

# MODUL 2

## PASSWORD MANAGEMENT

### DG SUDO, JOHN THE RIPPER

#### TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep dasar autentikasi password di linux
2. Memahami konsep shadow password
3. Mampu menganalisa kelemahan password dengan program password cracker yang ada.

#### DASAR TEORI

/etc/passwd

Untuk dapat mengakses sistem operasi Linux digunakan mekanisme password. Pada distribusi-distribusi Linux yang lama, password tersebut disimpan dalam suatu file teks yang terletak di /etc/passwd. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Contoh isi file /etc/passwd :

```
root:..CETo68esYsA:0:0:root:/root:/bin/bash
bin:jvXHHBGCK7nkg:1:1:bin:/bin:
daemon:i1YD6CckS:2:2:daemon:/sbin:
adm:bj2NcvrnubUqU:3:4:adm:/var/adm:
rms:x9kxv932ckadsf:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:ZeoW7CaIcQmjhl:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:IK40Bb5NnkAHk:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Keterangan :

Field pertama : nama login

Field kedua : password yang terenkripsi

Field ketiga : User ID

Field keempat : Group ID

Field kelima : Nama sebenarnya

Field keenam : Home directory user

Field ketujuh : User Shell

Password login yang terdapat pada file /etc/passwd dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut tidak mengurangi kemungkinan password tersebut dibongkar (crack). Karena penyerang (attacker) dapat melakukan dictionary-based attack dengan cara :

menyalin file /etc/passwd tersebut menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper ([www.openwall.com/john/](http://www.openwall.com/john/)).

/etc/shadow

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program utility shadow password yang menjadikan file /etc/passwd tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file /etc/shadow yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file /etc/passwd yang telah di-shadow :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Dengan demikian, penggunaan shadow password akan mempersulit attacker untuk melakukan dictionary-based attack terhadap file password.

Selain menggunakan shadow password beberapa distribusi Linux juga menyertakan program hashing MD5 yang menjadikan password yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu passphrase.

## KRITERIA PASSWORD

Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

1. Jangan menggunakan nama login anda dengan segala variasinya.
2. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
3. Jangan menggunakan nama pasangan atau anak anda.
4. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.
5. Jangan menggunakan password yang terdiri dari seluruhnya angka ataupun huruf yang sama.
6. Jangan menggunakan kata-kata yang ada di dalam kamus, atau daftar kata lainnya.
7. Jangan menggunakan password yang berukuran kurang dari enam karakter.
8. Gunakan password yang merupakan campuran antara huruf kapital dan huruf kecil.
9. Gunakan password dengan karakter-karakter non-alfabet.
10. Gunakan password yang mudah diingat, sehingga tidak perlu ditulis.
11. Gunakan password yang mudah diketikkan, tanpa perlu melihat pada keyboard.

Beberapa tool yang bisa dipakai untuk melihat strong tidaknya password adalah john the ripper. Kita bisa memakai utility ini untuk melihat strong tidaknya suatu password yang ada pada komputer.

## SUDO

Sudo berfungsi untuk memberikan otoritas kepada user tertentu untuk menjalankan command / perintah seperti yang dilakukan atau hanya dapat dijalankan oleh superuser atau root. Sudo juga melakukan logging dengan baik, sehingga admin dapat melakukan kontrol terhadap user mereka

## TUGAS PENDAHULUAN

1. Bagaimana cara instalasi john the ripper password ?
2. Jelaskan cara penggunaan john the ripper ?
3. Bagaimana kriteria password dikatakan strong atau tidak ?
4. Apa kegunaan shadow password pada linux ?

## PERCOBAAN

### SUDO

1. Buat 3 user, userbaru, userkanan dan userkiri.
2. Login sebagai root, ketik :  
# visudo  
Pada dasarnya visudo ini membuka file /etc/sudoers. File ini hanya bisa dibuka lewat visudo saja dan tidak bisa dibuka lewat vi atau gedit, yang merupakan editor linux.
