Praktikum Keamanan Server Linux Ubuntu

Lab 1. Pengamanan Boot Loader dan Single User dengan Password

Lab 1.1. Cara Masuk ke Sistem Linux sebagai Single User

- Pada saat booting, tampilkan menu grub dengan menekan tombol keyboard Esc.
- Pada menu grub, pilih menu Ubuntu kemudian tekan tombol “e”
- Posisikan kursor pada baris yang ada parameter kernel linux kemudian tekan tombol “End” agar kursor berpindah ke akhir baris
- Pad akhir baris, tambahkan salah satu parameter berikut:

  “single” atau

  systemd.unit=rescue.target
- Tekan tombol “Ctrl-x" atau F10 untuk booting ke Linux

Lab 1.2. Memberikan Password pada Grub

- Edit file konfigurasi grub, yaitu file /etc/grub.d/00_header. Tambahkan baris berikut di baris paling bawah:

```
cat << EOF
set superusers="admin"
password admin rahasia
EOF
```

- Update grub dengan menjalankan perintah berikut:

```
dudi@server-dudi:~$ sudo update-grub
```

- Reboot sistem linux dengan mengetikkan perintah berikut:

```
dudi@server-dudi:~$ sudo shutdown -r now
```

  atau

```
dudi@server-dudi:~$ reboot
```

- Untuk masuk ke menu grub, anda harus menekan tombol "p" dan memasukkan password yang sudah ditambahkan di file konfigurasi grub.

Lab 1.3. Membuat password yang terenkripsi

- Untuk membuat password yang terenkripsi dapat menggunakan perintah "grub-mkpasswd-pbkdf2" seperti contoh berikut:

```
dudi@server-dudi:~$ grub-mkpasswd-pbkdf2
Enter password: <ketikkan password>
Reenter password: (ketikkan password sekali lagi>
PBKDF2 hash of your password is
```

```
grub.pbkdf2.sha512.10000.2E5E38588127D1B46775FB57F68665EDD684CAEC7F93B
E48CB36F69EF1D519A91A6269959822F1CA6127286C406F272AD186579699601BAA8FC
4942FD5CF531E.1D93B0150ECC30D80ABEAB3857FB23DB9A6321A11F5BBC5C210AE81A
2BE23DB3E9D56961B2EA0B5CF6B6BAC9655B9DDEFD398B6F787AB716DC7696C5A6BD7F
B4
```

- Kemudian tambahkan password terenkripsi tersebut ke dalam file konfigurasi grub, yaitu file /etc/grub.d/00_header :

```
set superusers="admin"
password_pbkdf2 admin
grub.pbkdf2.sha512.10000.2E5E38588127D1B46775FB57F68665EDD684CAEC7F93B
E48CB36F69EF1D519A91A6269959822F1CA6127286C406F272AD186579699601BAA8FC
4942FD5CF531E.1D93B0150ECC30D80ABEAB3857FB23DB9A6321A11F5BBC5C210AE81A
2BE23DB3E9D56961B2EA0B5CF6B6BAC9655B9DDEFD398B6F787AB716DC7696C5A6BD7F
B4
```

- Update grub dengan menjalankan perintah berikut:

```
dudi@server-dudi:~$ sudo update-grub
```

- Reboot sistem linux dengan mengetikkan perintah berikut:

```
dudi@server-dudi:~$ sudo shutdown -r now
```

atau

```
dudi@server-dudi:~$ reboot
```

- Untuk masuk ke menu grub, anda harus menekan tombol "p" dan memasukkan password yang sudah ditambahkan di file konfigurasi grub.

Lab 2. Masuk ke Linux Single User dengan Password (Runlevel 1)

- Agar tidak sembarang orang dapat masuk ke runlevel 1 atau single user maka sebaiknya diberikan password, untuk Linux Ubuntu caranya dengan memberikan password ke user root (pada Linux Ubuntu secara default user root-nya di-disable)

```
dudi@server-dudi:~$ sudo passwd root
```

- Uji coba masuk ke single user dengan mengetikkan perintah:

```
dudi@server-dudi:~$ sudo systemctl rescue
```

Lab 3. Konfigurasi Otentikasi

Lab 3.1. Memeriksa apakah sistem Linux sudah menggunakan shadow password?

