Vault* yang sudah diterapkan di Lab *Net-centric Computing (NCC)* Program Studi Teknik Informatika Fakultas Teknik Universitas Ibn Khaldun Bogor. Topologi yang digunakan adalah topologi star dengan satu titik terpusat *device* menggambarkan sistem jaringan yang digunakan untuk memudahkan dan memahami konsep pada pembuatan penelitian ini. Topologi jaringan ditunjukan pada topologi fisik dan topologi logika.

a. Topologi Fisik Cloud Open Media Vault, seperti ditunjukan pada gambar 2.

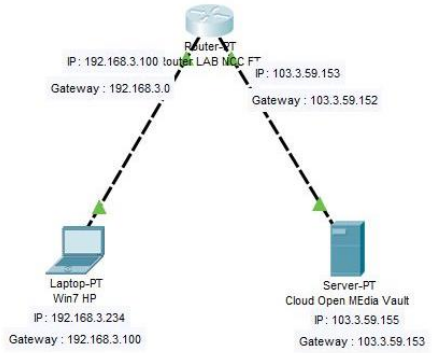
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 2. Topologi Fisik *Cloud Open Media Vault (OMV)*

Berdasarkan Gambar 2 bahwa topologi fisik jaringan menggambarkan desain struktur jaringan *Cloud Open Media Vault* di *Lab Net-centric Computing* Program Studi Teknik Informatika Universitas Ibn Khaldun Bogor.

b. Topologi Logika *Cloud Open Media Vault*, Seperti ditunjukan pada di Gambar 3

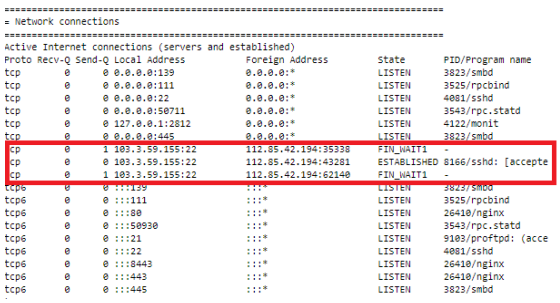


Gambar 3. Topologi Logika *Cloud Open Media Vault (OMV)*

Topologi logika pada *Cloud Open Media Vault* menggambarkan pengalamatan ip address pada struktur jaringan komputer sever *Cloud Open Media Vault*, dimana server *Cloud Open Media Vault*, dengan ip public 103.3.59.155 dan client memiliki ip address 192.168.3.234.

3. Monitoring

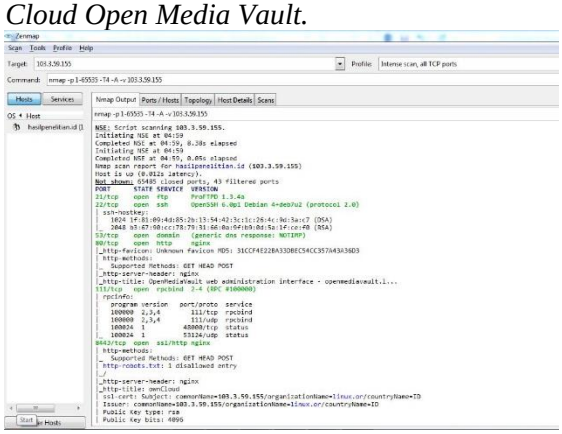
Scan jaringan yang dilakukan di *Operating System NAS Cloud Open Media Vault* menggunakan Netstat, mendapatkan IP yang telah mengakses server NAS *Cloud Open Media Vault.* Gambar berikut menjelaskan mengenai *scan* jaringan yang dilakukan.



```
================================================================================
= Network connections
================================================================================
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      3823/smbd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      3525/rpcbind
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      4081/sshd
tcp        0      0 0.0.0.0:50711           0.0.0.0:*               LISTEN      3543/rpc.statd
tcp        0      0 127.0.0.1:2812          0.0.0.0:*               LISTEN      4122/monit
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      3823/smbd
tcp        0      1 103.3.59.155:22         112.85.42.194:35338     FIN_WAIT1   -
tcp        0      0 103.3.59.155:22         112.85.42.194:43281     ESTABLISHED 8166/sshd: [accepte
tcp        0      1 103.3.59.155:22         112.85.42.194:62140     FIN_WAIT1   -
tcp6       0      0 :::139                  :::*                    LISTEN      3823/smbd
tcp6       0      0 :::111                  :::*                    LISTEN      3525/rpcbind
tcp6       0      0 :::80                   :::*                    LISTEN      26410/nginx
tcp6       0      0 :::50930                :::*                    LISTEN      3543/rpc.statd
tcp6       0      0 :::21                   :::*                    LISTEN      9103/proftpd: (acce
tcp6       0      0 :::22                   :::*                    LISTEN      4081/sshd
tcp6       0      0 :::8443                 :::*                    LISTEN      26410/nginx
tcp6       0      0 :::443                  :::*                    LISTEN      26410/nginx
tcp6       0      0 :::445                  :::*                    LISTEN      3823/smbd
```

