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

Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi

Kotim Subandi[1]*,Victor Ilyas Sugara
*Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pakuan ,Jl. Pakuan, RT.02/RW.06, Tegallega,Kecamatan Bogor Tengah, Kota Bogor, Jawa Barat 16129
**Corresponding Author* : kotim.subandi@unpak.ac.id

Abstrak

Semenjak terjadi Pandemi covid-19 Perusahaan yang berak dibidang retail sempat mengalami keterpurukan dampak dari peraturan pemerintan seperti PSBB(Peraturan Sosial berskala Besar)sehingga seluru aktifitas dilakukan dari rumah atau *Work From Home* (WFH). Untuk menunjang kegiatan dari perusahaan/instansi yang mempunyai berbagai macam sistem informasi dalam menjalankan kegiatan usaha dan operasionalnya. Sever ini menjadi salah satu yang paling penting di Perusahaan Retail. Pembukaan beberapa akses dari jaringan umum (internet) menuju ke *Local Area Network* (LAN). Keamanan jaringan LAN yang diakses dari jaringan umum biasanya merupakan masalah dari seorang administrator. Seringkali masalah keamanan baik jaringan dan seluruh sistem aplikasi maupun *web server* terabaikan hanya untuk memenuhi kegiatan operational berjalan lancar pengamanan baru disadari setelah terjadi bencana. Tanpa adanya pengamanan jaringan dan sistem aplikasi yang baik, penerapan teknologi secangih apapun akan sangat membahayakan perusahaan ,institusi atau organisasi itu sendiri. Maka dibutuhkan Analisa keamanan seluruh aktifitas ke dalam LAN, server ,perangkat lain untuk mencegah terjadinya Mitigasi serta untuk lebih mewaspadai keamanan server dari serangan Vulnarebilities. Berdasarkan latar belakang permasalahan yang ada, maka dibutuhkan analisa dengan menggunakan metode *penetration testing*. Sebagai bahan pendukung penelitian ini juga menggunakan pedoman dari modul CEH *(Certified Ethical Hacker)* dan web resmi Acunetix. Pengujian penelitian ini adalah bertujuan untuk menemukan kelemahan server milik perusahaan/instasi yang ada. Permasalahan yang ditemukan setelah dilakukan pengujian, antara lain: kelemahan berhasil ditemukan cukup banyak dimana setiap kelemahan ini mempunyai penanganan yang berbeda, *port* yang seharusnya diblokir tapi dibuka secara bebas, dan *IP public* yang kurang penting sebaiknya ditutup aksesnya. Solusi yang disampaikan untuk mengangulangi permasalahan tersebut antara lain: Pemakaian standar Acunetix ini dapat dipertahankan dan dilanjutkan, pengujian jauh lebih baik bila dilakukan lebih dari 2 kali, melakukan *upgrade* SNMP yang lebih baru secara berkala, melakukan filter port yang rentan, meningkatkan tingkat keamanan server, migrasi antivirus yang berkualitas, upgrade sistem operasi yang sudah expired

Kata kunci: Vulnarabilities,Mitigation ,Pentration Testing,Pandemic,WFH

Abstract

Since the Covid-19 Pandemic occurred, companies that operate in the retail sector have experienced a downturn in the impact of government regulations such as the PSBB (Large-scale Social Regulations) so that all activities are carried out from home or Work From Home (WFH). To support the activities of companies / agencies that have various kinds of information systems in carrying out business activities and operations. This sever is one of the most important in a Retail Company. Opening some access from the public network (internet) to the LAN network security accessed from the public network is usually a problem of an administrator. Often times, security issues both for the network and the entire application system as well as the web server are neglected just to fulfill operational activities to run smoothly.

