Keamanan Sistem dan Jaringan

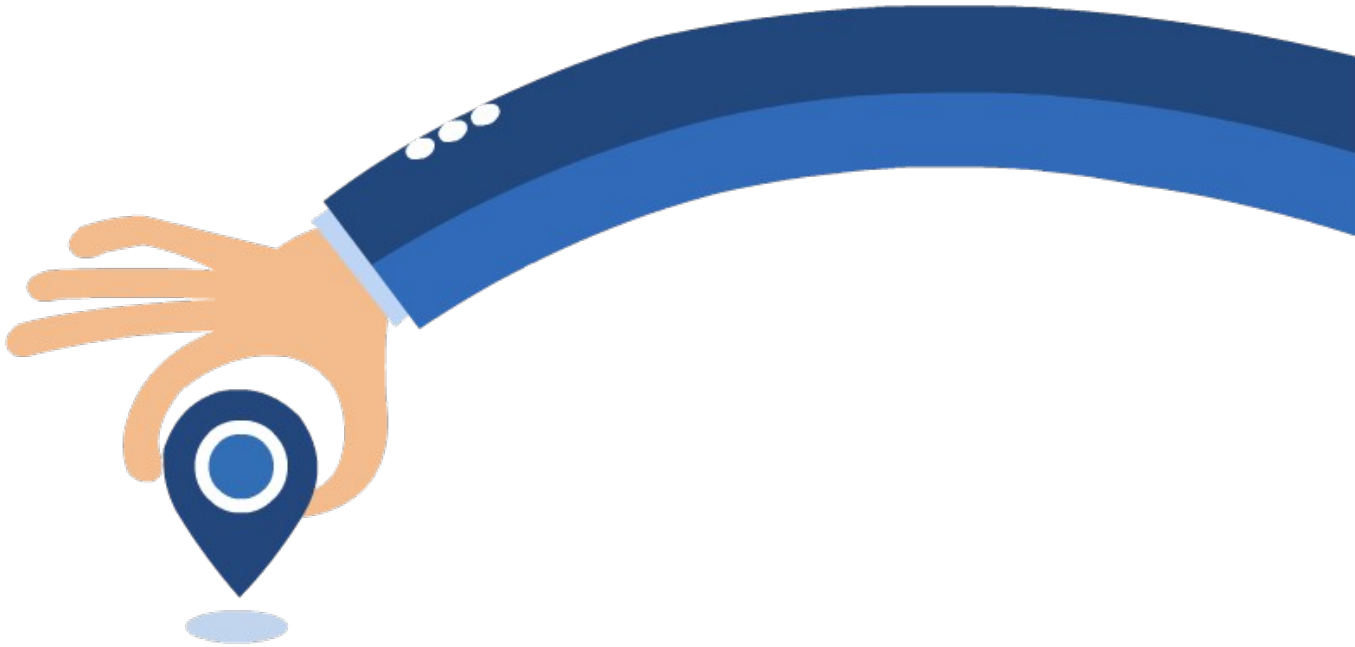
Pertemuan ke-1 dan ke-2

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id 021 7788 6691 info@petik.or.id

Keamanan Server Linux Ubuntu

Pengamanan Boot Loader

- Boot loader yang tidak diamankan memungkinkan user untuk masuk ke dalam sistem Linux Ubuntu sebagai single user (runlevel 1)
- Boot Loader yang digunakan di Linux Ubuntu adalah GRUB 2.
- GRUB 2 dapat menerapkan password untuk masuk ke dalam menunya.
- Password dapat diterapkan baik untuk seluruh menu maupun menu entri tertentu.
- Password dapat berupa teks biasa ataupun teks yang terenkripsi.

Mencegah masuk single user tanpa password

- Hindari penggunaan single user oleh user yang tidak berhak untuk mencegah hal-hal yang tidak diinginkan.
- Pada Linux Ubuntu, agar ketika akan masuk ke single user harus memasukkan password root terlebih dahulu maka caranya cukup dengan memberikan password ke user root.

Konfigurasi Otentikasi

- Setiap user yang akan mengakses sistem Linux harus mempunyai *account* (username dan password).
- User yang terdaftar pada sistem Linux disimpan di file /etc/passwd.
- Sayangnya file ini sifatnya dapat dibaca oleh semua user padahal di dalamnya terdapat informasi mengenai password user meskipun dalam format terenkripsi.

Konfigurasi Otentikasi

- Untuk mengamankannya, password user disimpan terpisah dalam file /etc/shadow.
- Pada sistem Linux sekarang ini umumnya sudah menerapkan shadow password secara default.
- Ciri sistem Linux yang sudah menggunakan shadow password adalah kolom password (kolom kedua) pada file /etc/passwd berisi karakter "*" atau "x" dan terdapat file yang bernama /etc/shadow.

