Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

Software Security Hardening Pada Virtual Private *Server* Berdasarkan NIST SP 800-123 di Universitas XYZ

Faishal Rizqi Irfandi*, Umar Yunan Kurnia Septo Hedianto, Ahmad Almaarif

Fakultas Rekayasa Industri, Sistem Informasi, Universitas Telkom, Bandung
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia
Email: [1,*]faishalrizqiirfandi@student.telkomuniversity.ac.id, [2]umaryunan@telkomuniversity.ac.id, [3]ahmadalmaarif@telkomuniversity.ac.id
Email Penulis Korespondensi: faishalrizqiirfandi@student.telkomuniversity.ac.id
Submitted: **26/09/2022**; Accepted: **17/10/2022**; Published: **31/10/2022**

Abstrak−Tingkat perkembangan teknologi saat ini sangat pesat. Contoh yang paling menonjol adalah penggunaan website di lingkungan industri maupun pemerintahan. Website memberikan kemudahan dalam mendukung proses bisnis yang berlangsung serta dapat membantu pekerjaan dalam menyelesaikan permasalahan yang terjadi di sebuah organisasi. Dalam penggunaan website tentunya diperlukan sebuah server untuk memproses permintaan data atau memberikan informasi kepada pengguna. Pada Fakultas XYZ di Universitas XYZ mempunyai server virtualxyz yang di dalamnya berisikan website yang digunakan untuk menunjang kegiatan akademik maupun administrasi. Namun dalam perkembangan teknologi tentunya akan dibarengi dengan perkembangan kerentanan atau serangan terhadap aplikasi tersebut. Oleh karena itu, pada server virtualxyz perlu dilakukan proses Security Hardening berdasarkan National Institute of Standards and Technology (NIST) Special Publication 800-123. Hal ini dilakukan dikarenakan pada server virtualxyz belum pernah dilakukan pengecekan keamanan berdasarkan standar tertentu pada software servernya pada. Dilakukannya penelitian ini bertujuan untuk melakukan analisis keamanan server software virtualxyz untuk meminimalisir serangan yang terjadi. Hasil dari penelitian ini dapat digunakan sebagai acuan untuk memperkuat keamanan server software pada server virtualxyz. Hasil yang didapat dari analisis pada server software berdasarkan NIST SP 800-123 ditemukan 6 prosedur yang belum diterapkan pada server virtualxyz.

Kata Kunci: Server; Website; VPS; Security Hardening; NIST SP 800-123

Abstract−The current level of technological development is very rapid. The most prominent example is the use of websites in industry and government environments. The website provides convenience in supporting ongoing business processes and can assist work in solving problems that occur in an organization. In using the website, of course, a server is needed to process data requests or provide information to users. The XYZ Faculty at XYZ University has a virtualxyz server which contains a website that is used to support academic and administrative activities. However, the development of technology will of course be accompanied by the development of vulnerabilities or attacks against these applications. Therefore, on the virtualxyz server, it is necessary to carry out a Security Hardening process based on the National Institute of Standards and Technology (NIST) Special Publication 800-123. This is done because the virtualxyz server has never done a security check based on certain standards on the server software. The purpose of this research is to analyze the security of the virtualxyz software server to minimize attacks that occur. The results of this study can be used as a reference to strengthen the security of the server software on the virtualxyz server. The results obtained from the analysis on the server software based on NIST SP 800-123 found 6 procedures that have not been implemented on the virtualxyz server.

Keywords: Server; Website; VPS; Security Hardening; NIST SP 800-123

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) membuat banyak perubahan dalam kehidupan manusia, TI diciptakan untuk memudahkan kehidupan manusia dalam melakukan kegiatan sehari-hari. Perkembangan teknologi yang sangat pesat memiliki banyak manfaat. Namun, di balik banyaknya manfaat yang diberikan, tentunya tidak sedikit pula celah keamanan dan kerentanan yang akan ditimbulkan. Hampir tidak mungkin jika sebuah sistem memiliki tingkat bebas kerentanan sebesar 100%. Namun, dengan meningkatkan keamanan sistem dan jaringan, maka kerentanan tersebut dapat berkurang[1]. Pada sebuah sistem, kerentanan memiliki potensi yang relatif tinggi. Sehingga penyerang dapat memanfaatkan kondisi seperti ini untuk melakukan eksploitasi dan mendapatkan informasi atau akses ke sebuah sistem secara tidak resmi. Kaspersky telah mengungkapkan bahwa Indonesia berada di peringkat ke-23 sebagai negara yang paling terpapar serangan ransomware pada tahun 2019. Dari September hingga Desember 2019, Kaspersky mendeteksi dan memblokir serangan terhadap 229.643 pengguna produknya. Terjadi penurunan sebesar 11% dibandingkan periode yang sama tahun lalu [2].

