

# **PRAKTIKUM KEAMANAN KOMPUTER**

## **PERTEMUAN 3**

### **PASSWORD MANAGEMENT**



**Disusun Oleh :**

**Nama : Febriyan Fathur RF**  
**NIM : 1600631002**

**JURUSAN**

**MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2017**

## 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

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:triawan:/home/rms:/bin/bash
dmr:ZeoW7CalcQmjhl:101:101:victor:/home/dmr:/bin/bash
linus:IK40Bb5NnkAHk:102:102:mudafiq:/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 :

1. Menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper ([www.openwall.com/john/](http://www.openwall.com/john/)).

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:victor:/home/rms:/bin/bash

dmr:x:101:101:triawan:/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.

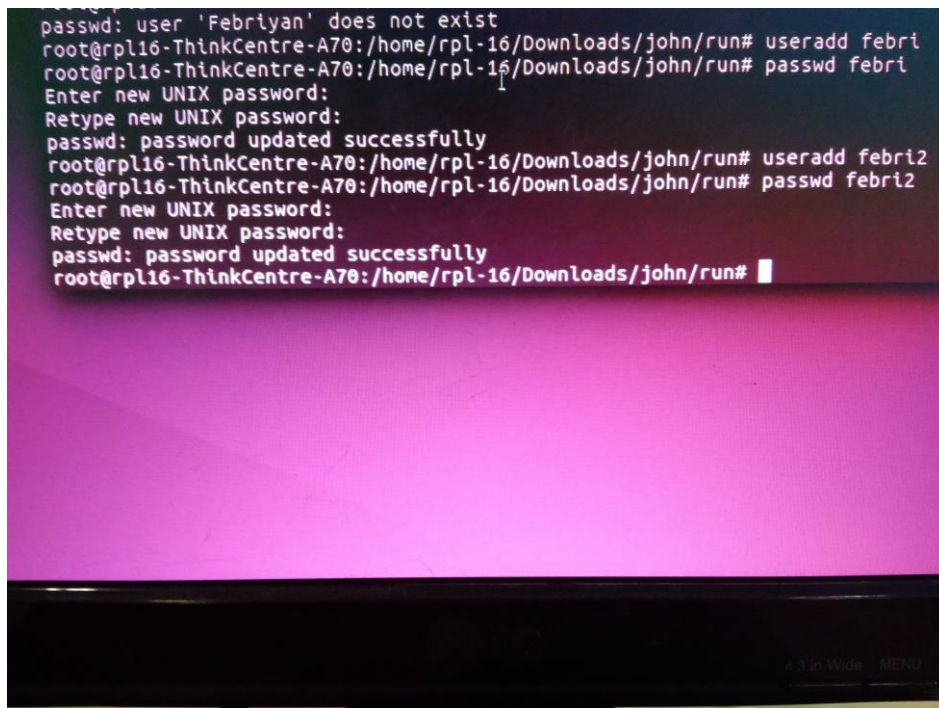
Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

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. lihat pada

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.

