JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 1, Maret 2023, Pp. 230-241

SECURITY HARDENING SISTEM OPERASI *VIRTUAL PRIVATE SERVER* PADA INSTANSI PENDIDIKAN XYZ BERDASARKAN NIST SP 800-123

M. Alwi Zein*[1)], Umar Yunan Kurnia Septo Hediyanto [2)], Ahmad Almaarif[3)]
1. Universitas Telkom, Bandung, Indonesia
2. Universitas Telkom, Bandung, Indonesia
3. Universitas Telkom, Bandung, Indonesia

Article Info
Kata Kunci: Hardening, NIST, Server

Keywords: Hardening, NIST, Server

Article history:
Received 16 November 2022
Revised 30 November 2022
Accepted 7 Decemeber 2022
Available online 1 March 2023

DOI :
https://doi.org/10.29100/jipi.v8i1.3438

* Corresponding author.
Corresponding Author
E-mail address:
zeinalwi@student.telkomuniversity.ac.id

ABSTRAK
Penggunaan aplikasi berbasis web sudah menjadi bagian penting dalam institusi pendidikan saat ini khususnya perguruan tinggi. Aplikasi berbasis web ini dapat berkembang dengan adanya dukungan hosting server yang menjadi bagian penting dalam penyimpanan data aplikasi berbasis web, menjadikan hosting server sebagai sasaran utama serangan untuk mendapatkan data penting dari aplikasi berbasis web. Serangan pada server saat ini berkembang sangat pesat dikarenakan data-data yang ada pada server bisa disalahgunakan oleh pihak yang tidak bertanggung jawab, metode *security hardening* yang digunakan akan membantu proses keamanan data pada sebuah server. Penelitian ini mengindentifikasi keamanan yang terdapat pada server virtualxyz dan melakukan proses hardening untuk meningkatkan keamanan. Langkah-langkah penelitian ini menggunakan standar NIST SP 800-123 yang bertujuan untuk melakukan *checklist* yang mencakup *update patch*, konfigurasi, keamanan tambahan, dan *testing* pada server, setelah proses pengecekan dilakukan dilanjutkan dengan proses hardening yang bertujuan untuk melakukan pengecekan secara langsung pada server untuk menemukan rokomendasi yang tepat. Objek utama dalam penelitian ini adalah penguatan keamanan pada sistem operasi virtualxyz. Hasil dari pengecekan ditemukan 22 *checklist* yang tidak terpenuhi dari total 29 *checklist* yang ada. Hasil dari proses hardening memberikan rokemendasi yang dilakukan evaluasi terlebih dahulu untuk memastikan rekomendasi sudah tepat untuk meningkatkan keamanan pada server.

ABSTRACT
The use of web-based applications has become an important part of today's educational institutions, especially universities. This web-based application can develop with the support of hosting servers which are an important part of web-based application data storage, making server hosting the main target of attacks to get important data from web-based applications. Attacks on servers are currently growing very rapidly because the data on the server can be misused by irresponsible parties, the security hardening method used will help the process of data security on a server. This study identifies the security contained in the virtualxyz server and performs a hardening process to improve security. The steps of this research use the NIST SP 800-123 standard which aims to carry out a checklist that includes patch updates, configurations, additional security, and testing on the server, after the checking process is carried out, it is continued with the hardening process which aims to check directly on the server for find the right recommendation. The main object of this research is the strengthening of security on the virtualxyz operating system. The results of the checking found 22 checklists that were not fulfilled from a total of 29 existing checklists. The results of the hardening process provide recommendations that are evaluated first to ensure the recommendations are correct to improve server security.

I. PENDAHULUAN

WEB application di Indonesia memiliki perkembangan yang begitu cepat. Web application adalah sebuah program komputer yang dijalankan menggunakan web browser dan diakses melalui internet, hal ini memungkinkan pengguna untuk berinteraksi dengan pemilik web apps seperti contohnya mengisi kolom

komentar, mengisi form, dan juga mendaftar pada web apps tersebut. Salah satu instansi yang membutuhkan web application adalah pendidikan, karena dengan menggunakan web application informasi yang disebarkan menjadi lebih efektif dan efisien.

Pembuatan web application membutuhkan tempat penyimpanan untuk menampilkan content didalamnya. Salah satu tempat penyimpanan yang bisa digunakan adalah server hosting. Server hosting adalah sistem komputer yang memiliki layanan untuk menyimpan berbagai macam data seperti dokumen dan web application. Server hosting dapat dibedakan menjadi shared hosting dan virtual private server. Shared hosting adalah jenis hosting yang digunakan secara bersama. Sedangkan untuk Virtual Private Server adalah jenis hosting yang resourcenya digunakan secara pribadi. Jadi pada dasarnya shared hosting menggunakan server yang yang resourcenya dibagi oleh user lain, dan kelemahan dalam shared hosting ini adalah ketika ada user yang menggunakan resource berlebihan akan memiliki dampak ke user lainnya. Untuk virtual private server, resource yang digunakan hanya oleh satu user.

Perkembangan *web application* menimbulkan sebuah bentuk kejahatan yang biasa disebut dengan kejahatan siber. Kejahatan siber memanfaatkan celah keamanan untuk mengeksploitasi sistem dan mengambil informasi yang ilegal. Badan Siber dan Sandi Negara (BSSN) memaparkan 1.637.973.022 kejahatan siber telah terdeteksi dari 1 januari sampai 31 desember 2021, BSSN mencatat serangan terbanyak adalah malware, denian-of-service(dos), trojan [1].

Salah satu cara meningkatkan keamanan sistem adalah dengan cara melakukan security hardening. Security hardening adalah suatu proses meningkatkan keamanan sistem yang bertujuan untuk mengurangi ancaman dan meningkatkan keamanan sistem[2]. Security hardening memiliki 4 tahapan yaitu access, analyze, remediate dan manage. Pada peneliatian ini proses security hardening hanya akan sampai tahap remediate. Tahapan tersebut diawali dengan access yang berfungsi untuk mengidentifikasi keamanan server. Tahap selanjutnya adalah analyze, tahapan ini memperkirakan tingkat keamanan server dengan memenuhi checklist yang terdapat pada NIST SP 800-123. Pada tahapan terakhir adalah remediate, tahapan ini akan fokus untuk memberikan rekomendasi untuk memenuhi checklist yang belum terpenuhi pada tahapan analyze.

Standar yang digunakan untuk meningkatkan keamanan pada server virtualxyz adalah NIST SP 800-123. Standar NIST (National Institute Standard Technology) adalah standar yang dirancang sebagai perhitungan kualitatif dan berdasarkan analisis sistem keamanan. Publikasi NIST SP 800-123 yang memiliki judul guide to general server security membahas masalah keamanan umum pada server. Penggunaan standar NIST 800-123 diperlukan melihat fokus yang dilakukan pengamanan adalah server dan juga implementasi yang mudah untuk dilakukan dikarenakan NIST 800-123 memberikan list-list apa saja yang akan dilakukan pada server. Pada pemenuhan list yang telah diberikan akan dilakukan pengecekan langsung pada sistem dan wawancara dengan narasumber untuk mendapatkan informasi kondisi eksisting yang terdapat pada server virtualxyz.

Server yang menjadi target percobaan adalah virtualxyz yang dimiliki oleh fakultas XYZ. Virtualxyz merupakan sebuah server yang berisikan kumpulan aplikasi yang digunakan oleh fakultas XYZ, yang didalamnya terdapat beberapa web application seperti menpag.virtualxyz.id, recpag.virtualxyz.id, sap.virtualxyz.id. Pada target percobaan ini akan lebih fokus pada sistem operasi yang digunakan oleh server virtualxyz, peningkatan keamanan pada sistem operasi sangat penting untuk dilakukan, dikarenakan ketika sistem operasi mengalami masalah maka server yang berjalan akan menjadi down.

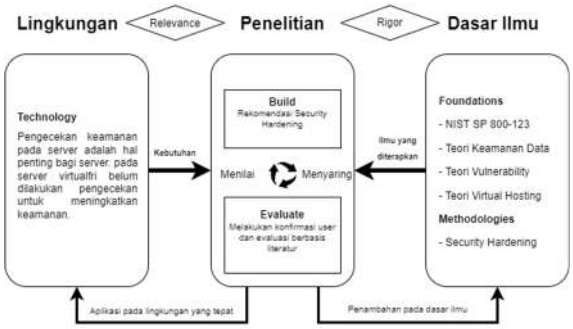
Melakukan security hardening pada sever virtualxyz diperlukan untuk mengurangi ancaman yang bisa muncul dengan mengonfigurasi dan menonaktifkan aplikasi dan layanan yang tidak digunakan. Dengan cara menginstal firewall dan antivirus, membuat password yang aman dan menghapus aplikasi yang tidak dibutuhkan. Tujuan dilakukannya security hardening pada virtualxyz adalah sebelum penelitian ini dilakukan server virtualxyz belum melakukan pengecekan keamanan yang diperlukan, melihat fungsi server virtualxyz adalah tempat penyimpanan data untuk web application yang digunakan oleh seluruh entitas fakultas xyz, maka diperlukannya peningkatan keamanan untuk menghindari kejahatan siber yang bisa saja terjadi.

II. METODOLOGI PENELITIAN

A. *Model Konseptual*

Model konseptual adalah set hubungan antara faktor-faktor tertentu yang mempengaruhi atau mengarah pada suatu keadaan. Model konseptual adalah gambaran yang dilakukan untuk memahami,melaksanakan, dan mengevaluasi penelitian dalam bidang sistem informasi [3].

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 1, Maret 2023, Pp. 230-241

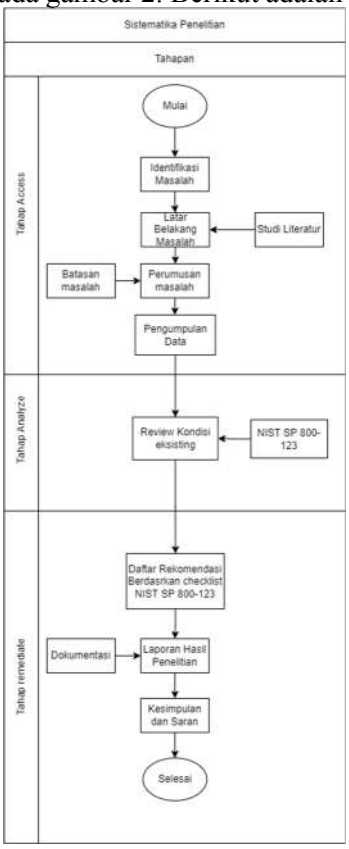


Gambar 1 Model Konseptual

Gambar 1 menunjukan model konseptual yang akan dilakukan oleh peneliti dalam menjalankan aktivitas penelitian pada server virtualxyz. Dimana terdapat 3 ruang lingkup untuk menjalankan aktivitas penelitian yaitu: 1). Lingkungan 2). Penelitian 3). Dasar ilmu.

B. Sistematika Penelitian

Sistematika penelitian ini merupakan bagian yang berisi tentang tahapan-tahapan yang disusun secara terencana dan sistematis. Adapun tahapan yang ada pada sistematika penelitian ini yaitu tahap access, tahap analyze, dan tahap remediate seperti yang ditampilkan pada gambar 2. Berikut adalah sistematika penelitian yang digunakan:



Gambar 2 Sistematika Penelitian

1) Tahap Acces

Pada tahap access dimulai dengan melakukan identifikasi masalah, kemudian dilanjutkan dengan membuat latar belakang masalah yang bertujuan untuk menggambarkan topik masalah yang akan diselesaikan, dengan itu akan ditemukan solusi yang mengacu pada studi literatur. Setelah itu akan didapatkan rumusan masalah yang akan mengacu pada batasan masalah. Batasan masalah bertujuan agar penyusunan penelitian bisa lebih efisien, efektif, dan tidak keluar dari topik permasalah yang diangkat. Serta mengumpulkan data untuk mengetahui kondisi server.

2) Tahap Analyze

Pada tahap hardening yang kedua akan dilakukan tahap Analyze. Tahap ini akan berfokus pada pengecekan kondisi eksiting pada server. Pengecekan ini akan dilakukan dengan memenuhi daftar checklist yang diberikan oleh NIST SP 800- 123, pengecekan ini akan dilakukan dengan pengumpulan data yang telah dilakukan pada tahap access.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 1, Maret 2023, Pp. 230-241

3) Tahap Remediate

Pada tahap selanjutnya yaitu tahap remediate. Tahap ini akan memberikan rekomendasi berdasarkan pengecekan yang telah dilakukan berdasarkan NIST SP 800-123. Pada tahap ini juga akan diberikan dokumentasi berupa checking list yang telah dilakukan pada setiap list yang terdapat pada NIST SP 800-123, dan juga hasil dari penelitian ini akan berupa kesimpulan serta rekomendasi yang akan diberikan kepada developer server virtualxyz.

III. HASIL DAN PEMBAHASAN

A. *Analisis Kondisi Eksisting*

Pada proses ini peneliti melaksanakan pengumpulan data checklist dari wawancara dengan developer yang bertanggung jawab untuk mendapatkan kondisi server yang sedang berjalan, data ini juga dikumpulkan dengan pengecekan ke server untuk melihat langsung kondisi server virtualxyz. Dengan data yang telah dikumpulkan maka identifikasi keamanan pada server akan mudah untuk dilakukan dikarenakan checklist yang sudah disediakan oleh NIST SP 800-123. Kondisi yang diterapkan pada checklist ditandai dengan (V) terpenuhi (X) belum terpenuhi. Pengumpulan data eksisting ini nantinya akan memunculkan rekomendasi-rekomendasi keamanan yang bisa diberikan peneliti untuk developer server virtualxyz. Adapun fokus pengecekan berdasarkan NIST SP 800-123 akan dibagi menjadi 4 subbab. Adapun pembagiannya sebagai berikut:

TABEL I
CHECKLIST NIST SP 800-123

No	Judul	Total checklist
1	Patch and Upgrade Operating System	4
2	Hardening and Securely Configuring the OS	18
3	Install and Configure Additional Security Controls	4
4	Security Testing the Operating System	2

Total pengecekan yang dilakukan untuk memenuhi checklist dari NIST SP 800-123 adalah 28 checklist. Alasan pemilihan checklist ini adalah untuk menyesuaikan dengan kebutuhan yang dimiliki oleh virtual private server. Pemenuhan checklist ini menggunakan metode pengecekan langsung dan tanya jawab narasumber. Pengecekan langsung ini dilakukan untuk memenuhi checklist yang bersifat langsung ke sistem server, sedangkan untuk tanya jawab narasumber dilakukan untuk memenuhi checklist yang bersangkutan dengan dokumen dan protokol apa saja yang telah dilakukan sebelumnya.

B. *Kondisi Eksisting* Patch and Upgrade Operating System

Pada kondisi eksisting ini akan menjelaskan tentang *patch* dan upgrade operating *system* pada dasarnya setelah OS diinstall menerapkan *patch* atau peningkatan yang diperlukan untuk memperbaiki kerentanan yang diketahui adalah penting. Setiap kerentanan yang ditemukan pada OS harus diperbaiki sebelum menggunakannya. Pada pembahasan ini akan dijelaskan tentang *checklist* yang ada serta referensi kondisi *checklist*nya, adapun kondisi *checklist* pada pembahasan ini adalah sebagai berikut:

TABEL II
EKSISTING PATCH AND UPGRADE OPERATING SYSTEM

No	*Checklist*	Referensi	Kondisi *Checklist*
1	*patching process*	Berdasarkan wawancara narasumber belum ada pembuatan dokumen *patching process*	X
2	*Identify vulnerabilities.*	Berdasarkan wawancara narasumber belum dilakukannya identifikasi kerentanan	X
3	*Mitigate vulnerabilities temporarily*	Berdasarkan wawancara narasumber belum dilakukan pengurangan pada kerentanan	X
4	*Install permanent fixes*	Berdasarkan wawancara narasumber belum dilakukannya penginstalan perbaikan permanen	X

1) Patching Process

Pada checklist pertama ini menjelaskan bagaimana pembuatan dokumen patching process, patching process adalah dokumen yang menjelaskan prosedur yang akan dilakukan pada server lebih tepatnya ketika ada kerentanan yang ditemukan atau pembaruan patch.

2) Identify vulnerabilities and applicable patches.

Pada checklist kedua ini akan membahas tentang identifikasi kerentanan dan patch yang berlaku, identifikasi ini dilakukan bisa menggunakan software atau dengan pengecekan langsung pada server.

3) Mitigate vulnerabilities temporarily

Pada checklist ini membahas tentang cara untuk mengurangi kerentanan sementara jika dibutuhkan dan memungkinkan, kerentanan yang ditemukan pada checklist kedua akan dicoba untuk dikurangi dengan melihat kerentanan apa saja yang bisa dilakukan terlebih dahulu.

4) *Install permanent fixes*
Pada checklist terakhir yang ada pada pada bagian ini adalah menginstal permanent fixes dari setiap kerentanan yang ada agar server bisa siap digunakan dan aman dari kerentanankerentanan yang ada yang bisa menyebabkan kerusakan pada server.

C. *Kondisi* Eksisting *Hardening and Securely Configuring the OS*

Pada *checklist* ini akan membahas tentang kondisi eksisting konfigurasi pada sistem operasi yang dibagi menjadi 3 bagian yaitu menghapus service, aplikasi dan protokol jaringan, yang kedua adalah user autentikasi, dan yang terakhir adalah mengatur resource control dengan tepat. Adapun *checklist* yang dilakukan adalah sebagai berikut:

a. *Remove or Disable Unnecessary Services, Applications, and Network Protocols*

TABEL III
EKSISTING REMOVE OR DISABLE SERVICE, APPLICATIONS, AND NETWORK PROTCOLS

No	*Checklist*	Referensi	Kondisi *Checklist*
1	*File and printer sharing services*	Berdasarkan pengecekan *service* tidak ditemukan *File and printer sharing services*	V
2	*Wireless networking services*	Berdasarkan *checking service* tidak ditemukan *Wireless networking services, server* menggunakan koneksi eth0	V
3	*remote access programs*	Berdasarkan pengecekan sistem login menggunakan SSH	X
4	*Directory services*	Pengecekan server tidak ditemukan *directory service* dan langsung pengecekan LDAP tidak terinstall pada *server*	V
5	*Web servers and services*	*Checking server*, nginx adalah *web server* yang digunakan	X
6	*Email services*	Berdasarkan wawancara tidak dibutuhkan *email service* pada server dan berdasarkan pengecekan *service* tidak ditemukan *email service* pada server	V
7	*Language compilers*	Pada pengecekan ditemukan *compiler* pada *server*	X
8	*System development tools*	Berdasarkan pengecekan ditemukan *development tools* yaitu *build-essential*	X
9	*network management tools*	Secara *default* ubuntu menggunakan *systemd-networkd.service* untuk mengatur *network management*	X

1) *File and printer sharing services*
Pada remove aplikasi yang pertama adalah file dan sharing printer service yang digunakan untuk bertukar file pada 2 komputer.
2) *Wireless Networking Services*
Pada penghapusan yang kedua adalah mengenai tentang wireless networking, ini adalah bagaimana server bisa terhubung dengan wifi.
3) Remote Access Programs
Pada checklist ketiga ini membahas tentang remote control dan remote access programs, remote acces program ini digunakan untuk dapat mengakses server dari jarak jauh dengan terhubung ke dalam satu jaringan.
4) *Directory Services*
Pada remove aplikasi yang selanjutnya adalah membahas tentang directory service, directoyi service ini biasa dikenal dengan active directory. Fungsi dari aktif direktori ini adalah menyimpan resource yang dibutuhkan seperti aturan, dan hak akses.
5) *Web Servers and Services*
Pada remove service ini membahas tentang web server, web server memiliki fungsi untuk menerima permintaan HTTP atau HTTPS dari web browser.
6) *Email services*
Selanjutnya adalah email service atau mail server ini adalah program yang mengatur agar email bisa dikirimkan ke user dengan cepat.
   a) *Language Compilers*
   Compiler ini adalah service yang mengubah source code pemrograman menjadi bahasa mesin agar dapat dibaca.
   b) *System Development Tools*
   Sistem ini memiliki hubungan dengan compiler dikarenakan untuk mendapatkan service compiler maka harus menginstall development tools, development tools yang digunakan pada ubuntu adalah build-essential. Build essential berisi paket untuk mengkompilasi.
   c) *Network Management Tools*
   Pada checklist terakhir ini membahas tentang management tools yang dimiliki oleh server.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 1, Maret 2023, Pp. 230-241

7) *Configure OS User Authentication*

TABEL IV
EKSISTING CONFIGURE OS USER AUTHENTICATION

No	*Checklist*	Referensi	Kondisi *Checklist*
1	*Remove or Disable Default Accounts*	Berdasarkan pengecekan login SSH menggunakan root	X
2	*Disable Non-Interactive Accounts*	Didalam pengecekan terdapat user yang sudah tidak digunakan	X
3	*Create the User Groups*	Grup yang dibuat tidak sesuai kebutuhan	X
4	*Create the User Accounts*	User yang dibuat tidak sesuai kebutuhan	X
5	*Configure Automated Time Synchronization*	Berdasarkan pengecekan ditemukan sistem NTP pada server yang secara *default* sudah terpasang pada ubuntu yaitu timedatectl	V
6	*Password Policy*	Berdasarkan wawancara *password* tidak memiliki aturan	X
7	*Prevent Password Guessing*	Pada pengecekan server tidak ditemukan pengaturan *failed attempt* pada *login*	X
8	*Install and Configure Other Security Mechanisms to Strengthen Authentication*	Berdasarkan wawancara tidak ada pengamanan ganda pada server	X

a) *Remove or Disable Unneeded Default Accounts*
Pada checklist pertama dalam konfigurasi user ini adalah menghapus atau menonaktifkan default akun yang tidak digunakan.

b) *Disable Non-Interactive* Accounts
Pada checklist yang kedua ini membahas tentang menghapus non-interactive akun.

c) *Create the User Groups*
Pada checklist create the user group ini membahas tentang bagaimana server memiliki grup yang sesuai dengan kebutuhan yang server.

d) *Create the User Accounts*
Pada checklist selanjutnya ini mengenai tentang user yang akan masuk pada group yang sudah dibuat sesuai kebutuhan.

e) *Configure Automated Time Synchronization*
Pada bagian checklist selanjutnya ini membahas tentang NTP atau network time protocol.

f) *Password Policy*
Password Policy adalah cara untuk mengatur komposisi password yang baik.

g) *Prevent Password Guessing*
Pada checklist ini membahas tentang mengatur failed attempt, failed attempt sendiri adalah ketika user melakukan percobaan login gagal yang terlalu sering maka user akan di disable.

h) *Install and Configure Other Security Mechanisms*
Pada checklist terakhir ini membahas tentang 2FA atau 2 factor authentication, 2FA sendiri berfungsi menjadi keamanan ganda ketika login kedalam password.

8) Configure Resource Controls Appropriately

TABEL V
EKSISTING CONFIGURE RESOURCE CONTORLS APPROPRIATELY

No	*Checklist*	Referensi	Kondisi *Checklist*
1	*Resource Controls*	Berdasarkan pengecekan user yang dibuat tidak diatur *privilegenya* dengan sesuai	X

a) *Resource Controls*
Pada checklist terakhir pada bagian konfigurasi sistem operasi ini membahas tentang mengatur privilege dari setiap user yang sudah dibuat atau yang sudah ada, lebih spesifiknya adalah folder-folder apa saja yang akan diberikan pada user yang ada, pengaturan ini nantinya akan berupa read, write, dan execute.

D. Kondisi Eksisting Install and Configure Additional Security Controls

Pada *checklist* ini membahas tentang bagian ketiga dalam pengecekan *checklist* server, pengecekan kali ini akan fokus pada keamanan tambahan pada server, keamanan tambahan ini bermaksud untuk menjaga server dari serangan-serangan yang merugikan server. Adapun *checklist* pada bagian ini mencakup:

TABEL VI
EKSISTING INSTALL AND CONFIGURE ADDITIONAL CONTROLS

No	*Checklist*	Referensi	Kondisi *Checklist*

1	*Anti-malware software*	Berdasarkan pengecekan dan wawancara tidak ditemukan *anti malware software.*	X
2	*intrusion detection and prevention software (IDPS)*	Berdasarkan wawancara IDPS ini ada pada *provider*, ketika ada ancaman maka akan ada email yang dikirimkan.	V
3	*firewalls*	Pengecekan server status *firewall* adalah active	V
4	*vulnerability management softare*	Berdasarkan pengecekan dan wawancara belum ditemukan *patch management* atau *vulnerability management software* pada server	X

1) Anti-malware software

Pada checklist pertama ini akan berfokus pada anti malware software atau bisa disebut juga anti virus. Anti virus sendiri memberikan perlindungan dan keamanan pada data komputer agar terhindar dari malware.

2) intrusion detection and prevention software (IDPS)

Pada bagian selanjutnya ini akan membahas tentang IDPS, pada dasarnya IDPS ini adalah teknologi yang bertanggung jawab untuk mendeteksi adanya intrusi dan menghentikan intrusi.

3) Host-based firewalls

Pada checklist selanjutnya ini membahas tentang firewall, fungsi dari firewall adalah menjaga jaringan saat terhubung ke internet.

4) Patch management or vulnerability management software

Vulnerability software ini adalah tools yang digunakan untuk mencari celah keamanan yang terdapat pada server, tools ini bisa digunakan dalam waktu tertentu untuk scanning kerentanan.

E. Kondisi *Eksisting Security Testing The Operating System*

Pada bagian akhir *checklist* ini akan berfokus pada security testing yang dilakukan pada sistem operasi, *checklist* ini akan membahas tentang impact yang terjadi pada production server, data-data sensitive pada server, dan bagaimana kesamaan konfigurasi antara production dan non-production server. Adapun *checklist*nya sebagai berikut:

TABEL VII
EKSISTING SECURITY TESTING THE OPERATING SYSTEM

No	*Checklist*	Referensi	Kondisi *Checklist*
1	*The possible impact to the production server*	Berdasarkan wawancara belum dilakukan *test* pada *production server*	X
2	*The presence of sensitive personally identifiable information (PII)*	Berdasarkan wawancara data yang digunakan untuk login di get melalui API igracias telkom	V

1. The possible impact to the production server
   Pada bagian ini akan dilakukan tes yang berdampak pada production server.
2. The presence of sensitive personally identifiable information (PII)
   Pada bagian tes selanjutnya akan melakukan pengujian pada data sensitif, data sensitif ini mencakup informasi-informasi.

F. Analisis Rekomendasi

Pada proses ini peneliti mengumpulkan setiap checklist yang telah dilakukang sebelumnya untuk menemukan rekomendasi yang tepat untuk setiap checklist yang belum terpenuhi pada analisis kondisis eksisting, rekomendasi ini diharapkan dapat menutup celah keamanan yang ditemukan. Proses hardening pada server virtualxyz ini menggunakan checklist yang terdapat pada NIST SP 800-123, checklist ini menentukan guideline apa saja yang harus dilakukan pengecekan. Berdasarkan guideline ini pengecekan akan lebih efisien dan menyeluruh.

1) Patching Process

Pada saat ini fakultas XYZ tidak memiliki dokumen *patching process* yang penting untuk bisa dibuat dan di implementasi untuk keamanan server virtualxyz yang menjalankan aplikasi yang digunakan oleh mahasiswa, karyawan dan dosen untuk melakukan aktivitas, dokumen *patching process* bertujuan untuk menjaga sistem TI dalam kondisi yang baik dan mencegah ancaman dari eksploitasi kerentanan dan menghapus kerentanan sepenuhnya. Pada dokumen *patching process* mencakup [5]:

a) *Reduce Patching-Related Disruptions*
   Instansi berusaha untuk mengurangi jumlah kerentanan dengan cara menggunakan metode dengan memperkuat software yang digunakan seperti contohnya hal ini bisa juga dilakukan dengan menghapus instalan software, fitur, komponen, yang berada dalam server yang tidak digunakan terutama aset yang kritis guna mengurangi privilege pada fungsionalitas server XYZ.
b) *Inventory Your Software and Assets*
   Instansi memelihara inventaris software terkini untuk aset komputasi fisik dan virtual yang digunakan termasuk aset IT dan container docker. Selain itu, memperbarui inventaris secara terus-menerus untuk

semua teknologi dan lingkungan yang digunakan saat ini dengan memerlukan kombinasi teknik dan alat otomatisasi. Dalam penggunaan VPS, organisasi harus memanfaatkan kemampuan inventaris yang dibangun ke dalam platform dan aset misalnya API yang dibangun ke dalam VPS dapat memungkinkan pembaruan terus-menerus dari informasi inventaris untuk software pada platform tersebut, serta karakteristik platform lainnya yang berguna untuk tujuan Patch Management.

c) *Define Risk Response Scenarios*
Instansi harus menentukan skenario respons risiko kerentanan seperti skenario:
- Melakukan patch yang rutin
- Melakukan patch yang darurat
- Melakukan mitigasi patch yang darurat
- Isolasi aset yang tidak di patch

d) Kategori *kerentanan*
Pengkategorian ini dilakukan untuk menentukan prioritas yang harus dilakukan pada dasarnya ini akan dibedakan dengan kategori high, medium, dan low. Dengan kategori ini memudahkan *process patching* yang dilakukan.

e) *Define Maintenance Plans for Each Maintenance Group*
Instansi harus menetapkan rencana pemeliharaan untuk setiap grup pemeliharaan untuk setiap skenario respons risiko yang berlaku. Rencana pemeliharaan mendefinisikan tindakan yang akan diambil ketika skenario terjadi untuk kelompok pemeliharaan, termasuk kerangka waktu untuk memulai dan mengakhiri setiap tindakan, bersama dengan informasi terkait lainnya. Maintenance plans dibagi menjadi sebagai berikut:

1. Maintenance Plans for Scenario 1, Routine Patching Instansi harus mempertimbangkan untuk mengadopsi penerapan bertahap untuk tambalan rutin di mana sebagian kecil aset yang akan ditambal menerima tambalan terlebih dahulu.
2. Maintenance Plans for Scenario 2, Emergency Patching Instansi harus mempertimbangkan untuk menggunakan pendekatan umum yang sama untuk penambalan darurat seperti untuk penambalan rutin, kecuali dengan jadwal yang sangat dipercepat.
3. Maintenance Plans for Scenario 3, Emergency Mitigation Instansi harus merencanakan implementasi cepat dari berbagai jenis mitigasi darurat untuk melindungi aset yang rentan.
4. Maintenance Plans for Scenario 4, Unpatchable Assets Instansi harus merencanakan untuk menerapkan beberapa jenis metode mitigasi risiko jangka panjang selain patch untuk melindungi aset yang rentan. Instansi harus merencanakan untuk menerapkan beberapa jenis metode mitigasi risiko jangka panjang selain patch untuk melindungi aset yang rentan. Instansi harus merencanakan untuk secara berkala mengevaluasi kembali alternatif mereka untuk menambal.
5. Exceptions to Maintenance Plans Instansi harus melacak dan memantau dengan cermat semua pengecualian untuk rencana pemeliharaan.

f) *Choose Actionable Enterprise-Level Patching Metrics*
Organisasi harus memanfaatkan metrik tingkat rendah yang ada untuk mengembangkan tingkat metrik yang mencerminkan kepentingan relatif dari setiap kerentanan dan patch.

g) *Consider Software Maintenance in Procurement*
Organisasi harus mempertimbangkan pemeliharaan software saat pengadaan.

B) Identify Vulnerabilities

Pada saat ini server virtualxyz belum melakukan identifikasi kerentanan dan update patch secara berkala, pada kondisi checklist terlihat identifikasi vulnerability belum dilakukan. Rekomendasi ini adalah bagaimana server bisa mengidentifikasi dari penemuan kerentanan dengan mencari cara untuk mengurangi kerentanan ini nantinya. Pada identifikasi ini peneliti mencoba mengidentifikasi kerentanan yang ada pada server menggunakan nessus. Vulnerabilities ini bisa dikategorikan dengan beberapa threats seperti critical, high, medium. Berikut pengkategorian dari hasil scan nessus:

TABEL VIII
KATEGORI VULNERABILITES

No	Kategori	Deskripsi
1	*Critical*	- *PHP Unsupported Version Detection*
2	*High*	- *DNS Server Spoofed Request Amplification Ddos*
3	*Medium*	- *SSL Certificate cannot be trusted*

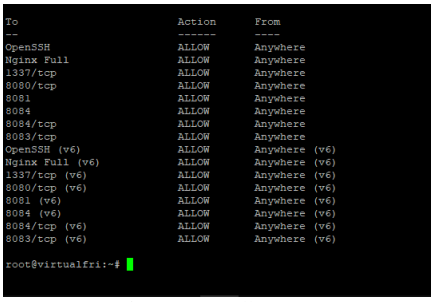
C) Mitigate vulnerabilities temporarly

Pada rekomendasi ini membahas tentang mengurangi kerentanan yang ada pada server dan melakukan penginstalan perbaikan, melihat dari kondisi sebelumnya server virtualxyz belum melakukan identifikasi kerentanan yang ada pada server. Hal yang seharusnya dilakukan adalah dengan melakukan identifikasi, maka akan muncul list-list kerentanan yang ada pada server virtualxyz. List ini akan mempermudah untuk mengurutkan kerentanan apa saja yang bisa diperbaiki terlebih dahulu. Rekomendasi yang bisa dilakukan untuk mengurangi kerentanan sementara ada dengan cara melakukan update patch pada server, Pada sistem ubuntu server virtualxyz terdapat beberapa update yang mencakup service keamanan, terdapat total 87 paket yang bisa di update. Pada hasil ini ditemukan permasalah yang seharusnya update patch bisa dilakukan secara disiplin. Beberapa kerentanan bisa terjadi jika update os tidak dilakukan secara teratur salah satunya adalah munculnya malware atau ransomware.

D) Install Permanent Fixes

Pada subbab ini membahas tentang bagaimana kerentanan yang ditemukan bisa dilakukan penutupan, kerentanan ini memberikan dampak yang berbahaya jika tidak segera dilakukan penutupan beberapa cara yang bisa dilakukan untuk menutup kerentanan berdasarkan identifikasi kerentanan adalah sebagai berikut:

1) *Update* PHP *version web apps*
   Pada checklist terdapat kerentanan pada php version yang digunakan oleh server, pada nessus terdapat juga solusi untuk melakukan update pada version php, berdasarkan pengecekan pada wawancara beberapa web apps pada server virtualxyz menggunakan versi php 5 dan 7. Php sendiri telah merilis versi php terbaru yaitu php 8.
2) *DNS Amplification Ddos*
   Pada rekomendasi ini akan fokus pada pada penggunaan *firewall*, DNS menggunakan UDP untuk mengirimkan permintaan dan tanggapan. Akibatnya, pengguna jahat dapat membuat permintaan DNS palsu dengan sangat mudah, sebagai perlindungan tingkat pertama mekanisme pencegahan *spoof* harus menggunakan *firewall* [6]. Pada saat ini beberapa web apps belum diatur pada *firewall* dan hanya port tertentu yang sudah allow pada *firewall*.



Gambar 3 *Firewall*

3) SSL *certificate*
   Pada dasarnya saat ini SSL certificate yang ada terdeteksi pada nessus tidak bisa dipercaya, untuk solusi yang diberikan oleh nessus adalah dengan membeli sertifikat SSL yang dapat dipercaya, dalam hal ini ada kemungkinan bahwa SSL certificate yang dimiliki sudah expired.

E) Remote Access Programs

Remote access yang digunakan oleh server saat ini adalah secure shell (SSH). SSH adalah aturan yang dijalankan untuk melakukan pertukaran data melalui jaringan yang terjaga keamanannya[7]. Pengaturan ssh ini diatur menggunakan port 22, port ini adalah port default dari ssh yang berbahaya jika tidak diganti dalam pengaturannya, port 22 ini adalah hal yang pertama yang akan hacker lakukan untuk mengakses ssh port.

F) Web servers and Service

Analisis ini juga berdasarkan dari pengaturan sertifikat (secure socket layer). Sertifikat SSL digunakan untuk memastikan terjaganya keamanan data yang dikirim melalui sistem jaringan.[8]. Pengaturan ssl pada server virtualxyz saat ini hanya di beberapa web aplikasi dan belum dilakukan pada semua web aplikasi yang ada pada server dan akan menyebabkan serangan man in the middle (MITM).

G) Language Compiler and System Development Tools

Pada dasarnya compiler dan development tools adalah satu kesatuan yang terinstall secara bersama dimana ketika menginstall development tools pada ubuntu akan langsung menginstall compiler pada server. Development tools yang digunakan pada ubuntu adalah build-essential, build-essential adalah paket meta yang diperlukan untuk

mengkompilasi perangkat lunak, dan didalamnya terdapat GNU debugger, kumpulan compiler g++/GNU, dan library yang diperlukan untuk mengkompilasi sebuah program. Rekomendasi yang peneliti berikan adalah untuk menginstall compilers dan development tools package sebaiknya pada non-production server [9].

H) Remove or Disable Unneeded Default Accounts

Pada srekomendasi ini menjelaskan bagaimana untuk pembatasan akses user root yang biasanya digunakan untuk default login, penggunaan root untuk login melalui ssh ini akan menciptakan celah keamanan pada login server yaitu bagaimana hacker dengan mudahnya untuk masuk ke sistem server yang berjalan, penggunaan root untuk login ini berbahaya dikarenakan akun root adalah superuser yang bisa mengatur semua kondisi server, dengan akses root bisa diakses oleh hacker maka akses server bisa diambil alih dan menciptakan kerugian yang besar. Ada beberapa cara untuk mengatasi permasalahan root user, Adapun cara itu dibagi sebagai berikut [10]:

1) Password root harus aman. Dalam faktanya semua password user harus memiliki keamanan yang bagus.
2) Remote access dilarang digunakan menggunakan root login, login yang dilakukan harus menggunakan user yang sudah ada.
3) User seharusnya tidak banyak menghabiskan waktu menggunakan root user, user harus login menggunakan akun masing-masing dan untuk menggunakan root user bisa mengakses menggunakan su atau sudo.
4) Wajib menginstall service denial program, ini adalah mencegah usaha login dari ip tertentu yang melakukan upaya kegagalan yang terus-menerus.

I) Disable Non-Interactive Accounts

Pada pengecekan kali ini membahas tentang user yang sudah tidak digunakan, pada server virtualxyz ini terdapat beberapa akun yang tidak digunakan dan beberapa akun ini perlu untuk di disable, disable ini bersifat sementara atau permanent tergantung penggunaanya apakah masih diperlukan atau tidak. Saat ini server virtualxyz hanya menggunakan root untuk login ke ssh server dan beberapa user tidak lagi digunakan atau tidak lagi berfungsi, maka dari itu user-user ini akan di disable dengan menggunakan perintah *usermod -s /sbin/nologin username*

J) Create the User Group

Pada rekomendasi kali ini mengenai user group yang terdapat pada server virtualxyz, group yang sudah ada tidak diklasifikasikan sesuai kebutuhan, grup yang ada hanya dibuat untuk testing dan percobaan terdahulu. Dengan adanya beberapa web apps yang di develop oleh server maka diperlukannya grup sesuai dengan web apps yang ada untuk memudahkan pengembangan. Berdasarkan data yang diterima dari narasumber ada 11 web apps yang didevelop oleh server virtualxyz.

K) Create the User Accounts

Setelah pembuatan grup maka pembuatan user diperlukan untuk mengatur isi user dari group yang sudah dibuat, peneliti memberikan rekomendasi untuk user yang dibuat sesuai dengan penanggung jawab dari setiap web apps yang di develop pada server virtualxyz, untuk penanggung jawab dan nama usernya akan dibagi sebagai berikut:

TABEL IX
LIST USER

Penanggung jawab	Nama User
PIC 1	Developer1
PIC 2	Developer2
PIC 3	Developer3
PIC 4	Developer4
PIC 5	Developer5
Admin	Administrator

L) Password Policy

Sebelum penambahan user dilakukan penginstalan pwquality modul terlebih dahulu yang berfungsi untuk mengatur konten atau isi dari password user yang akan dibuat, dengan menggunakan modul ini pengaturan password bisa dilakukan dengan lebih aman seperti panjang password, pengaturan huruf besar dan huruf kecil, penambahan angka dan simbol, dan juga mengatur password tidak ada sangkutannya dengan nama user, dengan ini maka password akan bisa lebih terjaga keamananya. Setelah penginstalan maka akan dilakukan pengaturan untuk password user baru dengan ketentuan sebagai berikut [11] :

1) Panjang password minimal 8 karakter
2) Memiliki minimal 1 huruf besar
3) Memiliki minimal 1 huruf kecil
4) Memiliki minimal 1 angka
5) Memiliki minimal 1 simbol

6) Tidak boleh bersangkutan dengan nama user

M) Configure Computers to Prevent Password Guessing

Pada analisis ini menjelaskan bahwa server sebaiknya dipasangkan tools untuk melakukan pembatasan terhadap ip atau akun yang mencoba login dengan kegagalan yang berulang, saat ini pada server virtualxyz belum diterapkan aturan ini. Peneliti menyarankan untuk melakukan pembatasan login dengan maksimal yaitu 3X kegagalan maka ip yang mencoba login ini akan otomatis terblock, tools yang digunakan adalah fail2ban. Fail2ban (Failtoban) adalah software open source yang bisa digunakan secara gratis, yang di dikembangkan menggunakan menggunakan bahasa pemrograman python, yang bertujuan untuk membatasi akses dan membuat aturan terhadap akses sebuah server [12].

N) Install and Configure Other Security Mechanism

Pada rekomendasi ini membahas tentang authenticator, lebih tepatnya kasus yang ada pada server ini adalah belum adanya two-factor authenticator (2FA). Saat ini server hanya menggunakan ssh key. Dengan adanya *checklist* tentang authenticator ini peneliti memberikan rekomendasi berupa penggunakan 2FA pada server. 2FA adalah sistem otentikasi yang menggabungkan otentikasi pertama dengan factor kedua, performa yang sama dengan berbasis kata sandi. 2FA harus memasukan informasi tambahan dalam bentuk token atai one time password (OTP), token yang diterima bisa didapatkan menggunakan aplikasi pihak ketiga [13]. Pada saat ini 2FA yang bisa digunakan oleh server virtualxyz adalah google authenticator. Sistem 2FA yang ada pada google merupakan suatu sistem OTP (one time password), kode OTP yang diberikan akan melakukan sinkronisasi waktu antara sistem 2FA google dan server[14].

O) Configure Resource Controls Appropiately

Pengecekan ini dilakukan untuk menentukan folder apa saja yang bisa diakses oleh setiap user, dengan adanya list yang telah diberikan maka penentuan privilege bisa dilakukan dengan mudah. User-user ini akan diberikan privilege sesuai dengan web aplikasi yang di develop, dengan privilege ini user yang tidak memiliki kepentingan tidak bisa merubah pengaturan dari setiap web aplikasi yang ada, karena user yang ada hanya bisa merubah web aplikasi yang mereka develop saja. Pada pengaturan privilege ini folder yang akan diatur adalah folder www, karena letak dari setiap web aplikasi terletak pada folder /var/www/. Pengaturan privilege dari setiap user akan dibagi sebagai berikut:

TABLE X
RESOURCE CONTROLS

	Assessment	Ta1	kppm	adm	iris	sap	sofi	rpl	pipe	dms	menta wai
Developer 1	RWX	RWX	RWX	-	-	-	-	-	-	-	-
Developer 2	-	-	-	RWX	RWX	RWX	-	-	-	-	-
Developer 3	RWX	-	-	-	-	-	RWX	RWX	-	-	-
Developer 4	-	-	-	-	-	-	-	-	RWX	RWX	-
Developer 5	-	-	-	-	-	-	-	-	-	-	RWX
Administrator	RWX	RWX	RWX	RWX	RWX	RWX	RWX	RWX	RWX	RWX	RWX

P) Anti-Malware Software

Anti virus pada *linux* sebenarnya memang tidak terlalu dibutuhkan karena beberapa aplikasi yang disimpan pada repositori ubuntu pastinya sudah dicek aman dari virus tetapi tidak menutup kemungkinan malware bisa saja berada pada file-file yang ada pada server, maka dari itu untuk mencegah adanya virus pada setiap file diperlukan adanya antivirus. Anti virus berfungsi untuk meminimalkan kerusakan yang disebabkan oleh malware[15]. Pada analisis ini peneliti memberikan rekomendasi untuk menginstall antivirus clamAV. Clamav bersifat open source dan dapat digunakan dalam berbagai situasi.