Saat ini, keamanan sistem informasi menjadi salah satu fokus penting dalam perkembangan TI. Jika berkembangnya TI tidak dibarengi dengan perkembangan tingkat keamanan sistemnya, *Hacker* dengan mudah untuk mengambil alih sebuah sistem yang sedang dibangun[2]. *Hacker* merupakan seseorang yang ahli dalam bidang komputer, jaringan dan pemrograman sehingga mampu untuk menembus keamanan sebuah sistem dan jaringan. Dalam melakukan aksinya, *hacker* menyerang titik kerentanan yang ada pada sebuah sistem. Seringkali tindakannya dapat merugikan pihak tertentu dan termasuk dalam tindakan kriminal. *Server* adalah sistem komputer yang terdapat pada jaringan berfungsi sebagai penyedia layanan bagi pengguna yang biasa disebut dengan *client*[3]. Untuk menampilkan *website* pada *web browser* sehingga bisa diakses oleh publik maka perlu dilakukan *hosting*. *Hosting* merupakan tempat untuk penyimpanan file dan data yang berupa gambar, video, *database* dll.

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

Sehingga *website* dapat diakses banyak orang. *Hosting* memiliki 3 bentuk layanan yaitu *Virtual Private Server* (*VPS*), *Shared Hosting* dan *Cloud Hosting*. Disini virtualxyz menggunakan vps sebagai layanan *hosting*nya.

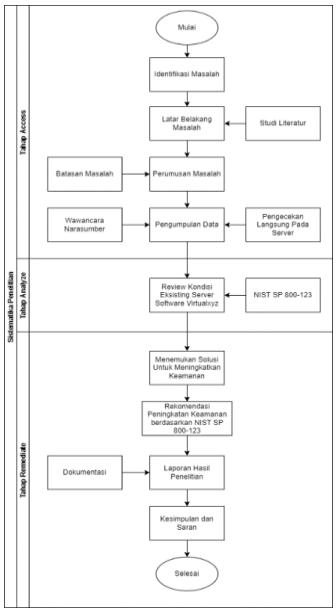
Virtualxyz merupakan sebuah *server* yang digunakan oleh entitas yang ada di Fakultas XYZ Universitas XYZ yang didalamnya berisikan 11 *web apps* yang digunakan mahasiswa ataupun pegawai untuk menunjang kegiatan dalam perkuliahan maupun administrasi. Beberapa *website* yang digunakan adalah manpeg.virtualxyz.id, recprak.virtualxyz.id, pilpro.virtualxyz.id dan sap.virtualxyz.id. Hardening dalam arti yang paling sederhana adalah proses pengerasan lapisan lunak sehingga lapisan menjadi keras[4]. Prinsip ini juga berlaku terhadap *server*, Proses *Security Hardening* adalah menguatkan tingkat keamanan suatu *server* sehingga mengurangi kerentanan pada *server* tersebut. Proses *Security Hardening* pada virtualxyz bertujuan untuk melakukan pengamanan data yang ada di virtualxyz, jika terjadi serangan terhadap *server*, maka dapat berpengaruh terhadap kinerja virtualxyz itu sendiri. Dalam proses *Security Hardening* diperlukan standarisasi sebagai pedoman untuk pemenuhan standar dan kualitas. Standarisasi yang akan diterapkan pada virtualxyz adalah berdasarkan NIST *Special Publication* 800-123. NIST SP 800-123 merupakan dokumen panduan keamanan untuk keamanan *server* pada sisi *Operating system* (OS) dan *server software* yang direkomendasikan oleh *National Institute of Standards and Technology* (NIST).

Terdapat beberapa penelitian sejenis yang telah dilakukan oleh (Saputra & Anggrainy, 2020) mengenai pemanfaatan teknologi sistem jaringan untuk untuk membangun sistem keamanan jaringan yang mengacu pada standar keamanan jaringan internasional dan penelitian yang dilakukan oleh (Perdana, 2018) mengenai audit keamanan sistem informasi akademik menggunakan standarisasi NIST SP 800-26 studi kasus Universitas Sangga Buana YPKP Bandung. Perbedaan penelitian ini dengan penelitian sebelumnya terdapat pada standar yang digunakan dan objek dilakukannya penelitian. Berdasarkan latar belakang di atas, pada *server software* virtualxyz perlu dilakukan pengecekan menggunakan standar tertentu. Pemilihan *server software* dalam penelitian ini bertujuan untuk melindungi dan meminimalisir serangan yang akan menyerang *server software*. Dalam hal ini, peneliti memilih menggunakan NIST SP 800-123 yang didalamnya memiliki 17 prosedur yang bisa diterapkan pada *server software* virtualxyz. Hasil yang diharapkan pada penelitian ini adalah penerapan prosedur berdasarkan NIST SP 800-123 dapat meningkatkan keamanan dan meminimalisir serangan yang akan terjadi pada *server software* virtualxyz.

2. METODOLOGI PENELITIAN

2.1 Sistematika Penelitian

Pada sistematika penelitian ini terdiri dari beberapa tahapan atau langkah yang dijabarkan secara terstruktur dan sistematis. Adapun Sistematika penelitian dijelaskan pada Tabel 2.



Gambar 1 Sistematika Penelitian

2.1.1 Tahap Access

Pada tahap *Access* ini bertujuan untuk mengidentifikasi permasalahan yang terjadi, dimulai dari identifikasi masalah untuk menentukan latar belakang masalah berdasarkan studi literatur, lalu merumuskan masalah berdasarkan batasan masalah yang sudah ditentukan dan melakukan pengumpulan data yang didapat dari melakukan wawancara pada narasumber dan melakukan pengecekan langsung pada *server* virtualxyz.