Gambar 4. Scan Jaringan di NAS Cloud Open Media Vault (OMV) menggunakan Netstat

Berdasarkan hasil Gambar 4 tampak pada hasil scan Netstat menunjukan bahwa pada Port TCP dengan *Local Address* yaitu 103.3.59.155 IP dari server *Cloud Open Media Vault* telah diakses 3 IP berbeda dalam *Foreign Address* dengan berstatus *FIN_WAIT1* dan *ESTABLISHED. Scan* jaringan menggunakan Nmap menampilkan host-host dan port yang terbuka serta host detail dari port yang di scan, selain itu akan terlihat topologi dari IP target yang di scan dimana IP yang di *scan* adalah 103.3.59.155 *(Server Cloud Open Media Vault).* Gambar berikut ini akan menjelaskan mengenai scan jaringan Server *Cloud Open Media Vault.*



Gambar 5. Scan jaringan *Cloud Open Media Vault* di Nmap

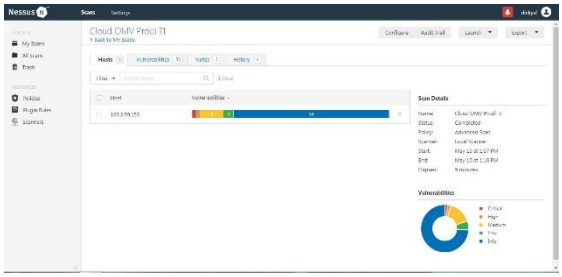
Berdasarkan Gambar 5 tampak pada hasil scan yang dilakukan oleh Nmap menggunakan versi GUI pada sistem operasi windows7 melalui IP yang di scan 103.3.59.155 menunjukan port, state, service dan version dari IP yang di scan. Terdapat beberapa port yang terbuka pada server Cloud Open Media Vault diantaranya port 21, port 22, port 53, port 80, port 111, dan port 8443. Tugas dari port tersebut adalah sebagai berikut :

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

Tabel 1. Hasil Monitoring Scan Port menggunakan Nmap

Port	Fungsi
21	- Terbuka : Port ini digunakan untuk mengkoneksi FTP Server. FTP (*File Transmission Protocol*) untuk dapat saling menghubungkan komputer satu dengan komputer lainnya. - Tertutup : Port ini tidak akan terkoneksi dengan FTP Server dan tidak bisa menggunakan hal berbagi file.
22	- Terbuka : Port ini merupakan port yang digunakan untuk mengaktifkan SSH atau *Secure Shell* pada jaringan komputer dan memberikan kerahasiaan atau integritas dalam pengiriman data - Tertutup : Port ini menyebabkan rentan terhadap intersepsi dan menggunakan penganalisa paket sehingga tidak terjaga kerahasiaan data saat sedang berbagi file.
53	- Terbuka : Port ini adalah port *Domain Name Server* (DNS). Untuk menjawab pertanyaan yang terkait dengan penerjemahan nama domain ke IP *Address*. - Tertutup : Port ini menjadi tidak bisa membaca DNS atau menerjemahkan DNS ke IP *Address*.
80	- Terbuka : Port ini biasanya digunakan untuk *web server*, paling umum digunakan untuk mengakses internet atau bisa disebut HTTP port server - Tertutup : Port ini akan menutup jalan atau akses ke internet
111	- Terbuka : Port ini digunakan untuk menentukan port tempat layanan lain dalam sistem berjalan. Disebut sebagai "*portmapper*". - Tertutup : Port ini tertutup akan berakibat kerentanan keamanan untuk sistem *UNIX*.
8443	- Terbuka : Port default yang digunakan *Tomcat* untuk membuka layanan teks SSL. File konfigurasi default yang digunakan diport adalah 8443. - Tertutup : Port ini tidak akan aman karna tidak adanya layanan teks SSL.