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

Security is only realized after a disaster occurs. Without good network security and application systems, the application of any technology will seriously endanger the company, institution or organization itself. So it takes a security analysis of all activities on the LAN, servers, other devices to prevent mitigation and to be more aware of server security from Vulnerability attacks. Based on the background of the existing problems, it is necessary to analyze using the penetration testing method. As supporting material for this research, we also use the guidelines from the CEH (Certified Ethical Hacker) module and the official website of Acunetix. This research test is aimed at finding weaknesses of the company / existing server. The problems that were found after testing included: quite a lot of weaknesses were found where each of these weaknesses had different handling, ports that should be blocked but opened freely, and public IPs that were less important should have their access closed. The solutions presented to overcome these problems include: The use of this Acunetix standard can be maintained and continued, testing is much better if it is done more than 2 times, regularly upgrades to newer SNMPs, filtering vulnerable ports, increasing the level of server security, quality antivirus migration, upgrade operating systems that have expired

Keywords Vulnarabilities,Mitigation ,Pentration Testing,Pandemic,WFH

PENDAHULUAN

Untuk menunjang kegiatan operasional perusahaan yang berbasis teknologi informasi sangat membutuhkan keberadaaan jaringan komputer. Perusahaan-perusahaan yang berkembang saat ini sudah banyak yang menggunakan server. Maka, suatu perusahaan haruslah memperhatikan faktor keamanan dalam infrastruktur jaringan baik yang terhubung secara LAN maupun WAN . Perusahaan membuat investasi pada sistem keamanan jaringan agar seluruh aset terlindungi dari berbagai ancaman kejahatan secara *virtual* seperti *hacker* atau bahaya virus.Keamanan jaringan didalam komunikasi wajib diperlukan untuk mampu memberikan layanan yang aman saat pengiriman data atau pesan secara terus menerus bagi para *use*r atau *client* .

Dalam upaya mengurangi kerugian yang diakibatkan oleh para serangan dari hacker atau virus yang berdampak Migitasi, maka kebijakan yang harus dikembangkan adalah melakukan analisa dan evaluasi terhadap keamanan server. Internet sudah menjadi bagian dari kehidupan manusia dimasa seperti saat ini (pandemi) untuk menunjang kegiatan *Work From Home* (WFH), dimana sebuah initernet menjadi pengubung jaringan umum menuju jaringan *Local Area Network* (LAN) sangat dibutuhkan dikarenakan dapat memebantu akses diinginkan secara mudah, cepat, dan murah.

Perkembangan internet telah meluas fungsinya. Di masa sebelumnya aktifitas kegiatan operasional dilakukan secara statis,atau hanya berada diruang lingkup LAN, setelah masa pandemi terjadi maka seluruh koneksi jaringan haruslah dapat mendukung kegiatan operasioanl yang dilakukan secara daring. Ketika seluruh kegiatan komunikasi dilakukan di ruang lingkup local kerentanan , *vulnerability* relatif kecil, , ketika jumlah user atau pengguna layanan jaringan umum (interner) menuju jaringan berbasis LAN semakin banyak, maka akses pembukaan *port* jaringan menyebabkan kerentanan terhadap serangan dan tindak kehajatan semakin meningkat

Perkembangan teknologi saat ini membawa dampak perubahan yang signifikan dalam proses pembangunan sistem penyedia layanan dalam jaringan umum /internet. Teknologi ini selalu diharapkan mampu menyediakan layanan untuk kemudahan didalam aktifitas *Work From Home*(WFH). Namun dibalik kemudahan itu semua, teknologi ini memiliki permasalahan dari sisi keamanan.

Dengan semakain berkembangnya teknologi dan Internet, menyebabkan lalulintas pergerakan sistem informasi untuk menggunakannya sebagai basis. Ada beberapa sistem yang memang tidak terhubung langsung ke Internet tetapi tetap menggunakan basis web sebagai basis untuk sistem informasinya yang

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

dipasang di jaringan Intranet, hal ini yang perlu diberikan akses secara personal kepada seluruh user/karyawan/penggunakan untuk dapat melakukan pekerjaan secara daring. Maka, keamanan sistem informasi yang berbasis web dan teknologi Internet bergantung kepada kebijakan dan prosedur keamanan sistem web yang diterapkan.