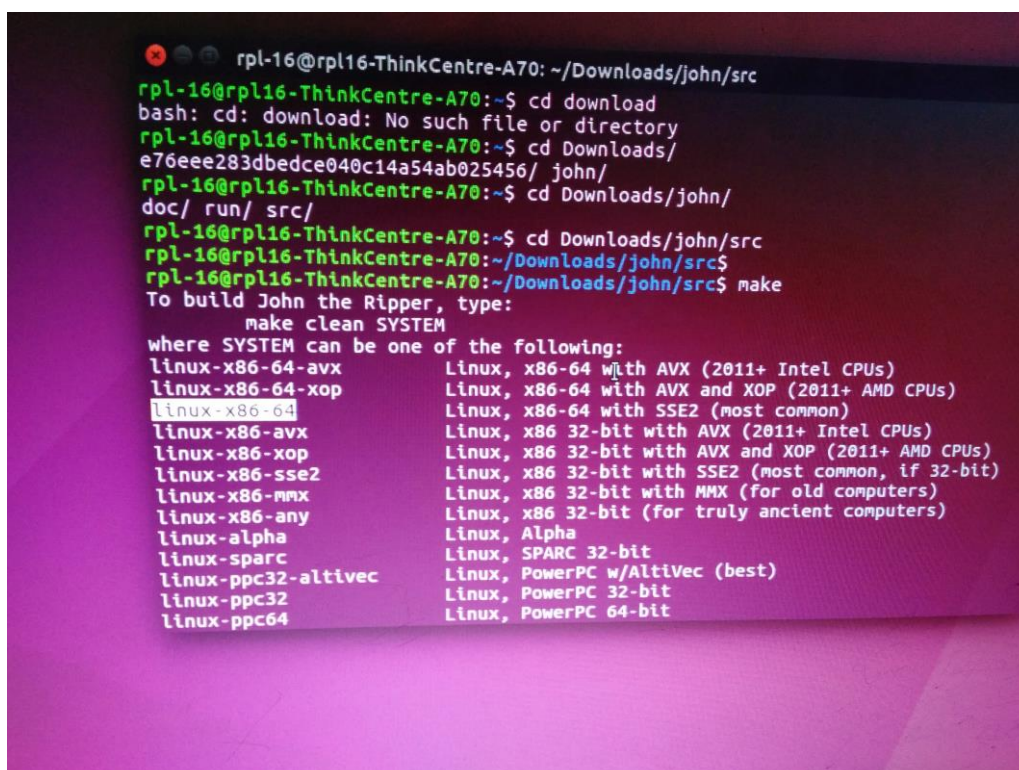
## PERCOBAAN

1. Login sebagai root dan buatlah beberapa 5 user baru, selanjutnya beri password setiap komputer. Berikan 3 user baru bad password yang hanya terdiri dari 4 karakter. Selanjutnya sisanya buat strong password buat minimal 8 karakter didalamnya kombinasi angka huruf dan karakter spesial seperti \$#@%^&.

A terminal window showing the process of creating users. The user 'Febriyan' is not found. Then, three users are created: 'febri', 'febri2', and 'febri3'. Each user is created with a password of '1234'. The terminal output is as follows:

```
passwd: user 'Febriyan' does not exist
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# useradd febri
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# passwd febri
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# useradd febri2
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# passwd febri2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run#
```

2. Lakukan instalasi john the ripper, ambil source yang sudah disiapkan oleh dosen/asisten praktikum

A terminal window showing the installation of john the ripper. The user navigates to the source directory and runs 'make'. The output shows the system configuration and the list of supported architectures. The terminal output is as follows:

```
rpl-16@rpl16-ThinkCentre-A70: ~/Downloads/john/src
rpl-16@rpl16-ThinkCentre-A70:~$ cd download
bash: cd: download: No such file or directory
rpl-16@rpl16-ThinkCentre-A70:~$ cd Downloads/
e76eee283dbedce040c14a54ab025456/ john/
rpl-16@rpl16-ThinkCentre-A70:~$ cd Downloads/john/
doc/ run/ src/
rpl-16@rpl16-ThinkCentre-A70:~$ cd Downloads/john/src
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/src$
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/src$ make
To build John the Ripper, type:
    make clean SYSTEM
where SYSTEM can be one of the following:
linux-x86-64-avx      Linux, x86-64 with AVX (2011+ Intel CPUs)
linux-x86-64-xop      Linux, x86-64 with AVX and XOP (2011+ AMD CPUs)
linux-x86-64         Linux, x86-64 with SSE2 (most common)
linux-x86-avx         Linux, x86 32-bit with AVX (2011+ Intel CPUs)
linux-x86-xop         Linux, x86 32-bit with AVX and XOP (2011+ AMD CPUs)
linux-x86-sse2        Linux, x86 32-bit with SSE2 (most common, if 32-bit)
linux-x86-mmx         Linux, x86 32-bit with MMX (for old computers)
linux-x86-any         Linux, x86 32-bit (for truly ancient computers)
linux-alpha           Linux, Alpha
linux-sparc           Linux, SPARC 32-bit
linux-ppc32-altivec   Linux, PowerPC w/Altivec (best)
linux-ppc32           Linux, PowerPC 32-bit
linux-ppc64           Linux, PowerPC 64-bit
```



3. Jalankan john the ripper : # cd /var/lib/john

# umask 077

# unshadow /etc/passwd /etc/shadow > mypasswords # john mypasswords

Untuk melihat password jalankan command berikut : # john -show mypasswords

Analisa hasilnya mana yang bad dan strong password

Anda dapat menginstruksikan john the ripper untuk melihat password user atau group tertentu