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

2.1.2 Tahap Analyze

Tahap berikutnya adalah tahap analyze, pada tahapan ini dilakukan analisis kondisi eksisting *server software* pada *server* virtualxyz berdasarkan standar NIST SP 800-123. Tahap ini dilakukan bertujuan untuk mengetahui kondisi pada *server* software virtualxyz berdasarkan standarisasi. Jika ada langkah langkah yang belum diterapkan pada *server*, nantinya akan diberikan rekomendasi untuk diterapkan untuk memperkuat keamanan *server* virtualxyz.

2.1.3 Tahap Remediate

Tahap yang terakhir adalah tahap *remediate*. Pada tahap ini dilakukan pencarian solusi-solusi berdasarkan anaIisis pada kondisi eksisting yang sebelumnya telah dilakukan pada tahap *analyze*, lalu diberikan rekomendasi terbaik untuk meningkatkan keamanan pada *server* virtualxyz. Selanjutnya adalah penyelesaian laporan penelitian dengan menggunakan dokumentasi-dokumentasi serta memberikan kesimpulan dan saran[7].

2.2 Web *Server*

Web server adalah bagian dari *software* yang diinstal di *server* dan dirancang khusus dalam menangani *request* dari HTTP atau HTTPS sebelum meneruskannya ke *web browser* kembali. *web server* menerjemahkan terlebih dahulu permintaan yang dikirimkan oleh *web browser* sebelum dikembalikan lagi oleh *web server*[8]. Selain untuk melakukan pengolahan data, web *server* juga berfungsi untuk mengirimkan data yang berbentuk video dan foto sesuai dengan permintaan *client*[9].

2.3 Virtual Private *Server*

VPS atau *Virtual private server* adalah tipe *server* yang mengubah *server* fisik menjadi sejumlah *server* virtual menggunakan teknologi virtualisasi[10]. Karena setiap VPS memiliki akses ke *server* utama, tetapi *server* utama tidak mengalami gangguan selama operasi dijalankan, tidak ada gangguan antara satu VPS dengan yang lain[11]. Setiap *server* VPS memiliki akses root penuh, sistem operasinya sendiri, dan pengaturan untuk menjalankan i*nit script*, *users*, dan pemrosesan, serta sumber daya seperti RAM dan CPU[12].

2.4 Security Hardening

Security Hardening adalah metode atau prosedur yang digunakan untuk meminimalisir ancaman pada suatu sistem dengan cara memperkuat sistem atau jaringan tersebut agar terhadap serangan, metode ini digunakan untuk meningkatkan keamanan sistem atau jaringan[4]. Tujuan dari *Security Hardening* ini adalah untuk mengurangi resiko ancaman yang kemungkinan bisa terjadi pada sebuah sebuah sistem.

2.5 NIST SP 800-123

National Institute of Standards and Technology (NIST) memiliki tanggung jawab atas standar dan pedoman untuk menyediakan keamanan informasi[13]. Pada NIST SP 800-123 ini membahas tentang panduan untuk mengamankan *server*. Standar NIST ini memiliki tujuan untuk meningkatkan organisasi dalam pencegahan, mendeteksi serta memberikan respon terhadap serangan dunia maya. Berikut merupakan tahapan untuk mengamankan *server* menurut NIST SP 800-123:

1. Melakukan perencanaan instalasi dan penerapan pada sistem serta komponen lainnya
2. Melakukan proses instalasi dan konfigurasi untuk mengamankan *operating system*
3. Melakukan proses instalasi dan konfigurasi untuk mengamankan *server software*
4. Pada *server* yang memiliki konten, pastikan konten tersebut diamankan
5. Menggunakan mekanisme perlindungan jaringan yang sesuai
6. Melakukan proses *maintenance* dan administrasi yang aman

3. HASIL DAN PEMBAHASAN

3.1 Analisis Kondisi Eksisting

Sebelum dilakukan proses pengecekan kondisi eksisting *server software* pada *server* virtuaxyz, perlu diketahui terlebih dahulu tahapan atau langkah-langkah yang akan dilakukan pada *server*. Langkah-langkah yang sudah diterapkan ditandai dengan tanda “V” dan langkah yang belum diterapkan ditandai dengan tanda “X”. NIST SP 800-123 membagi langkah pengamanan *server software* menjadi empat bagian sebagai berikut.

Tabel 1. *Checklist* NIST SP 800-123

No.	Judul	Total *checklist*
1	*Installing the Server Software Securely*	9
2	*Establishing Access Controls*	3
3	*Limited Server Resources*	4
4	*Technologies for Authentication and Encryption Selection and Implementation*	1

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

Berdasarkan Tabel 1 diatas, tahapan pengcekan keamanan *software server* dibagi menjadi empat tahap. Berikut merupakan penjelasan dari masing-masing tahapan.