Q) Vulnerability Management Software

Pada rekomendasi ini peneliti memberikan rekomendasi untuk menggunakan software *vulnerability* management untuk mencari celah-celah pada server. Rekomendasi yang bisa diberikan adalah menggunakan nessus. Nessus adalah perangkat lunak yang dikelola oleh tenable. Nessus telah menjadi salah satu pemindai kerentanan paling populer, dan faktanya bahwa nessus awalnya merupakan software open source sampai tahun 2005[16].

R) The Possible Impact to the Production Server

Pada rekomendasi ini akan membahas bagaimana testing yang dilakukan akan berdampak pada production server. Maka dari itu peneliti memberikan rekomendasi untuk melakukan penetration testing yang bisa diterima oleh production server. Penetration testing adalah metode untuk mencari kelemahan pada sebuah sistem,

konfigurasi sistem yang kurang baik, dan kelemahan *hardware* dan *software*[17]. Penetration testing dilakukan menggunakan metasploit framework, metasploit framework adalah sebuah tool yang digunakan untuk penetration testing, kelebihannya adalah teknik yang digunakan cukup powerfull untuk melakukan penetrasi ke dalam sebuah sistem[18].

IV. KESIMPULAN

Berdasarkan hasil penelitian dan analisis pada server virtualxyz fakultas XYZ, pada pengujian keamanan menggunakan list NIST SP 800-123 dibagi menjadi 4 bagian checklist, dari total 28 checklist yang dilakukan terdapat 22 checklist yang tidak terpenuhi. Proses security hardening yang dilakukan pada server virtualxyz ini adalah dengan memberikan rekomendasi untuk memenuhi checklist yang terdapat pada NIST SP 800-123, proses ini merupakan tahap untuk melakukan analisis dan memberikan rekomendasi pada celah keamanan yang telah ditemukan pada server virtualxyz.

Dalam keberlanjutan penelitian ini diperlukan validasi dari rekomendasi-rokemendasi yang telah diberikan untuk meminimalkan celah-celah keamanan yang telah ditemukan. Pengecekan dan pembahuruan pada sistem server juga harus diperhatikan melihat tidak ada sistem keamanan yang benar-benar aman dari kerentanan, pengecekan diharapkan bisa dilakukan secara berkala.

DAFTAR PUSTAKA

[1] BSSN, “Laporan Tahunan Monitoring Keamanan Siber Tahun 2021 | bssn.go.id.” 2021. [Online]. Available: https://bssn.go.id/laporan-tahunan-monitoring-keamanan-siber-tahun-2021/

[2] A. Laurensius Faleddo Giri Retza, “Security Hardening Dengan Cloud Web Service Untuk Pengamanan Website Berbasis Wordpress,” *Univ. dian nuswantoro*, pp. 1–10, 2016.

[3] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Q. Manag. Inf. Syst.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[4] F. Sirait and M. K. Sofyan Putra, “Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan,” *Univ. Mercu Buana*, vol. 9, no. 1, p. 16, 2018.

[5] U. of Portsmouth, “Patch anagement,” 2020.

[6] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, “Detecting DNS amplification attacks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5141 LNCS, no. June 2014, pp. 185–196, 2008, doi: 10.1007/978-3-540-89173-4_16.

[7] Desmira and R. Wiryadinata, “Rancang Bangun Keamanan Port Secure Shell (SSH),” *J. Inov. dan Sains Tek. Elektro*, vol. 3, no. 1, pp. 1–5, 2022, [Online]. Available: http://jurnal.bsi.ac.id/index.php/insantek

[8] Sahren, “Implementasi Ssl Untuk Pencegahan Man in the Middle Attack Pada Ftp Server,” *J. Sci. Soc. Res.*, vol. IV, no. 1, pp. 28–33, 2021, [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR

[9] N. Deshpande, S. Joshi, S. Pawar, and A. Parkavi, “Application of C / C ++ Compiler,” *Int. J. Res. Eng. Sci. Manag.*, vol. 2, no. 5, pp. 409–411, 2019, [Online]. Available: www.ijresm.com

[10] J. Bartlett, *Building Scalable PHP Web Applications Using the Cloud*. 2019. doi: 10.1007/978-1-4842-5212-3.

[11] H. Koskinen, “SECURING LINUX SYSTEMS IN AN ADVANCED IOT,” p. 31, 2020.

[12] K. A. Prasetyo, M. Idhom, and H. E. Wahanani, “SISTEM PENCEGAHAN SERANGAN BRUTEFORCE PADA MULTIPLE SERVER DENGAN MENGGUNAKAN FAIL2BAN,” vol. 1, no. 3, pp. 789–796, 2020.

[13] M. C. I. Putri, P. Sukarno, and A. A. Wardana, “Two factor authentication framework based on ethereum blockchain with dapp as token generation system instead of third-party on web application,” *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 6, no. 2, pp. 74–85, 2020, doi: 10.26594/register.v6i2.1932.

[14] H. D. Lie, M. M. Engel, F. T. Informasi, and U. C. Surabaya, “LIBRARY SELF SERVICE SYSTEM USING NFC AND 2FA GOOGLE AUTHENTICATOR SISTEM PEMINJAMAN MANDIRI PERPUSTAKAAN MENGGUNAKAN NFC DAN 2FA GOOGLE AUTHENTICATOR,” vol. 3, no. 3, 2022.

[15] S. H. Han, H. K. Lee, G. Y. Gim, and S. J. Kim, “Empirical Study on Anti-Virus Architecture for Container Platforms,” *IEEE Access*, vol. 8, pp. 134940–134949, 2020, doi: 10.1109/ACCESS.2020.3005591.

[16] M. A. Muin, T. Yusnanto, and I. Managenent, “Campus Website Security Vulnerability Analysis Using Nessus,” *J. IJCIS*, vol. 03, no. 02, pp. 79–82, 2020, [Online]. Available: https://ijcis.net/index.php/ijcis/index

[17] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[18] R. Darman, *Metasploid Pada Android Menggunakan Kali Linux untuk Menyadap Kamera, SMS, dan Kontak Telepon*. 2017. doi: 10.13140/RG.2.2.25589.42722.