Secure Linux Server Hardening & Audit

Nama : Rakadian Audiga Pratama

Bidang : DevOps

Langkah-langkah

1. Membuat user dengan akses sudo menggnuankan password dan pubkey

Langkah pertama adalah membuat user baru menggunakan sudo adduser

```
sevima@semesta-lab-04: /home/semesta
sevima@semesta-lab-04:/home/semesta$ ls
adm.pub
sevima@semesta-lab-04:/home/semesta$ vi adm.pub
sevima@semesta-lab-04:/home/semesta$ sudo adduser sevima-adm1
info: Adding user `sevima-adm1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `sevima-adm1' (1002) ...
info: Adding new user `sevima-adm1' (1002) with group `sevima-adm1 (1002)' ...
info: Creating home directory `/home/sevima-adm1' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sevima-adm1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `sevima-adm1' to supplemental / extra groups `users' ...
info: Adding user `sevima-adm1' to group `users' ...
sevima@semesta-lab-04:/home/semesta$
```

Kemudian menambahkan user tsb ke grup sudo

```
sevima@semesta-lab-04: /home/semesta
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* fi
les
  -r, --remove                  remove the user from only the supplemental GROUP
S
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account

sevima@semesta-lab-04:/home/semesta$ sudo usermod -aG sudo sevima-adm1
sevima@semesta-lab-04:/home/semesta$
```

Dilanjutkan membuat direktori ssh untuk user baru dan mengcopy pubkey dan set permission untuk sudo

```
sevima@semesta-lab-04: /home/semesta
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* fi
les
  -r, --remove                  remove the user from only the supplemental GROUP
S
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account

sevima@semesta-lab-04:/home/semesta$ sudo usermod -aG sudo sevima-adm1
sevima@semesta-lab-04:/home/semesta$ sudo mkdir -p /home/sevima-adm1/.ssh
sevima@semesta-lab-04:/home/semesta$ sudo cp /home/semesta/adm.pub /home/sevima-
adm1/.ssh/authorized_keys
sevima@semesta-lab-04:/home/semesta$
```

```
sevima@semesta-lab-04: /home/semesta
  -r, --remove                  remove the user from only the supplemental GROUP
S
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account

sevima@semesta-lab-04:/home/semesta$ sudo usermod -aG sudo sevima-adm1
sevima@semesta-lab-04:/home/semesta$ sudo mkdir -p /home/sevima-adm1/.ssh
sevima@semesta-lab-04:/home/semesta$ sudo cp /home/semesta/adm.pub /home/sevima-
adm1/.ssh/authorized_keys
sevima@semesta-lab-04:/home/semesta$ sudo chown -R sevima-adm1:sevima-adm1 /home
/sevima-adm1/.ssh
sevima@semesta-lab-04:/home/semesta$ sudo chmod 700 /home/sevima-adm1/.ssh
sevima@semesta-lab-04:/home/semesta$ sudo chmod 600 /home/sevima-adm1/.ssh/autho
rized_keys
sevima@semesta-lab-04:/home/semesta$
```

2. Membuat lvm dari sdb dan dienkripsi

Encrypt menggunakan luksformat dan volume nya diberi nama hackthon-syamd7

```
sevima@semesta-lab-04: ~
  MOUNTPOINTS  all locations where device is mounted
         TRAN  device transport type
         TYPE  device type
         UUID  filesystem UUID
       VENDOR  device vendor
        WSAME  write same max bytes
          WWN  unique storage identifier
        ZONED  zone model
      ZONE-SZ  zone size
   ZONE-WGRAN  zone write granularity
     ZONE-APP  zone append max bytes
      ZONE-NR  number of zones
    ZONE-OMAX  maximum number of open zones
    ZONE-AMAX  maximum number of active zones

For more details see lsblk(8).
sevima@semesta-lab-04:~$ sudo pvcreate /dev/mapper/luks_sdb
  Physical volume "/dev/mapper/luks_sdb" successfully created.
sevima@semesta-lab-04:~$ sudo vgcreate hackathon-syamd7 /dev/mapper/luks_sdb
  Volume group "hackathon-syamd7" successfully created
sevima@semesta-lab-04:~$ sudo lvcreate -l 100%FREE -n  securevol hackathon-syamd
7
  Logical volume "securevol" created.
sevima@semesta-lab-04:~$
```