Pada tahap *Securely Installing the Server Software* dijelaskan bagaimana prosedur penginstalan *software* yang aman, mulai dari menghapus *default user account* yang terbuat saat penginstalan *software*, menghapus atau menonaktifkan aplikasi, *service* ataupun *script* yang sudah tidak digunakan, hingga melakukan konfigurasi untuk menghindari ancaman yang dapat mengancam server. Pada tahap *Securely Installing the Server Software* jumlah langkah yang dapat dilaksanakan pada server virtualxyz berjumlah sembilan langkah

Pada tahap *Configuring Access Controls* dijelaskan bagaimana melakukan pembatasan kontrol akses kepada pengguna dalam mengakses data yang berada pada *server*. Hal ini dilakukan untuk melindungi informasi-informasi sensitif yang tersimpan pada *server* serta menghindari pencurian data pada *server*. Tahap *Configuring Access Controls* memiliki tiga langkah yang bisa diterapkan pada server virtualxyz.

Pada tahap *Server Resource Constrains* dijelaskan bagaimana cara untuk mengatur sumber daya pada *server*. Hal ini dilakukan pengamanan pada file-file yang akan di *upload* untuk menghindari penyisipan *malware* serta mengatur ruang penyimpanan untuk mengoptimalkan kinerja *server* dan menghindari serangan pada *server* yang mengakibatkan file log meningkat. Tahap *Server Resource Constrains* memiliki empat langkah yang dapat diterapkan pada *server* virtualxyz

Pada tahap *Selecting and Implementing Authentication and Encryption Technologies* dilakukan pemilihan teknologi autentikasi dan enkripsi yang bertujuan untuk membatasi siapa saja yang dapat mengakses *server* dan untuk melindungi informasi yang dikirimkan antara *server* dan *client*.

3.2 Kondisi eksisting Securely Installing the *Server* Software

Dalam proses instalasi *software* pada *server*, ada beberapa langkah yang harus dilakukan agar *server* tetap dalam kondisi aman dan terhindar dari kerentanan. Adapun kondisi eksisting *Securely Installing the Server Software* pada *server* virtualxyz berdasarkan NIST SP 800-123 dijelaskan pada Tabel 2.

Tabel 2. Eksisting Securely Installing the *Server* Software

No.	*Checklist*	Referensi	Kondisi *Checklist*
1	*Apply any patches or upgrade*	Berdasarkan pengecekan pada *server*	V
2	*Remove or disable all unneeded service*	Berdasarkan pengecekan pada *server*	V
3	*Disable or remove all unnecessary default accounts*	Berdasarkan pengecekan pada *server*	X
4	*Remove all manufactures documentation*	Berdasarkan wawancara dengan narasumber	X
5	*Delete all test or sample files from the server*	Berdasarkan wawancara dengan narasumber	X
6	*Remove all unneeded compilers*	Berdasarkan pengecekan pada *server*	V
7	*Apply the relevant security template or hardening script*	Berdasarkan wawancara dengan narasumber	X
8	*Service banners should be reconfigured to not report the server and OS version.*	Berdasarkan pengecekan pada *server*	X
9	*Set up each network service on the required TCP and UDP ports*	Berdasarkan wawancara dengan narasumber	V

Dari hasil analisis yang dilakukan pada *server* virtualxyz berdasarkan NIST SP 800-123. Ditemukan beberapa langkah yang diterapkan pada *server* virtualxyz. Adapun penjelasan dari setiap kondisi eksisting adalah sebagai berikut.

a. *Apply any patches or upgrade*
   Pada *checklist* pertama ini bertujuan untuk memperbaiki kerentanan dan meningkatkan keamanan pada *server*. Dengan melakukan *upgrade* pada *software*, maka akan mendapatkan *patch* terbaru yang berfungsi untuk memperbaiki *bug* dan kerentanan yang membahayakan *server*.
b. *Remove or disable all unneeded service*
   Pada *checklist* kedua ini bertujuan untuk mencegah serangan yang dapat mengancam keamanan pada *server*. Hal ini dilakukan untuk menghindari orang lain melakukan transfer file atau data yang dapat membahayakan *server*.
c. *Disable or remove all unnecessary default accounts*
   Pada *checklist* ketiga ini dilakukan penghapusan atau penonaktifan *Default User Account* Secara *default*, instalasi *server* akan membuat *Default User Account*. Dalam hal ini, *hacker* dapat mengeksploitasi akun yang

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

tidak digunakan dan kadaluarsa di dalam sistem. Sehingga melakukan penghapusan atau penonaktifan *Default User Account* penting dilakukan untuk menghindari serangan yang dilakukan dari luar.

d. *Remove all manufactures documentation*
Pada *checklist* keempat ini dilakukan penghapusan dokumentasi manufaktur. Tentunya dalam penginstalan *server* pertama kali akan meninggalkan dokumen-dokumen sisa dari proses penginstalan, jika dokumen tersebut dibiarkan berada di dalam *server*, maka akan membuat penyimpanan *server* menjadi penuh.

e. *Delete all test or sample files from the server*
Pada *checklist* kelima ini dilakukan penghapusan semua test file baik itu dari penginstalan *server* atau uji *server*, termasuk contoh konten, *script* dan *executable code*.

f. *Remove all unneeded compilers*
Pada *checklist* keenam ini dilakukan penghapusan semua *compiler* yang tidak dibutuhkan. Langkah ini dilakukan bertujuan untuk untuk menghindari *compiler* tersebut mengcompile kode yang ada pada *server*.

