VULNERABILITY ASSESSMENT SISTEM MANAJEMEN KEAMANAN INFORMASI e-GOVERNMENT PEMERINTAH KOTA DENPASAR

I Gede Putu Krisna Juliharta[1)],Ni Luh Putu Ning Septyarini Puja Astawa[2)], Komang Tri Werthi[3)]
Sistem Informasi[1,2)], Sistem Informasi Akuntansi[3)]
STMIK Primakara, Denpasar Selatan, Bali
krisna@primakara.ac.id, ningseptyarini28@gmail.com, komang.triwerthi@gmail.com

ABSTRACT

Vulnerability Assessment (VA) is one way of measuring system and network security. VA is one part of the prevention and control of information technology (IT) control, Denpasar City Government has many applications to the community that are integrated within the scope of e-government. In this study, vulnerability assessment was carried out on application service systems,amatya, and esewakadharma, the results obtained were 23 vulnerabilities for application systems, 37 vulnerabilities for theamatya system, and 34 vulnerabilities for esewakadharma services.
keywords: *Vulnerability assessment*, server , *information technology*

ABSTRAK

Vulnerability Assessment (VA) adalah salah satu cara pengukuran terhadap keamanan sistem dan jaringan. VA merupakan salah satu bagian pengendalian *preventif* dalam rangkaian pengendalian teknologi informasi (TI), di Pemerintah Kota Denpasar ada banyak aplikasi layanan kepada masyarakat yang terintegrasi dalam lingkup e-government. Dalam penelitian ini dilakukan pengukuran *vulnerability assessment* terhadap sistem layanan aplikasi, amatya, dan esewakadharma, hasil didapatkan 23 vulnerability untuk system aplikasi, 37 vulnerability untuk system amatya, dan 34 vulnerability untuk layanan esewakadharma.
Kata Kunci : *Vulnerability assessment*, server, teknologi informasi.

PENDAHULUAN

Vulnerability Assessment (VA) adalah salah satu cara pengukuran terhadap keamanan sistem. VA merupakan salah satu bagian pengendalian *preventif* dalam keseluruhan rangkaian pengendalian teknologi informasi (TI), disamping berbagai metode pengendalian terhadap keamanan yang lain seperti detektif dengan IDS (*Intrusion Detection System*), atau pencegahan dengan firewall dan antivirus. VA diharapkan dapat menjadi tolak ukur dalam proses pengawasan dan pengendalian akan keamanan informasi dalam organisasi.

Pada prakteknya di industri, permintaan akan VA umumnya datang setelah terjadi proses pemeriksaan TI yang kemudian berlanjut pada pemeriksaan keamanan data. VA seringkali merupakan tindak lanjut dari proses perencanaan strategi keamanan informasi, kelengkapan standar industri hingga faktor regulasi. Di Indonesia sebagian besar permintaan VA datang dari industri yang memiliki ketergantungan tinggi pada TI seperti industri perbankan atau telekomunikasi atau pun dari industri yang sudah matang dalam pengelolaan TI-nya mereka sangat memahami bahwasanya keamanan adalah hal yang penting dalam menjaga kepercayaan pelanggan.

LANDASAN TEORI

1. Keamanan sistem informasi

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem.

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan *(cheating)* atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti

fisik[3]. Menurut John D. Howard dalam bukunya "*An Analysis of Security Incidents on The Internet"* menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab [3].

2. Aspek Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan[6]. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1. *Confidentiality* (Kerahasiaan) Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan [3].
2. *Integrity* (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang *(authorized),* menjaga keakuratan dan keutuhan informasi serta metode pro-sesnya untuk menjamin aspek integrity ini [3].
3. *Availability* (Ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memasti- kan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bila- mana diperlukan) [3].

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privasi, integrity, authentication dan availabilit*[7]. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce,* yaitu *access control* dan *non-repudiation* [7].

3. Faktor Keamanan Jaringan

Keamanan jaringan merupakan aktivitas yang dilakukan untuk melindungi jaringan yang ada. Menggunakan penerapan teknologi dan proses pengamanan untuk melindungi jaringan dari ancaman yang berasal dari luar maupun dalam jaringan. Keamanan jaringan melibatkan seluruh pihak dalam organisasi ataupun institusi untuk ikut bersama melindungi isi dan informasi dari institusi tersebut. Keamanan jaringan yang efektif adalah membagi factor factor jaringan dan jenis ancamannya, untuk bisa melakukan penanggualangkan atau bahkan menghilangkannya dari jaringan yang ada.

