Jurnal Asiimetrik: Jurnal Ilmiah Rekayasa Dan Inovasi
Terakreditasi **"Peringkat 4"** oleh Kemenristek/BRIN, Nomor SK: 200/M/KPT/2020
Volume 4 Nomor 2 Tahun 2022, Juli 2022, Halaman 125-132
Website : http://journal.univpancasila.ac.id/index.php/asiimetrik/

p-ISSN 2655-1861
e-ISSN 2716-2923

Analisis Serangan Vulnerabilities Terhadap Server Selama *Work from Home* saat Pandemi Covid-19 sebagai Prosedur Mitigasi

Analysis of Vulnerability Attacks on Servers while Work from Home during the COVID-19 Pandemic as a Mitigation Procedure

Kotim Subandi* dan 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, Indonesia

Informasi artikel

Diterima:
02/03/2022
Direvisi:
05/04/2022
Disetujui:
24/04/2022

Abstract

Since the COVID-19 Pandemic occurred, companies engaged in the retail sector have experienced a decline in the impact of government regulations such as PSBB (Large-Scale Social Restrictions) so that all activities were carried out from home or Work from Home (WFH). to assist companies or agencies with various types of information systems in carrying out their business activities and operations This server is one of the most important in the retail company. The opening of several accesses from the public network (internet) to the local area network (LAN) The security of a LAN network that is accessed from a public network is usually an administrator's problem. Often, the security problems of both the network and the entire application system, as well as the web server, are neglected just to ensure that operational activities run smoothly, and security is only realised after a disaster occurs. Without a good network security and application system, the application of any sophisticated technology will be very dangerous for the company, institution, or organisation itself. So, it takes a security analysis of all activities on the LAN, servers, and other devices to prevent mitigation and to be more aware of server security vulnerabilities. Based on the context of the existing issues, a penetration testing analysis is required. As supporting material, this research also uses guidelines from the CEH (Certified Ethical Hacker) module and the official Acunetix website. The test of this research is aimed at finding the weaknesses of the existing company/institution servers. Among others, quite a lot of weaknesses were found, where each of these weaknesses has a different handling, ports that should be blocked but are opened freely, and access to public IPs that are less important should be closed. The solutions proposed to overcome these problems include: the use of this Acunetix standard can be maintained and continued; testing is much better if carried out more than two times; periodically upgrading SNMP (Simple Network Management Protocol) vulnerable; increasing the level of server security; migration of quality antivirus; and upgrade of expired operating systems.

***Keywords**: vulnerability, mitigation, pentration testing, pandemic, WFH.*

Abstrak

Semenjak terjadi Pandemi covid-19 Perusahaan yang bergerak dibidang retail sempat mengalami keterpurukan dampak dari peraturan pemerintan seperti PSBB (Pembatasan 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 (*Simple Network Management Protocol*.) 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: *vulnerability, mitigation, pentration testing, pandemic*, WFH.

*Penulis Korespondensi. Tel: -; Handphone: +62 815 1339 4498
email : chotim.subandi@gmail.com

1. 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 harus memperhatikan faktor kea-manan dalam infrastruktur jaringan baik yang terhubung secara LAN (*Local Area Network*) maupun WAN (*World Area Network*). Perusahaan membuat investasi pada sistem keamanan jaringan agar seluruh aset terlindungi dari berbagai ancaman kejahatan secara *virtual* seperti *hacker* atau bahaya *virus*. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan atau mendeteksi adanya tidak kejahatan di sebuah sistem berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik (Nazwita dan Ramadhani, 2017).

Dalam upaya mengurangi kerugian yang diakibatkan dari serangan *hacker* atau *virus* yang berdampak *mitigasi*, 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 internet menjadi pengubung jaringan umum menuju jaringan *Local Area Network* sangat dibutuhkan dikarenakan dapat membantu 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 (*Local Area Network*), 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 lokal. *Vulnerability* relatif sedikit, ketika jumlah *user* atau pengguna layanan jaringan umum *(internet)* menuju jaringan berbasis LAN semakin banyak, maka akses pembukaan *port* jaringan terus bertambah hal ini menyebabkan kerentanan terjadi dan tindak kehajatan semakin meningkat.

Perkembangan teknologi saat ini membawa dampak perubahan yang signifikan dalam proses pembangunan sistem penyedia layanan dalam jaringan umum. 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 (Juardi, 2017).

Dengan semakin berkembangnya teknologi dan Internet, menyebabkan lalu lintas pergerakan sistem informasi untuk menggunakannya sebagai basis. Ada beberapa sistem yang memang tidak ter-hubung langsung ke Internet tetapi tetap menggunakan basis *web* sebagai basis untuk sistem informasinya yang dipasang di jaringan *Intranet*, hal ini yang perlu diberikan akses secara personal kepada seluruh *user* /karyawan/ pengguna sistem informasi 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 (Kamilah, Ritzkal dan Hendrawan, 2019).