Keamanan jaringan dan server yang diakses oleh pengguna ini menjadi masalah dari seorang administrator jaringan Dengan membuka akses jaringan umum ke jaringan LAN, maka membuka celah kepada orang luar yang tidak memiliki kepentingan. Apabila server dan jaringan local terhubung ke Internet dan memang akses web server disiapkan untuk publik, maka keamanan jaringan harus ditingkatkan karena hal ini membuka pintu akses ke seluruh penggunakan layanan internet tanpa terkecuali

Masalah keamanan jaringan seringkali terabaikan, pengamanan sistem informasi baru disadari setelah terjadi bencana (mitigasi). Apabila pengamanan sistem informasi dan jaringan kurang baik, penerapan teknologi secanggih apapun tetap sangat membahayakan perusahaan atau organisasi itu sendiri.

Vulnerability adalah suatu kelemahan yang menjadi acaman nilai *integrity*, *confidentiality*, dan *availability* dari suatu asset. *Penetration testing* atau yang lebih dikenal dengan sebutan pentest adalah salah satu metode yang dapat digunakan untuk melakukan analisa dan evaluasi terhadap suatu jaringan komputer. Selain itu,*vulnerability* juga perlu dilakukan untuk prosedur mitigasi.

Perusahaan yang bergerak dibidang retail saat ini bertumbuh semakin pesat dan mempunyai berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya . Beberapa server yang paling akses adalah mailserver (retail.co.id) dan beberapa server lain, seperti SAP, Intranet, proint untuk kepentingan kegiatan secara daring *work form home* (WFH). Mailserver adalah salah satu yang sering diakses oleh karyawan untuk berkomunikasi.

Maka dari itu, dengan melakukan analisa *vulnerabilities*, hal ini diharapkan administrator jaringan dapat lebih waspada terhadap kelemahan dan kerentanan yang ada server. Supaya, administrator jaringan dapat melakukan pemeliharaan secara berkala untuk mencegah hal serupa terjadi kembali.

Keamanan jaringan ini mempunyai tujuan agar pemilik sistem informasi dan jaringan dapat menjaga sistem informasinya tidak gamapang ditembus atau disusupi oleh orang yang tidak memiliki keabsahan, yang suatu saat nanti dapat memimbulkan mitgasi didalam sistem. Adapun jenis dn tipe dari penyusup ini dapat berupa: *malware, the curious, the malicious, the high-profile intruder, dan the competition*. Berbagai segi keamanan jaringan yang ada antara lain: *confidentiality, integrity, availability, nonrepudiation, authentication, dan accountability*.

METODE

Analisa Permasalahan

Melalukan *scanning* terhadap server-server yang diakses oleh seluruh karyawan dari layanan jaringan umum. Hal ini dikarenakan server tersebut merupakan salah satu akses pertukaran data serta penyimapan seluruh informasi terkait dengan kepentingan bisnis. Scanning ini dilakukan dengan tujuan untuk mengetahui *vulnerability* yang ada didalam server. Dari beberapa *IP address server* yang di*scanning*, nantinya akan diketahui IP address yang memiliki *hostname* dan yang tidak memiliki *hostname.* Setelah itu di-*scanning* lagi dengan *tools* yang lain untuk melihat kelemahan serta kerentanan didalam sever. Hasil dari scanning ini nantinya akan menjadai evaluasi untuk analisa bagi tim pengelola *infrastructure, Network security* dan *data centre* untuk lebih peduli dan sigap lagi terhadap kelemahan yang ada.

Analisa Kebutuhan

Yang menjadi alasan perlu dilakukan *penetration testing* didalam penelitian ini adalah

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

untuk menemukan kerentanan serta kelemahan dan *vulnerabilities system*, sebelum kerentanan dan kelemahan tersebut dieksploitasi oleh para penyerang seperti hacker yang akan memberikan dampak tidak baik bahkan mitigasi bagi keamanan server didalam perusahaan. Selain itu, penetration testing ini dilakukan sebagai gambaran dan analisa bahwa manajemen terhadap sistem keamanan server, kemanan jaringan, keamanan sistem informasi merupakan suatu hal penting yang harus diterapkan sebagai prosedur, serta melakukan uji coba terhadap mekanisme alur keamanan sistem, dan melakukan evaluasi apakah sistem yang digunakan saat ini sudah memenuhi standar keamanan sistem informasi sudah yang sesuai ISO27001.