dengan option sebagai berikut : -users:u1,u2,... or -groups:g1,g2,...,

# john -users:nama\_user1,nama\_user2,nama\_user3 mypasswords

```
rpl-16@rpl16-ThinkCentre-A70: ~/Downloads/john/run
make[1]: Leaving directory '/home/rpl-16/Downloads/john/src'
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/src$ cd ..
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john$ cd run
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/run$ ./john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

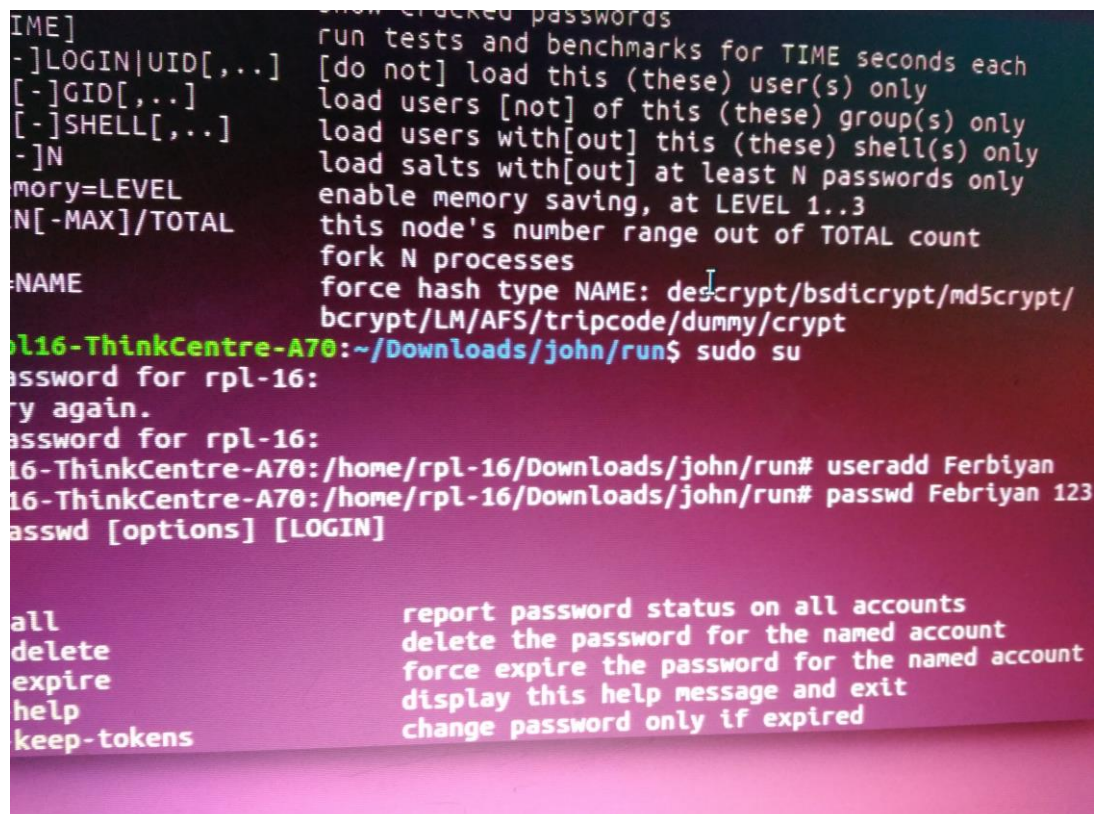
Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--external=MODE          external mode or word filter
--stdout[=LENGTH]       just output candidate passwords [cut at LENGTH]
--restore[=NAME]         restore an interrupted session [called NAME]
--session=NAME           give a new session the NAME
--status[=NAME]          print status of a session [called NAME]
--make-charset=FILE      make a charset, FILE will be overwritten
--show                  show cracked passwords
--test[=TIME]            run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,...] [do not] load this (these) user(s) only
--groups=[-]GID[,...]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]N             load salts with[out] at least N passwords only
```

```
rpl-16@rpl16-ThinkCentre-A70: ~/Downloads/john/src
beos-x86-sse2          BeOS, x86 with SSE2 (best)
beos-x86-mmx           BeOS, x86 with MMX
beos-x86-any           BeOS, x86
generic               Any other Unix-like system with gcc
Linux rpl16-ThinkCentre-A70:~/Downloads/john/src$ uname -a
Linux rpl16-ThinkCentre-A70 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:
UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/src$ make clean ^C
rpl-16@rpl16-ThinkCentre-A70:~/Downloads/john/src$ make clean linux-x86-64
rm -f ../run/john ../run/unshadow ../run/unafs ../run/unique ../run/john.bt
run/john.com ../run/unshadow.com ../run/unafs.com ../run/unique.com ../run/
exe ../run/unshadow.exe ../run/unafs.exe ../run/unique.exe
rm -f ../run/john.exe john-macosx-* *.o *.bak core
rm -f detect bench generic.h arch.h tmp.s
cp /dev/null Makefile.dep
ln -sf x86-64.h arch.h
make ../run/john ../run/unshadow ../run/unafs ../run/unique \
JOHN_OBJS="DES_fmt.o DES_std.o DES_bs.o DES_bs_b.o BSDI_fmt.o MDS_fm
MDS_std.o BF_fmt.o BF_std.o AFS_fmt.o LM_fmt.o trip_fmt.o dummy.o batch.o be
o charset.o common.o compiler.o config.o cracker.o crc32.o external.o formats
getopt.o idle.o inc.o john.o list.o loader.o logger.o math.o memory.o misc.o
ions.o params.o recovery.o rpp.o rules.o signals.o single.o status.o t
o wordlist.o unshadow.o unafs.o unique.o c3_fmt.o x86-64.o" \
CFLAGS="-c -Wall -Wdeclaration-after-statement -O2 -fomit-frame-point
-DHAVE_CRYPT" \
```