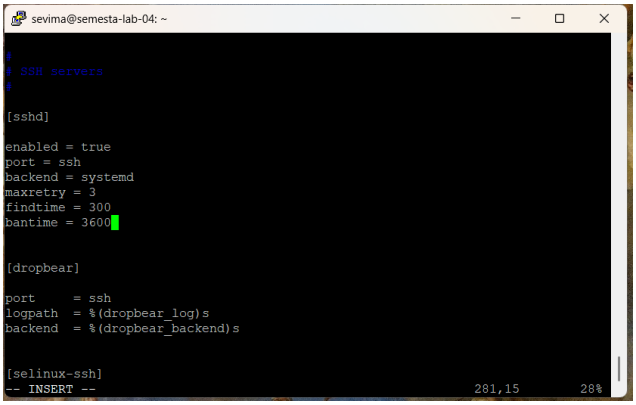
3. awdawdawd

4. Root login masih diizinkan

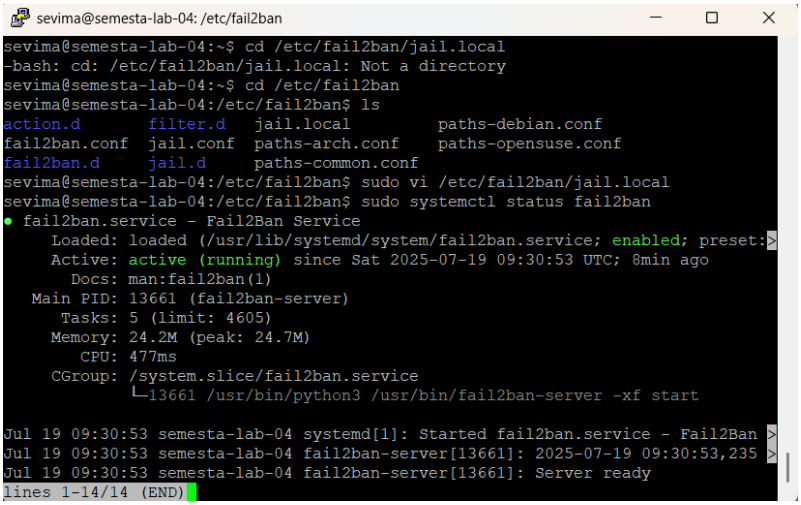
Permasalahan ini terdapat di konfigurasi ssh daemon yang Dimana root user dapat login melalui ssh. Untuk merubahnya, yang harus dilakukan adalah merubah PermitLoginRoot yes menjadi PermitLoginRoot no.

5. Pembatasan terhadap login gagal

Untuk permasalahan ini dapat menggunakan tool tambahan, yakni fail2ban yang akan meng-ban Alamat IP jika ada aktivitas mencurigakan seperti login gagal berulang. Fail2ban akan berjalan secara otomatis setelah mengatur konfigurasi nya. Buat konfigutasi seperti ini:



Lalu cek status fail2ban apakah sudah berjalan.



```
sevima@semesta-lab-04: /etc/fail2ban
     Memory: 24.2M (peak: 24.7M)
        CPU: 477ms
     CGroup: /system.slice/fail2ban.service
             └─13661 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jul 19 09:30:53 semesta-lab-04 systemd[1]: Started fail2ban.service - Fail2Ban >
Jul 19 09:30:53 semesta-lab-04 fail2ban-server[13661]: 2025-07-19 09:30:53,235 >
Jul 19 09:30:53 semesta-lab-04 fail2ban-server[13661]: Server ready
lines 1-14/14 (END)
[3]+  Stopped                 sudo systemctl status fail2ban
sevima@semesta-lab-04:/etc/fail2ban$ fail2ban-client status sshd
2025-07-19 09:40:37,502 fail2ban                [13818]: ERROR   Permission deni
ed to socket: /var/run/fail2ban/fail2ban.sock, (you must be root)
sevima@semesta-lab-04:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
sevima@semesta-lab-04:/etc/fail2ban$
```

Seperti di gambar, status fail2ban sudah aktif. Jadi jika ada yang mecncoba login dan gagal 3 kali, akan ter-ban selama 1 jam.

6. Konfigurasi firewall

Untuk mengonfigurasi firewall, bisa menggunakan ufw (uncomplicated firewall). Langkah pertama adalah mengizinkan akses melalui ssh.

```
sevima@semesta-lab-04: /etc/fail2ban
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
sevima@semesta-lab-04:/etc/fail2ban$ sudo apt install ufw-y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package ufw-y
sevima@semesta-lab-04:/etc/fail2ban$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
  apache2-data apache2-utils ssl-cert
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 82 not upgraded.
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw status verbose
Status: inactive
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
sevima@semesta-lab-04:/etc/fail2ban$
```