Analisa Perangkat Lunak *(Software)*

Dalam penelitian ini, program aplikasi yang akan digunakan adalah program yang sesuai dengan metode dalam setiap *step penetration testing*. Pada Tabel 1 dapat dilihat *software* yang digunakan untuk penetration testing dalam pengerjaan penelitian ini.

Tabel 1. *Software* yang digunakan dalam Penelitian

No	*STEP(METODE)*	*TOOLS*
1	*Foot printing*	*Angry IP Scanner*
2	*Scanning Fingerprinting*	*Acunetix Web Vulnerability Scanner 9.5*
3	*Enumeration*	*Softperfect network scanner*

Komponen Pendukung Penelitian

Berikut beberapa komponen yang diperlukan untuk mendukung kinerja penelitian ini. Beberapa komponen tersebut antara lain:

Perusahaan /Organisasi

Perusahaan/organisasi yang dianalisa dalam penelitian ini adalah Perusahaan Retail yang ber-kantor pusat di Gedung SSC Jakarta Pusat

Wi-Fi

Wi-Fi berada di Gedung SSC lantai 38 kantor pusat

Target Analisa

Target *penetration testing* dan analisa untuk penelitian ini adalah sebanyak 10 unit server

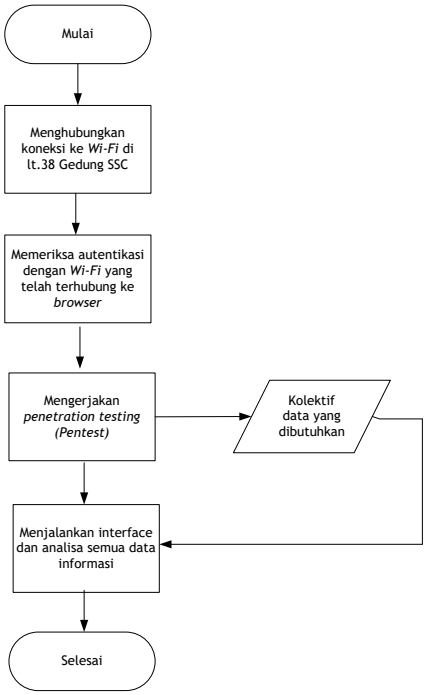
Range IP Address

Dalam metode pengumpulan data (*penetration testing*) enggunakan *range IP address*. Berikut *range IP Address server* : 192.168.xxx.33 – 192.168.xxx.254 secara random

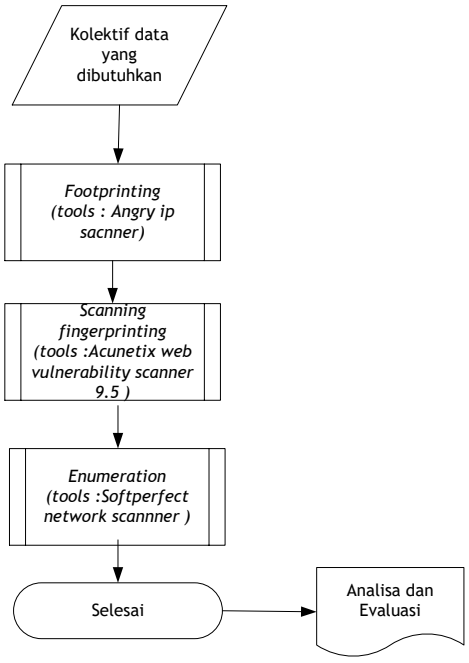
Penetration Testing

Pada Gambar 1 dapat dilihat *Flowchart* saat melakukan penelitian ini menggunakan metode penetration testing. Langkah awal penelitian ini dimulai dari menghubungkan koneksi dengan internet sampai melakukan *interface* kelemahan. Selanjutnya hal-hal apa saja yang dilakukan saat penetration testing dapat dilihat pada Gambar 2.

