15 Tips Keamanan server VPS

Keamanan server VPS memerlukan pengaturan lebih lanjut supaya lebih aman. Mencari pengaturan keamanan yang sesuai untuk VPS dengan sistem operasi Linux merupakan tugas yang cukup penting. Salah sedikit saja dapat membuat VPS Anda mudah untuk dibobol dan diakses oleh orang yang tidak bertanggung jawab.

Memperkecil risiko dengan melakukan beberapa usaha kecil dapat membantu Anda memaksimalkan keamanan server VPS. Tidak hanya itu, Anda juga bisa mengembangkan dan memperluas fungsi dari VPS Linux menjadi lebih andal.

Setidaknya ada lebih dari 15+ tips keamanan server VPS yang akan dibahas pada artikel ini, yaitu:

1. Menggunakan SSH untuk masuk ke dalam server
2. Mengubah port untuk login ke SSH
3. Menggunakan password yang rumit
4. Menonaktifkan akun root
5. Menjaga update keamanan terbaru
6. Menghindari mengunduh perangkat lunak kecuali dari sumber yang terpercaya
7. Menonaktifkan port network yang tidak terpakai
8. Menggunakan enkripsi GnuPG
9. Mengkonfigurasi firewall
10. Menggunakan SFTP di samping FTP
11. Membuat folder/boot menjadi read-only
12. Mengaktifkan update otomatis CMS
13. Menginstall anti-malware/antivirus
14. Mengaktifkan cPHulk jika menggunakan WHM
15. Memblokir akses anonymous ke FTP
16. Menginstall rootkit scanner

Berikut masing-masing penjelasannya.

15+ Tips Keamanan Server di VPS

Masing-masing tips keamanan server VPS ini tidak wajib Anda jalankan semua. Anda hanya perlu menyesuaikan dengan environment yang dipakai dalam server dan dibutuhkan oleh aplikasi yang akan dipasang.

1. Menggunakan SSH untuk masuk ke dalam server

Cara yang paling aman untuk login ke server VPS secara remote adalah melalui Secure Shell (SSH). Sebuah network protokol yang dilengkapi dengan enkripsi kriptografi untuk menjalankan service di network. Jadi koneksi menggunakan SSH akan lebih aman dibandingkan menggunakan cara lainnya.

Protokol SSH menawarkan kepada Anda level enkripsi tinggi dan Anda dapat menerima langsung trafik yang tidak aman menjadi lebih aman.

Jadi sejauh ini akses menggunakan SSH ke server merupakan pilihan yang terbaik. Selain ringan, juga lebih aman.

2. Mengubah port untuk login ke SSH
Cara kedua adalah mengubah port untuk login ke SSH. Seperti yang sudah diketahui pada umumnya port default untuk SSH adalah 22. Jadi akan lebih baik Anda mengubahnya sehingga tidak sembarang orang dapat mengetahuinya.

Dengan mengubah port default, orang lain akan kesulitan untuk login tanpa mengetahui port custom yang sudah Anda buat. Selain itu, mengubah port SSH juga dapat mencegah script jahat yang menyerang langsung ke default port.

Jika ingin mengubah port SSH di VPS, Anda hanya perlu mengakses file konfigurasi SSH (/etc/ssh/sshd_config) atau sesuai dengan sistem operasi yang Anda pakai. Kemudian cari baris untuk mengatur port dan Anda dapat mengubahnya sesuai dengan port yang Anda inginkan.

Namun, pastikan jika port yang Anda pakai tidak bertabrakan dengan aplikasi lain karena menggunakan port yang sama. Jika di dalam satu sistem terdapat dua aplikasi yang sama bisa menimbulkan error di **VPS Hosting**.

3. Menggunakan password yang rumit
Password yang lemah atau asal-asalan bisa menjadi sebuah mimpi buruk.
Sebab **password** merupakan ancaman terbesar dalam dunia keamanan online. Jadi jangan sampai menggunakan password yang mudah ditebak, misalnya ‘abcde’, ‘indonesia’. ‘revolusi’, dan semacamnya.
Anda dapat meningkatkan sistem keamanan menggunakan password yang terdiri dari kombinasi huruf kecil dan huruf kapital. Selain itu, untuk menghindari kata yang ada di kamus sebaiknya tambahkan juga angka dan simbol ke dalam password.