Scan jaringan menggunakan Nessus menampilkan *Vulnerability* dari IP target yang di scan, selain itu setelah hasil dari *vulnerability* tersebut didapat maka Nessus akan menampilkan detail *vulnerability* dari IP yang di scan beserta solusi untuk mengatasi *vulnerability* tersebut. Dalam analisis IP yang di scan adalah 103.3.59.155. gambar berikut akan menjelaskan mengenai scan jaringan pada server *Cloud Open Media Vault* menggunakan Nessus.



Gambar 6. Vulnerability pada server *Cloud Open Media Vault*

Dari hasil scan IP 103.3.59.155 yang dilakukan Nessus didapatkan *vulnerability*, pada *icon* yang diwarnai terdapat keterangan dari setiap informasi, *icon* warna merah menunjukan *Critical*, *icon* warna *orange* menunjukan *High*, *icon* warna kuning menunjukan *Medium*, *icon* warna biru menunjukan *Info*. Selain itu didapat juga informasi berupa deskripsi data yang diolah dalam sebuah *table* untuk mempermudah dalam menganalisa hasil dari pengolahan data. Berikut adalah data *vulnerability* dari hasil *scan* menggunakan Nessus berdasarkan tingkatan kategori kerentanan.

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

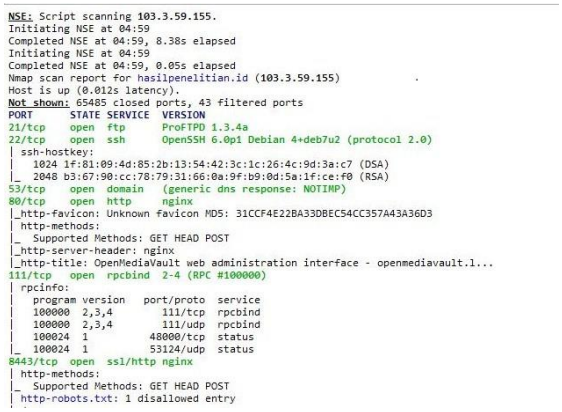
Tabel 2. Tabel alert founds Nessus berdasarkan kategori kerentanan

No	Kategori	Tampilan
1.	Critical	- Deteksi Versi Sistem Operasi Unix yang tidak didukung
2.	High	- Modul otentikasi PostgreSQL (mod_sql) untuk parameter nama pengguna ProFTPD SQL Injection
3.	Medium	- *SSL Certificate Cannot Be Trusted* - *DNS Server Cache Snooping Remote Information Disclosure* - *SSH Weak Alghoritms Supported* - *DNS Server Recursive Wuery Cache Poisoning Weakness* - *mDNS Detection (Remote Network*)
4.	Info	- *Nessus SYN Scanner* - *DNS Server Detection* - *Service Detection* - *RPC Service Enumeration* - *TLS Version 1.0 Protocol Detection* - *Backported Security patch Detection (FTP)* - *ICMP Timestamp Request Remote Date Disclosure* - *Inconsistent Hostname and IP Address* - *TCP/IP Timestamp Supported* - *Web Server robots.txt Information Disclosure*