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



Gambar 1. Flowchart pengerjaan penelitian



Gambar 2. Proses Eksekusi *Penetration testing*

Footprinting

Adalah suatu proses yang digunakan mengungkap dan mengumpulkan data informasi sebanyak mungkin mengenai target berada didalam jaringan. Footprinting mempunyai tujuan antara lain mengumpulkan informasi mengenai network target, sistem informasi target, dan informasi suatu perusahaan /organisasi. [1] Metode teknik ini, menggunakan *tools Angry IP Address*.

Scanning Fingerprinting

Scanning fingerprinting merupakan salah satu prosedur yang berguna untuk mengidentifikasi host, port, dan services dalam infrastruktur jaringan. Selain itu, scanning fingerprinting merupakan tanda awal munculnya sebuah serangan dari hacker (*pre-attack*). Melalui *scanning fingerprinting* ini, *hacker* akan mencari berbagai celah untuk disusupi masuk ke dalam jaringan dengan tujuan untuk mengambil alih komputer korban. [2] Pada penelitian ini, dari jenis *scanning* yang ada, *vulnerability scanning* adalah jenis yang akan digunakan untuk analisa keamanan dari jaringan server.

Enumeration

Enumeration merupakan suatu proses penyusupan melalui celah atau lubang yang rentan untuk mendapatkan *usernames*, nama mesin, *resources, shares, dan services* dari sebuah sistem informasi. [3]

SNMP

SNMP *(Simple Network Management Protocol*) menjadi salah satu metode yang digunakan pada langkah *enumeration*. *Tools* yang digunakan pada teknik ini adalah *SoftPerfect network scanner*

HASIL DAN PEMBAHASAN

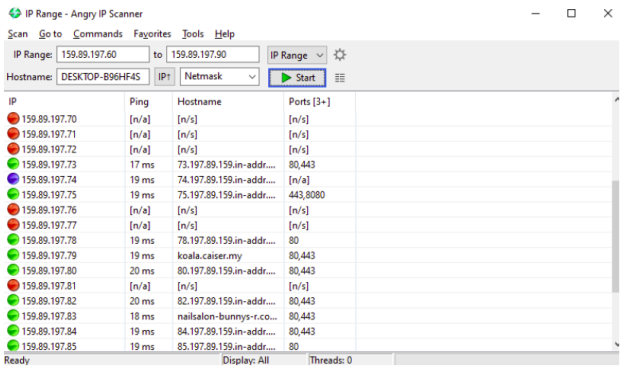
Perang katLunak (*Software*) untuk *Penetration Testing*

Footprinting

Untuk menjalnakan *footprinting* ini tool yang akan digunakan *Angry IP Scanner* karena tool ini mampu menampilkan secara detail *range IP Address*. Dalam *system administrator*, tool ini sangat membantu pekerjaan menjadi lebih cepat dan efisien ketika memonitoring jaringan dari pihak-pihak yang tidak berwenang yang terhubung ke jaringan. Ketika perangkat

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

(*laptop/workstation*) yang dikategorikan mencurigakan yang terhubung dengan jaringan, dapat langsung terditeksi sedini mungkin. Pada Gambar 3 dapat dilihat tampilan tool Angry IP address.

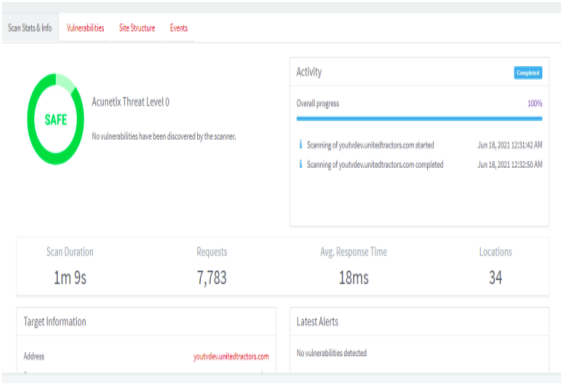


Gambar 3 .*Software tool Angry IP Address*

Hasil dan pembahasan menyajikan penjabaran data hasil penelitian yang dilengkapi dengan tabel dan gambar. Data hasil yang didapatkan dilakukan proses analisis dan dijelaskan secara terperinci sebab akibat dari data hasil yang didapatkan dan mengaitkan dengan sumber rujukan yang relevan.