- Periksa kolom kedua pada file /etc/passwd apakah berisi karakter "*" atau "x"?

```
dudi@server-dudi:~$ grep dudi /etc/passwd
dudi:x:1000:1000:Dudi Fitriahadi:/home/dudi:/bin/bash
```

- Periksa apakah terdapat file /etc/shadow?

```
dudi@server-dudi:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1078 Jan 17 17:44 /etc/shadow
```

Lab 3.2. Mengubah shadow password menjadi password standar

- Ketikkan perintah pwunconv pada shell prompt

```
dudi@server-dudi:~$ sudo pwunconv
```

- Periksa kolom kedua pada file /etc/passwd

```
dudi@server-dudi:~$ grep dudi /etc/passwd
dudi:$6$MmecLEmB1adQNEdM$.a99QA/
TUuHGkCWpzcWMC8Hem1FF1Jw5WwRlHsGZzy82Dv.2bmLwv8grTpmBpCMi/1d3/
qgb9MfTqWT/oapCg/:1000:1000:Dudi Fitriahadi:/home/dudi:/bin/bash
```

- Periksa apakah terdapat file /etc/shadow?

```
dudi@server-dudi:~$ ls -l /etc/shadow
ls: cannot access /etc/shadow: No such file or directory
```

Lab 3.3. Mengubah password standar menjadi shadow password

- Ketikkan perintah pwconv pada shell prompt:

```
dudi@server-dudi:~$ sudo pwconv
```

- Periksa kolom kedua pada file /etc/passwd apakah berisi karakter "*" atau "x"?

```
dudi@server-dudi:~$ grep dudi /etc/passwd
dudi:x:1000:1000:Dudi Fitriahadi:/home/dudi:/bin/bash
```

- Periksa apakah terdapat file /etc/shadow?

```
dudi@server-dudi:~$ ls -l /etc/shadow
-r--r----- 1 root shadow 1092 Jan 18 19:08 /etc/shadow
```

Lab 4. Menerapkan strong password

Pada praktikum kali ini Anda akan menerapkan strong password dengan ketentuan minimal terdiri dari 10 karakter, dan terdiri dari minimal 1 karakter numerik, minimal 1 karakter huruf besar, minimal 1 karakter lainnya selain numerik dan percobaan perubahan password minimal 3 kali jika lebih dari itu maka program passwd berakhir:

- Lakukan instalasi modul libpam-cracklib:

```
dudi@server-coba:~$ sudo apt install libpam-cracklib
dudi@server-coba:~$ apt list libpam-cracklib
Listing... Done
libpam-cracklib/focal-updates,now 1.3.1-5ubuntu4.3 amd64 [installed]
N: There is 1 additional version. Please use the '-a' switch to see it
dudi@server-coba:~$
```

- Edit file /etc/pam.d/common-password, kemudian ubah baris berikut:

```
password    requisite     pam_cracklib.so retry=3 minlen=8 difok=3
```

sehingga menjadi:

```
password    requisite     pam_cracklib.so retry=3 minlen=10 difok=3
lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1
```

- Ujicoba dengan mengganti password user oleh user itu sendiri

Lab 5. Membatasi Terminal Login untuk root

- Edit file /etc/pam.d/common-auth, tambahkan baris berikut:

  auth required pam_securetty.so

- Edit file /etc/securetty, tambahkan terminal-terminal yang boleh digunakan oleh root untuk login.

```
dudi@server-dudi:~$ sudo vim /etc/securetty
tty1
tty2
```

- Cobalah login dari virtual terminal yg terdaftar di file /etc/securetty misalnya virtual terminal kedua. Apakah berhasil login?
  Untuk menampilkan virtual terminal kedua, tekan tombol Ctrl+Alt+F2 (Ctrl kanan+F2 di VirtualBox).

```
Ubuntu 20.04.3 LTS server-dudi tty2

server-dudi login: root
Password: <password root>

Last login: Tue Jan 18 19:34:37 on tty3
root@server-dudi:~#
```

- Sekarang cobalah login dari virtual terminal yg tidak terdaftar di file /etc/securetty misalnya virtual terminal keempat. Apakah berhasil login?
  Untuk menampilkan virtual terminal keempat, tekan tombol Ctrl+Alt+F4 (Ctrl kanan+F2 di VirtualBox)..

```
Ubuntu 20.04.3 LTS server-dudi tty4
server-dudi login: root
Password: <password root>

Login incorrect
server-dudi login:
```

Lab 6. Membatasi user yg boleh menjalankan perintah su

Untuk membatasi hanya user-user yang tergabung ke dalam group root saja yang boleh menjalankan perintah su, lakukan langkah berikut:

- Edit file /etc/pam.d/su, hapus tanda pagar pada baris berikut:

```
#auth            required        pam_wheel.so
```

  sehingga menjadi:

```
auth            required        pam_wheel.so
```

- Tambahkan user yang boleh menjalankan perintah su ke dalam group root, caranya:

```
dudi@server-dudi:~$ sudo gpasswd -a dudi root
```

- Ujicoba dengan menjalankan perintah su menggunakan user yang masuk ke dalam group root, contoh user dudi

```
dudi@server-dudi:~$ su -
Password: <masukan password root>
root@server-dudi:~#
```

- Berikutnya ujicoba dengan menjalankan perintah su menggunakan user yang tidak masuk ke dalam group root. Tambahkan user yang baru bila diperlukan.

```
badu@server-dudi:~$ su -
Password:
su: Permission denied
badu@server-dudi:~$
```

Lab 7. Menggunakan sudo

- Pada Linux Ubuntu, fasilitas sudo sudah aktif secara default. Pastikan terdapat baris berikut pada file konfigurasi /etc/sudoers:

```
dudi@server-dudi:~$ grep %sudo /etc/sudoers
%sudo   ALL=(ALL:ALL)   ALL
```

- Periksa user yang sudah terdaftar sebagai anggota group sudo:

```
dudi@server-dudi:~$ grep sudo /etc/group
sudo:x:27:dudi
```

- Ujicoba dengan menjalankan perintah sudo menggunakan user yang terdaftar sebagai anggota group sudo:

```
dudi@server-dudi:~$ sudo -i
[sudo] password for dudi:
root@server-dudi:~#
```

- Ujicoba dengan menjalankan perintah sudo menggunakan user yang tidak terdaftar sebagai anggota group sudo:

```
badu@server-dudi:~$ sudo -i
[sudo] password for badu:
badu is not in the sudoers file.  This incident will be reported.
badu@server-dudi:~$
```

Lab 8. Menonaktifkan fungsi tombol Ctrl+Alt+Del

- Pada console Linux, apabila tombol Ctrl+Alt+Del ditekan maka akan mengakibatkan sistem melakukan reboot.
- Untuk menonaktifkan fungsi penekanan tombol Ctrl+Alt+Del, lakukan perintah berikut:

```
dudi@server-dudi:~$ sudo systemctl mask ctrl-alt-del.target
dudi@server-dudi:~$ sudo systemctl daemon-reload
```

- Uji coba dengan cara menekan tombol Ctrl+Alt+Del dari console.
- Untuk mengaktifkan kembali fungsi penekanan tombol Ctrl+Alt+Del, lakukan perintah berikut:

```
dudi@server-dudi:~$ sudo systemctl unmask ctrl-alt-del.target
dudi@server-dudi:~$ sudo systemctl daemon-reload
```

Lab 9. Setting Login Time Out (TMOUT)

Setting terminal otomatis logout setelah idle selama 2 menit:

- Jalankan perintah berikut:

```
dudi@server-dudi:~$ sudo su -c 'echo "export TMOUT=120" >
/etc/profile.d/tmout.sh'
```

- Uji coba dengan cara login ke console menggunakan salah satu user dan biarkan tanpa aktivitas selama 2 menit.

Lab 10. Memanfaatkan Advanced Filesystem Attributes

Lab 10.1. Membuat file hanya bisa ditambah isinya (append only)

- Buat file kosong dengan menggunakan perintah touch
```
dudi@server-dudi:~$ touch latih1
```

- Lihat atribut file saat ini
```
dudi@server-dudi:~$ lsattr latih1
--------------e----- latih1
```

- Tambahkan atribut append only
```
dudi@server-dudi:~$ sudo chattr +a latih1
```

- Lihat hasil penambahan atribut append only
```
dudi@server-dudi:~$ lsattr latih1
-----a--------e----- latih1
```

- Ujicoba dengan meng-overwrite isi file. Hasilnya tidak diijinkan.
```
dudi@server-dudi:~$ echo hallo > latih1
-bash: latih1: Operation not permitted
```

- Ujicoba dengan menambahkan isi file. Hasilnya berhasil.
```
dudi@server-dudi:~$ echo hallo >> latih1
dudi@server-dudi:~$ cat latih1
hallo
```

Lab 10.2. Membuat file tidak bisa dihapus (immutable)

- Buat file kosong dengan menggunakan perintah touch
```
dudi@server-dudi:~$ touch latih2
```

- Lihat atribut file saat ini
```
dudi@server-dudi:~$ lsattr latih2
-------------e----- latih2
```