3. Coba baca isi file /etc/sudoers dg vi. Perhatikan isinya. Coba hapus baris paling bawah. Bisakah? Mengapa?
4. Coba login sebagai salah satu user dan nyalakan daemon httpd dengan perintah :  
# /etc/init.d/httpd start  
Berhasilkah anda menyalakan daemon httpd ? Mengapa?
5. Coba login sebagai root dan nyalakan daemon httpd dengan perintah :  
# /etc/init.d/httpd start  
Berhasilkah anda menyalakan daemon httpd ? Mengapa ?
6. Agar user biasa mampu menjalankan daemon httpd, anda harus mengedit file /etc/sudoers untuk memberikan hak tambahan user. Caranya dengan menambahkan baris dibawah pada visudo, lalu ketik I, yang berarti visudo berada dalam mode insert.  
userbaru localhost=NOPASSWD: /etc/init.d/httpd  
Arti baris ini adalah user userbaru dapat mengakses komputer yang bernama localhost untuk menjalankan daemon httpd tanpa password.
7. Setelah itu coba login sebagai userbaru lalu ketikkan :  
# sudo /etc/init.d/httpd start

Berhasilkah anda mengaktifkan daemon httpd sebagai userbaru? Apakah anda diprompt password?

8. Sekarang coba anda logi sebagai userkanan dengan perintah su  
# su userkanan  
Ketik passwordnya.
9. Kemudian jalankan perintah ini :  
# sudo /etc/init.d/httpd restart
10. Berhasilkah anda mengaktifkan daemon httpd sebagai userbaru? Apakah anda diprompt password? Setelah anda beri password, apakah anda bisa menjalankan httpd ? Apa peringatan yg diberikan ?
11. Sekarang coba anda tambahkan hak untuk melakukan mount cdrom pada userkiri.
12. Dalam keadaan normal, apakah anda dapat melakukan mount sebagai userkiri ?  
Siapakah user yang berhak melakukan mount ?
13. Untuk menambahkan hak mount pada userkiri, tambahkan baris berikut dibawah baris ini  
#%sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE,  
DELEGATING, PROCESSES, LOCATE, DRIVERS  
dengan baris :  
userkiri localhost = STORAGE
14. Artinya bahwa userkiri pada komputer localhost memiliki kemampuan manajemen Storage yang ditunjukkan oleh baris Cmd\_Alias berikut :  
Cmd\_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe,  
/bin/mount, /bin/umount
15. Kemudian sebagai userkiri, jalankan perintah sudo :  
# sudo mount /dev/cdrom /mnt/cdrom
16. Apakah userkiri berhasil melakukan mount cdrom? Apakah anda diprompt password ketika melakukan sudo ? Mengapa ?
17. Selain fdisk, userkiri mampu melakukan perintah fdisk, sfdisk, parted, partprobe dan mount
18. Coba lakukan perintah sudo dengan fdisk, sfdisk, parted, partprobr dan umount.
19. Untuk melakukan umount, cukup kerjakan ;  
# sudo umount /mnt/cdrom
20. Coba anda login sebagai userkanan dan lakukan sudo. Apakah berhasil ? Apa peringatan yang dituliskan?
21. Coba masuk sebagai root dan lakukan perintah ini :  
# tail /var/log/secure  
Dapatkah anda melihat bahwa pelanggaran yg dilakukan userkanan tercatat di file /var/log/secure ? Jika iya, copy paste pelanggaran tersebut.
22. Dari percobaan diatas, jawab pertanyaan ini :
  1. Terangkan apa fungsi SUDO ?
  2. Terangkan pula format log /var/log/secure ?
  3. Apa guna var/log/secure ? (selain merekan pelanggaran dari sudo)

## John The Ripper

1. Login sebagai root dan buatlah beberapa 4 user baru, selanjutnya untuk 3 nama user, beri password user sama dengan nama user . Nama user terserah anda. Contoh : Userkiri, passwd: userkiri; userkanan, passwd : userkanan; userbaru, passwd: userbaru. Satu user dengan password yang unik, contoh : niken, passwd :kenis34. Sedangkan root, passwdnya : 123456.
2. Login sebagai root dan install john the ripper dari source.
3. Cara instalasi source :  
# tar -xvzf john-1.7.2.tar.gz --dir=/usr/local  
Akan terbentuk direktori john-1.7.2 di usr/local
4. Setelah itu masuklah ke direktori john-1.7.2  
# cd john-1.7.2  
# cd src  
# make  
#make clean generic  
Tunggu sampai proses kompilasi selesai karena cukup memakan waktu, kemudian masuklah ke direktori run  
#cd ../run  
# ./john --test
5. Bila benar, anda akan melihat baris ini pada baris terbawah :