Menerapkan Strong Password

- Password adalah kata kunci yang digunakan untuk proses otentikasi ketika masuk ke dalam sistem.
- Hindari membuat password yang mudah ditebak orang lain sehingga dapat disalahgunakan.
- Sistem Linux mempunyai fasilitas untuk menerapkan strong password dengan menggunakan PAM module pam_cracklib.so.

Membatasi Terminal Login untuk root

- Untuk meningkatkan keamanan sistem linux ada baiknya kita membatasi terminal yang boleh digunakan untuk login sebagai root.
- Jika paranoid kita bisa saja melarang user root login secara langsung dari terminal manapun.
- File /etc/securetty digunakan untuk mengatur terminal mana saja yg boleh digunakan oleh root untuk login.

Membatasi user yg boleh menjalankan perintah su

- Perintah su digunakan untuk melakukan proses substitusi user atau switch user atau menjalankan shell dengan berganti menjadi user lain.
- Untuk meningkatkan keamanan kita dapat membatasi user siapa saja yang boleh dan dapat menjalankan perintah su.
- File /etc/pam.d/su digunakan untuk mengatur user-user siapa saja yang boleh menjalankan perintah su.

Menggunakan sudo

- Untuk mengurangi resiko keamanan sistem biasakan tidak login menggunakan *account* root secara langsung.
- Agar lebih aman gunakan perintah su atau sudo.
- Dengan sudo sistem dapat memberikan privilege kepada user-user tertentu untuk menjalankan atau mengeksekusi perintah-perintah yang hanya dapat dijalankan oleh user root.

Menggunakan sudo

- File /etc/sudoers digunakan untuk mengatur user-user siapa saja yang boleh menjalankan perintah dengan privilege superuser.
- File /etc/sudoers sebaiknya tidak diedit secara langsung tetapi dengan menggunakan perintah visudo.

Mendisable Ctrl+Alt+Del

- Secara default sistem Linux Ubuntu membolehkan user untuk merestart sistem dengan cara menekan tombol Ctrl+Alt+Del dari console.
- Untuk alasan keamanan, sebaiknya fitur restart sistem melalui penekanan tombol Ctrl+Alt+Del dari console dinonaktifkan.

Setting Login Time Out (TMOUT)

- Untuk menghindari resiko keamanan, hindarkan meninggalkan terminal dalam keadaan login.
- Terminal yang dibiarkan tanpa aktifitas dapat dibuat logout secara otomatis.
- Caranya dengan mengatur nilai variabel shell TMOUT.

Memanfaatkan Advanced Filesystem Attributes

- Filesystem Linux menyediakan keamanan tambahan untuk file selain permission standar r, w dan x yaitu Advanced Filesystem Attributes.
- Keamanan tambahan ini diantaranya append only dan immutable.
- Untuk melihat atribut file gunakan perintah lsattr.
- Untuk mengubah atribut file gunakan perintah chattr.

Menerapkan quota filesystem

- Pada sistem multiuser seperti Linux, sebaiknya setiap user diberikan batasan penggunaan space disk pada masing-masing home directory-nya.
- Hal ini untuk mencegah eksploitasi ruang hard disk yang menyebabkan habisnya space disk untuk sistem Linux itu sendiri dan dapat mengakibatkan crash atau tidak berjalannya service tertentu pada sistem Linux Anda.

Menerapkan quota filesystem

- Linux menyediakan fitur quota filesystem untuk membatasi penggunaan space disk per user.
- soft limit : batas bawah, batas masih bisa dilewati tetapi grace period akan mulai berjalan.
- hard limit : batas atas, dimana tidak bisa dilewati. Bila hard limit tidak ada maka soft limit menjadi hard limit.
- grace period adalah lama waktu soft limit dapat dilewati.

Menerapkan "Resource Limits"

- Penggunaan sumber daya sistem untuk user-user sistem Linux dapat dikontrol dan dibatasi.
- Hal ini untuk mencegah aksi serangan denial of service yang dapat mengkonsumsi jumlah memori dan proses secara berlebihan.
- Caranya dengan mengatur konfigurasi file /etc/security/limits.conf.

Membatasi akses Shell

- Demi keamanan kita bisa membatasi environment shell yang digunakan oleh user.
- Sehingga user hanya dapat menjalankan perintah-perintah yang sudah ditentukan saja.
- Untuk keperluan tersebut kita harus menggunakan shell khusus diantaranya ibsh (Iron Bars Shell) dan rssh (Restricted Shell) atau restricted bash (rbash).

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id