Anda juga dapat menambahkan *password aging* atau notifikasi secara otomatis ke user untuk mengganti passwordnya secara berkala.
Tidak kalah penting, Anda juga harus mengaktifkan sistem blokir ke user yang melakukan kesalahan login berulang kali. Hal ini untuk mengantisipasi ancaman brute force yang bisa jadi menyerang server.

4. Menonaktifkan akun root
Selain mengganti port SSH, salah satu hal yang penting sebelum melakukan release server adalah menonaktifkan akun root. Sebab akun root mempunyai akses yang cukup luas dan bebas membuka apa saja di dalam sistem.

Tentunya ini menjadi hal yang cukup berbahaya apabila ada pengguna yang bisa mengakses root tanpa sepengetahuan admin sistem.

Anda disarankan untuk membuat akun user yang unik untuk setiap layanan yang berjalan di dalam Linux VPS. Kemudian setiap user yang Anda buat harus menyertakan permission untuk melakukan tugasnya saja.

Selain akses ke dalam tugas mereka, user tidak diperkenankan untuk mengakses bagian lainnya. Jadi hal ini dapat meminimalisir kesalahan yang dilakukan oleh salah satu user dan mengakibatkan kerusakan pada sistem secara menyeluruh.

Terakhir, Anda juga harus menonaktifkan seluruh akun user yang sudah tidak diperlukan atau sudah tidak mempunyai tugas di dalam sistem.

5. Menjaga update keamanan terbaru
Hacker dapat dengan mudah mencari informasi dan potensi backdoor maupun lubang keamanan di berbagai macam perangkat lunak.

Pengembang dan ahli keamanan melakukan pembaruan keamanan untuk menanggulangi penerapan keamanan yang salah.

Kami menyarankan Anda untuk melakukan pengecekan pembaruan perangkat lunak paling tidak seminggu sekali. Jadi ketika ada pembaruan perangkat Anda bisa langsung memprosesnya sehingga server lebih aman.

Rilis major Linux tersedia di penyimpanan repository dan mailing list. Hal ini membuat Anda dengan mudah mengunduh dan menginstall hanya *patches* keamanan yang dibutuhkan saja.

6. Menghindari mengunduh perangkat lunak kecuali dari sumber yang terpercaya
Terkadang perangkat yang dibutuhkan tidak tersedia di dalam server sehingga Anda harus menginstall dari luar. Namun Anda perlu berhati-hati karena mengambil file instalasi dari sumber yang tidak terpercaya sangat berbahaya.

Jika Anda menginginkan perangkat lunak yang cukup spesifik dan Anda cukup familiar dengan *source code* yang disediakan, Anda bisa memprosesnya. Sebaliknya, jika terdapat risiko perangkat lunak dapat merusak sistem, sebaiknya Anda mengurungkan niat untuk meng-installnya.

7. Menonaktifkan port network yang tidak terpakai
Salah satu tips mengamankan server VPS lainnya adalah menonaktifkan port yang tidak terpakai di server. Port jaringan yang terbuka dan tidak dipakai oleh sistem dapat dengan mudah menjadi target hacker.

Maka dari itu, Anda perlu menonaktifkan port tersebut supaya dapat memproteksi server dari serangan.

Gunakan aplikasi semacam perintah ‘netstat’ untuk melihat daftar port yang saat ini terbuka dan *services* yang berhubungan. Anda juga perlu mempertimbangkan untuk menggunakan ‘iptables’ supaya dapat menutup port yang terbuka menggunakan ‘chkconfig’ untuk menonaktifkan layanan yang tidak diinginkan.
Jika menggunakan firewall seperti CSF atau semacamnya, Anda bisa mengoptimalkan potensi dari pemanfaatan aturan di iptables.