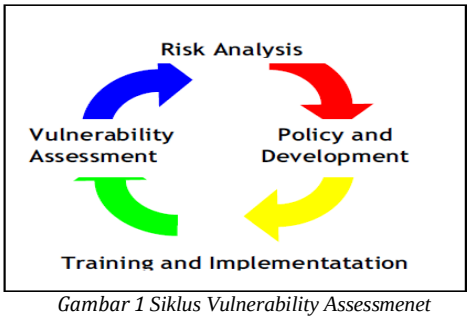
Ada beberapa faktor keamanan jaringan yaitu :

1. *Vulnerability*
   Vulnerabilities merupakan kelemahan atau kerentaan yang dapat menyebabkan para penyerang mendapatkan akses illegal untuk masuk kedalam suatu system. *Vulnerability* merupakan persimpangan dari tiga elemen yaitu : aliran system (gap/weakness), penyerang mengakses sistem yang cacat, dan penyerang mempunyai kemampuan untuk menyerang akses yang cacat tersebut (Hemantan, 2010). Ada empat faktor utama penyebab ancaman terhadap keamanan jaringan yaitu, *technology weakness, configuration weakness*, *security policy weakness*, *dan human error*.
2. *Threat*
   Thereat merukanan ancaman yang datang dari seseorang yang tertaring dan memiliki kemampuan untuk mengambil keuntungan dari kelemahan keamanan. Ada banyak peralatan, *script,* dan program yang dapat digunakan untuk menyerang jaringan dan perangkatnya. Secara umum, peralatan komputer yang sering menjadi target adalah *endpoints*, seperti server dan komputer desktop. Ancaman ada berbagai macam jenis diantaranya ancaman terhadap infrastuktur fisik yang meliputi ; ancaman terhadap perangkat keras, ancaman terhadap lingkungan, ancaman kelistrikan, dan ancaman pada saat perawatan. Ancaman yang berasal dari jaringan, yang bisa berasal dari dalam maupun dari luar jaringan.
3. *Attacks*
   Attacks atau serangan merupakan seseorang yang dengan sengaja melakukan aktivitas yang menyebabkan sesuatu yang buruk terjadi terhadap suatu sistem. Ada beberapa metode dalam melakukan serangan diataranya ; *network enumeration* (mencari informasi tentang jaringan), *vulnerabilities analysis* (menganalisa kelemahan), dan *exploitation*.
4. *Vulnerability Assessment*

Vulnerability Assessment (VA) merupakan bagian dari proses *risk assessment* seperti digambarkan dalam sebuah lingkaran siklus antara (Anjar, 2006):

- Analisa Resiko (*Risk analysis*)
- *Policy development*

- *Training & implementation*
- *Vulnerability assessment & penetration testing*



Gambar 1 Siklus Vulnerability Assessmenet

Sebagai sebuah proses yang terus menerus dan membentuk suatu kerangka siklus maka hasil dari VA akan digunakan untuk mengimplementasikan strategi keamanan informasi di perusahaan tersebut. Begitupun strategi keamanan yang telah dibuat harus tetap dievaluasi Sebagai suatu proses VA sebaiknya dilakukan secara kontinu dan terus menerus, umumnya VA ini dilakukan :

Saat implementasi program baru, pada implementasi program baru biasanya departemen TI akan membuka akses ke mesin *production* oleh pihak ketiga seperti *programmer*, *vendor* ataupun *consultant*. Implementasi ini dimungkinkan menyebabkan terbukanya lubang kerawanan baru yang belum ada.

Secara periodik dalam waktu-waktu tertentu, digunakan untuk memantau apabila ada perubahan yang dilakukan oleh pengguna akhir. VA secara periodik inilah yang dinilai sebagai cara yang paling baik. Proses VA sendiri memiliki berbagai tingkatan, sehingga perusahaan dapat memilih tingkatan mana yang akan digunakan dalam pengukurannya. Tingkatan ini dapat di sesuaikan dengan kondisi di masing-masing tempat.