4. Analisis

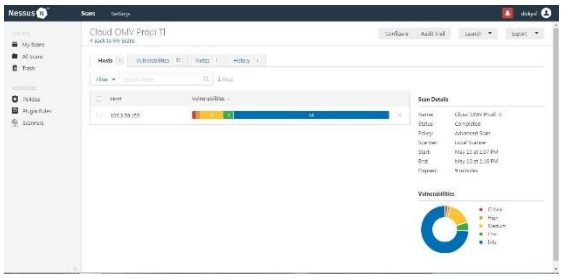
Analisis keamanan *Vulnerability* pada server *Cloud Open Media Vault* memiliki beberapa tahapan, tahap awal pada analisis yang dilakukan adalah mengumpulkan semua data yang dibutuhkan dalam proses analisis *Vulnerability*. Hasil *scan* yang dilakukan Nessus menghasilkan sebuah *output* berupa *Vulnerability* dari IP yang di *scan* Nessus, hasil *scan* tersebut menampilkan lima kategori Vulnerability.

a. Pengujian keamanan *vulnerability* dengan *tool* Nmap



Gambar 7. Hasil pengujian IP Server *Cloud Open Media Vault* Menggunakan Nmap

b. Pengujian keamanan *vulnerability* dengan *tool* Nessus



Gambar 8. Hasil pengujian scan IP *Cloud Open Media Vault* menggunakan Nessus

5. Rekomendasi

Maka tahap ini menjelaskan bagaimana solusi yang disarankan untuk mengatasi masalah *vulnerability* dari data yang sudah didapat, untuk solusi dari IP target *Cloud Open Media Vault* didapatkan dari setiap kategori, mulai dari *critical*, *high*, *medium* dan *info*.

Tabel 3. Kategori *Critical* dari hasil *scan* IP target

Vulnerability	Kategori	Solusi	Port
Unix Operating System Unsupported Version Detection	*Critical*	Tingkatkan ke versi sistem operasi Unix yang saat ini didukung	-

Kategori *High* yang didapat dari hasil scan IP target *Cloud Open Media Vault*, menunjukan bahwa terdapat kerentanan yang masuk dalam kategori *High*, dimana jika tidak ada tindak lanjut dari pengelola server, kemungkinan kerentanan yang ada tersebut akan menjadi *critical*.

Tabel 4. Kategori *High* dari hasil *Scan* IP target

Vulnerability	Kategori	Solusi	Port
PostgreSQL Authentication Module (mod_sql)	*High*	Jika server jarak jauh adalah ProFTPd, tingkatkan ke ProFTPD 1.2.10.	21

Kategori *Medium* yang didapat dari hasil *scan* IP target *Cloud Open Media Vault*, menunjukan bahwa terdapat kerentanan yang masuk dalam kategori *medium*, dimana jika tidak ada tindak lanjut dari pengelola server, bedar kemungkinan kerentanan yang ada tersebut akan menjadi *high* atau bahkan *critical.*

Tabel 5. Kategori *medium* dari hasil scan IP target

Vulnerability	Kategori	Solusi	Port
SSL Certificate Cannot Be Trusted	*Medium*	Beli atau hasilkan sertifikat yang sesuai untuk layanan ini.	8443
DNS Server Cache Snooping Remote Information Disclosure	*Medium*	Hubungi vendor perangkat lunak DNS untuk perbaikan.	53
SSH Weak Algorithms Supported	*Medium*	Hubungi vendor atau lihat dokumentasi produk untuk menghapus cipher yang lemah.	22
DNS Server Recursive Wuery Cache Poisoning Weakness	*Medium*	Batasi permintaan rekursif ke host yang harus menggunakan srver nama ini (seperti LAN yang terhubung dengannya.	53
mDNS Detection (Remote Network)	*Medium*	Saring lalu lintas masuk ke port UDP 5353, jika diinginkan	5353

Kategori *info* yang didapat dari hasil scan IP target *Cloud Open Media Vault*, menunjukan bahwa terdapat kerentanan yang masuk dalam kategori *info*, dimana kategori ini diberitahukan informasi mengenai kerentanan dari hasil *scan* dan jika tidak ada tindak lanjut dari pengelola server, kemungkinan kerentanan yang ada tersebut akan menjadi *low* atau bahkan *medium.*