8. Menggunakan enkripsi GnuPG
Hacker terkadang menargetkan data yang sedang dipertukarkan dalam jaringan. Inilah alasan mengapa sangat perlu mengenkripsi setiap transmisi password, keys, dan sertifikat selama proses pertukaran data.

Salah satu tool yang cukup populer dalam menjalankan tugas ini adalah GnuPG, sebuah sistem otentikasi berbasis kunci yang dipakai untuk mengenkripsi setiap komunikasi. Tool ini menggunakan kunci publik (*public key*) yang hanya bisa dibongkar menggunakan kunci privat (*private key*) yang dimiliki oleh penerima.
9. Konfigurasi firewall
Salah satu hal penting yang perlu Anda lakukan untuk mengamankan server adalah melakukan konfigurasi firewall.

Anda harus mengatur server untuk menggunakan beberapa aturan penggunaan port. Meskipun begitu, ada beberapa layanan (*services*) yang memerlukan beberapa port harus aktif sehingga layanan dapat berjalan.
Jadi aturan firewall Anda sehingga bisa mengarahkan setiap aplikasi atau program dapat menggunakan port tertentu tanpa harus mengganggu layanan lainnya.

Dengan begitu, pengaturan ini memungkinkan Anda untuk menghindari berbagai macam pelanggaran keamanan dan pengoptimalan dari sistem yang Anda gunakan.

10. Menggunakan SFTP di samping FTP
Salah satu aplikasi pertukaran data yang sering dipakai adalah File Transfer Protocol (FTP). Aplikasi sudah sejak lama dipakai untuk mengirimkan dan mengambil dari dua remote sistem. Tidak main-main, aplikasi ini sudah dipakai sejak tahun 1985 dan ternyata sekarang sudah tidak cukup aman.

Setiap aplikasi membutuhkan otentikasi untuk mengirimkan plain-text. Oleh karena itu, hacker dapat belajar dan membaca *detail* log antara Linux VPS dan client di komputer lokal.

Namun, tidak perlu khawatir karena ada pengembangan dari FTP yaitu SFTP. Anda dapat menggunakan SFTP secara gratis karena merupakan bagian dari aplikasi SSH yang tersedia di server.

Meskipun secara garis besar tugas SFTP sama dengan FTP, SFTP menggunakan dasar protokol yang terenkripsi sehingga pertukaran data lebih aman.

11. Membuat folder /boot menjadi read-only

Salah satu upaya supaya folder tidak dapat dibaca oleh sembarang orang adalah membuatnya read-only. Hal ini berlaku di pengaturan folder "/boot" dalam sistem Linux.

Namun, default level akses dari direktori "/boot" adalah "read-write". Jadi untuk mengantisipasi hal semacam ini, Anda perlu modifikasi file di dalam folder tersebut. Hal ini cukup penting supaya server Anda dapat berjalan dengan aman dan nyaman.

Untuk melakukan ini, Anda hanya perlul mengedit file di dalam "/edit/fstab" dan menambahkan "*LABEL=/boot /boot ext2 default, ro 1 2*" di bagian bawah.
Atau, jika memungkinkan Anda dapat membuat beberapa pengubahan dalam kernel untuk jangka panjangnya.

Jadi melalui proses ini Anda dapat dengan mudah mengembalikan pengaturan ke mode default 'read-write'. Kemudian Anda dapat membuatnya menjadi 'read only' ketika Anda sudah berhasil mengubahnya.

12. Mengaktifkan update otomatis CMS

Hacker selalu mencari lubang keamanan di dalam perangkat lunak, khususnya di website yang menggunakan Content Management System (CMS). Contohnya saja beberapa CMS yang cukup terkenal termasuk Joomla, WordPress, dan Drupal.
Karena banyaknya serangan hacker yang sering mencari celah keamanan CMS, kebanyakan dari CMS terus melakukan update supaya hacker tidak dapat menembus keamanan website.

Oleh karena itu, memperbarui versi CMS yang dipakai secara berkala adalah hal wajib. Anda juga dapat mengatur update secara otomatis. Dengan begitu, Anda tidak akan lupa untuk meng-update CMS yang Anda gunakan bahkan ketika Anda sedang sibuk.