- Tambahkan atribut immutable
```
dudi@server-dudi:~$ sudo chattr +i latih2
```

- Lihat hasil penambahan atribut immutable
```
dudi@server-dudi:~$ lsattr latih2
----i--------e----- latih2
```

- Ujicoba dengan cara menghapus file tersebut
```
dudi@server-dudi:~$ rm latih2
rm: cannot remove 'latih2': Operation not permitted
```

Lab 11. Menerapkan quota filesystem

- Tambahkan harddisk sebesar 10 GB pada mesin virtual, kemudian buat satu partisi sebesar 10 GB dan format dengan menggunakan filesystem ext4
- Buat direktori tempat mount point di /mnt
```
dudi@server-dudi:~$ sudo mkdir /mnt/data
```
- Edit file /etc/fstab, tambahkan baris berikut:
```
dudi@server-dudi:~$ sudo nano /etc/fstab
```

```
/dev/sdb1  /mnt/data  ext4  defaults,usrquota  0 0
```

- Mount ulang
```
dudi@server-dudi:~$ sudo mount -a
```
- Lakukan instalasi paket quota
```
dudi@server-dudi:~$ sudo apt install quota
```
- Buat file database quota
```
dudi@server-dudi:~$ sudo quotacheck -cu /mnt/data
dudi@server-coba:~$ ls -l /mnt/data
total 24
-rw------- 1 root root  6144 Jan 25 15:46 aquota.user
drwx------ 2 root root 16384 Jan 25 15:39 lost+found
dudi@server-coba:~$
```
- Membuat tabel penggunaan disk per file system
```
dudi@server-dudi:~$ sudo quotacheck -avu
```
- Buat aturan quota
```
dudi@server-dudi:~$ sudo setquota -u dudi 5 10 0 0 -a
```
- Aktifkan quota
```
dudi@server-dudi:~$ sudo quotaon -avu
```
- Menampilkan laporan quota
```
dudi@server-dudi:~$ sudo repquota -a
```
- Ujicoba dengan menyalin file ke partisi /mnt/data dengan ukuran melebihi soft limit dan hard limit

Lab 12. Menerapkan "Resource Limits"

Membatasi jumlah maksimum user login hanya dua:

- Pastikan pada file /etc/pam.d/login, terdapat baris berikut:
```
dudi@server-dudi:~$ grep pam_limits /etc/pam.d/login
session       required   pam_limits.so
```
- Edit file /etc/security/limits.conf dan tambahkan baris berikut:
```
dudi@server-dudi:~$ sudo nano /etc/security/limits.conf
dudi    -     maxlogins  2
```
- Ujicoba dengan mencoba login sebagai user dudi lebih dari dua kali

Lab 13. Membatasi akses shell dengan rbash

Lab 13.1. Menjalankan rbash dari shell prompt

- Jalankan restricted shell bash (rbash):
```
dudi@server-dudi:~$ bash -r
```
- Ujicoba jalankan beberapa perintah yang tidak boleh dilakukan dalam rbash
```
dudi@server-dudi:~$ cd
bash: cd: restricted
dudi@server-dudi:~$ ls -l > ls.txt
bash: ls.txt: restricted: cannot redirect output
dudi@server-dudi:~$ /bin/ls
bash: /bin/ls: restricted: cannot specify `/' in command names
dudi@server-dudi:~$ PATH=$PATH:/home/dudi/bin
bash: PATH: readonly variable
```
- Keluar dari rbash dan kembali ke shell semula dengan menjalankan perintah berikut:
```
dudi@server-dudi:~$ exit
```

Lab 13.2. Membatasi akses shell user badu dengan rbash

- Pastikan sudah dibuat symbolic link file /bin/rbash ke file /bin/bash

```
dudi@server-dudi:~$ ls -l /bin/rbash
lrwxrwxrwx 1 root root 4 Jun 18  2020 /bin/rbash -> bash
```

- Ubah shell user badu menjadi rbash

```
dudi@server-dudi:~$ grep badu /etc/passwd
badu:x:1001:1001::/home/badu:/bin/bash
dudi@server-dudi:~$ sudo usermod -s /bin/rbash badu
dudi@server-dudi:~$ grep badu /etc/passwd
badu:x:1001:1001::/home/badu:/bin/rbash
```

- Login sebagai user badu dan jalankan perintah yang tidak boleh dieksekusi dalam rbash

```
dudi@server-dudi:~$ su - badu
badu@server-dudi:~$ cd
-rbash: cd: restricted
```