Keamanan jaringan dan *server* yang diakses oleh pengguna ini menjadi masalah dari seorang administrator jaringan Dengan membuka akses jaringan umum ke jaringan LAN *(Local Area Network*), 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 (Babys, 2018).

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 (Mulya dan Tarigan, 2018).

Kelemahan (Vulnerability) sebuah sistem infromasi bisa disebabkan oleh faktor internal dan faktor eksternal. *Vulnerability Assessment* (VA) juga dapat dikatakan sebagai suatu bentuk kontrol

preventif seperti halnya antivirus yang akan mencegah terjadi insiden terhadap sistem yang bebasis teknologi informasi, maka tujuan VA sebenarnya adalah untuk meningkatkan kesadaran akan pentingnya keamanan informasi, yang seringkali menjadi prioritas kesekian dalam sebuah institusi (Masykur, 2015).

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 (Gunawan, Noertjahyana dan Rusli, 2014).

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* dan beberapa *server* lain, seperti SAP, *Intranet*, *proint* untuk kepentingan kegiatan secara daring *Work from 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.

Dengan melakukan analisa serangan terhadap *server* dengan cara *penetration testing* melalui pengujian sistem jaringan menggunakan *software* seperti *Angry IP Scanner, Acunetix Web Vulnerability Scanner 9.5* untuk menidteksi lebih awal dari tindak kejahatan di system agar terhindar dari mitigasi.

Maka untuk melindungi *server* pada *data center* tentunya diperlukan pening-katan sistem keamanan yang sangat handal. Langkah awal yang dapat dilakukan adalah dengan evaluasi sistem keamanan pada server yang berada di *data center* agar didapatkan data kelemahan *(vulnerability*) atau lubang-lubang keamanan yang dapat merugikan atau membahayakan serta dapat merusak sistem. Data kelemahan ini dapat dijadikan sebagai bahan masukan untuk tenaga IT dan *Administrator* yang bertugas sebagai pengelola infrastruktur jaringan dan *data center* sehingga perbaikandari sisi keamanan *server* akan terus meningkat.

2. METODOLOGI

2.1. Analisa Permasalahan

Melalukan *scanning* terhadap semua *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 pada *sever*. Hasil dari scanning ini nantin akan menjadi evaluasi untuk analisa bagi tim pengelola *infrastructure Network*, *Network security* dan *data centre* untuk lebih peduli dan sigap lagi terhadap kelemahan yang ada.

2.2. Analisa Kebutuhan

Yang menjadi alasan perlu dilakukan *penetration testing* didalam penelitian ini adalah untuk menemukan kerentanan serta kelemahan dan *vulnerabilities system*, sebelum kerentanan dan kelemahan ter-sebut dieksploitasi oleh para penyerang seperti hacker yang akan memberikan dam-pak tidak baik bahkan mitigasi bagi keamanan *server* didalam perusahaan. Selain itu, *penetration testing* ini dilakukan sebagai gambaran dan analisa bahwa mana-jemen 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 ISO 27001.

2.3. Analisa Perangkat Lunak *(Software)*

Dalam penelitian ini, program aplikasi yang akan digunakan adalah program yang sesuai dengan metode dalam setiap langkah *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*