g. *Apply the relevant security template or hardening script*
Pada *checklist* ini merupakan salah satu cara untuk mengamankan *server*. Pemilihan *template* atau *script* yang tepat dapat membuat *server* lebih kuat dalam menahan serangan yang dilakukan dari luar

h. *Service banners should be reconfigured to not report the server and OS version*
Pada *checklist* ini dilakukan untuk merahasiakan informasi yang ada di dalam *server* baik itu versi dari *server* ataupun OS yang sedang digunakan, hal ini dilakukan untuk menghindari *hacker* untuk mengetahui informasi dari *server*.

i. *Set up each network service on the required TCP and UDP ports*
Pada *checklist* yang terakhir dilakukan konfigurasi layanan hanya pada port TCP dan UDP yang diperlukan.

3.3 Kondisi Eksisting Configuring Access Controls

Pengaturan kontrol akses yang tepat dapat mengurangi atau mencegah penyebaran informasi-informasi sensitif untuk tidak disebarluaskan secara publik. Perangkat lunak *server* harus menerapkan mekanisme khusus untuk dapat mengakses file atau perangkat pada *host*, jika tidak, maka akan terjadi akses yang terlalu banyak. Adapun kondisi eksisting *Configuring Access Controls server* virtualxyz berdasarkan NIST SP 800-123 dijelaskan pada tabel 3.

Tabel 3 Eksisting Configuring Access Controls

No.	*Checklist*	Referensi	Kondisi *Checklist*
1	*Service processes are set up to run with highly limited access as users*	Berdasarkan pengecekan pada *server*	X
2	*Service processes are restricted to writing to server content directories and files*	Berdasarkan pengecekan pada *server*	V
3	*The server software limits the temporary files it creates to a specific, securely stored subdirectory.*	Berdasarkan wawancara narasumber dan pengecekan pada *server*	V

Pengaturan *access control* ini dapat membatasi pengguna dalam mengakses data yang ada di dalam *server*. Tanpa adanya *access control*, kemungkinan terjadi pencurian data menjadi meningkat. Adapun langkah-langkah yang harus dilakukan dengan *access control* adalah sebagai berikut.

a. *Service processes are set up to run with highly limited access as users*
Pada *checklist* ini dijelaskan ketika ada service yang berjalan pada *server* harus jelas pengaturan *privilege* atau hak istimewanya. Hal ini dilakukan untuk menghindari akses yang tidak diperlukan oleh *service*.

b. *Service processes are restricted to writing to server content directories and files*
Pada *checklist* kedua ini setiap service dipastikan memiliki hak akses *write* ke *server* file dan *directorynya*

c. *The server software limits the temporary files it creates to a specific, securely stored subdirectory*
Setiap *service* yang berjalan tentunya akan membuat *temporary files*. Pada langkah ini dijelaskan bahwa *temporary files* yang dibuat oleh *service* harus berada pada folder tertentu, temporary files yang terbuat oleh service tidak diizinkan untuk tersimpan pada kernel.

3.4 Kondisi Eksisting *Server* Resource Constraints

Untuk mengurangi efek dari serangan DoS, diperlukan konfigurasi pada *server* untuk membatasi sumber daya sistem operasi yang dapat digunakan. Adapun kondisi eksisting *Server Resource Constraints server* virtualxyz berdasarkan NIST SP 800-123 dijelaskan pada tabel 3.

Tabel 4 Eksisting *Server* Resource Constraints

No.	*Checklist*	Referensi	Kondisi *Checklist*
1	*Limiting the hard disk space set out for uploads*	Berdasarkan *List app* dan *online service*	V

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

No.	*Checklist*	Referensi	Kondisi *Checklist*
2	*If uploads are permitted, make sure the server cannot access these files until they have been manually or automatically filtered*	Berdasarkan pengecekan pada *server*	V
3	*Ensure log files are stored in an ideally sized space. Log files should ideally be located on a dedicated disk*	Berdasarkan wawancara narasumber dan pengecekan pada *server*	V
4	*Determining the highest number of connections or server processes the server should support*	Berdasarkan wawancara narasumber dan pengecekan pada *server*	V

a. *Limiting the hard disk space set out for uploads*
Memberikan limit atau batasan saat proses upload dapat mengurangi risiko ruang penyimpanan penuh atau *overload*. Langkah ini juga bertujuan untuk mengoptimalkan penggunaan ruang penyimpanan.

b. *If uploads are permitted, make sure the server cannot access these files until they have been manually or automatically filtered*
Pada *checklist* ini dijelaskan bahwa file-file yang diizinkan upload ke dalam *server* harus melewati peninjauan kembali, baik itu otomatis maupun manual. Tindakan ini bertujuan untuk mencegah *server* digunakan untuk melakukan penyebaran *malware*, *attack tools*, konten pornografi dll. Tindakan ini juga bertujuan untuk membatasi ukuran dari file yang akan di upload untuk menghindari DoS karena pengunggahan banyak file-file yang berukuran besar.