Scanning Fingerprinting

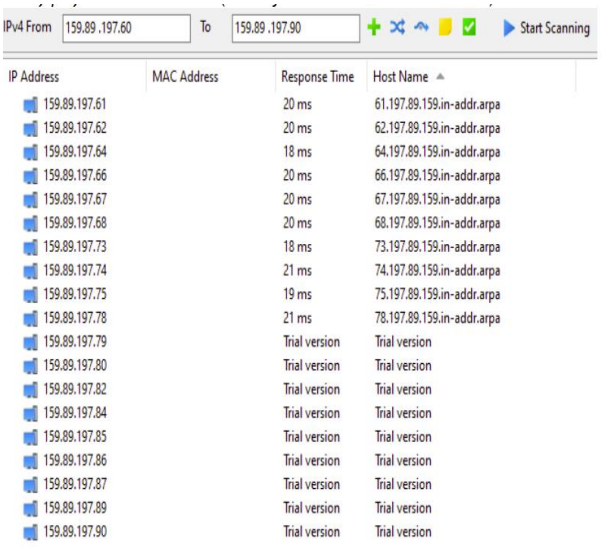
Metode *scanning fingerprinting* ini akan menggunakan *tool Acunetix Web Vulnerability Scanner 9.5*, karena tool ini mampu memberikan informasi secara detail mengenai range IP Address. Seorang administrator harus paham mengenai sistem ini, tool ini akan membantu dan memudahkan dalam menemukan vulnerability yang berada didalam sistem jaringan (*Ip address /hostname*). Tidak hanya menampilkan kelemahan atau celah dari suatu sumber, tetapi tool ini juga memberikan informasi level tingkat kelemahan dari *alerts (vulnerability)* yang akan ditemukan. Pada Gambar 4 berupa tampilan *tool vulnerability scanner (Acunetix Web Vulnerability Scanner 9.5).*



Gambar 4 Tampilan *tool vulnerability scanner* (Acunetix Web Vulnerability Scanner 9.5)

Enumeration

Metode *enumeration* tool yang digunakan adalah *SoftPerfect network scanner* karena tool ini mamapu menampilkan informasi secara detail dari suatu *range IP Address*, termasuk *port* apa saja yang terbuka dari suatu IP Address didalam infrastruktur jaringa, Sebagai seorang tester, akan dapat memonitoring serta mengevaluasi port yang terbuka, apakah port tersebut cocok dengan IP address yang terhubung secara langsung didalam jaringan LAN menuju Server. Pada Gambar 5 dapat akan ditampilkan tool *SoftPerfect network Scanner*.



Gambar 5 Tampilan tool SoftPerfect network Scanner

Hasil Pengujian Perangkat Lunak (*Software*)

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

Setelah *penetration testing* semua data dikumpulkan untuk segera dilakukan tahap (*footprinting, scanning fingerprinting, dan enumeration*) kemudian data tersebut direkap untuk dievaluasi dan analisa terhadap *vulnerability* kemudian memberikan solusi agar tidak menimbulkan mitigasi sistem informasi dan jaringan. Dalam Tabel 1 dapat dilihat hasil uji dengan tool Angry IP Scanner. Hasil ini adalah hasil yang sudah direkap yang hanya mempunyai

Tabel 2. Hasil Scaning Pentest

IP	OS	RESULT
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:TROJ_ROVNIX.PC
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:TROJ_XMLOIT
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:DDOS_DUCAU.A
159.89.xx.xx	Windows 2003 Service Pack 2	detected on port 5555 over TCP
159.89.xx.xx	Windows 2003 Service Pack 2	detected on port 3389 over TCP.#
159.89.xx.xx	Windows 2003 Service Pack 2	QID: 119237 detected on port 5555 over TCP
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:TROJ_ROVNIX.PC
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:TROJ_XMLOIT
159.89.xx.xx	Windows 2003 Service Pack 2	Malware ID:TROJ_ROVNIX.PC