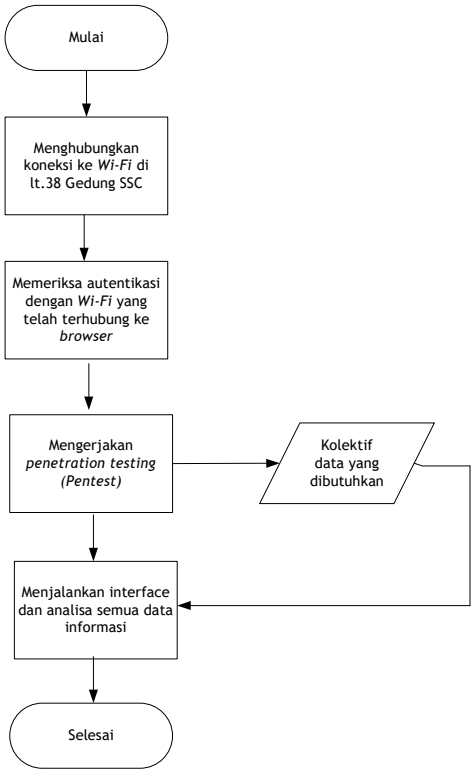
2.4. Komponen Pendukung Penelitian

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

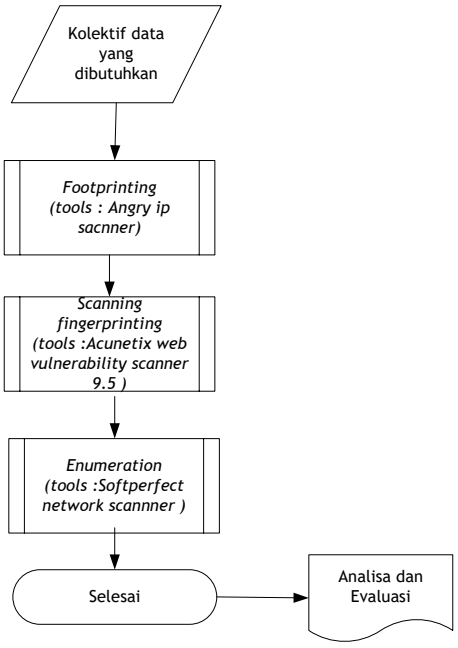
1) **Perusahaan /Organisasi**
   Perusahaan/organisasi yang dianalisa dalam penelitian ini adalah Perusahaan Retail yang berkantor pusat di Gedung SSC Jakarta Pusat.
2) ***Wi-Fi***
   Wi-Fi berada di Gedung SSC lantai 38 kantor pusat.
3) **Target Analisa**
   Target *penetration testing* dan analisa untuk penelitian ini adalah sebanyak 10 unit server.
4) ***Range IP Address***
   Dalam metode pengumpulan data (*penetration testing*) menggunakan *range IP address*. Berikut *range IP Address server*: 192.168.xxx.33 – 192.168.xxx.254 secara random.

2.5. 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.



Gambar 1. *Flowchart* pengerjaan penelitian



Gambar 2. Proses eksekusi *penetration testing*

2.5.1. *Footprinting*

Footprinting adalah suatu proses yang digunakan mengungkap dan mengumpulkan data infor-masi sebanyak mungkin mengenai target berada didalam jaringan. *Footprinting* mempunyai tujuan antara lain mengum-pulkan informasi mengenai network target, sistem informasi target, dan informasi suatu perusahaan /organisasi (Herdianti dan Umar, 2020). Metode teknik ini, menggunakan tools Angry IP Address.

2.5.2. *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 (Sofana dan Primartha, 2019). Pada penelitian ini, dari jenis *scanning* yang ada, *vulnerability scanning* adalah jenis yang akan digunakan untuk analisa keamanan dari jaringan server.

2.5.3. *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 (Yunus, 2019).

2.5.4. SNMP

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

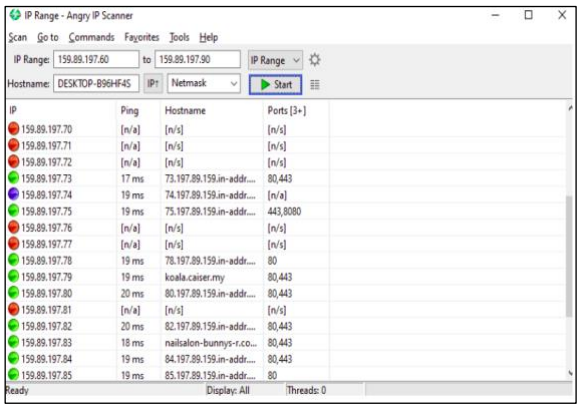
3. HASIL DAN PEMBAHASAN

3.1. Perangkat Lunak (*Software*) untuk *Penetration Testing*

3.1.1. *Footprinting*

Untuk menjalankan *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 *laptop dan 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.

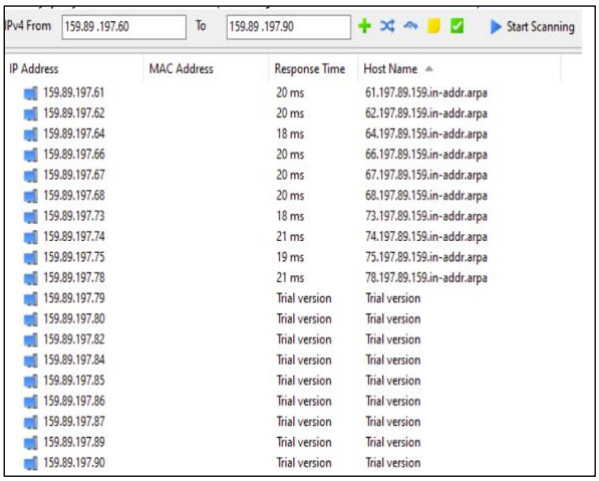
3.1.2. *Scanning Fingerprinting*

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 vulne-rability yang berada didalam sistem jaringan *Ip address* dan *hostname*. Tidak hanya menampilkan kelemahan atau celah dari suatu sumber, tetapi tool ini juga memberikan informasi tingkat kelemahan dari *alerts (vulnerability)* yang akan ditemukan. Pada Gambar 4, diperlihatkan tampilan *tool vulnerability scanner (Acunetix Web Vulnerability Scanner 9.5).*

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

3.1.3. *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 dilihat tampilan tool *SoftPerfect network Scanner*.