Kemudian mengizinkan akses http, https, dan nfs yang sudah disediakan.

```
sevima@semesta-lab-04: /etc/fail2ban
sevima@semesta-lab-04:/etc/fail2ban$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
  apache2-data apache2-utils ssl-cert
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 82 not upgraded.
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw status verbose
Status: inactive
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow from 192.168.99.3
Rules updated
sevima@semesta-lab-04:/etc/fail2ban$
```

Jika sudah, jalankan firewall dan cek status firewall. Gambar dibawah adalah contoh jika firewall sudah berjalan.

```
sevima@semesta-lab-04: /etc/fail2ban
[ 3] 443/tcp                   ALLOW IN    Anywhere
[ 4] Anywhere                  ALLOW IN    192.168.99.3
[ 5] OpenSSH (v6)              ALLOW IN    Anywhere (v6)
[ 6] 80/tcp (v6)               ALLOW IN    Anywhere (v6)
[ 7] 443/tcp (v6)              ALLOW IN    Anywhere (v6)

sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw allow from 192.168.99.3 to any por
t nfs
Rule added
sevima@semesta-lab-04:/etc/fail2ban$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] OpenSSH                    ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] Anywhere                   ALLOW IN    192.168.99.3
[ 5] 2049                       ALLOW IN    192.168.99.3
[ 6] OpenSSH (v6)               ALLOW IN    Anywhere (v6)
[ 7] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 8] 443/tcp (v6)               ALLOW IN    Anywhere (v6)

sevima@semesta-lab-04:/etc/fail2ban$
```

7. Service yang tidak digunakan masih berjalan

Untuk mengecek service yang sedang berjalan, bisa menggunakan command systemctl list-units –type=service –state=running, lalu akan muncul list seperti dibawah:

```
sevima@semesta-lab-04: /etc/fail2ban
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION                >
  cron.service                  loaded active running Regular background program >
  dbus.service                  loaded active running D-Bus System Message Bus
  fail2ban.service              loaded active running Fail2Ban Service
  fwupd.service                 loaded active running Firmware update daemon
  getty@tty1.service            loaded active running Getty on tty1
  ModemManager.service          loaded active running Modem Manager
  multipathd.service            loaded active running Device-Mapper Multipath Dev>
  mysql.service                 loaded active running MySQL Community Server
  polkit.service                loaded active running Authorization Manager
  rsyslog.service               loaded active running System Logging Service
  ssh.service                   loaded active running OpenBSD Secure Shell server
  systemd-journald.service      loaded active running Journal Service
  systemd-logind.service        loaded active running User Login Management
  systemd-networkd.service      loaded active running Network Configuration
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-timesyncd.service     loaded active running Network Time Synchronization
  systemd-udevd.service         loaded active running Rule-based Manager for Devi>
  udisks2.service               loaded active running Disk Manager
  unattended-upgrades.service   loaded active running Unattended Upgrades Shutdown
  upower.service                loaded active running Daemon for power management
  user@1000.service             loaded active running User Manager for UID 1000

lines 1-23/28 85%
```

Jika sudah muncul, pengguna dapat menentukan service trivial mana saja yang ingin di-stop. Fwupd dapat distop karena kita tidak perlu untuk mengupdate firmware otomatis, jadi bukan service penting sehingga bisa di-stop.

```
sevima@semesta-lab-04: /etc/fail2ban
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-timesyncd.service     loaded active running Network Time Synchronization
  systemd-udevd.service         loaded active running Rule-based Manager for Devi>
  udisks2.service               loaded active running Disk Manager
  unattended-upgrades.service   loaded active running Unattended Upgrades Shutdown
  upower.service                loaded active running Daemon for power management
  user@1000.service             loaded active running User Manager for UID 1000


sevima@semesta-lab-04:/etc/fail2ban$ sudo systemctl stop fwupd
sevima@semesta-lab-04:/etc/fail2ban$ systemctl list-units --type=service --state
=running
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION                >
  cron.service                  loaded active running Regular background program >
  dbus.service                  loaded active running D-Bus System Message Bus
  fail2ban.service              loaded active running Fail2Ban Service
  getty@tty1.service            loaded active running Getty on tty1
  ModemManager.service          loaded active running Modem Manager
  multipathd.service            loaded active running Device-Mapper Multipath Dev>
  mysql.service                 loaded active running MySQL Community Server
  polkit.service                loaded active running Authorization Manager
  rsyslog.service               loaded active running System Logging Service
  ssh.service                   loaded active running OpenBSD Secure Shell server
  systemd-journald.service      loaded active running Journal Service
```

8. Sistem log tersentralisasi dan aturan audit aktif

9. Konfigurasi NFS
10. Pembatasan penggunaan resource