4. Untuk memastikan password kita baik atau tidak, buatlah program di bawah ini untuk melakukan testing bagaimana password yang baik dan yang jelek

```
#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>
#include <crack.h>

#define DICTIONARY "/usr/lib/cracklib_dict" int main(int argc, char *argv[]) {
char *password;
char *problem;
int status = 0;
printf("\nEnter an empty password or Ctrl-D to quit.\n");
while ((password = getpass("\nPassword: ")) != NULL && *password ) {
if ((problem = FascistCheck(password, DICTIONARY)) != NULL) { printf("Bad password: %s. \n",
problem);
status = 1; }
else {
printf("Good password!\n");
} }
exit(status); }
```



```
IME]
-]LOGIN|UID[,..]
[-]GID[,..]
[-]SHELL[,..]
-]N
memory=LEVEL
N[-MAX]/TOTAL
-NAME
run tests and benchmarks for TIME seconds each
[do not] load this (these) user(s) only
load users [not] of this (these) group(s) only
load users with[out] this (these) shell(s) only
load salts with[out] at least N passwords only
enable memory saving, at LEVEL 1..3
this node's number range out of TOTAL count
fork N processes
force hash type NAME: des|crypt|bsdicrypt|md5crypt|
bcrypt|LM|AFS|tripcode|dummy|crypt
rpl16-ThinkCentre-A70:~/Downloads/john/run$ sudo su
password for rpl-16:
try again.
password for rpl-16:
rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# useradd Ferbiyan
rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# passwd Febriyan 123
passwd [options] [LOGIN]

all
delete
expire
help
keep-tokens
report password status on all accounts
delete the password for the named account
force expire the password for the named account
display this help message and exit
change password only if expired
```

5. Kompilasi program yang sudah anda buat dan jalankan (berikut contoh kompilasi dan cara menjalankan).

```
$ gcc cracktest.c -lcrack -o cracktest $
```

```
./cracktest
```

Enter an empty password or Ctrl-D to quit. Password: xyz

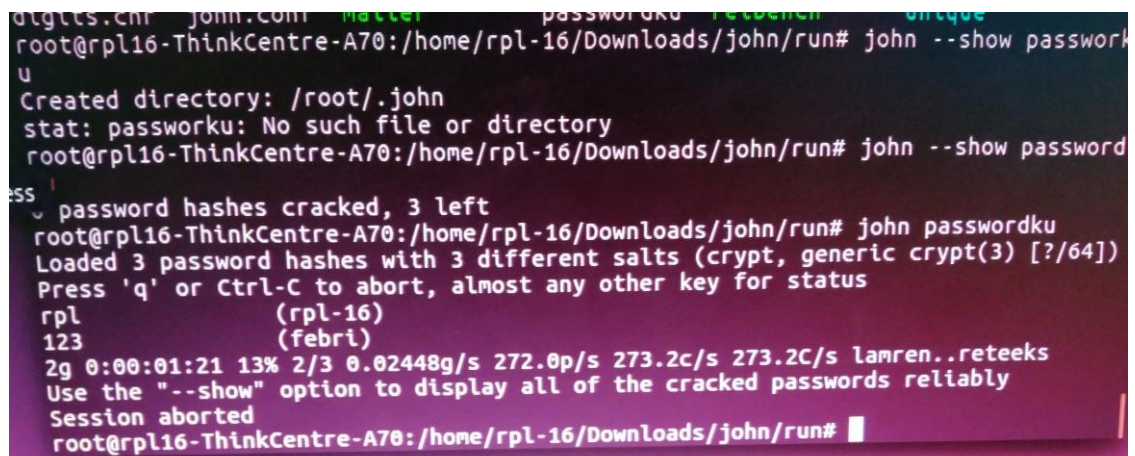
Bad password: it's WAY too short.

Password: elephant

Bad password: it is based on a dictionary word.

Password: kLu%ziF7

Good password!



```
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# john --show passwordku
Created directory: /root/.john
stat: passwordku: No such file or directory
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# john --show passwordku
3 password hashes cracked, 3 left
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run# john passwordku
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
rpl (rpl-16)
123 (febri)
2g 0:00:01:21 13% 2/3 0.02448g/s 272.0p/s 273.2c/s 273.2C/s lamren..reteeks
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@rpl16-ThinkCentre-A70:/home/rpl-16/Downloads/john/run#
```