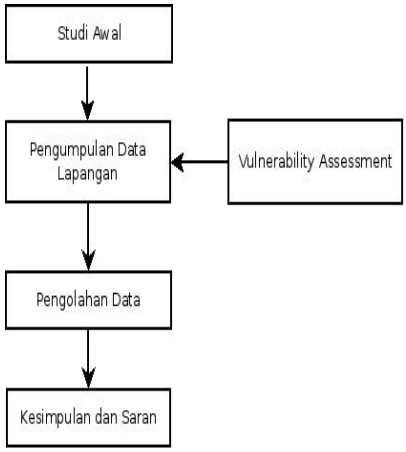
Tingkat I: Pengukuran peraturan dan kebijakan (*Policy assessment*) Pengukuran ini meliputi peraturan, kebijaksanaan, standar operasi di *client* dalam cakupan keamanan informasi.

Tingkat II: Evaluasi Jaringan Pengukuran ini meliputi kinerja jaringan, keamanan jaringan hingga ancaman-ancaman terhadap jaringan kerja. Pengukuran jenis ini memerlukan alat bantu seperti *scanning* atau *data capture*. Evaluasi jaringan ini bertujuan untuk mendapatkan informasi mengenai kondisi sebenarnya yang terjadi dilapangan, bagaimana tingkat kesadaran akan keamanan informasi yang sudah diterapkan selama ini.

Tingkat III: Test penetrasi (*Penetration Test*) *Penetration test* sebenarnya menggunakan prinsip yang sama dengan network evaluation dimana pembedanya bahwa *penetration test* dilakukan dalam kondisi gelap, tanpa mengetahui konfigurasi dan kondisi sebenarnya seperti apa.

METODE PENELITIAN

Vulnerability assessment dilakukan selama 30 hari. Langkah *assessment* (Gambar 2.) adalah dengan cara melakukan analisa ke mesin *Domain Name Server*, *mail server* dan *e-krs server* yang menggunakan jaringan di STMIK Primakara.



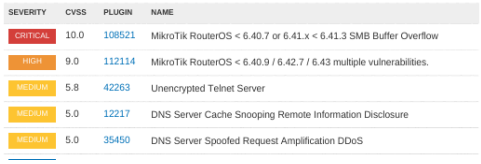
Gambar 2 Perancangan penelitian

Gambar 2. Menjelaskan mengenai perancangan penelitian yang meliputi :

1. Studi awal yang memiliki tujuan memahami dan mencari referensi dalam pelaksanaan penelitian vulnerability assessment
2. Pengumpulan data lapangan merupakan tahapan untuk melakukan proses VA dengan melakukan penilaian keamanan secara obyektif menggunakan *tools* yang diperuntukan untuk mengecek vulnerability pada sistem.
3. Hasil dari pengumpulan data adalah proses pengolahan data dan membuatnya menjadi laporan dan tulisan ilmiah serta memberikan kesimpulan dan saran

HASIL DAN PEMBAHASAN

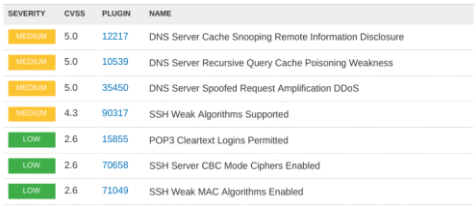
Berdasarkan hasil *vulnerability assessment* yang dilaksanakan pada empat sistem aplikasi Kota Denpasar, didapatkan hasil sebagai berikut :



SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	108521	MikroTik RouterOS < 6.40.7 or 6.41.x < 6.41.3 SMB Buffer Overflow
HIGH	9.0	112114	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	35450	DNS Server Spoofed Request Amplification DDoS

Gambar 3 Hasil Assessment Sistem Aplikasi Denpasar

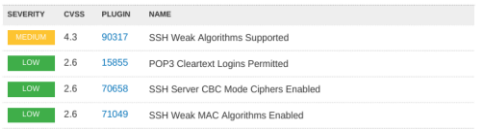
Gambar 3 untuk system aplikasi Denpasar, dari 23 vulnerability, terdapat 1 vulnerability level critical, 1 vulnerability level high dan 3 *vulnerability* level medium. Namun apabila dilihat lebih detail, *vulnerability critical* dan high bukan asli dari servernya, namun dari router Mikrotik yang kemungkinan besar berada di atas server, sehingga pada saat dilakukan scanning, router juga terkena scan.



SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	10539	DNS Server Recursive Query Cache Poisoning Weakness
MEDIUM	5.0	35450	DNS Server Spoofed Request Amplification DDoS
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	15855	POP3 Cleartext Logins Permitted
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Gambar 4 Hasil assessment sistem aplikasi Amatya

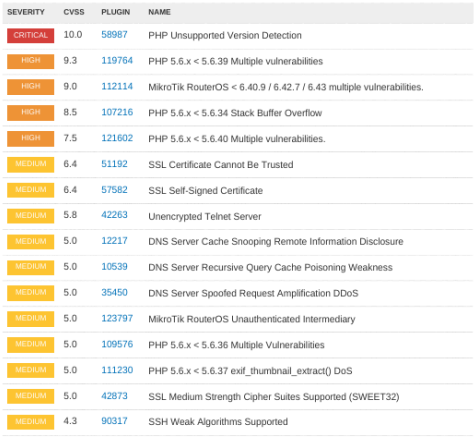
Gambar 4. Pada aplikasi amatya Dari 37 *vulnerability*, terdapat 4 *vulnerability* level medium dan 3 *vulnerability* level low. Hal ini dapat menunjukkan bahwa untuk sisi server, tidak ada masalah yang krusial mengenai keamanan server.



SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	15855	POP3 Cleartext Logins Permitted
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

Gambar 5 aplikasi esewakadharma

Gambar 5. Aplikasi esewakadharma memiliki 34 *vulnerability*, terdapat vulnerability 1 medium dan 3 Low. Namun apabila dilihat lebih detail, *vulnerability* medium dikarenakan pemilihan algoritma kriptografi untuk mengamankan SSH kurang tepat.



SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	9.0	112114	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.
HIGH	8.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	10539	DNS Server Recursive Query Cache Poisoning Weakness
MEDIUM	5.0	35450	DNS Server Spoofed Request Amplification DDoS
MEDIUM	5.0	123797	MikroTik RouterOS Unauthenticated Intermediary
MEDIUM	5.0	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Gambar 6 sistem aplikasi Bursa kerja

Gambar 6. Dalam aplikasi bursa kerja ada 61 *vulnerability*, terdapat 1 *vulnerability* level critical, 4 *vulnerability* level high, 11 *vulnerability* level medium, dan 3 *vulnerability* level low. *Vulnerability* critical dan high berkaitan dengan versi aplikasi PHP yang digunakan dalam aplikasi web bursa kerja.

SIMPULAN

Dalam penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa untuk proses manajemen *software* atau aplikasi belum dilakukan dengan baik hal tersebut dapat dilihat dari :

Aplikasi yang digunakan pada mesin server sudah kadarluarsa dan hingga saat ini belum dilakukan proses *update*.

Untuk mesin *router diperlukan juga pengelelolaan untuk memastikan router aman dalam proses operasionalnya*

vulnerability assessment baru dilakukan pada tiga mesin yang digunakan oleh public, kedepannya perlu lebih banyak lagi aplikasi di e-government Kota Denpasar yang diukur dengan vulnerability assessment

Dalam *proses vulnerability assessment* belum dilakukan perhitungan untuk dampak dari kerentanan yang ada. Untuk penelitian selanjutnya dapat dilakukan pengukuruan *business impact analysis.*

DAFTAR PUSTAKA

[1] Agung Nugroho (2009), "*Studi Kasus Celah Keamanan pada Jaringan Nirkael yang menerapkan WEP (Wired Equivalent Privacy*)",Yogyakarta, STMIK AMIKOM

[2] Andreas Hadiyono, Sutresna Wati, I. Wayan Simri Wicaksana. (2008) "*Analisa Log Router Untuk Meningkatkan Keamanan Jaringan*", Jakarta, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen.

[3] Anjar Priandoyo, 2006, "Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi". Jurnal Sistem Informasi Vol. 1 No. 2September. Jakarta Universitas Maranatha.

[4] Chris McNab.2007."*Network Security Assessment : know Your Network"*. USA.O'Reilly

[5] Faturachman Husein, "Implementasi Indeks KAMI di Universitas Sam Ratulangi" , E-Journal Teknik Informatika Vol. 12 No. 1 (2017) ISSN: 2301-8364

[6] I Gede Putu Krisna Juliharta, "Investigasi Keamanan Aplikasi Teknologi Informasi dengan Teknik Packet Sniffing", Seminar Nasional Informatika Vol.1 No.2, Universitas Pembangunan Nasional "Veteran" Yogyakarta, 2016.

[7] Insecure.org. 2009. "Free Security Scanner For Network Exploration & Security Audits" diakses pada tanggal 20 oktober 2018