Gambar 5. Tampilan *tool SoftPerfect network scanner*

3.2. Hasil Pengujian Perangkat Lunak (*Software*)

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 mem-berikan solusi agar tidak menimbulkan mitigasi sistem informasi dan jaringan. Dalam Tabel 2, dapat dilihat hasil uji dengan tool *Angry IP scanner*. Hasil ini adalah hasil yang sudah direkap dari pengujian menggunakan *software*.

Tabel 2. Hasil *scanning 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

Berdasarkan hasil pengujian seperti terlihat dalam Tabel 2, salah satu *server* dengan IP 159.89.xx.xx sudah ditemukan indikasi penyerang berupa *malware*. Hal ini sudah menunjukan kalau system jaringan tersebut terjadi *vulnerability*.

3.3. Summary Vulnerability

Pada Tabel 3 menampilkan hasil *summary* dari seluruh kelemahan dan kerentanan yang berhasil ditemukan setelah dilakukan pengujian. Dari semua kelemahan dan kerentanan yang ada, kelemahan yang sering disebutkan pada description adalah *SNMPv2 (Simple Network Management Protocol version 2), SQL injection,* dan kurangnya proteksi sertifikat SSL (*Secure Socket Layer*) mengaitkan entitas (orang, organisasi, host, dll.) dengan Kunci Publik. Dalam koneksi SSL, *client* mengotentikasi *server* jauh

menggunakan Sertifikat *server* dan mengekstrak Kunci Publik dalam Sertifikat untuk membuat koneksi aman.

Tabel 3. *Summary vulnerability* kategori *description*

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

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.*

4. SIMPULAN

Berdasarkan hasil pengujian didapatkan kesimpulan yaitu, pendeteksian kelemahan dengan menggunakan acunetix dapat dijelaskan dengan detail. Acaman yang paling sering muncul di server dikarenakan penyerang jarak jauh dapat memperoleh akses ke perangkat meng-gunakan kredensial default dan melakukan aktivitas berbahaya. Sistem berisiko tinggi terkena kerentanan keamanan karena vendor tidak lagi menyediakan pembaruan. Penyerang yang berhasil mengeks-ploitasi kerentanan ini dapat mengeksekusi kode arbitrer pada sistem target. Beberapa *vulnerability* hasil pengujian, diminta untuk melakukan *upgrade* (SNMP). 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. Keamanan pada *domain* berhasil ditemukan vulnerability setelah di *scanning* dengan vulnerability scanner. Ada beberapa *hostname* terditeksi *vulnerability* sangat banyak. *Domain* yang digunakan oleh perusahaan bahkan *IP address* belum dilakukan *update* dan *maintenance* secara berkala.

DAFTAR PUSTAKA

Babys, J.Y. (2018) 'Analisis Vulnerable Port Pada Client Pengguna Publik Wifi', *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, 9(1), hal. 261–268.

Gunawan, I., Noertjahyana, A. dan Rusli, H. (2014) 'Analysis and implementation of operational security management on computer center at the university X', *ARPN Journal of Engineering and Applied Sciences*, 9(10), hal. 1688–1696.

Herdianti, H. dan Umar, F. (2020) 'Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning', *INFORMAL: Informatics Journal*, 5(2), hal. 43–48.

Juardi, D. (2017) 'Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus', *Syntax Jurnal Informatika*, 6(1), hal. 11–19.

Kamilah, I., Ritzkal, R. dan Hendrawan, A.H. (2019) 'A nalisis Keamanan Vulnerability p ada Server Absensi Kehadiran L aboratorium di Program Studi Teknik Informatika', *Prosiding Semnastek* 2019, TINF - 006, hal. 1-9.

Masykur, F. (2015) 'Analisis Vulnerability Web Based Application Menggunakan Nessus', *PROSIDING SENATEK FAKULTAS TEKNIK UMP* [Cetak].

Mulya, B.W.R. dan Tarigan, A. (2018) 'Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea', *ILKOM Jurnal Ilmiah*, 10(2), hal. 190–200.

Nazwita, N. dan Ramadhani, S. (2017) 'Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata', in *Seminar Nasional Teknologi Informasi Komunikasi dan Industri*, hal. 308–317.

Sofana, I. dan Primartha, R. (2019) 'Network Security dan Cyber Security Network Security Dan Cyber Security : Teori dan Praktik CISCO CCNA, LINUX, WINDOWS, AMAZON AWS, ANDROID', *Bandung: Informatika* [Cetak].

Yunus, M. (2019) 'Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4', *Jurnal Ilmiah Informatika Komputer*, 24(1), hal. 37–48.