```
Benchmarking: NT LM DES [32/32 BS]... DONE  
Raw: 2727K c/s real, 2777K c/s virtual
```

6. Setelah mari mengcrack password dengan john the ripper.
7. Lakukan langkah-langkah berikut :
  - # umask 077  
Apa guna perintah umask ? Apa arti umask 077 ?
  - Masuk ke direktori run dari john-1.7-2
  - Jika password anda sudah ter-shadow, anda perlu melakukan unshadow  
# ./unshadow /etc/passwd /etc/shadow > mypasswd
  - Coba lihat isi mypasswd. Apakah benar sekarang semua password telah ter-unshadowed ? Copy paste baris yang mengandung 4 user dan account root. Untuk membuka, berikan perintah ini.  
# vi mypasswd
  - Untuk melihat password yang dicrack oleh john the ripper, lihat dengan perintah ini  
# john --show mypasswd
  - Lihatlah, apakah semua user yang anda buat dapat dicrack oleh john? Jika tidak, usermana yang tidak dapat dicrack ?
  - Dari apa yang anda lakukan, apa fungsi perintah unshadow?
8. Lanjutkan langkah-langkah berikut :

- Copy file berikut dan pastekan ke direktori berikut :  
#cd john-1.7.2/run
  - Lihatlah apakah file password.lst dan all.chr ada ? File password.lst berisi listing password yang biasa dipakai oleh unix.
  - Buatlah direktori /usr/share/john/password.lst dan kopikan file password.lst  
#cp password.lst /usr/share/john/password.lst  
#cp all.chr /usr/share/john/all.chr
9. Jalankan lagi john untuk mengcrack semua password user. Ini mungkin makan waktu lama.  
# ./john mypasswd  
Tunggulah sampai 10 menit, bila masih belum selesai, keluarkan perintah Ctrl C untuk menghentikan john bekerja. Capture hasilnya.
  10. Password yang dicrack ditempatkan di folder /john-1.7.2/run/john.pot. Tapi file ini tidak dapat dibuka.
  11. Untuk melihat hasil crack, jalankan perintah ini.  
# john --show mypasswd  
Capture-lah output perintah diatas.
  12. Untuk mengcrack user tertentu, anda dapat menggunakan opsi ini :  
# john -show --users=userbaru mypasswd
  13. Jika ingin mengetahui variasi perintah untuk john, lihat dokumentasi tambahan ttg john the ripper atau carilah di internet.
  14. Cracking paling baik dilakukan dengan menggunakan opsi incremental :  
# john -i mypasswd  
Bila terlalu lama hentikan proses.  
Capture hasilnya.
  15. Jika ada peringatan ini, Crash recovery file is locked: /root/.john/john.rec, artinya anda harus mengcopy file /root/.john/john.rec, lalu hapus file lama, dan ubah dari john(copy).rec menjadi john.rec

# LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Password Management

Dasar Teori :

Tugas Pendahuluan :

Daftar Pertanyaan

Berikan kesimpulan hasil praktikum yang anda lakukan.

Jelaskan cara kerja john the ripper dalam melihat password

Jelaskan cara kerja program yang anda buat dan bagaimana password bisa disebut strong dan bad ?