c. *Ensure log files are stored in an ideally sized space. Log files should ideally be located on a dedicated disk*
Pada *checklist* ini dijelaskan bahwa penyimpanan file *log* semestinya disimpan pada ruangan dengan ukuran yang tepat dan disimpan pada partisi yang terpisah dari *server*. Tindakan ini dilakukan untuk menghindari jika terjadi serangan yang menyebabkan ukuran file log meningkat, maka tidak akan mengganggu kinerja *server* utama.

d. *Determining the highest number of connections or server processes the server should support*
Melakukan kontrol terhadap jumlah proses yang berjalan pada *server* bertujuan untuk mengoptimalkan konsumsi sumber daya pada *server*. Jika langkah ini tidak dilakukan maka akan terjadi pemakaian sumber daya yang berlebih. Sebagai contoh, banyak pengguna yang menjalankan banyak proses, walaupun masing-masing proses tidak mengkonsumsi sumber daya yang terlalu banyak tapi jika diakumulasikan semua proses akan menguasai semua sistem.

3.5 Kondisi Eksisting Selecting and Implementing Authentication and Encryption Technologies

Tanpa menerapkan teknologi autentikasi dan enkripsi pada *server*, *server* tidak dapat membatasi akses ke pengguna yang berwenang. Semua layanan dan informasi dapat diakses oleh semua orang yang mempunyai akses ke *server*. Tanpa enkripsi, siapapun yang memiliki akses ke *server* dapat mengakses atau mungkin mengubah informasi sensitif yang ada di dalam *server*. Berdasarkan analisis pada *server* virtualxyz sudah menggunakan teknologi autentikasi dan enkripsi. Berikut merupakan teknologi yang digunakan pada *server* virtualxyz.

a. SSH
Secure Shell, juga dikenal sebagai SSH adalah protokol jaringan yang memungkinkan dua perangkat berbeda untuk bertukar data melalui saluran aman[14]. Penggunaan SSH banyak digunakan pada pengguna *operating system* Linux. Selain itu, SSH juga mendukung untuk melakukan pengiriman berkas melalui SFTP (*Secure File Transfer*). SSH biasanya menggunakan port 22 yang sudah ditetapkan sebagai jalur untuk *server* SSH.

b. SSL
Secure Socket Layer (SSL) adalah sebuah teknologi enkripsi untuk komunikasi internet yang aman[15]. SSL menjamin kerahasiaan data antara *client* dan *server* dengan melakukan enkripsi. Pada saat *client* melakukan pengiriman pesan ke *server*, maka *server* akan mengembalikan pesan tersebut beserta sertifikat dan informasi lainnya. Disini *client* menyelesaikan proses autentikasi dengan *server*. Jika proses autentikasi selesai dilakukan, kemudian *client* akan membuat kunci sesi untuk melakukan proses enkripsi dan dekripsi data. Sesi diidentifikasi oleh ID sesi yang diketahui *client* dan *server*. Keamanan koneksi internet bergantung pada saat validasi sertifikat kunci sesi yang dibuat dengan benar pada saat koneksi dibuat[16] . *Website* yang sudah menerapkan teknologi enkripsi SSL maka url *website* akan berubah menjadi HTTPS.

3.6 Analisis Rekomendasi

Pada subbab ini akan dijelaskan tentang rekomendasi solusi yang diusulkan oleh penulis berdasarkan hasil analisis kondisi eksisting *server* virtualxyz menggunakan standarisasi NIST SP 800-123.

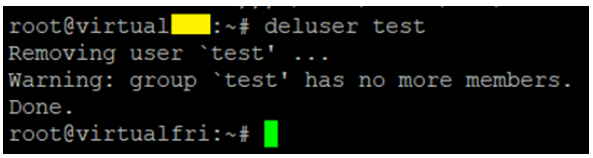
a. *Securely Installing the Server Software*
Dari analisis yang dilakukan pada Securely Installing the *Server* Software virtualxyz berdasarkan NIST SP 800-123. Terdapat rekomendasi solusi yang penulis usulkan. Adapun penjelasan rekomendasi dari setiap langkah adalah sebagai berikut.

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

1. *Managing default user account*
   Berdasarkan analisis kondisi eksisting pada *server* virtualxyz, direkomendasikan untuk melakukan pengelolaan *default user account* dengan melakukan penghapusan atau menonaktifkan *default user account* yang terbuat saat instalasi *server* jika tidak diperlukan lagi. Langkah ini dilakukan untuk menghindari eksploitasi *account* yang dapat dilakukan oleh *hacker*. *Command* yang bisa digunakan untuk menghapus *default user account* adalah:

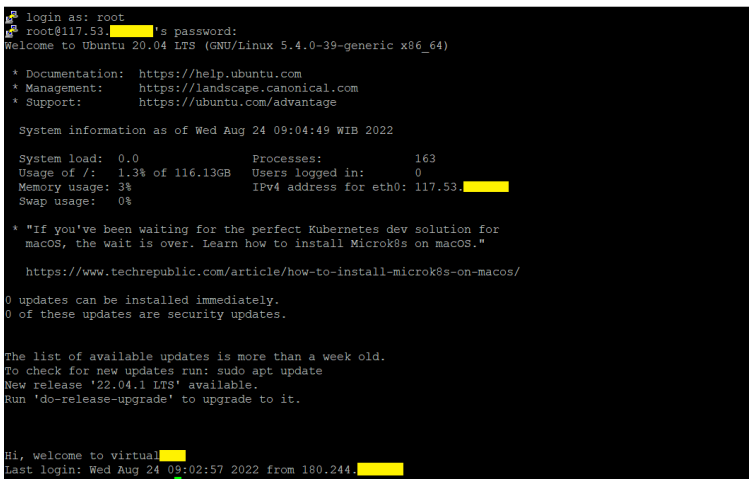
   $ deluser username

   Berikut merupakan tampilan saat dilakukan penghapusan *default user account*:



Gambar 2. Delete User

2. *Remove manufacturers' documentation*
   Berdasarkan pengecekan pada *server* virtualxyz masih ditemukan dokumentasi manufaktur pada saat penginstalan *server*. Pada subbab ini penulis memberikan saran untuk melakukan penghapusan dokumentasi manufaktur pada *server* virtualxyz yang bertujuan untuk mengoptimalkan ruang penyimpanan *server*.
3. *remove all test or sample file from the server*
   Berdasarkan pengecekan yang dilakukan pada *server* virtualxyz masih ditemukan test file baik itu dari penginstalan *server* atau uji *server*. Pada bagian ini penulis memberikan saran untuk melakukan penghapusan test file, termasuk contoh konten, script dan *Executable Code*. Langkah ini dengan tujuan untuk mengoptimalkan kinerja pada *server*, jika tidak dilakukan, dikhawatirkan test file yang masih berada di dalam *server* virtualxyz menyebabkan penuhnya ruang penyimpanan pada *server* sehingga kinerja dari *server* itu sendiri tidak maksimal.
4. *Apply hardening script or security template*
   Pada subbab ini penulis merekomendasikan untuk menerapkan *security template* atau *hardening script* pada *server* virtualxyz, dalam hal ini menggunakan CIS *benchmark* ubuntu. CIS (*Center of Internet Security*) menggunakan proses konsensus untuk menjadi standar dalam menjaga agar sebuah organisasi terlindungi dari serangan [17]. Penerapan CIS ini diharapkan dapat meningkatkan keamanan pada *server software* virtualxyz, sehingga dapat memperkuat *server* jika mendapat serangan dari luar. Dalam melakukan pengamanan dari serangan pada sistem, CIS akan menghapus antara lain:
   a. Program-program yang tidak aman
   b. Menonaktifkan file system yang tidak digunakan
   c. Menonaktifkan port atau layanan yang tidak diperlukan
   d. Mengaudit privileged operations
   e. Membatasi hak administratif
5. *Reconfigure service banner*
   Berdasarkan analisis pada *server* virtualxyz, pada saat *login* melalui ssh masih menampilkan informasi tentang versi dari *server* ataupun OS yang sedang digunakan. Pada subbab ini penulis memberikan saran untuk tidak menampilkan versi dari *server* ataupun OS yang digunakan dengan melakukan konfigurasi pada /etc/ssh/sshd_config. Berikut tampilan login banner sebelum dilakukan konfigurasi:



Gambar 3. Banner Eksisting

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

Berikut merupakan tampilan pada saat setelah *login* ssh setelah dilakukan konfigurasi pada sshd_config:

Gambar 4 Banner Targeting

b. Configuring Access Controls

Dari analisis yang dilakukan pada kondisi eksisting *Configuring Access Controls server* virtualxyz berdasarkan NIST SP 800-123. Terdapat rekomendasi solusi yang penulis usulkan. Adapun penjelasan rekomendasi dari setiap langkah adalah sebagai berikut :

1. *configure service processes to run rootless*

   Berdasarkan analisis kondisi eksisting pada *server* virtualxyz, service proses sebagian masih berjalan sebagai *root*. Pada subbab ini penulis memberikan saran agar *service* proses tidak dijalankan sebagai *root*. Karena untuk meminimalisir apabila terdapat *threat* pada *application layer*, maka *hacker* tidak langsung mendapat akses penuh untuk melakukan operasi pada sisi *server*. Berikut adalah penjelasan setiap service.

   a. Nginx, Untuk menjalankan proses utama sebagai pengguna *non-root*, kita harus mengubah kepemilikan file yang sebelumnya sudah ditentukan mengikuti arahan nginx. Ubah penggunaan portnya diatas port 1024. Masuk sebagai user yang diinginkan dan jalankan nginx dengan nginx -c /path/to/nginx.conf [18].

   b. New relic, menjalankan new relic secara *non-root* membuat new relic dapat mengumpulkan semua metrik yang tersedia seperti yang didokumentasikan untuk infrastructure agent. Pada saat instalasi, infrastructure agent yang dapat dieksekusi berada di (/usr/bin/newrelic-infra) diberikan dua kemampuan linux dengan akses READ untuk sebagian besar metrik *server*:
   CAP_SYS_PTRACE: Memungkinkan pemeriksaan dan penelusuran proses arbiter
   CAP_DAC_READ_SEARCH: Melewati pemeriksaan izin READ file dan direktori [19].