13. Menginstall anti-malware/antivirus

Salah satu tujuan dari adanya firewall adalah mencegah akses dari sumber trafik yang berbahaya. Cara ini cukup efektif untuk dijadikan layer di garis depan keamanan server.

Ada banyak berita server tidak dipasangi firewall yang mumpuni dan ini adalah sebuah kesalahan. Alasan yang paling umum adalah karena tidak ingin mengeluarkan biaya yang lebih untuk membeli perangkat lunak anti-malware/antivirus.

Pemahaman seperti di atas tentu perlu diluruskan kembali. Membeli antivirus adalah sebuah langkah preventif terhadap serangan online. Biaya yang Anda keluarkan untuk membeli antivirus tentu jauh lebih murah daripada server Anda dibobol orang yang tidak bertanggung jawab.

14. Mengaktifkan cPHulk jika menggunakan WHM
Jika Anda menggunakan WHM, biasanya di dalamnya sudah tersedia cPHulk. Ini merupakan add on yang cukup terkenal untuk mengatur firewall di dalam server website.

Firewall memang cukup aman, tapi mengandalkan satu lapis keamanan saja terkadang belum cukup. Sebab banyak sekali tipe serangan yang dapat masuk ke dalam server.

Nah, salah satu kelebihan dari cPHulk adalah kemampuannya untuk mengatasi ancaman serangan brute force.

cPHulk berperan layaknya pertahanan keamanan kedua. Mengantisipasi serangan brute force yang secara berulang mencoba melakukan login secara acak ke dalam server.

15. Memblokir akses anonymous ke FTP
Jika Anda mempunyai server baru dan menginstall FTP server, terkadang user yang tidak dikenal dapat dengan mudah mengaksesnya. Jadi Anda perlu menonaktifkannya terlebih dahulu.

Bagi Anda yang menggunakan cPanel atau Plesk tenang saja karena fitur ini sudah dinonaktifkan sehingga user asing tidak dapat mengakses dan mengunggah file.

Mengizinkan user tidak dikenal supaya bisa mengupload file ke server menggunakan FTP sangat berbahaya. Sebab setiap orang dapat dengan mudah mengunggah apa saja ke dalam server. Jadi sangat tidak direkomendasikan.

16. Menginstall rootkit scanner
Rootkit merupakan salah satu pengaturan yang berada di bawah sistem operasi (OS), di bawah perangkat lunak, dan aktivitasnya hampir tidak terdeteksi oleh server.

Beruntungnya, Anda dapat menggunakan tool yang bernama **‘chrootkit’**. Tool ini dapat mencari informasi server mana yang sudah terinfeksi. Akan tetapi, rootkit bukanlah masalah yang dapat dengan mudah dihapus. Dan cara yang paling mudah untuk mengatasi permasalah ini adalah melakukan reinstall sistem operasi.

Penutup: Keamanan Server VPS Itu Penting!
Itulah tadi beberapa tips keamanan server VPS yang dapat Anda terapkan di server. Sekali lagi, seluruh tips di atas tidak perlu Anda terapkan semuanya. Cukup pilih beberapa saja sesuai dengan kebutuhan server.

Setidaknya ada beberapa tips yang cukup penting di dalam mengamankan server, yaitu menggunakan firewall, mengganti port default, menonaktifkan port yang tidak terpakai, dan menggunakan koneksi SSH yang lebih aman.

Jangan lupa subscribe untuk mendapatkan informasi terbaru mengenai dunia teknologi, bisnis, dan digital marketing dari kami. Silakan tinggalkan komentar melalui kolom di bawah ini jika Anda masih mempunyai pertanyaan atau tips lain yang mungkin lebih lengkap.

DAFTAR PUSTAKA

Yasin K . 2021. 15+ Tips Keamanan Server VPS. Diakses pada tanggal 25 Januari 2021. Dari laman https://www.niagahoster.co.id/blog/keamanan-server-vps/?amp=1