#UpgradeYourSkills
UpgradeYourLive

ID-Networkers
Indonesian IT Expert Factory

Noctra Lupra

Materi Minggu 2 sesi 2

Start With Us

materi

- firewall (ufw)
- patch management
- access control

Firewall

outline

- Perintah Dasar UFW (Uncomplicated Firewall)
- Study Case: Mengamankan Server Web

install & cek status UFW

install ufw

- sudo apt update
- sudo apt install ufw

cek status

- sudo ufw status verbose

default rules

- sudo ufw default allow outgoing
- sudo ufw default deny incoming

allow koneksi penting

allow ssh

- sudo ufw allow ssh
- sudo ufw allow 22/tcp

allow ssh from specific ip

- sudo ufw allow from 192.168.1.100 to any port 22 comment 'Allow SSH from admin IP'

allow koneksi penting

allow http/https

- sudo ufw allow http
- sudo ufw allow https
- sudo ufw allow 80/tcp
- sudo ufw allow 443/tcp

delete, activate, reset

delete rule

- sudo ufw delete allow 80/tcp
- sudo ufw delete allow from 192.168.1.100 to any port 22

mengaktifkan rule

- sudo ufw enable

reset ufw

- sudo ufw reset

Study Case:
mengamankan server web

delete, activate, reset

Skenario: saya punya server Linux yang berfungsi sebagai server web:

- Server menerima koneksi SSH (*port* 22) dan HTTP (*port* 80) dari mana saja.
- Semua koneksi lain harus ditolak.
- Koneksi keluar dari server bebas (semua *outbound traffic* diizinkan).

penyelesaian dengan ufw

Set Default Policy:

- sudo ufw default deny incoming
- sudo ufw default allow outgoing

1. **Allow Koneksi yang Dibutuhkan**:
   - sudo ufw allow 22/tcp
   - sudo ufw allow 80/tcp
2. **Aktifkan UFW**:
   - sudo ufw enable
3. **Cek Hasil Konfigurasi**:
   - sudo ufw status verbose

patch management

patch management

Proses mengelola pembaruan (patch) untuk perangkat lunak dan sistem operasi yang sudah terpasang.

mendapatkan informasi terbaru

- sudo apt update

upgrade dependency

- sudo apt upgrade

upgrade dependency lebih agresif

- sudo apt full-upgrade

access control

memberi akses root menggunakan sudo

memberikan akses sudo tanpa password:

- username ALL=(ALL) NOPASSWD: ALL

membatasi perintah sudo untuk group:

- %devops ALL=(ALL) NOPASSWD: /usr/bin/systemctl restart apache2

membatasi perintah sudo untuk perintah spesifik

- bob ALL=(ALL) /usr/bin/apt update, /usr/bin/apt upgrade

melihat daftar perintah yang diizinkan user saat ini

- sudo -l

mengubah permission file/folder

menggunakan simbol

- u: user (*owner*)
- g: *group*
- o: *others*
- a: *all* (u+g+o)
- +: Tambahkan izin
- -: Hapus izin
- =: Atur izin secara eksplisit

menggunakan angka

- 4 = read (r)
- 2 = write (w)
- 1 = execute (x)
- owner, group, other

menggunakan simbol

- chmod u+rwx file.txt: Jadikan *file* bisa dibaca, ditulis, dan dieksekusi oleh *owner*.
- chmod g-w file.txt: Hapus izin tulis untuk *group*.
- chmod o-rwx file.txt: Hapus semua izin untuk *others*.
- chmod a+r,u+w file.txt: Semua bisa baca, dan *owner* juga bisa tulis.
- chmod g=rw file.txt: Atur izin *group* menjadi *read* dan *write* (hapus yang lain).
- chmod +x script.sh: Menambahkan izin eksekusi untuk semua kategori (*owner, group, others*). Umum untuk membuat skrip dapat dijalankan.

menggunakan angka

- chmod 644 file.txt
- chmod 755 script.sh
- chmod 700 private_dir

mengubah owner & group

memberikan akses sudo tanpa password:

- Sudo chown [owner]:[group] [file_or_folder]
- sudo chown rafly file.txt: Mengubah pemilik *file* menjadi rafly, tetapi *group* tetap sama.
- sudo chown :staff file.txt: Mengubah *group file* menjadi staff, tetapi pemilik tetap sama.
- sudo chown rafly:staff file.txt: Mengubah pemilik menjadi rafly dan *group* menjadi staff.
- sudo chown -R rafly:staff /var/www/html: Mengubah pemilik dan *group* secara rekursif (-R) untuk semua *file* dan direktori di /var/www/html.

terima kasih