Tabel 6. Kategori info dari hasil scan IP target

Vulnerability	Kategori	Solusi	Port
Nessus *SYN Scanner*	*Info*	Lindungi target dengan filter IP	21
DNS Server Detection	*Info*	Nonaktifkan layanan ini jika tidak diperlukan atau batasi akses ke	53

		host internal hanya jika layanan tersedia secara eksternal	
Service Detection	*Info*	-	21
RPC Service Enumeration	*Info*	-	111
TLS Version 1.0 Protocol Detection	*Info*	Aktifkan dukungan untuk TLS 1.1 dan 1.2, dan nonaktifkan dukungan untuk TLS 1.0	8443
ICMP Timestamp Request Remote Date Disclosure	*Info*	Memfilter permintaan stempel waktu ICMP (13), dan stempel waktu ICMP keluar (14)	-
Inconsistent Hostname and IP Address	*Info*	Perbaiki DNS terbalik atau file host	53
TCP/IP Timestamp Supported	*Info*	-	-
Web Server robots.txt Information Disclosure	*Info*	Tinjau konten file robots.txt situs tersebut, gunakan tag META Robots alih-alih antri dalam file robots.txt, dan sesuaikan kontrol akses server web untuk membatasi akses ka materi sensitif.	8443

SIMPULAN DAN SARAN

SIMPULAN

Berdasarkan penelitian yang dilakukan, hasil dan bahasan sebelumnya maka dapat ditarik kesimpulan sebagai berikut :

1. Hasil dari analisis dan monitoring didapatkan 6 port yang terbuka diantaranya port 21 *FTP*, Port 22 *SSH*, port 53 *DNS*, Port 80 *HTTP/WEB*, Port 111, Port 8443 dan *Host detail* yang statusnya up dari 65485 port, 43 port yang berstatus *filltered* serta 3 alamat IP yang berbeda mengakses kedalam server melalui Port 21 *FTP*
2. Hasil dari rekomendasi didapatkan solusi sebanyak 13 solusi yang disarankan untuk menyelesaikan masalah 17 *vulnerability*. 4 kategori *vulnerability* berupa 1% *vulnerability* untuk kategori *Critical*, 1% untuk kategori *High*, 5% untuk kategori *Medium*, dan 10% untuk kategori *Info*. Berarti untuk server *Cloud Open Media Vault* mendapatkan kerentanan untuk diretas, karena memiliki celah keamanan sebesar 17%.

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

SARAN

Setelah melakukan penelitian Analisis Keamanan *Vulnerability* pada server *Cloud Open Media Vault* di Fakultas Teknik Universitas Ibn Khaldun Bogor, maka dapat di ambil saran untuk pengembangan yang lebih baik, diantaranya :

1. Untuk penelitian selanjutnya diharapkan dapat mengembangkan perbandingan *Network Scanner* dengan pengujian serangan pada server *Cloud Open Media Vault.*
2. Mengatasi *vulnerability* yang ada pada server *Cloud Open Media Vault* di Fakultas Teknik Universitas Ibn Khaldun, agar *vulnerability* yang ada pada jaringan server tidak lagi pada kategori *Critical* yang sangat memungkinkan bisa merusak sistem yang ada.

DAFTAR PUSTAKA

Babys Yesi Yahanis. Kupang, 2018. Analisis Vulnerable Port Padaa Client Pengguna Publik Wifi. Jurnal Simetris.

Daniel, Ilham. Palembang, 2015. Evaluasi Celah Keamanan Web Server Pada Lpse Kota Palembang.

Didi Juardi, 2017. Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. Syntax. Inform. Vol. 6no. 1, 1–19.

Maharani, Bandung 2017. Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Matriks.

Marti Widya Sari. Analisis Keamanan Jaringan Wireless Local Area Network (Wlan) Menggunakan Metode Wardriving Di Fakultas Teknik Universitas Pgri Yogyakarta

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

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

Ritzkal, 2019. Keamanan Jaringan Cyber. Uika Press, Bogor.