Tabel 2 Summary vulnerability kategori description

No	Keterangan	Vulnerability	Total	level
	Cross Site Scripting (XSS)	jQuery cross site scripting	25	*High*
	SQL Injection	Blind SQL Injection	16	*Medium*
	CSRF (Cross Site Request Forgery) protection	HTML form without CSRF protection	36	*Medium*

Dari semua kelemahan dan kerentanan yang ada, kelemahan yang sering disebutkan pada description adalah SNMPv2, SQL injection, dan kurangnya proteksi sertifikat SSL mengaitkan entitas (orang, organisasi, host, dll.) dengan Kunci Publik. Dalam koneksi SSL, klien mengotentikasi server jauh menggu-nakan Sertifikat server dan mengekstrak Kunci Publik

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

dalam Sertifikat untuk membuat koneksi aman. Kelemahan yang ada biasa menimbulkan denial of service, dimana serangan ini dapat membuat server menjadi overload. Banyaknya rekomendasi agar dilakukan upgrade SNMP, Sistem Operasi expired, Migration Anti Virus

SIMPULAN DAN SARAN

Setelah hasil pengujian selesai maka disimpulkan sebagai berikut :

1. Pendeteksian kelemahan dengan menggunakan acunetix dijelaskan dengan detail. Acaman yang paling sering muncul di server dikarenakan :
   - Penyerang jarak jauh dapat memperoleh akses ke perangkat menggunakan kredensial default dan melakukan aktivitas berbahaya.
   - Sistem berisiko tinggi terkena kerentanan keamanan karena vendor tidak lagi menyediakan pembaruan.
   - Penyerang yang berhasil mengeksploitasi kerentanan ini dapat mengeksekusi kode arbitrer pada sistem target.

2. Beberapa *vulnerability* hasil pengujian, diminta untuk melakukan upgrade (SNMP).

3. Terdapat komputer yang menggunakan IP public dan membuka beberapa port yang tidak sesuai dengan kebutuhan pekerjaan.

Karena dapat menimbulkan celah yang dapat disusupi oleh penyerang.

4. Keamanan pada domain retail-indonesia-.co.id berhasil ditemukan vulnerability setelah di-*scanning* dengan *vulnerability scanner*. Ada beberapa *hostname* terditeksi *vulnerability* sangat banyak, sebanyak 150

5. Domain retail-indonesia.co.id bahkan *IP address* belum dilakukan *update* dan *maintainance* secara berkala.

UCAPAN TERIMAKASIH

Kami ucapan terimakasih kepada LPPM Universitas Pakuan Bogor telah memberikan kontribusi lain dalam penelitian sesuai SK Nomor:45/KEP/KET/LPPM/UP/2021 dan semua rekan-rekan angota penelitian

DAFTAR PUSTAKA

Hussain M.J. Almohri, Layne T.Watson, Danfeng Yao, Xinming Ou. “Security Optimization of Dynamic Network with Probabilitas Graph Modeling and Linier Programming,” IEEE Transactions on Dependable and Secure Computing, 2015

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

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.

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

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

Dwiyan, Wahyu. 2018. Perbandingan Kecepatan Server Tunggal Dengan Load Balancing Serta Mirroring Server Dalam Mengakses Layanan EMading. Skripsi tidak di terbitkan. Bogor : Universitas Ibnu Khaldun Bogor.

Juardi, Didi. 2017. Kajian Vulnerability Keamanan Jaringan Internet Meng-

gunakan Nessus. Jurnal Informatika. Karawang.

Betta, Avinanta.2018. Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan CVSS dan FMEA. ILKOM Jurnal Ilmiah Volume 10 Nomor 2 Agustus 2018. Malang

Penetration testing for IT Infrastructure,11-Dec-2017.[Online].Available:https://www.coresecurity.com/content/penetration-testing. [Accessed: 04-Juni-2021].

Intan, Ritzkal, dan Ade.,2019 Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika. Seminar Nasional Sains dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta.