**STANDAR PENGENDALIAN KEAMANAN WEB SERVER**

**{{nama organisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.1 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| … | … | … |
|  |  |  |

1. **TUJUAN**
   1. Untuk memberikan arahan bagi instansi dalam melakukan pengendalian keamanan Web Server terutama pada proses instalasi dan konfigurasi
   2. Memastikan Web Server yang dimiliki oleh instansi terjaga keamanannya, baik dari aspek Confidentiality, Integrity, maupun Availibility.
2. **RUANG LINGKUP**
   1. Pengendalian Dalam Instalasi & Konfigurasi Sistem Operasi
   2. Pengendalian Dalam Instalasi & Konfigurasi Web Server
   3. Pengendalian Web Bots/Crawler/Spider
3. **ISTILAH DAN DEFINISI**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | *LAN (virtual LAN)* | : | adalah suatu model jaringan yang membagi jaringan secara logikal ke dalam beberapa lan yang berbeda. VLAN tidak terbatas pada kondisi fisik jaringan seperti pada LAN, vlan dikonfigurasi secara virtual tanpa harus melihat kondisi peralatan. Oleh sebab itu, VLAN memiliki fleksibilitas di dalam pengaturan jaringan dan memudahkan administrator jaringan dalam membagi jaringannya  sesuai dengan fungsi dan kebutuhan keamanan jaringan tersebut |
| 2. | *Lightweight Directory Access Protocol [LDAP]* | : | Adalah suatu protocol untuk mengakses directory secara ringan. Disebut ringan karena LDAP menggunakan jaringan internet yang penggunaan paket-paketnya sangat ringan.  LDAP ini merupakan bagian dari Internet Protocol. LDAP ini digunakan untuk mengakses suatu directory misalnya directory telepon, directory email suatu organisasi. Pada LDAP ini tidak hanya membaca informasi, tetapi juga bisa menambah dan mengupdate informasi yang ada directory tersebut.  LDAP juga sudah dilengkapi SASL (Simple Authentication and Security Layer) untuk memerika dan memastikan apakah suatu user berhak dan diperbolehkan masuk atau tidak. Karena itulah LDAP juga banyak digunakan untuk ‘single sign on’, yaitu dengan sekali sign-on, user dapat mengakses berbagai aplikasi yang  telah disediakan |

|  |  |  |  |
| --- | --- | --- | --- |
| 3. | *Karberos* |  | Adalah protokol otentikasi jaringan komputer yang bekerja berdasarkan tiket untuk memungkinkan node berkomunikasi melalui jaringan yang tidak aman untuk membuktikan identitas  mereka satu sama lain secara aman. |
| 4. | *Secure Shell* | : | Adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman dan diberikan akses untuk melakukan perintah dari jarak jauh (remote) antara dua jaringan komputer. SSH ini berfungsi untuk mengakses ke dalam server dari  perangkat apa saja yang mendukung penggunaan SSH ini. |
| 5. | Proxy | : | adalah suatu sistem yang memungkinkan kita untuk bisa  mengakses jaringan internet menggunakan IP yang berbeda dengan yang diterima oleh perangkat. |
| 6. | Instansi | : | Kementerian/Lembaga, Instansi pusat atau daerah. |
| 7. | *Password* | : | Kata sandi yang digunakan bersamaan dengan *username* (*sign on/sign in/log-on/log-in*) oleh pemilik yang sah sebelum melakukan koneksi/akses ke sistem komputer. |

1. **REFERENSI**
   1. Pedoman Keamanan Web Server: Direktorat Jenderal Aptika - Kemkominfo
2. **STANDAR**
   1. **Pengendalian Dalam Instalasi & Konfigurasi Sistem Operasi**
      1. *Patch* dan *Upgrade* Sistem Operasi Web Server
         1. Menjaga server tidak terhubung dengan jaringan lain tapi dengan suatu jaringan terisolasi hingga seluruh *patch* telah dipindahkan ke server melalui alat *out-of-band media* (dalam bentuk CD/DVD)
         2. Menempatkan server dalam suatu *virtual local area network* (VLAN) atau segmen jaringan lain yang sangat membatasi tindakan apa yang dapat dijalankan oleh host pada server tersebut dan komunikasi apa yang dapat mencapai host,yaitu hanya memperbolehkan melakukan patch dan mengkonfigurasi host. Instansi yang berencana menggunakan VLAN harus memastikan bahwa VLAN dikonfigurasi dengan tepat dan setiap perubahan konfigurasi apapun diverifikasi dengan hati- hati.
         3. Melakukan pengujian terhadap patch yang akan diimplementasikan ke Web server dalam suatu sistem lain yang identik dan sudah dikonfigurasi.
      2. Menonaktifkan Layanan dan Aplikasi Yang Tidak Perlu
         1. Web server harus berada pada suatu host satu fungsi (*single purpose host*) yang sudah ditetapkan.
         2. Menginstalasi konfigurasi web server pada pilihan “instalasi minimum” dengan menghilangkan layanan-layanan yang tidak perlu diantaranya:
            * Layanan sharing *file* dan printer sharing, misalnya Windows Network berbasis Input/Output System [NetBIOS] sharing *file* dan printer, Network *File* System [NFS], *File*Transfer Protocol [FTP]
            * Program remote control dan remote access, khususnya bagi yang tidak mengenkripsi jalur komunikasinya (misalnya, Telnet). Jika suatu remote control atau remote acces benar-benar dibutuhkan dan komunikasinya tidak dienkripsi dengan kuat, harus diberi tunnel (saluran) melalui protokol yang menyediakan enkripsi, seperti secure shell (SSH) atau IP Security (IPSec).
            * Layanan direktori,misalnya Lightweight Directory Access Protocol [LDAP], Kerberos, Network Information System [NIS]
            * Layanan email (misalnya Simple Mail Transfer Protocol [SMTP])
            * Language compilers dan libraries
            * Tools pengembang sistem
            * Tool dan utilities manajemen sistem dan jaringan, termasuk Simple Network Management Protocol (SNMP).
      3. Konfigurasi Otentikasi Pengguna Sistem Operasi
         1. Menghapus atau menonaktifkan akun dan grup default yang tidak dibutuhkan atau noninteraktif

Konfigurasi default OS seringkali termasuk akun guest (dengan atau tanpa password), akun level administrator atau root,dan akun yang berkaitan dengan layanan-layanan lokal dan jaringan dimana nama dan password untuk akun-akun tersebut sangat populer. Sangat penting untuk menghilangkan atau menonaktifkan akun yang tidak perlu untuk meminimalisasi penggunaannya oleh penyerang, termasuk guest akun pada komputer yang mengandung informasi sensitif. Jika tidak ada kebutuhan untuk mempertahankan suatu guest atau grup akun, batasi akses dengan ketat dengan mengubah password.. Untuk sistem Unix/Linux, menonaktifkan login shell atau menyediakan suatu login shell dengan fungsi NULL (misalnya /bin/false).

* + - 1. Membuat grup-grup pengguna (cocok untuk jumlah pengguna yang besar) dengan membagi para pengguna kedalam grup-grup yang tepat. Kemudian menetapkan hak untuk grup, sebagaimana yang didokumentasikan dalam rencana distribusi.
      2. Membuat Akun Pengguna―Merencanakan distribusi dengan mengidentifikasikan siapa yang akan diberi wewenang untuk menggunakan setiap komputer dan layanan-layanannya.
      3. Mengecek Kebijakan Password Organisasi―Atur password akunsecara tepat. Kebijakan ini harus mencakup hal-hal berikut:
         * Ukuran―Panjang minimum suatu password. Menetapkan panjang minimum paling sedikit delapan karakter.
         * Kompleksitas―Disyaratkan campuran karakter. Password disyaratkan yang mengandung huruf besar dan huruf kecil dan paling sedikit suatu karakter non-alphabet, dan tidak merupakan kata dari kamus.
         * Durasi Waktu―Seberapa lama suatu passwordboleh tetap tidak berubah. Para pengguna disyaratkan untuk mengubah passwordmereka secara periodik. Password level administrator atau root sebaiknya diubah tiap 30 hingga 120 hari. Periode untuk password level pengguna sebaiknya ditentukan oleh kombinasi panjang dan kompleksitas passworddengan tingkat sensitivitas informasi yang dilindungi.
         * Penggunaan Kembali― Suatu password dimungkinkan untuk digunakan kembali dengan tidak mengizinkan hanya menambah karakter pada password yang telah digunakan, misalnya, password yang asli adalah ”password” diubah menjadi ”Xpassword” atau ”Passwordx”.
         * Otoritas―Pihak yang diijinkan untuk mengubah atau mengatur kembali password dan pembuktian seperti apa yang diperlukan sebelum memulai suatu perubahan.
         * Keamanan Password―Password harus diamankan, seperti halnya tidak menyimpan password yang tidak terenkripsi pada mail server, dan mensyaratkan para administrator untuk menggunakan password yang berbeda untuk akun administrasi email mereka dari akun adminstrasi mereka lainnya.
      4. Mengkonfigurasi komputer untuk mencegah untuk menebak kata sandi (*Password Guessing*)
         * Merupakan hal yang relatif mudah bagi seorang pengguna yang tidak sah untuk mencoba mendapatkan akses ke suatu komputer dengan menggunakan perangkat lunak tool otomatis yang mencoba semua password.
         * Mengkonfigurasi OS untuk meningkatkan periode waktu antara percobaan login dari setiap percobaan yang tidak berhasil.
         * Alternatif lainnya adalah menolak login setelah sejumlah percobaan gagal (misal, tiga). Atau akun dikunci untuk suatu periode waktu tertentu (contohnya 30 menit) atau hingga seorang pengguna dengan otoritas yang tepat mengaktifkannya kembali.
      5. Menginstal dan mengkonfigurasikan mekanisme keamanan lain untuk menguatkan otentikasi

Mempertimbangkan untuk menggunakan mekanisme otentikasi lain seperti *biometric, smart card,* sertifikat *client/server*, atau *sistem one-time password*. Mekanisme ini mungkin lebih sulit dan mahal untuk diimplementasikan, namun mungkin dapat dibenarkan dalam beberapa keadaan. Saat mekanisme otentikasi dan peralatan seperti itu digunakan, kebijakan organisasi harus menyesuaikan. Dimana beberapa kebijakan instansi mungkin perlu mensyaratkan pengggunaan mekanisme otentikasi yang kuat.

* + 1. Instalasi dan konfigurasi kontrol keamanan tambahan
       1. OS seringkali tidak menyertakan seluruh kontrol keamanan yang dibutuhkan untuk mengamankan OS, layanan-layanan, dan aplikasi-aplikasi.
       2. Dalam kasus seperti itu, para administrator perlu memilih, menginstal, dan mengkonfigurasikan perangkat lunak tambahan untuk menyediakan kontrol yang tidak ada.
       3. Kontrol-kontrol yang dibutuhkan secara umum adalah sebagai berikut:
          - Perangkat lunak Anti-malware, seperti perangkat lunak anti-virus, perangkat lunak anti- spyware, dan rootkit detector, untuk melindungi OS lokal terhadap malware, mendeteksi dan memberantas munculnya suatu infeksi.
          - Perangkat lunak pendeteksi dan pencegah penyerangan berbasis host, untuk mendeteksi serangan-serangan yang dijalankan terhadap Web server, termasuk serangan DoS.
          - Firewall berbasis host, untuk melindungi server dari akses yang tidak sah.
          - Perangkat lunak manajemen patch untuk memastikan bahwa kerentanan diatasi secara tepat. Perangkat lunak manajemen patch hanya dapat digunakan untuk mengaplikasikan patch atau juga untuk mengidentifikasi kerentanan baru dalam OS, layanan-layanan, dan aplikasi-aplikasi Web Server.
    2. Konfigurasi *Permission* terhadap file/direktori
       1. OS Web server harus membatasi file-file yang dapat diakses terkait proses-proses layanan Web server dengan memberikan akses read-only (hanya baca) terhadap file-file yang diperlukan untuk melakukan layanan dan tidak memiliki akses terhadap file-file lainnya, seperti file log server.
       2. Memastikan direktori dan file-file diluar struktur file konten web tidak dapat diakses, sekalipun jika para pengguna melakukan browsing langsung dengan cara mengakses URL dari file-file tersebut atau melalui *directory traversal attacks* (serangan lintas direktori) terhadap proses Web server.
  1. **Pengendalian Dalam Instalasi & Konfigurasi Software Web Server**
     1. Pengendalian Instalasi & Konfigurasi
        1. Prinsip dasar instalasi software web server adalah menginstal layanan-layanan yang dibutuhkan Web server dan mengurangi kerentanan apapun yang diketahui.
        2. Aplikasi, layanan, maupun script yang tidak perlu harus dihilangkan segera setelah proses instalasi selesai.
        3. Menginstal perangkat lunak Web server pada dedicated host atau pada Sistem Operasi dedicated guest jika menggunakan virtualisasi.
        4. Menginstal patch atau upgrade perangkat lunak Web Server untuk mengatasi kerentanan yang telah diketahui.
        5. Menyediakan media penyimpanan secara fisik atau partisi secara logic untuk konten Web, yang terpisah dari OS dan aplikasi Web server.
        6. Menghapus atau menonaktifkan layanan-layanan yang diinstall oleh aplikasi Web server namun tidak dibutuhkan, misal gropher, FTP, administrasi remote.
        7. Menghapus atau menonaktifkan semua akun login default yang tidak dibutuhkan, yang tercipta pada saat instalasi Web server.
        8. Menghapus semua dokumentasi manufaktur dari server.
        9. Menghapus semua file contoh atau tes dari server, termasuk script dan executable code.
        10. Menerapkan template keamanan yang sesuai atau script untuk memperkuat keamanan ke server.
        11. Mengkonfigurasikan kembali HTTP service banner (dan yang dibutuhkan lainnya untuk tidak mempublikasikan atau membuat pemberitahuan mengenai tipe dan versi Web server serta OS).
        12. Sebaiknya memberikan nama direktori, lokasi direktori dan nama file yang tidak Standar (umum). Karena banyak tools serangan dan worm yang menjadikan Web server sebagai targetnya, hanya dengan mencari file dan direktori dalam lokasi default.
     2. Pengendalian Akses File/Direktori
        1. Menetapkan access previleges bagi masing-masing individu untuk mengakses file, perangkat dan sumber daya lainnya.
        2. File-file yang secara umum dapat diterapkan kontrol aksesnya, yaitu:
           + File perangkat lunak aplikasi dan konfigurasi
           + File yang berkaitan langsung dengan mekanisme pengamanan:
           + File yang berisi nilai hash password dan file lainnya yang digunakan dalam otentikasi
           + File yang berisi informasi otorisasi yang digunakan untuk mengendalikan akses
           + Material kunci kriptografis yang digunakan dalam layanan konfidensialitas, integritas dan non- repudiasi
           + File log server dan audit sistem
           + File perangkat lunak sistem dan konfigurasi
           + File konten Web
        3. Untuk pengendalian akses file konten web melalui langkah – langkah:
           + Menentukan suatu hard drive atau partisi logik tunggal yang diperuntukkan bagi konten Web dengan membuat subdirektori terkait khusus untuk file konten web, termasuk grafik. Namun tidak memuat script dan program-program lain.
           + Menetapkan suatu pohon direktori tunggal khusus untuk seluruh script atau program eksternal yang dieksekusi sebagai bagian dari konten Web (misalnya, CGI, Active Server Page [ASP], PHP, ..NET, .JSP).
           + Menonaktifkan eksekusi script yang tidak secara khusus berada dibawah kontrol dari akun administratif. Tindakan ini dilakukan dengan pembuatan dan pengontrolan akses terhadap suatu direktori terpisah yang dimaksudkan untuk berisikan script yang sah.
           + Menonaktifkan penggunaan *hard links* atau *symbolic links.*
           + Mendefinisikan suatu matriks akses konten web yang lengkap dengan mengidentifikasi folder dan file dalam dokumen Web server yang harus dibatasi dan oleh siapa.
        4. Pengendalian URI dan Cookies
           + Dilarang menyembunyikan data sensitif seperti username dan password atau sumber daya yang tersembunyi dari server lainnya didalam URI.
           + Cookie tidak mengandung data yang dapat digunakan secara langsung oleh seorang penyerang (misal, nama pengguna, password).
           + Cookie dapat digunakan jika suatu keadaan yang memaksa untuk mengumpulkan data pada situs, dan harus melalui persetujuan, pemberitahuan, dan proteksi keamanan yang baik.
  2. **Pengendalian Web Bots/Crawler/Spider**

Web *bots* (juga dikenal sebagai *crawler* atau *spider*) merupakan aplikasi software yang digunakan untuk mengumpulkan, menganalisis, dan meng-indeks konten Web. Web bots digunakan oleh berbagai organisasi untuk berbagai tujuan.

* + 1. Jenis - jenis Web Bots diantaranya:
       1. MSNBot, Slurp, dan Googlebot dapat menganalisis, meng-indeks, dan mencatat situs Web untuk mesin pencari (search engines) Web seperti halnya Windows Live Search, Yahoo! dan Google.
       2. Mediabot digunakan oleh Google untuk mengAnalisis konten yang disajikan oleh suatu halaman AdSense sehingga iklan - iklan yang relevan secara konteks akan disediakan.
       3. Hyperlink “validator” digunakan oleh Webmaster untuk memvalidasi hyperlink secara otomatis pada situs Web mereka.
       4. Email Siphon dan Cherry Picker merupakan bots yang didesain secara khusus untuk bergerak dengan pelan pada situs Web guna mendapatkan alamat electronic mail(e-mail) untuk ditambahkan pada spam mailing list.
       5. Beberapa spam bots bergerak dengan pelan dalam situs Web untuk mencari formulir login yang digunakan untuk menciptakan alamat email gratis yang merupakan tempat asal pengiriman spam atau untuk spam blog, guestbook, wikis, dan forum - forumuntuk mendorong urutan search engine dari suatu situs Web tertentu.
       6. Screen scrapers mendapatkan kembali konten dari situs Web untuk meletakkan suatu copy pada server lain. Copy-copy tersebut dapat digunakan untuk pishing atau untuk berusaha menghasilkan ad revenue (bayaran dari iklan) dengan membuat para pengguna mengunjungi copy tersebut.
    2. Penanganan Web Bots berupa:
       1. Membuat suatu file teks terang yang bernama ”robots.txt”. File harus selalu memiliki nama ini, dan harus berada dalam direktori dokumen root Web server. Hanya satu file yang diperbolehkan per situs Web. Karena filerobots.txt merupakan salah suatu Standar yang digunakan oleh para pemrogram bot, sehingga bot tak dikenal (seperti EmailSiphon dan Cherry Picker) seringkali mengabaikan file ini. Filerobots.txt merupakan suatu file teks sederhana yang mengandung beberapa kata kunci dan spesifikasi file. Setiap baris file dapat saja kosong atau berisi kata kunci tunggal dan informasi yang terkait. Kata kunci digunakan untuk memberitahu robot bagian mana dari situs Web yang tidak disertakan. Kata kunci yang diperbolehkan antara lain User-agent dan disallow, misalkan untuk disallow suatu bot tertentu (dalam hal ini Googlebot) dari pemeriksaan suatu halaman Web tertentu:

**User-agent:GoogleBot**

**Disallow:tempindex.htm**

* + - 1. Perlindungan password merupakan jalan satu-satunya yang dapat diKitalkan untuk meniadakan noncompliant bots atau para pengguna yang ingin tahu. Seringkali, spambots mengabaikan robots.txt dan mencari alamat email pada situs Web dan/atau format dimana mereka dapat menambahkan konten yang berkaitan dengan spam.
    1. Teknik penanganan untuk mengurangi jumlah spam, yaitu:
       1. Memblokir formulir pengajuan yang menggunakan kata kunci yang berkaitan dengan spam.
       2. Menggunakan kata kunci rel=”nofollow”dalam semua link yang diajukan, yang akan mengakibatkan search engineuntuk menghilangkan link pada algoritma pageranking-nya, yang secara langsung mempengaruhi tujuan dari suatu spambot.
       3. Mensyaratkan pengusul untuk memecahkan suatu Automated Public Turing Test To Tell Computers And Humans Apart (CAPTCHA) sebelum diijinkan mengumpulkan konten.