4. KESIMPULAN

Berdasarkan analisis kondisi eksisting *server software* sesuai standar NIST SP 800-123 pada *server* virtualxyz, didapatkan kesimpulan bahwa setelah dilakukan pengecekan pada *server* virtualxyz diperoleh 11 prosedur yang memenuhi standar NIST SP 800-123 dari 17 prosedur yang direkomendasikan untuk diterapkan pada *server* virtualxyz. Dimana pada bagian *Securely Installing the Server Software* terdapat empat prosedur yang sudah diterapkan dari sembilan prosedur yang direkomendasikan, bagian *Configuring Access Controls* terdapat dua prosedur yang sudah diterapkan dari tiga prosedur yang direkomendasikan, bagian *Server Resource Constraints* terdapat terdapat empat prosedur yang sudah diterapkan dari empat prosedur yang direkomendasikan, serta pada bagian *Selecting and Implementing Authentication and Encryption Technologies* telah menerapkan prosedur yang direkomendasikan pada *server* virtualxyz. Sementara dalam meminimalisir serangan pada *server* virtualxyz, proses *Security Hardening* dilakukan hingga mencapai tahap *remediate*. Adapun rekomendasi yang dapat diterapkan pada *server* virtualxyz untuk meminimalisir serangan adalah dengan melakukan *managing default user account, remove manufacturers documentation, remove all test or sample file from the server, apply hardening script or security template, reconfigure service banner, dan configure service processes to run rootless.*

REFERENCES

[1] F. ’Sirait and M. S. K. . ’Putra, “Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan,” *J. Teknol. Elektro, Univ. Mercu Buana*, vol. Vol. 9, no. No. 1, p. 16, 2018.

[2] Yunanri, Riadi, and Yudnana, “Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 300–304, 2016.

[3] A. M. Fanggidae, H. Hermawan, and H. I. Pratiwi, “Sistem Monitoring Server Dengan Menggunakan SNMP,” *Widyakala J.*, vol. 6, no. 2, p. 163, 2019, doi: 10.36262/widyakala.v6i2.218.

[4] Y. S. Aditya, U. Yunan, K. Septo, and M. Fathinuddin, “Pengamanan Data Cloudfri Menggunakan Metode Security Hardening,” vol. 8, no. 5, pp. 9428–9438, 2021.

[5] B. Ahmad and T. Difa, “SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN PROXY SERVER DENGAN METODE ASSESSMENT & HARDENING,” 2020.

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 94−102
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2299

[6] R. S. Perdana, "AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 3, no. 1, pp. 9–14, 2018, doi: 10.32897/infotronik.2018.3.1.2.
[7] A. Laurensius Faleddo Giri Retza, "Security Hardening Dengan Cloud Web Service Untuk Pengamanan Website Berbasis Wordpress," *Univ. Dian Nuswantoro*, pp. 1–10, 2016.
[8] K. Y. LAYUK, *Analisis Keamanan Jaringan Web Server Menggunakan Suricata Pada Sekolah Menengah Pertama Negeri 1 Palopo*. 2021.
[9] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.
[10] D. P. Kuswandono, "TEKNOLOGI VPN (VIRTUAL PRIVATE NETWORK) BERBASIS DI CLOUD VPS (VIRTUAL PRIVATE SERVER) Domo Pranowo Kuswandono dan juga akses jarak jauh . Untuk mengakses jaringan yang ada dirumah dibutuhkan IP public , mudah untuk melakukan koneksi dengan mudah . Me," vol. 8, no. 2, p. 9, 2018.
[11] M. Metode, "Sistem Pendukung Keputusan Dalam Pemilihan Control Panel Virtual Private Server," vol. 5, no. 1, pp. 14–27, 2018.
[12] A. D. Djayali, Muhammad Muzammil, and Abjan Samad, "Implementasi Aplikasi Meeting Online Pada Virtual Private Server di Masa Pandemi," *Simkom*, vol. 6, no. 1, pp. 23–33, 2021, doi: 10.51717/simkom.v6i1.52.
[13] K. Scarfone, M. Tracy, and W. Jansen, "Guide to General Server Security," *NIST Spec. Publ. - 800 Ser.*, p. 53, 2008, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.
[14] D. Desmira and R. Wiryadinata, "Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking," *J. Ilmu Komput. dan Sist. Inf.*, vol. 5, no. 1, pp. 28–33, 2022, doi: 10.55338/jikomsi.v5i1.242.
[15] H. E. Wahanani, "Uji Coba Serangan Man In The Middle Pada Keamanan SSL Protokol HTTP," *J. Sist. Inf. dan Bisnis Cerdas*, vol. 13, no. 1, pp. 21–26, 2020, doi: 10.33005/sibc.v13i1.1769.
[16] W. Agustiara *et al.*, "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Packet Sniffing Pada Website Portal Berita Harian Umum Koran Padang," *J. Tek. Inform. Kaputama*, vol. 6, no. 1, 2022.
[17] ubuntu, "CIS Benchmark on Ubuntu." https://ubuntu.com/security/cis.
[18] F. Farhad, "Running Nginx as non root user," 2017. https://stackoverflow.com/questions/42329261/running-nginx-as-non-root-user.
[19] A. Do Nascimento, "Running the New Relic Infrastructure Agent as a Non-Root User," 2019. https://newrelic.com/blog/how-to-relic/non-root-user-infrastructure-agent.