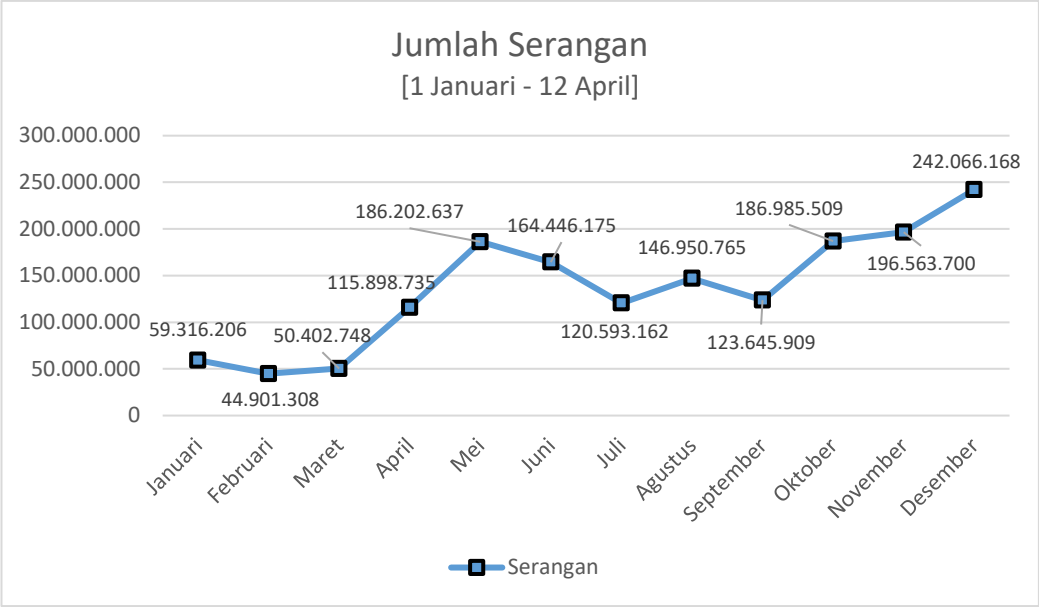
# BAB I PENDAHULUAN

## I.1 Latar Belakang

*Web application* di Indonesia memiliki perkembangan yang begitu cepat. *Web application* adalah sebuah program komputer yang memanfaatkan web browser untuk melakukan tugas-tugas melalui internet, hal ini memungkinkan pengguna untuk berinteraksi dengan pemilik website menggunakan form online, kolom komentar, content management systems, dan lain sebagainya. 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 dipakai secara bersama-sama. Sedangkan untuk *Virtual Private Server* adalah jenis hosting pribadi yang resourcenya dipakai oleh 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 bisa disebut dengan kejahatan siber. Kejahatan siber memanfaatkan kerentanan untuk mengeksploitasi sistem dan mendapatkan akses informasi yang ilegal. Pusat Operasi keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara (BSSN) mencatat 1.637.973.022 kejahatan siber telah terjadi sejak 1 januari hingga 31 desember 2021, BSSN mencatat serangan terbanyak adalah malware, denian-of-service(dos), trojan (BSSN, 2021). Berikut jumlah serangan yang ditunjukan pada Gambar I-1 berikut:




Gambar I-1 Daftar Jumlah Serangan

Salah satu cara meningkatkan keamanan sistem adalah dengan cara melakukan *security hardening*. *Security hardening* adalah suatu proses pengamanan sistem yang bertujuan untuk mengurangi kerentanan dan meningkatkan keamanan sistem terhadap berbagai serangan yang dapat terjadi. (Laurensius Faleddo Giri Retza, 2016). 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 untuk menjadi sesuatu perhitungan kualitatif dan didasarkan pada 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 meminimalkan ancaman yang ada dengan mengatur konfigurasi dan menonaktifkan aplikasi dan layanan yang tidak diperlukan. Dengan cara instalasi *firewall*, antivirus, menghapus *cookie*, membuat *password* dan menghapus program yang tidak diperlukan. Tujuan dilakukannya security hardening pada virtualxyz adalah sebelum penelitian ini dilakukan server virtualxyz belum melakukan pengecekan keamanan yang diperlukan, melihat fungsi server virtualfri 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.

## I.2 Perumusan Masalah

Berdasarkan uraian dari latar belakang di atas, maka rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana hasil identifikasi keamanan sistem operasi pada server *virtualxyz* menggunakan standar NIST SP 800-123?
2. Bagaimana proses identifikasi *security hardening* pada *server virtualxyz*?

## I.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Identifikasi keamanan sistem operasi pada server virtualxyz menggunakan list yang terdapat pada NIST SP 800-123.
2. Identifikasi proses *security hardening* yang akan diterapkan pada server virtualxyz.

## I.4 Batasan Penelitian

Adapun batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya berfokus pada NIST SP 800-123 publikasi juli 2008.
2. Penelitian menggunakan *security hardening* melakukan pemenuhan dari checklist yang disediakan oleh NIST SP 800-123.
3. Penelitian pada server virtualxyz dilakukan sampai tanggal 23 agustus 2022.

## I.5 Manfaat Penelitian

1. Bagi Kampus

   Hasil dari penelitian ini diharapkan dapat memberikan kewaspadaan dalam kehilangan data yang dapat merugikan pihak fakultas, dan meningkatkan keamanan server dari segala kerentanan yang ada pada server virtualxyz.
2. Bagi Masyarakat

   Hasil dari penelitian ini diharapkan dapat menambah pengetahuan tentang pentingnya meningkatkan keamanan pada sebuah sistem dengan menggunakan metode *security hardening* dan untuk menjaga dari kerusakan, perubahan, maupun pencurian data.
3. Bagi Peneliti

   Hasil dari penelitian ini dapat menambah pengetahuan dan pengalaman dibidang keamanan data dan menjadi modal awal peneliti untuk terjun dalam bidang keamanan jaringan.